

# GOLOD-SHAFAREVICH GROUPS: A SURVEY

MIKHAIL ERSHOV

ABSTRACT. In this paper we survey the main results about Golod-Shafarevich groups and their applications in algebra, number theory and topology.

## CONTENTS

1. Introduction	2
1.1. The discovery of Golod-Shafarevich groups	2
1.2. Golod-Shafarevich inequality	3
1.3. Applications in topology	3
1.4. General structure theory of Golod-Shafarevich groups	3
1.5. Counterexamples in group theory	4
1.6. Generalizations, relatives and variations of Golod-Shafarevich groups	4
2. Golod-Shafarevich inequality	5
2.1. Golod-Shafarevich inequality for graded algebras	5
2.2. First applications of the Golod-Shafarevich inequality	8
2.3. Golod-Shafarevich inequality for complete filtered algebras	9
3. Golod-Shafarevich groups	10
3.1. Definition of Golod-Shafarevich groups	10
3.2. First applications of Golod-Shafarevich groups	12
3.3. Word growth in Golod-Shafarevich groups	13
3.4. Golod-Shafarevich groups in characteristic zero	14
4. Generalized Golod-Shafarevich groups	15
4.1. Golod-Shafarevich inequality with weights	15
4.2. Generalized Golod-Shafarevich groups	16
4.3. Weight functions	18
5. Properties and applications of weight functions and valuations	19
5.1. Dependence on the generating set	19
5.2. Valuations	20
5.3. Weighted rank, index and deficiency	21
5.4. Proof of Theorem 5.7 (sketch)	23
5.5. $W$ -index and Quillen's theorem	24
5.6. A proof without Hilbert series	26
6. Quotients of generalized Golod-Shafarevich groups	26

---

*Date:* April 1st, 2012.

*2000 Mathematics Subject Classification.* Primary 20F05, 20F50, Secondary 20E18, 20E07, 20F69, 17B50.

*Key words and phrases.* Golod-Shafarevich groups, subgroup growth, class field tower problem, Burnside problem.

The author is supported in part by the NSF grant DMS-0901703 and the Sloan Research Fellowship grant BR 2011-105.

7. Free subgroups in generalized Golod-Shafarevich pro- $p$ groups	28
7.1. Sketch of proof of Theorem 7.1	28
8. Subgroup growth of generalized Golod-Shafarevich groups	30
8.1. Some generalities on subgroup growth	30
8.2. Subgroup growth of GGS groups	31
8.3. Subgroup growth of groups of non-negative deficiency	32
9. Groups of positive power $p$ -deficiency	34
10. Applications in number theory	36
10.1. Class field tower problem	36
10.2. Galois groups $G_{K,p,S}$	38
10.3. Examples with exponential subgroup growth	39
11. Applications in geometry and topology	40
11.1. Subgroup growth of 3-manifold groups	42
12. Golod-Shafarevich groups and Kazhdan's property $(T)$	42
12.1. Golod-Shafarevich groups with property $(T)$	42
12.2. Applications	43
12.3. Kazhdan quotients of Golod-Shafarevich groups	44
13. Residually finite monsters	47
13.1. Sketch of the proof of Theorem 13.2	47
14. Open questions	49
References	52

## 1. INTRODUCTION

**1.1. The discovery of Golod-Shafarevich groups.** Golod-Shafarevich groups have been introduced (or rather discovered) in connection with the famous class field tower problem, which asks whether the class field tower of any number field is finite. This classical number-theoretic problem, posed by Furtwängler in 1925, remained open for almost 40 years, with no clear indication whether the answer should be positive or negative. By class field theory, the problem is equivalent to the non-existence of a number field  $K$  whose maximal unramified prosolvable extension has infinite degree (over  $K$ ). A convenient way to construct  $K$  with the latter property (and thus settle the class field tower problem in the negative) would be to show that for some prime  $p$  the maximal unramified  $p$ -extension  $K_p$  of  $K$  has infinite degree, or equivalently, the Galois group  $G_{K,p} = \text{Gal}(K_p/K)$  is infinite (note that  $G_{K,p}$  is a pro- $p$  group, so if finite, it must be a  $p$ -group).

A major evidence for the negative answer to the class field tower problem was given by the 1963 paper of Shafarevich [Sh], where the formula for the minimal number of generators  $d(G_{K,p})$  of  $G_{K,p}$  and an upper bound for the minimal number of relations  $r(G_{K,p})$  were established. These results implied that for any prime  $p$ , there exists an infinite sequence of number fields  $\{K(n)\}$  such that if  $G_n = G_{K(n),p}$ , then  $d(G_n) \rightarrow \infty$  as  $n \rightarrow \infty$  and  $r(G_n) - d(G_n)$  remains bounded. Shafarevich conjectured that there cannot be any sequence of finite  $p$ -groups with these two properties (which would imply that in the above sequence  $G_n$  must be infinite for sufficiently large  $n$ ). A year later, in 1964, Golod and Shafarevich [GS] confirmed this conjecture by showing that for any finite  $p$ -group  $G$  the minimal numbers of generators  $d(G)$  and relators  $r(G)$  (where  $G$  is considered as a pro- $p$  group) are related by the inequality  $r(G) > (d(G) - 1)^2/4$  (this was improved to  $r(G) > d(G)^2/4$  in the subsequent works of Vinberg [Vi] and Roquette [Ro]).

**1.2. Golod-Shafarevich inequality.** The algebraic tool used to prove that  $r(G) > d(G)^2/4$  for a finite  $p$ -group is the so called *Golod-Shafarevich inequality*. It can be formulated in many different categories, including graded (associative) algebras, complete filtered algebras (algebras defined as quotients of algebras of power series  $K\langle\langle u_1, \dots, u_d \rangle\rangle$  in non-commuting variables  $u_1, \dots, u_d$ ), abstract groups and pro- $p$  groups, and relates certain growth function of an object in one of these categories with certain data coming from the presentation of that object by generators and relators. The main consequence of the Golod-Shafarevich inequality is that if the set of relators defining an object is “small” (in certain weighted sense) compared to the number of generators, then the object must be infinite in the case of groups and infinite-dimensional in the case of algebras. Groups and algebras which admit a presentation with such a “small” set of relators are called *Golod-Shafarevich*.

A well-known consequence of the Golod-Shafarevich inequality (which is sufficient for the solution of the class field tower problem) is that a pro- $p$  group  $G$  such that  $r(G) < d(G)^2/4$  must be infinite – this is an example of what it means for the set of relators to be “small”. However, as we already mentioned, the relators are counted with suitable weights, so even an infinite set of relators can be “small”. In particular, it is easy to see that there exist Golod-Shafarevich abstract groups which are torsion. This result was established by Golod [Go1] and yielded the first examples of infinite finitely generated torsion groups, thereby settling in the negative the general Burnside problem. This is the second major application of the Golod-Shafarevich inequality.

**1.3. Applications in topology.** The majority of works on Golod-Shafarevich groups in 70s and early 80s dealt with variations and generalizations of the inequality  $r(G) > d(G)^2/4$  both in group-theoretic and number-theoretic contexts, but no really new applications of Golod-Shafarevich groups were discovered. In 1983, Lubotzky [Lu1] made a very important observation that the fundamental groups of (finite-volume orientable) hyperbolic 3-manifolds (which can be equivalently thought of as torsion-free lattices in  $SL_2(\mathbb{C})$ ) are Golod-Shafarevich up to finite index. Using this result, in the same paper Lubotzky solved a major open problem, known at the time as Serre’s conjecture, which asserts that arithmetic lattices in  $SL_2(\mathbb{C})$  cannot have the congruence subgroup property. Lubotzky’s proof was highly original, and even though Golod-Shafarevich techniques constituted a relatively small (and technically not the hardest) part of the argument, it gave hope that other, possibly more difficult, problems about 3-manifolds could be settled with the use of Golod-Shafarevich groups. This line of research turned out to be quite successful, and even though no breakthroughs of the magnitude of the proof of Serre’s conjecture had been made, several important new results about hyperbolic 3-manifold groups had been discovered, including very strong lower bounds on the subgroup growth of such groups by Lackenby [La1, La2]. Equally importantly, the potential applications in topology served as an extra motivation for developing the general structure theory of Golod-Shafarevich groups, and many interesting (and useful for other purposes) results in that area were obtained in the past few years.

**1.4. General structure theory of Golod-Shafarevich groups.** The initial applications in the works of Golod and Shafarevich [GS, Go1] only required a sufficient condition for a group given by generators and relators to be infinite. However, the groups satisfying that condition (Golod-Shafarevich groups) turn out to be not only infinite – they are in fact big in many different ways. Already the arguments in the original paper [GS] show that for any Golod-Shafarevich group  $G$  with respect to a prime  $p$ , the graded algebra associated

to its group algebra  $\mathbb{F}_p[G]$  has exponential growth. Combining this result with Lazard's criterion, Lubotzky observed that Golod-Shafarevich pro- $p$  groups are not  $p$ -adic analytic – this was a key observation in the proof of Serre's conjecture in [Lu1]. In [Wi1], Wilson proved that every Golod-Shafarevich group has an infinite torsion quotient, using a simple modification of Golod's argument [Go1]. Two deeper results which required essentially new ideas had been established more recently. In [Ze1], Zelmanov proved a remarkable theorem asserting that every Golod-Shafarevich pro- $p$  group contains a non-abelian free pro- $p$  subgroup. This result, clearly very interesting from a purely group-theoretic point of view, is also important for number theory since many Galois groups  $G_{K,p}$  discussed above are known to be Golod-Shafarevich, and the fact that these groups have free pro- $p$  subgroups conjecturally implies that they do not have faithful linear representations over pro- $p$  rings. Very recently, in [EJ2], it was shown that every Golod-Shafarevich abstract group has an infinite quotient with Kazhdan's property  $(T)$ , which implies that Golod-Shafarevich abstract groups cannot be amenable. The proof in [EJ2] was based, among other things, on an earlier work [Er1], which established the existence of Golod-Shafarevich groups with property  $(T)$ . The latter result, originally obtained as a counterexample to a conjecture of Zelmanov [Ze2], turned out to have many other applications in geometric group theory.

**1.5. Counterexamples in group theory.** As we already mentioned, Golod-Shafarevich groups gave the first counterexamples to the general Burnside problem, which remained open for 60 years. Just a few years later, Novikov and Adyan [NA] gave a very long and technical proof of the fact that free Burnside groups of sufficiently large odd exponent are infinite, thereby providing the first examples of infinite finitely generated groups of bounded exponent (and thus solving THE Burnside problem). Another construction of infinite finitely generated torsion groups, very different from [GS] and [NA], was given by Grigorchuk [Gr] – these were also the first examples of groups of intermediate word growth. In addition, in the 80's, powerful methods had been developed to produce various kinds of infinite torsion groups with extremely unusual finiteness properties, starting with Ol'shanskii examples of Tarski monsters [Ol1] and continuing with even wilder examples constructed using the theory of hyperbolic and relatively hyperbolic groups (see, e.g., [Ol3, Os1]). In view of this, Golod-Shafarevich groups had been somewhat overshadowed as a potential source of exotic examples. However, in the last few years Golod-Shafarevich groups reappeared in this context and were used to solve several interesting problems where generally more powerful techniques from the area of hyperbolic groups are not applicable. For instance, the existence of Golod-Shafarevich groups with property  $(T)$  yielded the first examples of torsion non-amenable residually finite groups [Er1]. In [EJ3], Golod-Shafarevich groups were used to produce the first residually finite analogues of Tarski monsters. In § 6, we will discuss several other applications of this kind as well as a very general technique for discovering new such results.

**1.6. Generalizations, relatives and variations of Golod-Shafarevich groups.** A lot of attention in this paper will be devoted to *generalized Golod-Shafarevich groups* abbreviated as GGS groups (Golod-Shafarevich groups will be abbreviated as GS groups). Generalized Golod-Shafarevich groups are defined in the same way as Golod-Shafarevich groups except that generators are allowed to be counted with different weights. They have been introduced (without any proper name attached) shortly after Golod-Shafarevich groups (for instance, they already appear in Koch's book [Ko1] first published in 1970), and it is easy to extend all the basic properties of GS groups to GGS groups. However,

GGs groups have not been used much until recently, when it became clear that the class of GGS groups is more natural in many ways than that of GS groups. In particular, GGS groups played a key role in the construction of Kazhdan quotients of GS groups [EJ2] and residually finite analogues of Tarski monsters [EJ3].

Another interesting class of groups which strongly resemble Golod-Shafarevich groups both in their definition and their structure was introduced very recently by Schlage-Puchta [SP] and independently by Osin [Os2]. In the terminology of [SP], these are groups of positive  $p$ -deficiency (we will use the term *power  $p$ -deficiency* instead of  $p$ -deficiency to avoid terminological confusion). Perhaps, the most striking fact about these groups is that they provide by far the most elementary solution to the general Burnside problem (discovered almost 50 years after the initial counterexamples by Golod). These groups will be discussed and compared with Golod-Shafarevich groups in § 9.

Finally, we should make a remark about the term ‘Golod-Shafarevich groups’. Even though these groups have been studied for almost 50 years, there seemed to be no consensus on what a ‘Golod-Shafarevich group’ should mean until the last few years, and it was common for this term to have a more restricted meaning (say, pro- $p$  groups for which  $r(G) < d(G)^2/4$  and  $d(G) > 1$ ) or even the opposite meaning (that is, groups which are not Golod-Shafarevich in our terminology). It is also common, especially in older papers, to talk about *Golod groups* – these usually refer to the class of  $p$ -torsion groups constructed by Golod in [Go1]. These groups are defined as certain subgroups of Golod-Shafarevich graded algebras, but it is not clear whether the groups themselves are Golod-Shafarevich since they are not defined directly by generators and relators. Thus, a general theorem about Golod-Shafarevich groups does not formally apply to Golod groups, but in most cases the corresponding result for Golod groups can be obtained by using essentially the same argument.

**Acknowledgments:** The author is grateful to Andrei Jaikin for useful discussions and suggestions and to Ashley Rall for carefully reading the paper, providing useful feedback and proposing Problem 5 in § 14. The author would also like to thank Mark Sapir and the anonymous referee for helpful suggestions.

## 2. GOLOD-SHAFAREVICH INEQUALITY

**2.1. Golod-Shafarevich inequality for graded algebras.** Let  $K$  be a field,  $U = \{u_1, \dots, u_d\}$  a finite set, and denote by  $K\langle U \rangle = K\langle u_1, \dots, u_d \rangle$  the free associative  $K$ -algebra on  $U$ , that is, the algebra of polynomials in non-commuting variables  $u_1, \dots, u_d$  with coefficients in  $K$ . Let  $K\langle U \rangle_n$  be the degree  $n$  homogeneous component of  $K\langle U \rangle$ , so that

$$K\langle U \rangle = \bigoplus_{n=0}^{\infty} K\langle U \rangle_n.$$

Let  $R$  be a subset of  $K\langle U \rangle$  consisting of homogeneous elements of positive degree, and let  $A$  be the  $K$ -algebra given by the presentation  $(U, R)$ . This means that

$$A = K\langle U \rangle / I,$$

where  $I$  is the ideal of  $K\langle U \rangle$  generated by  $R$ .

Note that  $I$  is a graded ideal, that is,  $I = \bigoplus I_n$  where  $I_n = I \cap K\langle U \rangle_n$ , and  $A$  is a graded algebra:  $A = \bigoplus A_n$  where  $A_n = K\langle U \rangle_n / I_n$ . Let  $a_n = \dim_K A_n$ .

For each  $n \in \mathbb{N}$  let  $r_n$  be the number of elements of  $R$  which have degree  $n$ . Since  $K\langle U \rangle_n$  is a finite-dimensional subspace, we can (and will) assume without loss of generality that  $r_n < \infty$  for each  $n \in \mathbb{N}$ .

The sequences  $\{a_n\}$  and  $\{r_n\}$  are conveniently encoded by the corresponding Hilbert series  $\text{Hilb}_A(t) = \sum_{n=0}^{\infty} a_n t^n$  and  $H_R(t) = \sum_{n=1}^{\infty} r_n t^n$ . The following inequality relating these two series was established by Golod and Shafarevich [GS].

Given two power series  $f(t) = \sum f_n t^n$  and  $g(t) = \sum g_n t^n$  in  $\mathbb{R}[[t]]$ , we shall write  $f(t) \geq g(t)$  if  $f_n \geq g_n$  for each  $n$ .

**Theorem 2.1** (Golod-Shafarevich inequality: graded case). *In the above setting we have*

$$(2.1) \quad (1 - |U|t + H_R(t)) \cdot \text{Hilb}_A(t) \geq 1.$$

*Proof.* Even though the proof of this result appears in several survey articles and books (see, e.g., [Ha, Section 5]), we present it here as well due to its elegance and importance.

Let  $R_n = \{r \in R : \deg(r) = n\}$ , so that  $R = \sqcup_{n \geq 1} R_n$ . Recall that  $I$  is the ideal of  $K\langle U \rangle$  generated by  $R$  and  $I = \bigoplus_{n=1}^{\infty} I_n$  with  $I_n \subseteq K\langle U \rangle_n$ .

Now fix  $n \geq 1$ . Since each  $r \in R$  is homogeneous,  $I_n$  is spanned over  $K$  by elements of the form  $vrw$  for some  $v \in K\langle U \rangle_s$ ,  $w \in K\langle U \rangle_t$  and  $r \in R_m$ , where  $s + m + t = n$  and  $v$  and  $w$  are monic monomials.

If  $v \neq 1$ , then  $v = uv'$  for some  $u \in U$ , so  $vrw = uv'rw \in uI_{n-1}$ . If  $v = 1$ , then  $vrw = rw \in R_m K\langle U \rangle_{n-m}$ . Hence

$$I_n = \text{span}_K(U)I_{n-1} + \sum_{m=1}^n \text{span}_K(R_m)K\langle U \rangle_{n-m}. \quad (***)$$

For each  $i \in \mathbb{Z}_{\geq 0}$  choose a  $K$ -subspace  $B_i$  of  $K\langle U \rangle_i$  such that  $K\langle U \rangle_i = I_i \oplus B_i$ . Then  $\text{span}_K(R_m)K\langle U \rangle_{n-m} = \text{span}_K(R_m)B_{n-m} + \text{span}_K(R_m)I_{n-m}$  and  $\text{span}_K(R_m)I_{n-m} \subseteq \text{span}_K(U)I_{n-1}$ . Combining this observation with  $(***)$ , we conclude

$$(2.2) \quad I_n = \text{span}_K(U)I_{n-1} + \sum_{m=1}^n \text{span}_K(R_m)B_{n-m}.$$

Let  $d = |U|$ . Since  $A_i = K\langle U \rangle_i / I_i$ , we have  $a_i = \dim A_i = \dim K\langle U \rangle_i - \dim I_i = d^i - \dim I_i$ , and thus  $\dim B_i = a_i$ . Hence, computing the dimensions of both sides of (2.2), we get

$$d^n - a_n \leq d(d^{n-1} - a_{n-1}) + \sum_{m=1}^n r_m a_{n-m},$$

which simplifies to  $a_n - da_{n-1} + \sum_{m=1}^n r_m a_{n-m} \geq 0$ .

Finally observe that  $a_n - da_{n-1} + \sum_{m=1}^n r_m a_{n-m}$  is the coefficient of  $t^n$  in the power series  $(1 - dt + H_R(t)) \cdot \text{Hilb}_A(t)$ . The constant term of this power series is  $a_0 = 1$ . Therefore, we proved that  $(1 - dt + H_R(t)) \cdot \text{Hilb}_A(t) \geq 1 + \sum_{m=1}^{\infty} 0 \cdot t^i = 1$  as power series, as desired.  $\square$

As an immediate consequence of the Golod-Shafarevich inequality one obtains a sufficient condition for a graded algebra  $A$  given by a presentation  $(U, R)$  to be infinite-dimensional:

**Corollary 2.2.** *Assume that there exists a real number  $\tau > 0$  s.t.  $1 - d\tau + H_R(\tau) \leq 0$  (in particular, we assume that the series  $H_R(\tau)$  converges). Then*

- (i) *The series  $H_A(\tau)$  diverges.*
- (ii) *Assume in addition that  $\tau \in (0, 1)$  and  $1 - d\tau + H_R(\tau) < 0$ . Then the algebra  $A$  has exponential growth, that is, the sequence  $a_n = \dim A_n$  grows exponentially. In particular,  $A$  is infinite-dimensional.*

*Proof.* (i) Suppose that the series  $H_A(\tau)$  converges. Then, if we substitute  $t = \tau$  in (2.1), both factors on the left-hand side of (2.1) become convergent, so we should get a valid numerical inequality  $H_A(\tau)(1 - d\tau + H_R(\tau)) \geq 1$ . This cannot happen since clearly  $H_A(\tau) > 0$ , while by assumption  $1 - d\tau + H_R(\tau) \leq 0$ .

(ii) Since the series  $H_A(\tau)$  diverges, we must have  $\limsup \sqrt[n]{a_n} \geq \frac{1}{\tau} > 1$ . On the other hand, since by construction  $A$  is generated in degree 1, the sequence  $\{a_n\}$  is submultiplicative (that is,  $a_{n+m} \leq a_n a_m$  for all  $n, m$ ), which implies that  $\lim \sqrt[n]{a_n}$  exists. Therefore,  $\lim \sqrt[n]{a_n} > 1$ , so  $\{a_n\}$  grows exponentially.  $\square$

**Corollary 2.3.** *Let  $A$  be a finite-dimensional graded  $K$ -algebra, and let  $(U, R)$  be a graded presentation of  $A$ , which is minimal in the sense that no proper subset of  $U$  generates  $A$ . Then*

$$(2.3) \quad |R| > |U|^2/4.$$

*Proof.* We first note that  $r_1 = 0$ , that is,  $R$  has no relators of degree 1, since any such relator would allow us to express one of the generators in  $U$  as a linear combination of the others, contradicting the minimality of the presentation  $(U, R)$ . Therefore, for any  $\tau > 0$  we have  $1 - |U|\tau + H_R(\tau) \leq 1 - |U|\tau + |R|\tau^2$ .

On the other hand, since  $A$  is finite-dimensional, by Corollary 2.2, for any  $\tau > 0$  we have  $1 - |U|\tau + H_R(\tau) > 0$ . Thus,  $1 - |U|\tau + |R|\tau^2 > 0$  for any  $\tau > 0$ , and setting  $\tau = 2/|U|$ , we obtain  $|R| > |U|^2/4$ .  $\square$

**Remark:** Minimality of  $U$  is actually equivalent to the assumption  $r_1 = 0$ . Note that it is necessary to make this assumption in Corollary 2.3 – without it we could start with any finite presentation for  $A$  and then add any set of “artificial” generators  $S$  together with relations  $s = 0$  for each  $s \in S$ , violating (2.3) for sufficiently large  $S$ .

It is a very interesting question whether inequality (2.3) is optimal. More generally, fix a field  $K$ , and given an integer  $d \geq 2$ , let  $f(d)$  be the smallest positive integer for which there exists a subset  $R$  of  $K\langle u_1, \dots, u_d \rangle$  consisting of homogeneous elements of degree at least 2, with  $|R| = f(d)$ , such that the  $K$ -algebra  $\langle u_1, \dots, u_d \mid R \rangle$  is finite-dimensional.<sup>1</sup>

Corollary 2.3 implies that  $f(d) > d^2/4$ , and there is an obvious upper bound  $f(d) \leq (d^2 + d)/2$  yielded by any commutative algebra in which each  $u_i$  is nilpotent. That this upper bound is not optimal was immediately realized by Kostrikin [Kos] in 1965 who showed that  $f(d)$  is at most  $(d^2 - 1)/3 + d$ , at least when  $d$  is a power of 2.<sup>2</sup> In 1990, Wisliceny [Wis2] found a better upper bound which asymptotically coincides with the Golod-Shafarevich lower bound:  $f(d) \leq \frac{d^2}{4} + \frac{d}{2}$  if  $d$  is even and  $f(d) \leq \frac{d^2+1}{4} + \frac{d}{2}$  if  $d$  is odd. The final improvement was obtained very recently by Iyudu and Shkarin [IySh2] who proved that  $f(d) \leq \lceil \frac{d^2+d+1}{4} \rceil$  (where  $\lceil x \rceil$  is the smallest integer greater than or equal to  $x$ ). Examples of presentations yielding this bound (as well as examples from [Wis2]) are of very simple form, with every relation of the form  $u_i u_j = u_k u_l$  for some indices  $i, j, k$  and  $l$ . Algebras given by presentations of this form are called *quadratic semigroup algebras* in [IySh2], where it is proved that the bound  $f(d) \leq \lceil \frac{d^2+d+1}{4} \rceil$  is optimal for this class of associative algebras.

Another natural problem is when the Golod-Shafarevich inequality (2.1) becomes an equality. Anick showed that this happens if and only if the set of relators  $R$  is *strongly*

<sup>1</sup>It is not known whether the function  $f(d)$  depends on  $K$ .

<sup>2</sup>The paper [Kos] gives a construction of finite  $p$ -groups with the corresponding bound on the number of relators, but its easy modification yields the analogous result for associative algebras.

free [An1, Theorem 2.6], and if we assume that  $R$  is a minimal set of relators, then  $R$  is strongly free if and only if the algebra  $A = \langle U|R \rangle$  has global dimension  $\leq 2$  (see [An1, Theorem 2.12]); see also [Pi] for some related results. An easily verifiable sufficient condition for  $R$  to be strongly free is that the set of (suitably defined) leading terms of elements of  $R$  is combinatorially free (see [An1, Theorem 3.2]). Stronger results on this problem have been obtained for the class of quadratic algebras, that is, algebras given by a presentation with all relations homogeneous of degree two – see [An2, IySh1] and the books [Uf] and [PP].

**2.2. First applications of the Golod-Shafarevich inequality.** We now discuss two major applications of the Golod-Shafarevich inequality – the (negative) solutions to the Kurosh-Levitzky and the general Burnside problems.

**Problem** (Kurosh-Levitzky). *Let  $K$  be a field. Is it true that a finitely generated nil algebra over  $K$  must be finite-dimensional (and hence nilpotent)?*

**Theorem 2.4** (Golod, [Go1, Go2]). *Let  $K$  be a field and  $d \geq 2$  an integer. Then there exists a  $d$ -generated associative nil algebra over  $K$  which is infinite-dimensional.*

*Proof.* We start with the case when  $K$  is countable established in [Go1], where the argument is very simple. Let  $U = \{u_1, \dots, u_d\}$  and  $K\langle U \rangle^+$  the subset of  $K\langle U \rangle$  consisting of all polynomials with zero constant term. Since  $K$  is countable,  $K\langle U \rangle^+$  is also countable, so we can enumerate its elements:  $K\langle U \rangle^+ = \{f_1, f_2, \dots\}$ .

Let  $\tau \in (1/d, 1)$  and  $N \in \mathbb{N}$  be such that  $1 - d\tau + \sum_{n=N}^{\infty} \tau^n < 0$ . Choose  $N_1 \geq N$ , and write the element  $f_1^{N_1}$  as the sum of its homogeneous components:  $f_1^{N_1} = \sum_{i=1}^{k_1} f_{1,i}$ . Note that  $\deg(f_{1,i}) \geq N_1$  since  $f_1$  has zero constant term. Next choose  $N_2 \geq \max\{N_1 + 1, \{\deg(f_{1,i})\}\}$ , and let  $\{f_{2,i}\}_{i=1}^{k_2}$  be the homogeneous components of  $f_2^{N_2}$ . Next choose  $N_3 \geq \max\{N_2 + 1, \{\deg(f_{2,i})\}\}$  and proceed indefinitely.

Let  $R = \{f_{n,i} : n \in \mathbb{N}, 1 \leq i \leq k_n\}$ , consider the algebra  $A = \langle U|R \rangle$ , and let  $A^+$  be the image of  $K\langle U \rangle^+$  in  $A$ . By construction, the algebra  $A^+$  is  $d$ -generated and nil and has codimension 1 in  $A$ , so we only need to prove that  $A$  is infinite-dimensional. The choice of  $\{N_i\}$  ensures that the set of relations  $R$  contains at most one element of each degree and no elements of degree less than  $N$ . Therefore,  $1 - |U|\tau + H_R(\tau) \leq 1 - d\tau + \sum_{n=N}^{\infty} \tau^n < 0$ , so  $A$  is infinite-dimensional by Corollary 2.2.

*General case:* Let  $\Omega$  be the set of all non-empty finite sets of monic  $U$ -monomials of positive degree (this is clearly a countable set). Given  $\omega \in \Omega$ , let  $S_\omega$  be the set of all elements of  $K\langle U \rangle^+$  which are representable as a  $K$ -linear combination of elements of  $\omega$  and  $\omega$  is the smallest set with this property. Thus,  $K\langle U \rangle^+ = \sqcup_{\omega \in \Omega} S_\omega$ .

Now fix  $\omega = \{m_1, \dots, m_n\} \in \Omega$ . Every element  $f \in S_\omega$  can be written as a sum  $f = \sum_{i=1}^n c_i m_i$  where  $c_i$ 's are elements of  $K$ , which for the moment we treat as commuting formal variables. Given  $N \in \mathbb{N}$ , we have  $f^N = \sum_{i=1}^{d_{N,\omega}} \mu_{i,\omega,N}(c_1, \dots, c_n) p_{i,\omega,N}$  where each  $\mu_{i,\omega,N}(c_1, \dots, c_n)$  is a monic monomial in  $c_1, \dots, c_n$  of degree  $N$ ,  $d_{N,\omega}$  is the number of distinct such monomials, and each  $p_{i,\omega,N}$  is a polynomial in  $U$  with no terms of degree  $< N$ . Here are two key observations:

- (i) Fix  $\omega \in \Omega$  and  $N \in \mathbb{N}$ . If a set  $R$  contains all homogeneous components of  $p_{i,\omega,N}$  for each  $1 \leq i \leq d_{N,\omega}$ , then the image of every element of  $S_\omega$  in the algebra  $A = \langle U|R \rangle$  will be nilpotent.
- (ii) The sequence  $d_{N,\omega}$  grows polynomially in  $N$  (as  $\omega$  stays fixed) since  $c_i$ 's commute with each other.



Now fix  $\tau \in (1/d, 1)$ , for each  $\omega \in \Omega$  choose  $N_\omega \in \mathbb{N}$ , and let  $R$  be the set of all (nonzero) homogeneous components of the polynomials  $p_{i,\omega,N_\omega}$  with  $\omega \in \Omega$  and  $1 \leq i \leq d_{N_\omega}$ . Let  $A = \langle U | R \rangle$  and  $A^+$  the image of  $K\langle U \rangle^+$  in  $A$ .

Property (i) ensures that  $A^+$  is nil. Since homogeneous components of  $p_{i,\omega,N_\omega}$  have degree  $\geq N_\omega$ , we have

$$H_R(\tau) \leq \sum_{\omega \in \Omega} d_{N_\omega, \omega} \sum_{j=N_\omega}^{\infty} \tau^j = \sum_{\omega \in \Omega} d_{N_\omega, \omega} \frac{\tau^{N_\omega}}{1 - \tau}.$$

Property (ii) ensures that each term of this sum can be made arbitrarily small by choosing sufficiently large  $N_\omega$  (independently of other terms). In particular, we can make sure that  $1 - d\tau + H_R(\tau) < 0$ , so that  $A$  is infinite-dimensional, and we are done as in the case of countable  $K$ .  $\square$

Once Theorem 2.4 is proved, it is very easy to show that the general Burnside problem also has negative solution.

**Theorem 2.5** (Golod, [Go1]). *For every prime  $p$  and integer  $d \geq 2$  there exists an infinite  $d$ -generated  $p$ -torsion group.*

*Proof.* Let  $K = \mathbb{F}_p$ , the finite field of order  $p$ , and let  $A^+$  be the algebra constructed in the proof of Theorem 2.4. Since  $A^+$  is nil and  $K$  has characteristic  $p$ , the set  $1 + A^+ = \{1 + a : a \in A^+\}$  is a  $p$ -torsion group. We claim that the subgroup  $\Gamma$  of  $1 + A^+$  generated by  $1 + u_1, \dots, 1 + u_d$  is infinite (and hence satisfies all the required properties). The inclusion map  $\iota : \Gamma \rightarrow 1 + A^+$  induces a homomorphism  $\iota_* : \mathbb{F}_p[\Gamma] \rightarrow A$  (where  $\mathbb{F}_p[\Gamma]$  is the  $\mathbb{F}_p$ -group algebra of  $\Gamma$ ). The image of  $\iota_*$  contains 1 and  $1 + u_i$  for each  $i$  (hence also  $u_i$  for each  $i$ ), so  $\iota_*$  is surjective. Since  $A$  is infinite-dimensional, so must be  $\mathbb{F}_p[\Gamma]$ , whence  $\Gamma$  is infinite.  $\square$

Note that while the above construction of infinite finitely generated  $p$ -torsion groups uses very elementary tools, it has one disadvantage as we have no control over presentations of  $\Gamma$  by generators and relators. This problem will be addressed in the next section where we will provide an alternative version of Golod's construction (which uses Golod-Shafarevich groups), based on a more general form of the Golod-Shafarevich inequality.

**2.3. Golod-Shafarevich inequality for complete filtered algebras.** In order to define and study Golod-Shafarevich groups, one needs a more general version of the Golod-Shafarevich inequality dealing with complete filtered algebras. Below we shall essentially repeat the setup of § 2.1 with two changes: polynomials are replaced by power series and relators are allowed to be non-homogeneous.

As in § 2.1, we fix a finite set  $U$ , a field  $K$ , and let  $K\langle\langle U \rangle\rangle = K\langle\langle u_1, \dots, u_d \rangle\rangle$  be the algebra of power series over  $K$  in non-commuting variables  $u_1, \dots, u_d$ . As usual, given  $f \in K\langle\langle U \rangle\rangle$ , we define  $\deg(f)$  to be the smallest length of a monomial in  $U$  which appears in  $f$  with nonzero coefficient. For convenience we also set  $\deg(0) = \infty$ . Let  $K\langle\langle U \rangle\rangle_n = \{f \in K\langle\langle U \rangle\rangle : \deg(f) \geq n\}$ . The sets  $\{K\langle\langle U \rangle\rangle_n\}_{n \in \mathbb{N}}$  form a base of neighborhoods of 0 for the natural degree topology on  $K\langle\langle U \rangle\rangle$ .

Let  $I$  be a closed ideal of  $K\langle\langle U \rangle\rangle_1$ , let  $R \subseteq I$  be a subset which generates  $I$  as a (closed) ideal, and let  $r_n = |\{r \in R : \deg(r) = n\}|$ . As before, without loss of generality, we can assume that  $r_n < \infty$  for each  $n$ .

Let  $A = K\langle\langle U \rangle\rangle/I$ . Note that  $A$  is no longer a graded algebra, but it has a natural descending filtration  $\{A_n\}_{n \geq 0}$  where  $A_n = \pi(K\langle\langle U \rangle\rangle_n)$  and  $\pi : K\langle\langle U \rangle\rangle \rightarrow A$  is the natural projection. Since  $A$  is also complete with respect to topology determined by the filtration  $\{A_n\}$ , we will refer to such algebras as *complete filtered algebras*.

Define  $a_n = \dim_K A_n/A_{n+1}$ , and as in the graded case consider the Hilbert series  $Hilb_A(t) = \sum_{n=0}^{\infty} a_n t^n$  and  $H_R(t) = \sum_{n=1}^{\infty} r_n t^n$ .

**Theorem 2.6** (Golod-Shafarevich inequality: general case). *In the above setting we have*

$$(2.4) \quad \frac{(1 - |U|t + H_R(t)) \cdot Hilb_A(t)}{1 - t} \geq \frac{1}{1 - t}.$$

Inequality (2.4) was first proved by Vinberg [Vi] (see inequality (12) on p.212).<sup>3</sup> Its proof is similar to (but more technical than) the one in the graded case. This time it is not possible to give a good lower bound for  $a_n$ , but one can still give a bound for  $\dim A/A_{n+1} = a_0 + \dots + a_n$  which is the coefficient of  $t^n$  in the power series  $\frac{Hilb_A(t)}{1-t}$ .

Also note that inequality (2.4) follows from the one we had in the graded case by multiplying both sides by the power series  $\frac{1}{1-t}$  with positive coefficients. While inequality (2.4) is weaker than (2.1), all the key consequences of (2.1) established earlier in this section remain true in this setting:

**Proposition 2.7.** *Let  $A$  be a complete filtered algebra given by a presentation  $(U, R)$ .*

- (a) *Assume that there exists a real number  $\tau \in (0, 1)$  s.t.  $1 - |U|\tau + H_R(\tau) \leq 0$ . Then  $A$  is infinite-dimensional and  $Hilb_A(\tau)$  diverges. If  $1 - |U|\tau + H_R(\tau) < 0$ , the sequence  $\{a_n\}$  (defined above) has exponential growth.*
- (b) *If  $A$  is finite-dimensional and  $U$  is minimal, then  $|R| > |U|^2/4$ .*

**Definition.**

- (i) A presentation  $(U, R)$  in the category of complete filtered algebras will be said to satisfy the *Golod-Shafarevich (GS) condition* if  $1 - |U|\tau + H_R(\tau) < 0$  for some  $\tau \in (0, 1)$ .
- (ii) A complete filtered algebra  $A$  will be called *Golod-Shafarevich* if it has a presentation satisfying the GS condition.

### 3. GOLOD-SHAFAREVICH GROUPS

**3.1. Definition of Golod-Shafarevich groups.** Fix a prime number  $p$ , and let  $G$  be a finitely generated pro- $p$  group. Recall that  $G = \varprojlim_{N \in \Omega_p(G)} G/N$ , where  $\Omega_p(G)$  is the set of open normal subgroups of  $G$  (all of which have  $p$ -power index). We shall be interested in the completed group algebra  $\mathbb{F}_p[[G]]$  which is defined as the corresponding inverse limit of  $\mathbb{F}_p$ -group algebras:

$$\mathbb{F}_p[[G]] = \varprojlim_{N \in \Omega_p(G)} \mathbb{F}_p[G/N].$$

Suppose now that  $G$  is given in the form  $G = F/\langle R \rangle^F$  where  $F$  is a finitely generated free pro- $p$  group,  $R$  is a subset of  $F$  (and  $\langle R \rangle^F$  is the closed normal subgroup of  $F$  generated by  $R$ ). Then it is easy to see that there is a natural isomorphism  $\mathbb{F}_p[[G]] \cong \mathbb{F}_p[[F]]/I_R$  where  $I_R$  is the closed ideal of  $\mathbb{F}_p[[F]]$  generated by the set  $\{r - 1 : r \in R\}$ .

Let  $X = \{x_1, \dots, x_d\}$  be a free generating set of  $F$ . By a theorem of Lazard [Laz], the completed group algebra  $\mathbb{F}_p[[F]]$  is isomorphic to the algebra of power series  $\mathbb{F}_p\langle\langle u_1, \dots, u_d \rangle\rangle$  under the map  $x_i \mapsto 1 + u_i$ . Note that this map yields an embedding of  $F$  into  $\mathbb{F}_p\langle\langle u_1, \dots, u_d \rangle\rangle^\times$ ,

<sup>3</sup>Formally, [Vi] deals with polynomials and not power series, but this makes no difference as explained in the paragraph just before Theorem 2 in [Vi]. Similarly, the extra assumption  $r_1 = 0$  made in [Vi] is not essential for the proof.

the multiplicative group of  $\mathbb{F}_p\langle\langle u_1, \dots, u_d \rangle\rangle$ . This embedding is called the *Magnus embedding* (it was initially established by Magnus [Ma] in the case of free abstract groups).

The bottom line of the above discussion is that given a presentation  $(X, R)$  of a pro- $p$  group  $G$ , there is a corresponding presentation for the completed group algebra  $\mathbb{F}_p[[G]]$  as a quotient of  $\mathbb{F}_p\langle\langle U \rangle\rangle$  (with  $|U| = |X|$ ). A group  $G$  will be called *Golod-Shafarevich* if it has a presentation such that the corresponding presentation of  $\mathbb{F}_p[[G]]$  satisfies the GS condition.

**Definition.** Let  $X = \{x_1, \dots, x_d\}$  and  $U = \{u_1, \dots, u_d\}$  be finite sets of the same cardinality. Let  $F = F_{\widehat{p}}(X)$  the free pro- $p$  group on  $X$ , and let  $\iota : F \rightarrow \mathbb{F}_p\langle\langle U \rangle\rangle^\times$  be the Magnus embedding. Define the degree function  $D : F \rightarrow \mathbb{N} \cup \{\infty\}$  by

$$D(f) = \deg(\iota(f) - 1),$$

where  $\deg$  is the usual degree of a power series in  $u_1, \dots, u_d$ .

**Definition.**

- (i) A (pro- $p$ ) presentation  $(X, R)$  is said to satisfy the *Golod-Shafarevich (GS) condition* if there exists  $\tau \in (0, 1)$  such that  $1 - |X|\tau + H_R(\tau) < 0$  where  $H_R(t) = \sum_{r \in R} t^{D(r)}$ .
- (ii) A pro- $p$  group  $G$  is called a *Golod-Shafarevich (GS) group* if it has a presentation satisfying the GS condition.
- (iii) An abstract group  $G$  is called a *Golod-Shafarevich group* (with respect to  $p$ ) if its pro- $p$  completion  $G_{\widehat{p}}$  is Golod-Shafarevich.

**Remark:** It is more common to call an abstract group  $G$  Golod-Shafarevich if it has an *abstract* presentation  $(X, R)$  s.t.  $1 - |X|\tau + H_R(\tau) < 0$  for some  $\tau \in (0, 1)$ . This condition is certainly sufficient for  $G$  to be Golod-Shafarevich in our sense since if an abstract group  $G$  is given by a presentation  $(X, R)$ , then its pro- $p$  completion  $G_{\widehat{p}}$  is given by the same presentation  $(X, R)$ , considered as a pro- $p$  presentation (see, e.g., [Lu1, Lemma 2.1]). To the best of our knowledge, it is an open question whether these two definitions of Golod-Shafarevich abstract groups are equivalent. The advantage of our definition is that an abstract group  $G$  is Golod-Shafarevich if and only if the image of  $G$  in its pro- $p$  completion is Golod-Shafarevich.

**Theorem 3.1** (Golod-Shafarevich). *Golod-Shafarevich groups are infinite.*

*Proof.* If  $G$  is a Golod-Shafarevich pro- $p$  group, then by construction  $\mathbb{F}_p[[G]]$  is a Golod-Shafarevich algebra, hence infinite. This implies that  $G$  has infinitely many open subgroups, so  $G$  must be infinite. If  $G$  is a Golod-Shafarevich abstract group, its pro- $p$  completion is infinite, as we just argued, so  $G$  itself must be infinite.  $\square$

Before discussing applications of Golod-Shafarevich groups, we remark that the degree function  $D$  used above can also be described in terms of the Zassenhaus filtration which makes perfect sense in arbitrary (not just free) groups.

**Definition.** Let  $G$  be a finitely generated abstract (resp. pro- $p$ ) group. Let  $M$  be the augmentation ideal of the group algebra  $\mathbb{F}_p[G]$  (resp. completed group algebra  $\mathbb{F}_p[[G]]$ ), that is,  $M$  is the ideal generated by the set  $\{g - 1 : g \in G\}$ . For each  $n \in \mathbb{N}$  let  $D_n G = \{g \in G : g - 1 \in M^n\}$ . The series  $\{D_n G\}$  is called the Zassenhaus filtration of  $G$ .

If  $F$  is a finitely generated free pro- $p$  group and  $f \in F \setminus \{1\}$ , it is easy to see that  $D(f) = n$  if and only if  $f \in D_n F \setminus D_{n+1} F$ . In particular, this shows that the function  $D$  does not depend on the choice of a free generating set  $X$  of  $F$ .

It is well known (see, e.g., [DDMS, Ch. 11,12]) that the terms of Zassenhaus filtration can also be defined as verbal subgroups:

**Proposition 3.2.** *The Zassenhaus filtration  $\{D_n G\}$  can be alternatively defined by*

$$D_n G = \prod_{i \cdot p^j \geq n} (\gamma_i G)^{p^j}.$$

**3.2. First applications of Golod-Shafarevich groups.** As an immediate consequence of Theorem 3.1, we can construct infinite finitely generated torsion groups, which are explicitly given by generators and relators. The argument below is very similar (and actually simpler) than the one used in the solution to the Kurosh-Levitzky problem over countable fields. To the best of our knowledge, this argument was first used by Wilson in [Wil].

**Theorem 2.5** (Golod). *For every prime  $p$  and integer  $d \geq 2$  there exists an infinite  $d$ -generated  $p$ -torsion group.*

*Second proof of Theorem 2.5.* Let  $X$  be any finite set with  $|X| = d$  and  $F = F(X)$  the free group on  $X$ . Since  $F$  is countable, we can enumerate its elements  $F = \{f_1, f_2, \dots\}$ . Now take a sequence of integers  $n_1, n_2, \dots$ , and consider a group  $G = \langle X | R \rangle$  where  $R = \{f_1^{p^{n_1}}, f_2^{p^{n_2}}, \dots\}$ . By construction,  $G$  is  $p$ -torsion.

It is easy to see that  $D(f^{p^k}) = D(f)^{p^k}$  for any  $f \in F$ , so for any  $\tau \in (0, 1)$  we have

$$1 - |X|\tau + H_R(\tau) \leq 1 - |X|\tau + \sum_{i=1}^{\infty} \tau^{p^{n_i}}.$$

Now fix  $\tau \in (1/|X|, 1)$ . Then  $1 - |X|\tau < 0$ , so we can choose the sequence  $\{n_i\}$  such that  $\sum_{i=1}^{\infty} \tau^{p^{n_i}} < -(1 - |X|\tau)$ . Then  $G$  will be Golod-Shafarevich and therefore infinite.  $\square$

The following stronger version of Theorem 3.2, also due to Golod, was announced in [Go1] and proved in [Go2].

**Theorem 3.3** (Golod). *For every prime  $p$  and integer  $d \geq 2$  there exists an infinite  $d$ -generated  $p$ -torsion group in which every  $(d-1)$ -generated subgroup is finite.*

**Remark:** Theorem 3.3 was deduced in [Go2] from the corresponding result for graded algebras (which can also be found in the book by Kargapolov and Merzlyakov [KaMe]) in essentially the same way Theorem 2.5 follows from Theorem 2.4. Below we give a “direct” group-theoretic proof of this result, generalizing the argument in the second proof of Theorem 2.5.

*Proof of Theorem 3.3.* Take any set  $X$  with  $|X| = d$ , and construct a  $p$ -torsion Golod-Shafarevich group  $G = \langle X | R \rangle$  as in the second proof of Theorem 2.5 with the extra requirement that  $1 - |X|\tau + H_R(\tau) < 0$  for some  $\tau \in (\frac{1}{d}, \frac{1}{d-1})$ . Let  $\varepsilon = -(1 - |X|\tau + H_R(\tau))$  and  $\delta = \tau(d-1)$ . Since  $\delta < 1$ , we can find an integer sequence  $\{m_i\}$  such that  $\sum_{i=1}^{\infty} \delta^{m_i} < \varepsilon$ .

Now let  $\Omega = \{\omega^{(1)}, \omega^{(2)}, \dots\}$  be the set of all ordered  $(d-1)$ -tuples of elements of  $F(X)$  (the free group on  $X$ ) listed in some order. If  $\omega^{(i)} = (f_1^{(i)}, \dots, f_{d-1}^{(i)})$ , let  $R_i$  be the set of all left-normed commutators of length  $m_i$  involving  $f_1^{(i)}, \dots, f_{d-1}^{(i)}$ .

We claim that the group  $G' = \langle X | R \cup \bigcup_{i \geq 1} R_i \rangle$  has the required properties. By construction, every  $(d-1)$ -generated subgroup of  $G'$  is nilpotent and  $p$ -torsion (since  $G'$  is a quotient of  $G$ ) and hence finite. If  $c = [y_1, \dots, y_m]$  is a left-normed commutator of length  $m$ , then

$D(c) \geq D(y_1) + \dots + D(y_m)$ . Therefore, if  $S_i = \{(y_1, \dots, y_{m_i}) : y_j \in \{f_1^{(i)}, \dots, f_{d-1}^{(i)}\}\}$ , then

$$H_{R_i}(\tau) \leq \sum_{(y_1, \dots, y_{m_i}) \in S_i} \tau^{D(y_1) + \dots + D(y_{m_i})} \leq \left( \sum_{j=1}^{d-1} \tau^{D(f_j^{(i)})} \right)^{m_i} \leq (\tau(d-1))^{m_i} = \delta^{m_i}.$$

Hence  $1 - |X|\tau + H_R(\tau) + \sum_{i \geq 1} H_{R_i}(\tau) < 0$ , so  $G'$  is Golod-Shafarevich, hence infinite.  $\square$

We now turn to the proof of the famous inequality  $|R| > |X|^2/4$  for finite  $p$ -groups which was used in the solution of the class field tower problem. Recall that for a pro- $p$  group  $G$  we denote by  $d(G)$  and  $r(G)$  the minimal number of generators and relators of  $G$ , respectively.

**Theorem 3.4.** *Let  $p$  be a prime.*

- (a) *Let  $G$  be a finitely presented pro- $p$  group such that  $r(G) \leq d(G)^2/4$ . Then  $G$  is infinite. If in addition  $r(G) < d(G)^2/4$  and  $d(G) > 1$ , then  $G$  is Golod-Shafarevich.*
- (b) *Let  $\Gamma = \langle X | R \rangle$  be a finitely presented abstract group, and let  $d_p(\Gamma) = \dim_{\mathbb{F}_p}(\Gamma/[\Gamma, \Gamma]\Gamma^p)$ . If  $|R| < d_p(\Gamma)^2/4 - d_p(\Gamma) + |X|$  and  $d_p(\Gamma) > 1$ , then  $\Gamma$  is Golod-Shafarevich (with respect to  $p$ ).*

**Lemma 3.5.** *Let  $(X, R)$  be a presentation of a pro- $p$  group  $G$ , with  $X$  finite,  $F = F_{\hat{p}}(X)$  and  $\pi : F \rightarrow G$  the natural projection. The following hold:*

- (i)  *$|X| = d(G)$  if and only if  $R$  lies in  $\Phi(F) = [F, F]F^p$ , the Frattini subgroup of  $F$  (which holds if and only if  $D(r) \geq 2$  for all  $r \in R$ ). Moreover,  $R$  contains at least  $|X| - d(G)$  elements of degree 1.*
- (ii) *Assume that  $R$  is finite. Then  $G$  has a presentation with  $d(G)$  generators and  $|R| - |X| + d(G)$  relators. More precisely, there exists a subset  $X'$  of  $X$ , with  $|X'| = d(G)$  and a subset  $R'$  of  $R$  with  $|R'| = |R| - |X| + d(G)$  with the following properties:  $\pi(F(X')) = G$  and if  $\theta : F_{\hat{p}}(X) \rightarrow F_{\hat{p}}(X')$  is the unique homomorphism which acts as identity on  $X'$  and sends  $X \setminus X'$  to 1, then  $\theta(R')$  generates  $\text{Ker } \pi \cap F(X')$  as a closed normal subgroup of  $F(X')$ , and thus  $(X', \theta(R'))$  is a presentation of  $G$ . In particular,*

*Proof.* Part (i) easily follows from the fact that  $d(G) = d(G/[G, G]G^p)$ . Part (ii) follows from the proof of [Wi2, Prop. 12.1.5]; the first assertion of (ii) is also proved in [Lu1, Lemma 1.1].  $\square$

*Proof of Theorem 3.4.* In view of Lemma 3.5(i), (a) can be proved by the same argument as Corollary 2.3. For part (b) let  $G = \Gamma_{\hat{p}}$  be the pro- $p$  completion of  $G$ . Then  $d(G) = d_p(\Gamma)$ , and the result follows from (a) and Lemma 3.5(ii).  $\square$

As in the case of graded algebras, given  $d \in \mathbb{N}$ , it is natural to ask what is the minimal number  $f(d)$  for which there exists a finite  $p$ -group  $G$  with  $d(G) = d$  and  $r(G) = f(d)$ . The best currently known bound is due to Wisliceny [Wis1] who proved that  $f(d) \leq \frac{d^2}{4} + \frac{d}{2}$  (note that this coincides with the corresponding bound for graded algebras from [Wis2] obtained several years later).

**3.3. Word growth in Golod-Shafarevich groups.** In view of our informal statement “Golod-Shafarevich groups are big”, it is natural to expect that GS abstract groups at least have exponential growth. In fact, more is true: Golod-Shafarevich groups always have uniformly exponential growth, and this fact has a surprisingly simple proof.

**Proposition 3.6** ([BaGr]). *Golod-Shafarevich abstract groups have uniformly exponential growth.*

*Proof.* Let  $\Gamma$  be a GS group with respect to a prime  $p$  and  $M$  the augmentation ideal of  $\mathbb{F}_p[\Gamma]$ . If  $G = \Gamma_{\widehat{p}}$  is the pro- $p$  completion of  $\Gamma$  and  $\overline{M}$  is the augmentation ideal of  $\mathbb{F}_p[[G]]$ , it is easy to show that for every  $n \in \mathbb{N}$  the natural map  $\mathbb{F}_p[\Gamma]/M^n \rightarrow \mathbb{F}_p[[G]]/\overline{M}^n$  is an isomorphism. Thus, by Proposition 2.7(a), the sequence  $a_n = \dim_{\mathbb{F}_p} \mathbb{F}_p[\Gamma]/M^{n+1}$  grows exponentially in  $n$ . Now let  $X$  be any generating set of  $\Gamma$ . Then  $\mathbb{F}_p[\Gamma]/M^{n+1}$  is spanned by products of the form  $(1 - x_1)(1 - x_2) \dots (1 - x_m)$  with  $0 \leq m \leq n$  and  $x_i \in X$ . Each such product lies in the  $\mathbb{F}_p$ -span of  $B_X(n)$ , the ball of radius  $n$  with respect to  $X$  in  $\Gamma$ . Hence  $|B_X(n)| \geq a_n$ .  $\square$

It is now known that Golod-Shafarevich groups are uniformly non-amenable [EJ2, Appendix 2] (which strengthens the assertion of Proposition 3.6), but the proof of this result is much more involved. We will discuss the proof of non-amenability of Golod-Shafarevich groups in § 12.3.

**3.4. Golod-Shafarevich groups in characteristic zero.** In this subsection we will briefly discuss groups which are defined in the same way as Golod-Shafarevich groups in § 3.1, except that  $\mathbb{F}_p$  will be replaced by a field of characteristic zero. Unlike the positive characteristic case, we will begin the discussion with abstract groups.

Let  $K$  be a field of characteristic zero,  $X = \{x_1, \dots, x_d\}$  and  $U = \{u_1, \dots, u_d\}$  finite sets of the same cardinality. The map  $x_i \rightarrow 1 + u_i$  still extends to an embedding of the free group  $F(X) \rightarrow K\langle\langle U \rangle\rangle^\times$ . As in § 3.1, we define the degree function  $D_0 : F(X) \rightarrow \mathbb{N} \cup \{\infty\}$  by

$$D_0(f) = \deg(f - 1) \text{ for all } f \in F(X).$$

Again, the function  $D_0$  admits two alternative descriptions, one in terms of the augmentation ideal and another one in terms of the lower central series, which replaces the Zassenhaus filtration.

**Proposition 3.7.** *Let  $F = F(X)$ . Given  $f \in F \setminus \{1\}$  and  $n \in \mathbb{N}$ , the following are equivalent:*

- (i)  $D_0(f) = n$ ;
- (ii)  $f - 1 \in M^n \setminus M^{n+1}$  where  $M$  is the augmentation ideal of  $K[F]$ ;
- (iii)  $f \in \gamma_n F \setminus \gamma_{n+1} F$ .

**Definition.** Let  $\Gamma$  be a finitely generated abstract group. We will say that  $\Gamma$  is *Golod-Shafarevich in characteristic zero* if there is a presentation  $\Gamma = \langle X | R \rangle$  s.t.  $1 - |X|\tau + \sum_{r \in R} \tau^{D_0(r)} < 0$  for some  $\tau \in (0, 1)$ .

**Observation 3.8.** *If an abstract group  $\Gamma$  is GS in characteristic zero, then  $\Gamma$  is GS with respect to  $p$  for any prime  $p$ .*

*Proof.* Let  $F$  be a finitely generated free group and  $D$  the degree function on  $F$  coming from the Magnus embedding in characteristic  $p$  (as defined in § 3.1). Then  $D_0(f) \leq D(f)$  for any  $f \in F$  by Propositions 3.2 and 3.7. This immediately implies the result.  $\square$

In view of Observation 3.8, any result about GS (abstract) groups with respect to a prime  $p$  automatically applies to GS groups in characteristic zero. Somewhat surprisingly, nothing much beyond that seems to be known about GS groups in characteristic zero. It will be very interesting to prove some results about GS groups in characteristic zero (which do not apply to or not known for GS groups with respect to a prime  $p$ ) since the

former class includes some important groups, e.g. free-by-cyclic groups with first Betti number at least two.

The counterparts of GS pro- $p$  groups in characteristic zero are *Golod-Shafarevich pronipotent groups*. Let  $K$  be a field of characteristic zero. A pronipotent group over  $K$  can be defined as an inverse limit of unipotent groups over  $K$ . Given a natural number  $d$ , the free pronipotent group of rank  $d$  over  $K$ , denoted here by  $F_{\hat{K}}(d)$ , can be defined as the closure (in the degree topology) of the subgroup of  $K\langle\langle u_1, \dots, u_d \rangle\rangle^\times$ , generated by the elements  $(1 + u_i)^\lambda$  for all  $\lambda \in K$  (where by definition  $(1 + u_i)^\lambda = \sum_{m=0}^\infty \binom{\lambda}{m} u_i^m$ , which makes sense since  $K$  has characteristic zero). Thus, the function  $D_0$  originally defined on free abstract groups can be naturally extended to free pronipotent groups, and one can define Golod-Shafarevich pronipotent groups in the same way as Golod-Shafarevich groups in characteristic zero, replacing abstract presentations by presentations in the category of pronipotent groups over  $K$ . If  $\Gamma$  is a GS abstract group in characteristic zero, its pronipotent completion is a GS pronipotent group, but it is not clear whether the converse is true.

The general theory of pronipotent groups as well as the theory of Golod-Shafarevich pronipotent groups was developed by Lubotzky and Magid in [LuMa1, LuMa2, LuMa3]. Another notable result about Golod-Shafarevich pronipotent groups is due to Kassabov [Ka] who proved that they always contain non-abelian free pronipotent subgroups – this is a characteristic zero analogue of Zelmanov’s theorem [Ze1] discussed in § 7.

#### 4. GENERALIZED GOLOD-SHAFAREVICH GROUPS

In this section we introduce a more general form of the Golod-Shafarevich inequality and define the notion of generalized Golod-Shafarevich groups. Similarly one can define generalized Golod-Shafarevich algebras (graded or complete filtered) – see the end of § 4.2.

**4.1. Golod-Shafarevich inequality with weights.** In this subsection we essentially repeat the setup of § 2.3 with two differences:

- (i) generators will be counted with (possibly) different weights;
- (ii) the number of generators will be allowed to be countable.

By allowing countably many generators we will avoid some unnecessary restrictions in many structural results about generalized Golod-Shafarevich groups. However, all the key applications could still be achieved if we considered only the finitely generated case, so the reader may safely ignore the few minor subtleties arising from dealing with the countably generated case.

Let  $K$  be a field,  $U = \{u_1, u_2, \dots\}$  a finite or a countable set and  $A = \mathbb{F}_p\langle\langle U \rangle\rangle$ . Define a function  $d : A \rightarrow \mathbb{R}_{\geq 0} \cup \{\infty\}$  as follows:

- (i) Choose an arbitrary function  $d : U \rightarrow \mathbb{R}_{> 0}$ , and if  $U$  is countable, assume that  $d(u_i) \rightarrow \infty$  as  $i \rightarrow \infty$ .
- (ii) Extend  $d$  to the set of monic  $U$ -monomials by  $d(u_{i_1} \dots u_{i_k}) = d(u_{i_1}) + \dots + d(u_{i_k})$ . By convention we set  $d(1) = 0$ .
- (iii) Given an arbitrary nonzero power series  $f = \sum c_\alpha m_\alpha \in A$  (where  $\{m_\alpha\}$  are pairwise distinct monic monomials in  $U$  and  $c_\alpha \in K$ ), we put

$$(4.1) \quad d(f) = \min\{d(m_\alpha) : c_\alpha \neq 0\}.$$

Finally, we set  $d(0) = \infty$ .

**Definition.**

- (i) Any function  $d$  obtained in this way will be called a *degree function on  $\mathbb{F}_p\langle\langle U \rangle\rangle$  with respect to  $U$* .
- (ii) If  $U$  is finite, the unique degree function  $d$  such that  $d(u) = 1$  for all  $u \in U$  will be called *standard*.

Given a subset  $S \subseteq A$  such that for each  $\alpha \in \mathbb{R}$ , the set  $\{s \in S : d(s) = \alpha\}$  is finite, we put

$$H_{S,d}(t) = \sum_{s \in S} t^{d(s)}.$$

Note that we do not require that  $d$  is integer-valued, so  $H_{S,d}(t)$  is not a power series in general. It is easy to see, however, that for any degree function  $d$  the set  $\text{Im}(d)$  of possible values of  $d$  is discrete. Therefore, we can think of  $H_{S,d}(t)$  as an element of the ring  $K\{\{t\}\}$  whose elements are formal linear combinations  $\sum_{\alpha \geq 0} c_\alpha t^\alpha$  where  $c_\alpha \in K$  and the set  $\{\alpha : c_\alpha \neq 0\}$  is discrete. The latter condition ensures that the elements of  $K\{\{t\}\}$  can be multiplied in the same way as usual power series.

For each  $\alpha \geq 0$ , let

$$K\langle\langle U \rangle\rangle_\alpha = \{f \in K\langle\langle U \rangle\rangle : d(f) \geq \alpha\} \text{ and } K\langle\langle U \rangle\rangle_{>\alpha} = \{f \in K\langle\langle U \rangle\rangle : d(f) > \alpha\}.$$

As in § 2.3, let  $I$  be a closed ideal of  $K\langle\langle U \rangle\rangle_{>0}$ , let  $A = K\langle\langle U \rangle\rangle/I$  and  $R \subseteq I$  a subset which generates  $I$  as a (closed) ideal and such that  $r_\alpha = |\{r \in R : d(r) = \alpha\}|$  is finite for all  $\alpha$ . Let  $\pi : K\langle\langle U \rangle\rangle \rightarrow A$  be the natural projection. For each  $\alpha \geq 0$  let  $A_\alpha = \pi(K\langle\langle U \rangle\rangle_\alpha)$  and  $A_{>\alpha} = \pi(K\langle\langle U \rangle\rangle_{>\alpha})$  and  $a_\alpha = \dim_K A_\alpha/A_{>\alpha}$ . Finally, define the Hilbert series by

$$\text{Hilb}_{A,d}(t) = \sum_{\alpha \geq 0} a_\alpha t^\alpha.$$

In order to get a direct generalization of Theorem 4.1 we have to assume that the degree function  $d$  is integer-valued.

**Theorem 4.1** (Golod-Shafarevich inequality: weighted case). *Assume that  $d$  is an integer-valued degree function. Then in the above setting we have*

$$(4.2) \quad \frac{(1 - H_{U,d}(t) + H_{R,d}(t)) \cdot \text{Hilb}_{A,d}(t)}{1 - t} \geq \frac{1}{1 - t}.$$

We are not aware of any reference where this theorem is proved as stated above, but the proof of Theorem 2.6 extends to the weighted case almost without changes. Further, inequality (4.2) is proved in [Ko2] in a more restrictive setting (see formula (2.11) on p.105), but again the same argument can be used to establish Theorem 4.1.

**4.2. Generalized Golod-Shafarevich groups.** Let  $X = \{x_1, \dots, x_m\}$  and  $U = \{u_1, \dots, u_m\}$  be finite sets of the same cardinality,  $F = F_{\hat{p}}(X)$  the free pro- $p$  group on  $X$ , and embed  $F$  into  $\mathbb{F}_p\langle\langle U \rangle\rangle$  via the Magnus embedding  $x_i \mapsto 1 + u_i$ .

**Definition.**

- (a) A function  $D$  is called a *degree function on  $F$  with respect to  $X$*  if there exists a degree function  $d$  on  $\mathbb{F}_p[[F]]$  with respect to  $U = \{x - 1 : x \in X\}$  such that  $D(f) = d(f - 1)$  for all  $f \in F$ . We will say that  $D$  is the *standard degree function* if  $d$  is standard (equivalently if  $D(x) = 1$  for all  $x \in X$ ).
- (b) Given a subset  $S$  of  $F$  we put  $H_{S,D}(t) = \sum_{s \in S} t^{D(s)}$ .



Now let  $G$  be a pro- $p$  group,  $(X, R)$  a presentation of  $G$ ,  $D$  a degree function on  $F = F_{\widehat{p}}(X)$  with respect to  $X$  and  $d$  the corresponding degree function on  $\mathbb{F}_p[[F]]$ . If  $D$  is integer-valued, Golod-Shafarevich inequality (4.2) yields the following

$$(4.3) \quad \frac{(1 - H_{X,D}(t) + H_{R,D}(t)) \cdot \text{Hilb}_{\mathbb{F}_p[[G]],d}(t)}{1 - t} \geq \frac{1}{1 - t}.$$

**Definition.**

- (a) A pro- $p$  group  $G$  is called a *generalized Golod-Shafarevich (GGS) group* if there exists a presentation  $(X, R)$  of  $G$ , a real number  $\tau \in (0, 1)$  and a degree function  $D$  on  $F_{\widehat{p}}(X)$  with respect to  $X$  such that  $1 - H_{X,D}(\tau) + H_{R,D}(\tau) < 0$ .
- (b) An abstract group  $G$  is called a GGS group (with respect to  $p$ ) if its pro- $p$  completion is a GGS group.

**Remark:** It is clear that a pro- $p$  group is GS if and only if it satisfies condition (a) for the standard degree function  $D$ .

The reader may find it strange that we did not require  $D$  to be integer-valued in the definition of GGS groups, since this assumption is necessary for (4.3) to hold. The reason is that this would not make any difference:

**Lemma 4.2.** ([EJ2, Lemma 2.4]) *If  $(X, R)$  is a presentation and  $\tau \in (0, 1)$  is such that  $1 - H_{X,D}(\tau) + H_{R,D}(\tau) < 0$  for some degree function  $D$  on  $F = F_{\widehat{p}}(X)$  with respect to  $X$ , then there exists an integer-valued degree function  $D_1$  on  $F$  with respect to  $X$  and  $\tau_1 \in (0, 1)$  such that  $1 - H_{X,D_1}(\tau_1) + H_{R,D_1}(\tau_1) < 0$ . Moreover, we can assume that  $\tau_1^{D_1(f)} \leq \tau^{D(f)}$  for all  $f \in F$ .*

The proof of this lemma is not difficult, but the result becomes almost obvious when restated in the language of weight functions, discussed in the next subsection.

Thanks to this lemma, we can state the following consequence of (4.3) without assuming that  $D$  is integer-valued:

**Corollary 4.3.** *In the notations of (4.3) assume that  $1 - H_{X,D}(\tau) + H_{X,R}(\tau) < 0$  for some  $\tau \in (0, 1)$ . Then the series  $\text{Hilb}_{\mathbb{F}_p[[G]],d}(\tau)$  is divergent (so in particular,  $G$  is infinite).*

All properties of Golod-Shafarevich groups established so far trivially extend to generalized Golod-Shafarevich groups. The main reason we are concerned with GGS groups in this paper is the following result, which does not have a counterpart for GS groups:

**Theorem 4.4.** *Open subgroups of GGS pro- $p$  groups are GGS.*

This theorem, whose proof will be sketched in § 5, plays a crucial role in the proofs of some structural results about GS groups, so consideration of GGS groups is necessary even if one is only interested in GS groups. To give the reader a better feel about GGS groups, we shall provide a simple example of a pro- $p$  group, which is GGS, but not GS.

**Proposition 4.5.** *Let  $p > 3$ , let  $F = F_{\widehat{p}}(2)$  be the free pro- $p$  group of rank 2, let  $k \geq 2$ , and let  $\mathbb{Z}_p^k$  denote the  $k^{\text{th}}$  direct power of  $\mathbb{Z}_p$  (the additive group of  $p$ -adic integers). Then the group  $G = F \times \mathbb{Z}_p^k$  is GGS, but not GS.*

*Proof.* The group  $G$  has a natural presentation

$$\langle z_1, z_2, y_1, \dots, y_k \mid [z_i, y_j] = 1, [y_i, y_j] = 1 \rangle. \quad (***)$$

Thus, we have  $k + 2$  generators and  $\binom{k+2}{2} - 1 = k(k + 3)/2$  relators of degree 2, and an easy computation shows that this presentation does not satisfy the GS condition for

$k \geq 2$ . To prove that no other presentation of  $G$  satisfies the GS condition, we can argue as follows. First, by Lemma 3.5 it is sufficient to consider presentations  $(X, R)$  with  $|X| = d(G) = k + 2$ . We claim that in any such presentation  $R$  has at least  $k(k + 3)/2$  relators of degree 2 (this will finish the proof). It is easy to see that the number of relators of degree 2 in  $R$  is at least  $\log_p |D_2 F_{\widehat{p}}(X)/D_3 F_{\widehat{p}}(X)| - \log_p |D_2 G/D_3 G|$  (recall that  $\{D_n H\}$  is the Zassenhaus filtration of a group  $H$ ). If  $x_1, \dots, x_{k+2}$  are the elements of  $X$ , it is easy to see that a basis for  $D_2 F_{\widehat{p}}(X)/D_3 F_{\widehat{p}}(X)$  is given by the images of commutators  $[x_i, x_j]$  for  $i \neq j$  (here we use that  $p > 3$ ), while  $D_2 G/D_3 G$  is cyclic of order  $p$  spanned by the image of  $[z_1, z_2]$ . Thus, the same computation as above finishes the proof.

To prove that  $G$  is a GGS group, let  $(X, R)$  be the presentation of  $G$  given by (\*\*\*), and consider the degree function  $D$  on  $F_{\widehat{p}}(X)$  with respect to  $X$  given by  $D(z_1) = D(z_2) = 1$  and  $D(y_i) = N$  for  $1 \leq i \leq k$ , where  $N$  is a large integer. Then  $D([z_i, y_j]) = N + 1$  and  $D([y_i, y_j]) = 2N$ , so  $1 - H_{X,D}(\tau) + H_{R,D}(\tau) = 1 - 2\tau - k\tau^N + 2k\tau^{N+1} + \binom{k}{2}\tau^{2N}$ . This expression can be clearly made negative by first choosing  $\tau \in (1/2, 1)$  and then taking a large enough  $N$ . Thus,  $G$  is indeed a GGS group.  $\square$

**Remark:** Essentially the same argument shows that the direct product of any GGS pro- $p$  group  $G$  with any finitely generated pro- $p$  group  $H$  will be GGS.

In complete similarity to the group case, we will call a graded or a complete filtered  $K$ -algebra  $A$  *generalized Golod-Shafarevich* if there exists a presentation (in the corresponding category)  $(U, R)$  of  $A$ , a real number  $\tau \in (0, 1)$  and a degree function  $d$  on  $K\langle\langle U \rangle\rangle$  such that  $1 - H_{U,d}(\tau) + H_{R,d}(\tau) < 0$ . However, it is not clear whether key properties of generalized Golod-Shafarevich groups (e.g. Theorem 4.4) would remain true for algebras. In fact, the arguments of Voden [Vo] strongly suggest that even if  $A$  is a non-abelian free graded algebra, finite codimension graded subalgebras of  $A$  may not be generalized Golod-Shafarevich algebras. At the same time Voden [Vo] proves that if a graded algebra  $A = \bigoplus_{n=0}^{\infty} A_n$  has a minimal presentation  $(U, R)$ , with  $|R| < \frac{1}{4}(\frac{|U|}{2} - 1)^2$  and  $|U| > 1$ , then the Veronese power  $A^{(k)}$  is Golod-Shafarevich for infinitely many values of  $k$ , where by definition  $A^{(k)} = \bigoplus_{n=0}^{\infty} A_{kn}$ , with  $k \in \mathbb{N}$ . At the moment it is not clear what should be the “right” substitute for the notion of generalized Golod-Shafarevich algebra (if any) which would lead to an interesting theory.

**4.3. Weight functions.** In this subsection we introduce multiplicative counterparts of degree functions, called weight functions. Even though weight functions are obtained from degree functions merely by exponentiation, they provide a very convenient language for working with generalized Golod-Shafarevich groups.

**Definition.** Let  $F$  be a free pro- $p$  group,  $X$  a free generating set of  $F$  and  $U = \{x - 1 : x \in X\}$  so that  $\mathbb{F}_p[[F]] \cong \mathbb{F}_p\langle\langle U \rangle\rangle$ .

- (i) A function  $w : \mathbb{F}_p[[F]] \rightarrow [0, 1)$  is called a *weight function on  $\mathbb{F}_p[[F]]$  with respect to  $U$*  if there exists  $\tau \in (0, 1)$  and a degree function  $d$  on  $\mathbb{F}_p[[F]]$  with respect to  $U$  such that

$$w(f) = \tau^{d(f)}.$$

- (ii) A function  $W : F \rightarrow [0, 1)$  is called a *weight function on  $F$  with respect to  $X$*  if there exists  $\tau \in (0, 1)$  and a degree function  $D$  on  $F$  with respect to  $X$  such that

$$W(f) = \tau^{D(f)}.$$

Equivalently,  $W$  is a weight function on  $F$  with respect to  $X$  if there is a weight function  $w$  on  $\mathbb{F}_p[[F]]$  with respect to  $U$  such that  $W(f) = w(f - 1)$  for all  $f \in F$ .

If  $S$  is a subset of  $F$  and  $W$  is a weight function on  $F$ , we define  $W(S) = \sum_{s \in S} W(s)$ . Thus, in our previous notations, if  $W = \tau^D$  for a degree function  $D$ , then  $W(S) = H_{S,D}(\tau)$ . The definition of generalized Golod-Shafarevich groups can now be expressed as follows:

**Definition.** A pro- $p$  group  $G$  is a generalized Golod-Shafarevich group if there exists a presentation  $(X, R)$  of  $G$  and a weight function  $W$  on  $F_{\hat{p}}(X)$  with respect to  $X$  such that

$$1 - W(X) + W(R) < 0.$$

A weight function  $W$  will be called *uniform* if  $W = \tau^D$  for some  $\tau$  and the standard degree function  $D$  (that is,  $D(x) = 1$  for all  $x \in X$ ).

## 5. PROPERTIES AND APPLICATIONS OF WEIGHT FUNCTIONS AND VALUATIONS

**5.1. Dependence on the generating set.** So far we defined weight functions with respect to a fixed generating set  $X$ . For many purposes it is convenient to have a “coordinate-free” characterization of weight functions, where the set  $X$  need not be specified in advance.

**Definition.** Let  $F$  be a free pro- $p$  group. A function  $W : F \rightarrow [0, 1]$  is called a *weight function on  $F$*  if  $W$  is a weight function on  $F$  with respect to  $X$  for some free generating set  $X$  of  $F$ . Any set  $X$  with this property will be called  *$W$ -free*.

The first basic question is which sets are  $W$ -free for a given weight function  $W$  on  $F$ ? If  $W$  is a uniform weight function (that is,  $W = \tau^D$  for the standard degree function  $D$ ), then any free generating set  $X$  will be  $W$ -free, since the standard degree function can be defined without reference to a specific free generating set. However, if  $W$  is not uniform, there always exists a free generating set  $X$  which is not  $W$ -free. This follows from Theorem 5.3 below and is illustrated by the following example.

**Lemma 5.1.** *Let  $F$  be a finitely generated free pro- $p$  group,  $X = \{x_1, \dots, x_m\}$  a free generating set of  $F$  and  $W$  a weight function on  $F$  with respect to  $X$ . Let  $f = x_{i_1}^{n_1} \dots x_{i_k}^{n_k}$  where the indices  $i_1, \dots, i_k$  are distinct and each  $n_i$  is not divisible by  $p$ . Then  $W(f) = \max\{W(x_{i_j})\}_{j=1}^k$ .*

*Proof.* Let  $u_i = x_i - 1 \in \mathbb{F}_p[[F]]$ . Then by definition  $W(f) = w(f - 1)$ , where  $w$  is the unique weight function on  $\mathbb{F}_p[[F]]$  with respect to  $U = \{u_1, \dots, u_m\}$  such that  $w(u_i) = W(x_i)$ . Note that  $f - 1 = \sum n_j u_{i_j} + h$  where  $h$  is a sum of monomials, each of which involves at least two  $u_{i_j}$ 's. Since each  $n_j \neq 0$  in  $\mathbb{F}_p$  by assumption, we get  $W(f) = w(f - 1) = \max\{w(u_{i_j})\}_{j=1}^k = \max\{W(x_{i_j})\}_{j=1}^k$ .  $\square$

**Example 5.2.** Let  $X = \{x_1, x_2\}$ ,  $F = F_{\hat{p}}(X)$  and  $\alpha, \beta \in (0, 1)$ . Let  $W$  be the unique weight function on  $F$  with respect to  $X$  such that  $W(x_1) = \alpha$  and  $W(x_2) = \beta$ . Let  $X' = \{x_1, x_1 x_2\}$ . We claim that if  $\alpha > \beta$ , then  $W$  is NOT a weight function with respect to  $X'$ . Indeed, by Lemma 5.1,  $W(x_1 x_2) = \max\{\alpha, \beta\} = \alpha$ . If  $W$  was also a weight function with respect to  $X'$ , Lemma 5.1 would have implied that  $W(x_2) = W(x_1^{-1} \cdot x_1 x_2)$  is equal to  $\max\{W(x_1), W(x_1 x_2)\} = \alpha$ , which is false.

If we assume that  $\alpha \leq \beta$  in the above example, then  $W$  will be a weight function with respect to  $\{x_1, x_1 x_2\}$ , although this is harder to show by a direct computation. In general, we have the following criterion for  $W$ -freeness.

**Theorem 5.3.** *Let  $W$  be a weight function on a free pro- $p$  group  $F$ , let  $X$  be a free generating set of  $F$ , and assume that  $W(X) < \infty$ . The following are equivalent.*

- (i)  $X$  is  $W$ -free.

- (ii) If  $X'$  is any free generating set of  $F$ , then  $W(X) \leq W(X')$ .
- (iii) If  $X'$  is any free generating set of  $F$ , then there is a bijection  $\sigma : X \rightarrow X'$  such that  $W(x) \leq W(\sigma(x))$  for all  $x \in X$ .

*Proof.* This is an easy consequence of results in [EJ3, § 3]. More specifically, let us say that  $X$  is a  $W$ -optimal generating set if it satisfies condition (ii). The definition of a  $W$ -optimal generating set in [EJ3] is different, but the two definitions are equivalent by Proposition 3.6 and Corollary 3.7 of [EJ3]. Proposition 3.9 of [EJ3] then shows the equivalence of (i) and (ii) and Proposition 3.6 easily implies the equivalence of (ii) and (iii).  $\square$

One of the most important properties of weight functions is the following theorem:

**Theorem 5.4.** [EJ2, EJ3] *Let  $F$  be a free pro- $p$  group and  $W$  a weight function on  $F$ . If  $K$  is a closed subgroup of  $F$ , then  $W$  restricted to  $K$  is also a weight function.*

This theorem appears as [EJ2, Cor. 3.6] in the case when  $K$  is open in  $F$  and  $F$  is finitely generated and as [EJ3, Cor. 3.4] in the general case. The second proof is more conceptual (see a brief sketch in § 5.2), while the first one has the advantage of producing an algorithm for finding a  $W$ -free generating set for an open subgroup  $K$  (see a sketch in § 5.3).

**5.2. Valuations.** One inconvenience in working with weight functions is that they are defined on free pro- $p$  groups and not on the groups given by generators and relators we are trying to investigate. However, as we will explain below, given a pro- $p$  group  $G$  and a free presentation  $\pi : F \rightarrow G$  (that is, an epimorphism from a free pro- $p$  group  $F$  to  $G$ ), every weight function on  $F$  will induce a function on  $G$  satisfying certain properties. Such functions will be called valuations.

**Definition.** Let  $G$  be a pro- $p$  group. A continuous function  $W : G \rightarrow [0, 1]$  is called a *valuation* if

- (i)  $W(g) = 0$  if and only if  $g = 1$ ;
- (ii)  $W(fg) \leq \max\{W(f), W(g)\}$  for any  $f, g \in G$ ;
- (iii)  $W([f, g]) \leq W(f)W(g)$  for any  $f, g \in G$ ;
- (iv)  $W(g^p) \leq W(g)^p$  for any  $g \in G$ .

It is easy to check that any weight function on a free pro- $p$  group is a valuation, but the converse is not true – for instance, if  $W$  is a weight function on a free pro- $p$  group  $F$  such that  $W(f) < 1/2$  for all  $f \in F$ , the function  $W'(f) = 2W(f)$  will be a valuation, but not a weight function. It is also not hard to show that given a free generating set  $X$  of  $F$  and a weight function  $W$  on  $F$  with respect to  $X$  the following is true:

If  $W'$  is any valuation on  $F$  such that  $W'(x) = W(x)$  for all  $x \in X$ , then  $W'(f) \leq W(f)$  for all  $f \in F$ .

There are two simple ways to get new valuations from old.

- (i) If  $W$  is a valuation on  $G$  and  $H$  is a closed subgroup of  $G$ , then  $W$  restricted to  $H$  is clearly a valuation on  $H$  (we will denote the restricted valuation also by  $W$ ).
- (ii) If  $\pi : H \rightarrow G$  is an epimorphism of pro- $p$  groups, then every valuation  $W$  on  $H$  induces the corresponding valuation  $W'$  on  $G$  given by

$$W'(g) = \inf\{W(h) : h \in H, \pi(h) = g\}.$$

In the special case when  $G$  is defined as a quotient of  $H$  and  $\pi : G \rightarrow H$  is the natural projection, we will usually denote the induced valuation on  $G$  also by  $W$ .

An important special case of (ii) is that if  $G$  is a pro- $p$  group and  $\pi : F \rightarrow G$  is a free presentation of  $G$ , then every weight function on  $F$  will induce a valuation on  $G$ . By [EJ3, Prop. 4.7], the converse is also true: every valuation on  $G$  is induced from some weight function in such a way; however, if  $G$  is finitely generated, one cannot guarantee that  $F$  can be chosen finitely generated.

Given a valuation  $W$  on  $G$  and  $\alpha \in (0, 1)$ , define the subgroups  $G_{\alpha, W}$  and  $G_{<\alpha, W}$  of  $G$  by

$$G_{\alpha, W} = \{g \in G : W(g) \leq \alpha\} \quad \text{and} \quad G_{<\alpha, W} = \{g \in G : W(g) < \alpha\}.$$

The associated graded restricted Lie algebra  $L_W(G)$  is defined as follows: as a graded abelian group  $L_W(G) = \bigoplus_{\alpha \in \text{Im}(W)} G_{\alpha, W} / G_{<\alpha, W}$ , the Lie bracket is defined by

$$[gG_{<\alpha, W}, hG_{<\beta, W}] = [g, h]G_{<\alpha\beta, W} \text{ for all } g \in G_{\alpha, W} \text{ and } h \in G_{\beta, W}$$

(where  $[g, h] = g^{-1}h^{-1}gh$ ) and the  $p$ -power operation is defined by

$$(gG_{<\alpha, W})^{[p]} = g^p G_{<\alpha^p, W} \text{ for all } g \in G_{\alpha, W} \text{ and } h \in G_{\beta, W}.$$

If  $H$  is a closed subgroup of  $G$ , it is easy to see that  $L_W(H)$  (the Lie algebra of  $H$  with respect to the induced valuation) is naturally isomorphic to a subalgebra of  $L_W(G)$ . The following characterization of weight functions among all valuations is obtained in [EJ3].

**Theorem 5.5.** ([EJ3, Corollary 3.3]) Let  $F$  be a free pro- $p$  group. A valuation  $W$  on  $F$  is a weight function if and only if  $L_W(F)$  is a free restricted Lie algebra.

Since subalgebras of free restricted Lie algebras are free restricted, Theorem 5.4 follows from Theorem 5.5 and a paragraph preceding it.

**5.3. Weighted rank, index and deficiency.** Given a pro- $p$  group  $G$  and a valuation  $W$  of  $G$ , there are three important numerical invariants –

- (i) the  $W$ -rank of  $G$ , denoted by  $rk_W(G)$ ,
  - (ii) the  $W$ -deficiency of  $G$ , denoted by  $def_W(G)$ , and
  - (iii) for every closed subgroup  $H$  of  $G$ , the  $W$ -index of  $H$  in  $G$ , denoted by  $[G : H]_W$
- which behave very similarly to their usual (non-weighted) counterparts.

The definition of the  $W$ -rank is the obvious one:

**Definition.** The  $W$ -rank of a pro- $p$  group  $G$ , denoted by  $rk_W(G)$ , is the infimum of the set  $\{W(X)\}$  where  $X$  ranges over all generating sets of  $G$ . In fact, a standard compactness argument shows that if this infimum is finite, it must be attained on some set  $X$ .

Before defining  $W$ -deficiency, we need some additional terminology.

**Definition.** A valuation  $W$  on a pro- $p$  group  $G$  is called *finite* if there is a free presentation  $\pi : F \rightarrow G$  and a weight function  $\widetilde{W}$  on  $F$  which induces  $W$  and such that  $rk_{\widetilde{W}}(F) < \infty$ .

Note that in many cases finiteness of a valuation  $W$  holds automatically: this is the case if  $W$  is a weight function on a finitely generated free pro- $p$  group  $F$  or if  $W$  is quotient-induced from such a weight function. In applications of Golod-Shafarevich groups all valuations will be obtained in such way, so the problem of verifying finiteness of a valuation never arises in practice. In more theoretical contexts, one can use the following criterion ([EJ3, Prop. 4.7]): a valuation  $W$  on  $G$  is finite if and only if there is a subset  $Y$  of  $G$ , with  $W(Y) < \infty$ , s.t. the elements  $\{yG_{<W(y), W} : y \in Y\}$  generate the Lie algebra  $L_W(G)$ .

**Definition.**

- (a) A weighted presentation is a triple  $(X, R, W)$  where  $(X, R)$  is a (pro- $p$ ) presentation and  $W$  is a weight function on  $F_{\widehat{p}}(X)$  with respect to  $X$ .
- (b) Let  $(X, R, W)$  be a weighted presentation, where  $W(X) < \infty$ . We set  $\text{def}_W(X, R) = W(X) - W(R) - 1$ .
- (c) Let  $G$  be a pro- $p$  group and  $W$  a finite valuation on  $G$ . The  $W$ -deficiency of  $G$ , denoted by  $\text{def}_W(G)$ , is defined to be the supremum of the set  $\{\text{def}_{\widetilde{W}}(X, R)\}$  where  $(X, R, \widetilde{W})$  ranges over all weighted presentations such that  $G = \langle X | R \rangle$ ,  $\widetilde{W}$  induces  $W$  and  $\widetilde{W}(X) < \infty$ .

Note that we can now rephrase the definition of GGS groups as follows.

**Definition.** A pro- $p$  group  $G$  is GGS if and only if  $\text{def}_W(G) > 0$  for some finite valuation  $W$  of  $G$ .

Thus, GGS groups can be thought of as groups of positive weighted deficiency (explaining the title of [EJ3]). We will not use the latter terminology in this paper, but we will work with the quantity  $\text{def}_W(G)$ , which is very convenient.

Recall two classical inequalities relating the usual (non-weighted) notions of rank, deficiency and index.

**Theorem 5.6.** *Let  $G$  be a finitely generated abstract or a pro- $p$  group and  $H$  a finite index subgroup of  $G$ . Then*

- (a)  $d(H) - 1 \leq (d(G) - 1)[G : H]$ . *Moreover, if  $G$  is free, then  $H$  is free and equality holds.*
- (b)  $\text{def}(H) - 1 \geq (\text{def}(G) - 1)[G : H]$ .

Part (a) is just the Schreier formula, and (b) is an easy consequence of (a) and the Reidemeister-Schreier rewriting process (see, e.g., [Os2, Lemma 2.1]).

It turns out that one can define  $W$ -index  $[G : H]_W$  in such a way that the weighted analogues of (a) and (b) will hold.

**Definition.** Let  $W$  be a valuation on a pro- $p$  group  $G$  and  $H$  a closed subgroup of  $G$ . For each  $\alpha \in \text{Im}(W)$  let  $c_{\alpha, W}(G/H) = \log_p |G_{\alpha, W} H / G_{< \alpha, W} H|$ . The quantity

$$[G : H]_W = \prod_{\alpha \in \text{Im}(W)} \left( \frac{1 - \alpha^p}{1 - \alpha} \right)^{c_{\alpha, W}(G/H)}$$

is called the  $W$ -index of  $H$  in  $G$ .

In the next subsection we will reveal where the above formula comes from. At this point we just observe that the usual index  $[G : H]$  is given by the formula  $[G : H] = p^{\sum_{\alpha \in \text{Im}(W)} c_{\alpha, W}(G/H)}$ . Hence, if we fix  $H$  and consider a sequence  $\{W_n\}$  of valuations on  $G$  which converges pointwise to the constant function 1 on  $G \setminus \{1\}$ , then the sequence  $[G : H]_{W_n}$  will converge to  $[G : H]$ .

Here is the weighted counterpart of Theorem 5.6. We will discuss the idea of its proof in the next subsection.

**Theorem 5.7.** *Let  $W$  be a valuation on a pro- $p$  group  $G$  and let  $H$  be a closed subgroup of  $G$  with  $[G : H]_W < \infty$ . Then*

- (a)  $\text{rk}_W(H) - 1 \leq (\text{rk}_W(G) - 1)[G : H]_W$ . *Moreover, if  $G$  is free and  $W$  is a weight function, then equality holds.*
- (b)  $\text{def}_W(H) \geq \text{def}_W(G)[G : H]_W$ .

Note that part (b) immediately implies that an open subgroup of a GGS pro- $p$  group is also a GGS pro- $p$  group, the result stated earlier as Theorem 4.4.

Below are some properties of  $W$ -index which we shall need later:

**Proposition 5.8.** Let  $W$  be a valuation on a pro- $p$  group  $G$ . Then  $W$ -index is multiplicative, that is, if  $K \subseteq H$  are closed subgroups of  $G$ , then  $[G : K]_W = [G : H]_W \cdot [H : K]_W$ .

**Proposition 5.9** (Continuity lemma). *Let  $W$  be a valuation on a pro- $p$  group  $G$ , let  $H$  be a closed subgroup of  $G$ , and let  $\{U_n\}$  be a descending chain of open subgroups of  $G$  such that  $H = \cap U_n$ . Then*

- (i)  $[G : H]_W = \lim_{n \rightarrow \infty} [G : U_n]_W$ .
- (ii) If  $[G : H]_W < \infty$ , then  $rk_W(H) = \lim_{n \rightarrow \infty} rk_W(U_n)$ .
- (iii) If  $[G : H]_W < \infty$ , then  $def_W(H) = \lim_{n \rightarrow \infty} def_W(U_n)$ .

Proposition 5.8 is straightforward, and Continuity Lemma is established in [EJ3]: (i) is [EJ3, Lemma 3.15], (ii) is [EJ3, Lemma 3.17] and (iii) follows from the proof of [EJ3, Prop. 4.3] although it is not explicitly stated there.

**5.4. Proof of Theorem 5.7 (sketch).** Proposition 5.9 reduces both (a) and (b) to the case when  $H$  is an open subgroup. By Proposition 5.8, it suffices to consider the case when  $[G : H] = p$ .

(a) We first treat the case when  $G$  is free and  $W$  is a weight function. Let  $X$  be any  $W$ -free generating set of  $F$ . First, replacing  $X$  by another  $W$ -free generating set, we can always assume that

There is just one element  $x \in X$  which lies outside of  $H$ . (\*\*\*)

To achieve this, we let  $x$  be the element of the original set  $X$  which lies outside of  $H$  and has the smallest  $W$ -weight among all such elements and then, for each  $z \in X \setminus \{x\} \setminus H$ , replace  $z$  by  $zx^m$  for suitable  $m \in \mathbb{Z}$  so that  $zx^m \in H$  (such  $m$  exists since  $G/H$  is cyclic of prime order and  $x \notin H$ ). Condition (ii) in the definition of a valuation and Theorem 5.3 ensure that the new generating set of  $F$  is still  $W$ -free.

From now on we shall assume that (\*\*\*) holds. A standard application of the Schreier method shows that  $H$  is freely generated by the set  $X' = \{y^{x^i} : y \in X \setminus \{x\}\} \cup \{x^p\}$ . This set, however, is not  $W$ -free by Theorem 5.3 since it clearly does not have the smallest possible  $W$ -weight – for instance, one can replace  $y^x$  by  $y^{-1}y^x = [y, x]$ , thereby decreasing the total weight as  $W([y, x]) \leq W(y)W(x) < W(y) = W(y^x)$ . It is not difficult to show that the  $W$ -weight will be minimized on the generating set

$$(5.1) \quad \tilde{X} = \cup_{y \in X \setminus \{x\}} \{y, [y, x], [y, x, x], \dots, [y, \underbrace{x, \dots, x}_{p-1 \text{ times}}]\} \cup \{x^p\}.$$

Informally, this happens because if we let  $U = \{x - 1 : x \in X\}$  (so that  $\mathbb{F}_p[[F]] \cong \mathbb{F}_p\langle\langle U \rangle\rangle$ ) and expand elements of the set  $\tilde{U} = \{\tilde{x} - 1 : \tilde{x} \in \tilde{X}\}$  as power series in  $U$ , then the monomials of maximal  $W$ -weight in those expansions will all be distinct (this is a Gröbner basis type of argument). Thus, by Theorem 5.3,  $\tilde{X}$  is  $W$ -free.

Note that if  $\tau = W(x)$ , then in the above formula we have

$$W(\tilde{X}) - 1 = (W(X) - \tau)(1 + \tau + \dots + \tau^{p-1}) + \tau^p - 1 = (W(X) - 1) \cdot \frac{1 - \tau^p}{1 - \tau}.$$

Again by Theorem 5.3 we have  $W(X) = rk_W(F)$  and  $W(\tilde{X}) = rk_W(H)$ . Moreover, it is not difficult to show that  $c_{\alpha, W}(G/H)$  is equal to 1 for  $\alpha = \tau$  and 0 for  $\alpha \neq \tau$ . Hence  $[G : H]_W = \frac{1-\tau^p}{1-\tau}$ , and we are done.

In the case when  $G$  is an arbitrary group, we can essentially repeat the above argument, assuming at the beginning that  $X$  is a generating set of  $G$  with  $W(X) = rk_W(G)$ . The set  $\tilde{X}$  given by (5.1) will still generate  $H$ , but we no longer know whether  $W(\tilde{X})$  equals  $rk_W(H)$ ; this is why we can only claim inequality in the formula.

(b) follows easily from (a) and the Schreier method. First, by Propositions 5.8 and 5.9 we can again assume that  $[G : H] = p$ . Consider any weighted presentation  $(X, R, \tilde{W})$  of  $G$  where  $\tilde{W}$  induces  $W$  and  $\tilde{W}(X) < \infty$ . As before, we can assume that (\*\*\*) from (a) holds. Then  $H$  is given by the presentation  $(\tilde{X}, R')$  where  $\tilde{X}$  is as before and  $R' = \{r^{x^i} : r \in R\}$ . Again, we can replace the set of relators  $R'$  by the set  $\tilde{R} = \cup_{r \in R} \{r, [r, x], [r, x, x], \dots, [r, \underbrace{x, \dots, x}_{p-1 \text{ times}}]\}$ , and by direct computation  $\tilde{W}(\tilde{R}) \leq \tilde{W}(R)[G :$

$H]_W$ . Since  $\tilde{W}(\tilde{X}) - 1 = (\tilde{W}(X) - 1)[G : H]_W$  by the proof of (a), we conclude that  $def_{\tilde{W}}(\tilde{X}, \tilde{R}) \geq def_{\tilde{W}}(X, R)[G : H]_W$ , which yields (b) by taking the supremum of both sides over all triples  $(X, R, \tilde{W})$ .

**5.5.  $W$ -index and Quillen's theorem.** Although we already gave some indication why the notion of  $W$ -index is a useful tool, its definition may still appear mysterious. Below we state another formula generalizing (a version of) Quillen's theorem, where  $W$ -index naturally appears. In order to state it, we have to go back to degree functions and also introduce some additional notations.

Let  $G$  be a pro- $p$  group,  $\pi : F \rightarrow G$  a free presentation of  $G$ ,  $d$  a degree function on  $\mathbb{F}_p[[F]]$  and  $D$  the corresponding degree function on  $F$ , that is,  $D(a) = d(a - 1)$ . Then  $D$  induces a function on  $G$  (by abuse of notation also denoted by  $D$ ) given by

$$D(g) = \inf\{D(f) : f \in F, \pi(f) = g\}.$$

For each  $\lambda \in \mathbb{R}_{>0}$  let  $G^{\lambda, D} = \{g \in G : D(g) \geq \lambda\}$ ,  $G^{>\lambda, D} = \{g \in G : D(g) > \lambda\}$  and  $c^{\lambda, D}(G) = [G^{\lambda, D} : G^{>\lambda, D}]$

**Theorem 5.10.** *Let  $G, F, \pi, d, D$  be as above.*

(a) (Quillen's theorem) *The following equality of generalized power series holds:*

$$(5.2) \quad Hilb_{\mathbb{F}_p[[G]], d}(t) = \prod_{\lambda \in \text{Im}(D)} \left( \frac{1 - t^{p\lambda}}{1 - t^\lambda} \right)^{c^{\lambda, D}(G)}.$$

(b) *Let  $\tau \in (0, 1)$ , and define the function  $W : G \rightarrow [0, 1]$  by  $W(g) = \tau^{D(g)}$ . Then  $W$  is a valuation on  $G$  and  $Hilb_{\mathbb{F}_p[[G]], d}(\tau) = [G : \{1\}]_W$ , the  $W$ -index of the trivial subgroup.*

*Sketch of proof.* The idea of the proof of (a) is very simple. Consider the graded restricted Lie algebra  $L^D(G) = \oplus_{\lambda \in \text{Im}(D)} G^{\lambda, D} / G^{>\lambda, D}$  associated to the degree function  $D$  and the graded associative algebra  $gr_d \mathbb{F}_p[[G]] = \oplus_{\lambda \in \text{Im}(d)} \mathbb{F}_p[[G]]^{\lambda, d} / \mathbb{F}_p[[G]]^{>\lambda, d}$  associated to the degree function  $d$  (in fact,  $L^D(G)$  coincides with the Lie algebra  $L_W(G)$  defined in § 5.2, corresponding to the valuation  $W = \tau^D$  for any  $\tau \in (0, 1)$ ). It turns out that the restricted universal enveloping algebra  $\mathcal{U}(L^D(G))$  is isomorphic to  $gr_d \mathbb{F}_p[[G]]$  as a graded associative algebra. Hence  $Hilb_{\mathbb{F}_p[[G]], d}(t)$ , which by definition is the Hilbert series of  $gr_d \mathbb{F}_p[[G]]$ , must



equal the Hilbert series of  $\mathcal{U}(L^D(G))$ , which is equal to the right-hand side of (5.2) by the Poincare-Birkhoff-Witt theorem for restricted Lie algebras.

In the case when  $D$  is the standard degree function, the isomorphism  $gr_d \mathbb{F}_p[[G]] \cong \mathcal{U}(L^D(G))$  is known as Quillen's theorem and its detailed proof can be found, for instance, in [DDMS][Ch.11,12]. In [EJ2, Prop. 2.3], (a) is proved for the case of integer-valued degree functions  $D$ , but the same argument works for arbitrary  $D$ .

(b) It is clear that  $W$  is a valuation on  $G$ . Note that  $G^{\lambda,D} = G_{\tau^\lambda, W}$  and  $G^{>\lambda,D} = G_{<\tau^\lambda, W}$ , so  $c^{\lambda,D}(G) = c_{\tau^\lambda, W}(G/\{1\})$ . Therefore, if we set  $t = \tau$  in (5.2), the right-hand side becomes equal to  $[G : \{1\}]_W$  by definition.  $\square$

**Corollary 5.11.** *Let  $G$  be a GGS pro- $p$  group, and let  $W$  be a valuation on  $G$  such that  $\text{def}_W(G) > 0$ . Then  $[G : \{1\}]_W = \infty$ , and therefore by Proposition 5.9 (Continuity lemma), the set  $\{[G : U]_W\}$ , where  $U$  runs over open subgroups of  $G$ , is unbounded from above.*

*Proof.* Let  $(X, R, \widetilde{W})$  be a weighted presentation of  $G$  such that  $\text{def}_{\widetilde{W}}(X, R) > 0$  and  $\widetilde{W}$  induces  $W$ . By definition  $\widetilde{W} = \tau^D$  for some  $\tau \in (0, 1)$  and degree function  $D$  on  $F = F_{\widehat{p}}(X)$  with respect to  $X$ . Let  $d$  be a degree function on  $\mathbb{F}_p[[F]]$  corresponding to  $D$ . By Corollary 4.3, the series  $\text{Hilb}_{\mathbb{F}_p[[G]], d}(\tau)$  diverges, so the result follows from Theorem 5.10(b).  $\square$

Using Quillen's theorem, we can also interpret inequality in Theorem 5.7(b) (or rather a slightly stronger version of it) as yet another generalization of GS inequality.

First we restate Theorem 5.7(b) in terms of weight functions (formally the statement below is stronger, but it follows immediately from the proof):

**Theorem 5.12.** *Let  $G$  be a pro- $p$  group given by a presentation  $(X, R)$  and let  $W$  be a weight function on  $F_{\widehat{p}}(X)$  with respect to  $X$ . Let  $K$  be an open subgroup of  $G$ . Then  $K$  has a presentation  $(X', R')$ , with  $X' \subset F_{\widehat{p}}(X)$ , such that*

$$(1 - W(X') + W(R')) \leq (1 - W(X) + W(R)) \cdot [G : K]_W.$$

Suppose now that  $W = \tau^D$  for a degree function  $D$  and  $\tau \in (0, 1)$ . As in the proof of Theorem 5.10(b) we have  $c^{\lambda,D}(G/K) = c_{\tau^\lambda, W}(G/K)$ , so Theorem 5.7 can now be restated as a numerical inequality

$$(5.3) \quad 1 - H_{X', D}(\tau) + H_{R', D}(\tau) \leq (1 - H_{X, D}(\tau) + H_{R, D}(\tau)) \cdot \prod_{\lambda \in \text{Im}(D)} \left( \frac{1 - \tau^{\lambda p}}{1 - \tau^\lambda} \right)^{c^{\lambda, D}(G/K)}.$$

One can show (see [EJ2, Theorem 3.11(a)]) that if  $D$  is integer-valued (this time it is an essential assumption), then by dividing both sides of (5.3) by  $1 - \tau$  and replacing a real number  $\tau$  by the formal variable  $t$ , we get a valid inequality of power series (the proof of this result follows the same scheme as that of Theorem 5.7(b)):

**Theorem 5.13.** ([EJ2, Theorem 3.11(a)]) *Let  $G$  be a pro- $p$  group,  $(X, R)$  a presentation of  $G$  and  $D$  an integer-valued degree function on  $F = F_{\widehat{p}}(X)$  with respect to  $X$ . Let  $K$  be an open subgroup of  $G$ . Then there exists a presentation  $(X', R')$  of  $K$ , with  $X' \subset F_{\widehat{p}}(X)$ , such that the following inequality of power series holds:*

$$(5.4) \quad \frac{1 - H_{X', D}(t) + H_{R', D}(t)}{1 - t} \leq \frac{1 - H_{X, D}(t) + H_{R, D}(t)}{1 - t} \cdot \prod_{n \in \text{Im}(D)} \left( \frac{1 - t^{np}}{1 - t^n} \right)^{c^{n, D}(G/K)}.$$

Finally, assume that  $K$  is normal in  $G$ . Then applying Theorem 5.10(a) to the quotient group  $G/K$  and letting  $d$  be the degree function compatible with  $D$ , we can rewrite (5.4) as follows:

$$(5.5) \quad \frac{1 - H_{X',D}(t) + H_{R',D}(t)}{1 - t} \leq \frac{1 - H_{X,D}(t) + H_{R,D}(t)}{1 - t} \cdot \text{Hilb}_{\mathbb{F}_p[[G/K]],d}(t).$$

This inequality can be thought of as a finitary version of the generalized Golod-Shafarevich inequality (4.3); in fact, (4.3) can be deduced from (5.5), as explained in [EJ2] (see a remark after Theorem 3.11). Moreover, (5.5) remains true even without the assumption that  $K$  is normal in  $G$ , but  $\text{Hilb}_{\mathbb{F}_p[[G/K]],d}(t)$  will need to be defined differently.

**5.6. A proof without Hilbert series.** In conclusion of this long section we shall give a short alternative proof of the fact that GGS pro- $p$  groups are infinite, which does not use Hilbert series. The proof is based on the following lemma, which we shall also need later for other purposes.

**Lemma 5.14.** *Let  $G$  be a pro- $p$  group and  $(X, R, W)$  a weighted presentation of  $G$ , where  $W$  is finite. Then*

- (a)  $d(G) \geq W(X) - W(R)$ .
- (b) *Let  $\alpha > 0$ , and given a subset  $S$  of  $F(X)$ , let  $S_{\geq \alpha} = \{s \in S : W(s) \geq \alpha\}$ . Then  $d(G) \geq W(X_{\geq \alpha}) - W(R_{\geq \alpha})$ .*

*Proof.* Note that (a) follows from (b) by letting  $\alpha \rightarrow 0$ , so we shall only prove (b). Since  $G$  is pro- $p$ , there is a subset  $Y \subseteq X$  such that  $Y$  generates  $G$  and  $|Y| = d(G)$ . Then the presentation  $(X, R \cup Y)$  defines the trivial group. Hence  $R \cup Y$  generates  $F_{\hat{p}}(X)$  as a normal subgroup, and since  $F_{\hat{p}}(X)$  is pro- $p$ ,  $R \cup Y$  generates  $F_{\hat{p}}(X)$  as a pro- $p$  group. Since  $X$  is  $W$ -free, by Theorem 5.3(i)(iii), we have  $W(X_{\geq \alpha}) \leq W((R \cup Y)_{\geq \alpha})$ , whence  $W(X_{\geq \alpha}) \leq W(R_{\geq \alpha}) + W(Y_{\geq \alpha}) \leq W(R_{\geq \alpha}) + |Y_{\geq \alpha}| \leq W(R_{\geq \alpha}) + d(G)$ .  $\square$

Using Lemma 5.14 and Theorem 5.7(b), it is now very easy to show that GGS pro- $p$  groups are infinite. Indeed, suppose that  $G$  is a GGS pro- $p$  group, so that  $\text{def}_W(G) > 0$  for some  $W$ . Then  $\widetilde{W}(X) - \widetilde{W}(R) > 0$  for some weighted presentation  $(X, R, \widetilde{W})$  of  $G$ , so by Lemma 5.14(a),  $G$  is non-trivial and in particular has an open subgroup of index  $p$ , call it  $H$ . By Theorem 5.7,  $H$  is also GGS. We can then apply the same argument to  $H$  and repeat this process indefinitely, thus showing that  $G$  is infinite.

## 6. QUOTIENTS OF GENERALIZED GOLOD-SHAFAREVICH GROUPS

One of the reasons (generalized) Golod-Shafarevich groups are so useful is that they possess infinite quotients with many prescribed group-theoretic properties. Some results of this type are deep and require original arguments, but in many cases all one needs is the following obvious lemma:

**Lemma 6.1.** *Let  $G$  be a pro- $p$  group and  $W$  a valuation on  $G$ . If  $S$  is any subset of  $G$ , then  $\text{def}_W(G/\langle S \rangle^G) \geq \text{def}_W(G) - W(S)$ .*

As the first application of this lemma, we shall prove a simple but extremely useful result due to J. Wilson [Wi2].

**Theorem 6.2.** *Every GS (resp. GGS) abstract group has a torsion quotient which is also GS (resp. GGS).*

*Proof.* The argument is just a minor variation of the second proof of Theorem 2.5, but we shall state it using our newly developed language. Let  $\Gamma$  be a GGS abstract group (which can be assumed to be residually- $p$ ),  $G = \Gamma_{\widehat{p}}$  and  $W$  a valuation on  $G$  such that  $\text{def}_W(G) > 0$ . For each  $g \in \Gamma$  we can choose an integer  $k(g) \in \mathbb{N}$  such that if  $R = \{g^{p^{k(g)}} : g \in \Gamma\}$ , then  $W(R) < \text{def}_W(G)$ .

Let  $\Gamma' = \Gamma / \langle R \rangle^\Gamma$ . Then  $\Gamma'$  is torsion; on the other hand, the pro- $p$  completion of  $\Gamma'$  is isomorphic to  $G' = G / \langle R \rangle^G$  which is GGS by Lemma 6.1.

If  $\Gamma$  is GS, then we can assume that the initial  $W$  is induced by a uniform weight function, whence  $\Gamma'$  is also GS.  $\square$

The argument used to prove Theorem 6.2 has the following obvious generalization:

**Observation 6.3.** *Let  $(P)$  be some group-theoretic property such that*

- (i)  *$(P)$  is inherited by quotients,*
- (ii) *given an abstract group  $\Gamma$ , a valuation  $W$  on its pro- $p$  completion  $G = \Gamma_{\widehat{p}}$  and  $\varepsilon > 0$ , there exists a subset  $R_\varepsilon$  of  $\Gamma_{\widehat{p}}$  such that  $W(R_\varepsilon) < \varepsilon$  and the image of  $\Gamma$  in  $G / \langle R_\varepsilon \rangle^G$  has  $(P)$ .*

*Then any GGS group (resp. GS group) has a GGS quotient (resp. GS quotient) with  $(P)$ .*

Of course, in the proof of Theorem 6.2  $(P)$  was the property of being a  $p$ -torsion group. Below we state several other results which can be proved using Observation 6.3.

**Theorem 6.4.** ([EJ3, Theorem 1.2]) *Every GGS abstract group has a GGS quotient with property LERF.*

**Theorem 6.5** ([Er2]). *Every GGS abstract group has a GGS quotient whose FC-radical (the set of elements centralizing a finite index subgroup) is not virtually abelian.*

**Theorem 6.6** ([MyaOs]). *Every recursively presented GS abstract group has a GS quotient  $Q$  which is algorithmically finite (this means that no algorithm can produce an infinite set of pairwise distinct elements in  $Q$ ).*

For the motivation and proofs of these results the reader is referred to the respective papers (the first two theorems will be mentioned again in § 12). Here we remark that verification of condition (ii) in the proofs of these three theorems is not as straightforward as it was in Theorem 6.2. In particular, the set of additional relators  $R_\varepsilon$  cannot be described “right away”; instead it is constructed via certain iterated process.

We finish this section with two useful technical results, which are also based on Lemma 6.1.

**Lemma 6.7** (Tails Lemma). *Let  $G$  be a GGS pro- $p$  group. Let  $\Lambda$  and  $\Gamma$  be countable subgroups of  $G$  with  $\Lambda \subseteq \Gamma$  and  $\Lambda$  dense in  $\Gamma$ . Then  $G$  has a GGS quotient  $G'$  such that  $\Lambda$  and  $\Gamma$  have the same image in  $G'$ .*

*Proof.* Let  $W$  be a valuation on  $G$  such that  $\text{def}_W(G) > 0$ . Since  $\Lambda$  is countable and dense in  $\Gamma$  and  $W$  is continuous, for each  $g \in \Gamma$ , we can choose  $l_g \in \Lambda$  such that if  $R = \{l_g^{-1}g : g \in \Gamma\}$ , then  $W(R) < \text{def}_W(G)$ . It is clear that the group  $G / \langle R \rangle^G$  has the required property.  $\square$

**Remark:** The terminology ‘tails lemma’ is based on the following “visualization” of the above procedure: we represent each element  $g \in \Gamma$  as  $l_g \cdot (l_g^{-1}g)$  where  $l_g$  is a good approximation of  $g$  by an element of  $\Lambda$  and  $l_g^{-1}g$  is a tail of  $g$  (which is analogous to a tail of a power series). The desired quotient  $G'$  of  $G$  is constructed by cutting all the tails.

**Lemma 6.8.** *Let  $G$  be a GGS pro- $p$  group. Then some quotient  $Q$  of  $G$  has a weighted presentation  $(X, R, W)$  such that  $\text{def}_W(X, R) > 0$  and  $X$  is finite (in particular,  $Q$  is a finitely generated GGS pro- $p$  group).*

*Proof.* By definition,  $G$  has a weighted presentation  $(X_0, R_0, W)$  with  $\text{def}_W(X_0, R_0) > 0$ . Choose a finite subset  $X \subseteq X_0$  such that  $W(X \setminus X_0) < \text{def}_W(X_0, R_0)$ . Then it is easy to check that the group  $Q = G/\langle X \setminus X_0 \rangle^G$  has the required property.  $\square$

## 7. FREE SUBGROUPS IN GENERALIZED GOLOD-SHAFAREVICH PRO- $p$ GROUPS

As we saw in § 3, Golod-Shafarevich abstract groups may be torsion and therefore need not contain free subgroups. In this section we shall discuss a remarkable theorem of Zelmanov [Ze1] which asserts that Golod-Shafarevich pro- $p$  groups always contain non-abelian free pro- $p$  subgroups. In fact, we will show that the proof of this result easily extends to generalized Golod-Shafarevich pro- $p$  groups.

**Theorem 7.1** (Zelmanov). *Every generalized Golod-Shafarevich pro- $p$  group contains a non-abelian free pro- $p$  subgroup.*

It is not a big surprise that Golod-Shafarevich pro- $p$  groups contain non-abelian free abstract groups since the latter property seems to hold for all known examples of non-solvable pro- $p$  groups. However, containing a non-abelian free pro- $p$  subgroup is a really strong property for a pro- $p$  group. For instance, pro- $p$  groups linear over  $\mathbb{Z}_p$  or  $\mathbb{F}_p[[t]]$  cannot contain non-abelian free pro- $p$  subgroups [BL], and it is conjectured that the same is true for pro- $p$  groups linear over any pro- $p$  ring.

We start with some general observations. Let  $G$  be a finitely generated pro- $p$  group. There is a well-known technique for proving that  $G$  contains a non-abelian free abstract subgroup. Let  $F(2)$  be the free abstract group of rank 2, and suppose that  $F(2)$  does not embed into  $G$ . Then for any  $g, h \in G$  there exists a non-identity word  $w \in F(2)$  such that  $w(g, h) = 1$ . Thus

$$G \times G = \bigcup_{w \in F(2) \setminus \{1\}} (G \times G)_w \text{ where } (G \times G)_w = \{(g, h) \in G \times G : w(g, h) = 1\}. \quad (***)$$

It is easy to see that each subset  $(G \times G)_w$  is closed in  $G \times G$ , and since  $F(2)$  is countable, while  $G \times G$  is complete (as a metric space), Baire category theorem and (\*\*\*) imply that for some  $w \in F(2) \setminus \{1\}$ , the set  $(G \times G)_w$  is open in  $G \times G$ , so in particular, it contains a coset of some open subgroup. The latter has various strong consequences (e.g. it implies that the Lie algebra  $L(G)$  satisfies an identity), which in many cases contradicts some known property of  $G$ .

The following technical result is a (routine) generalization of [Ze1, Lemma 1] from GS to GGS groups and is proved similarly to Theorem 3.3.

**Lemma 7.2.** Let  $K$  be a countable field, and let  $A$  be a generalized Golod-Shafarevich complete filtered algebra, that is,  $A$  has a presentation  $\langle U | R \rangle$  s.t.  $1 - H_{U,d}(\tau) + H_{R,d}(\tau) < 0$  for some  $\tau \in (0, 1)$  and some degree function  $d$  on  $K\langle\langle U \rangle\rangle$ . Let  $A_{abs}$  be the (abstract) subalgebra of  $A$  (without 1) generated by  $U$ . Then there exist an epimorphism  $\pi : A \rightarrow A'$ , with  $A'$  also GGS, and a function  $\nu : \mathbb{N} \rightarrow \mathbb{N}$  such that for any  $n \in \mathbb{N}$ , any  $n$  elements of  $\pi(A_{abs}^{\nu(n)})$  generate a nilpotent subalgebra.

**7.1. Sketch of proof of Theorem 7.1.** The proof of Theorem 7.1 roughly consists of two parts – reducing the problem to certain question about associative algebras (Proposition on p.227 in [Ze1]) and then proving the proposition. This proposition is actually the deeper part of Zelmanov's theorem, but since it is not directly related to GS groups or algebras

and its proof is somewhat technical, we have chosen to skip this part in our survey and concentrate on the first part of the proof. This will be sufficient to make it clear that the proof applies to GGS groups and not just GS groups as stated in [Ze1].

Let  $G$  be a GGS pro- $p$  group and assume that it does not contain a free pro- $p$  group of rank 2, denoted by  $F_2$ . As above, denote by  $F(2)$  the free abstract group of rank 2. Let  $D$  denote the standard degree function defined in § 3.1 (not the degree function which makes  $G$  a GGS group!) In this proof we shall use the definition of  $D$  in terms of the Zassenhaus filtration (see Proposition 3.2).

*Step 1:* Since  $F_2$  is uncountable, the above approach for proving the existence of a non-abelian free abstract subgroup cannot be applied directly. However we can still say that for any  $g, h \in G$  there exists a non-identity element  $w \in F_2$  (this time  $w$  may be an infinite word) such that  $w(g, h) = 1$ . Equivalently, for any  $g, h \in G$  there is a non-identity word  $w \in F(2)$  such that  $w(g, h) = w'(g, h)$  for some  $w' \in F_2$  with  $D(w') > D(w)$ .

*Step 2:* The same application of the Baire category theorem as above implies that there is  $w \in F(2)$ , elements  $g_0, h_0 \in G$  and an open subgroup  $K$  of  $G$  such that for any  $g, h \in K$  we have  $w(g_0g, h_0h) = w'(g_0g, h_0h)$  for some  $w' \in F_2$  (depending on  $g$  and  $h$ ) with  $D(w') > D(w)$ .

*Step 3:* Since Steps 1 and 2 can be applied to any open subgroup of  $G$ , we can assume in Step 2 that  $W(g_0)$  and  $W(h_0)$  are as small as we want, where  $W$  is a valuation on  $G$  s.t.  $\text{def}_W(G) > 0$ . In particular, by Lemma 6.1, we can ensure that the group  $G' = G/\langle g_0, h_0 \rangle^G$  is also GGS. The image of  $K$  in  $G'$ , call it  $K'$ , is also GGS by Theorem 4.4. Thus, replacing  $G$  by  $K'$  (and changing the notations), we can assume that

for any  $g, h \in G$  there is  $w' \in F_2$ , with  $D(w') > D(w)$ , s.t.  $w(g, h) = w'(g, h)$  (\*\*\*)

*Step 4:* If  $k = D(w)$ , then we can multiply  $w$  by any element of  $D_{k+1}F_2$  without affecting (\*\*\*). In this way we can assume that  $w$  is as a product of elements  $c^{p^e}$  where  $c$  is a left-normed commutator of degree  $k/p^e$ . Next note that if some  $w$  satisfies (\*\*\*) and  $v \in F_2$  is such that  $D([w, v]) = D(v) + D(w)$ , then (\*\*\*) still holds with  $w$  replaced by  $[w, v]$ . After applying this operation several times, we can assume that  $w = c_1 \dots c_t$  where each  $c_i$  is a left-normed commutator of length  $D(w)$ .

*Step 5:* Now let  $L_2$  be the free  $\mathbb{F}_p$ -Lie algebra of rank 2 and  $\text{Lie}(w) = \text{Lie}(c_1) + \dots + \text{Lie}(c_t) \in L_2$  where  $\text{Lie}(c_i)$  is the Lie commutator corresponding to  $c_i$ . It is not difficult to see that condition (\*\*\*) can now be restated as the following equality in  $\mathbb{F}_p[[G]]$ : for any  $g, h \in G$  we have

$$\text{Lie}(w)(g-1, h-1) = O_{k+1}(g-1, h-1) \quad (!!!)$$

where  $\text{Lie}(w)(g-1, h-1)$  is simply the element  $\text{Lie}(w)$  evaluated at the pair  $(g-1, h-1)$  and, for a finite set of elements  $a_1, \dots, a_s$ ,  $O_{k+1}(a_1, \dots, a_s)$  is a (possibly infinite) but converging sum of products of  $a_1, \dots, a_s$ , with each product of length  $\geq k+1$  (recall that  $k = D(w)$ ).

Thinking of  $\text{Lie}(w)$  as an element of the free associative  $\mathbb{F}_p$ -algebra of rank 2, we can consider the full linearization of  $\text{Lie}(w)$ , call it  $f$ . Then  $f$  is a polynomial of degree  $k$  in  $k$  variables, and it is easy to check that for any  $g_1, \dots, g_k \in G$  we have  $f(g_1-1, \dots, g_k-1) = O_{k+1}(g_1-1, \dots, g_k-1)$ .

*Step 6:* Let  $(X, R)$  be a presentation for  $G$  satisfying the GGS condition. Then the algebra  $A = \mathbb{F}_p[[G]]$  is GGS (with presentation  $(U, R_{\text{alg}})$  where  $U = \{x-1 : x \in X\}$  and  $R_{\text{alg}} = \{r-1 : r \in R\}$ ). Let us apply Lemma 7.2 to  $A$ , and let  $\pi : A \rightarrow A'$  be as in the conclusion of that lemma. Note that we do not know whether the group  $G' = \pi(G)$

is GGS, but the fact that  $A'$  is a GGS algebra will be sufficient. Let  $B = \pi(A_{abs})$  (in the notations of Lemma 7.2), and let  $\Gamma$  be the abstract subgroup of  $G'$  generated by (the image of)  $X$ . Note that  $\Gamma \subset 1 + B = \{1 + b : b \in B\}$ , and moreover  $D_m \Gamma \subset 1 + B^m$  for all  $m \in \mathbb{N}$ . Therefore, we have the following (with part (ii) being a consequence of Step 5).

- (i) There exists a function  $\nu : \mathbb{N} \rightarrow \mathbb{N}$  such that for any  $n \in \mathbb{N}$ , any  $n$  elements of  $B^{\nu(n)}$  generate a nilpotent subalgebra.
- (ii) There exists a multilinear polynomial  $f$  of degree  $k$  such that for any  $g_1, \dots, g_k \in D_{\nu(k)} \Gamma$ , the element  $f(g_1 - 1, \dots, g_k - 1)$  is equal to a finite sum of products of  $g_1 - 1, \dots, g_k - 1$ , with each product of length at least  $k + 1$  (the sum must be finite by (i)).

As proved in [Ze1, Proposition, p.227], if  $B$  is a finitely generated  $\mathbb{F}_p$ -algebra and  $\Gamma$  is a subgroup of  $1 + B$  such that (i) and (ii) above hold, then  $B$  is nilpotent (and hence finite-dimensional). This yields the desired contradiction since in our setting  $\mathbb{F}_p + B$  is a dense subalgebra of  $A' = \pi(A)$ , which is GGS and therefore infinite-dimensional. This concludes our sketch of proof of Theorem 7.1.

As we already mentioned, the characteristic zero counterpart of Theorem 7.1 was established by Kassabov in [Ka], who showed that every Golod-Shafarevich pronipotent group contains a non-abelian free pronipotent subgroup.

## 8. SUBGROUP GROWTH OF GENERALIZED GOLOD-SHAFAREVICH GROUPS

In this section we shall discuss various results about subgroup growth of GGS groups. We shall pay particular attention to this topic in this paper not only because of its intrinsic importance, but also because there are two classes which contain many Golod-Shafarevich groups – Galois groups  $G_{K,p,S}$  and fundamental groups of hyperbolic 3-manifolds – where subgroup growth has a direct number-theoretic (resp. topological) interpretation.

We shall restrict our discussion to GGS *pro-p* groups. Since the majority of the results we state deal with lower bounds on subgroup growth and the subgroup growth of an abstract group  $\Gamma$  is bounded below by the subgroup growth of its *pro-p* completion, these results yield the corresponding lower bounds for the subgroup growth of GGS abstract groups.

**8.1. Some generalities on subgroup growth.** If  $G$  is a finitely generated *pro-p* group, denote by  $a_m(G)$  the number of open subgroup of  $G$  of index  $m$  (note that  $a_m(G) = 0$  unless  $m$  is a power of  $p$ ). The asymptotic behaviour of the sequence  $\{a_{p^k}(G)\}_{k \geq 1}$  is closely related to that of the sequence  $\{r_k(G)\}$  defined below, the latter being much easier to control.

**Lemma 8.1.** *Let  $G$  be a finitely generated *pro-p* group. For each  $k \in \mathbb{N}$  let*

$$r_k(G) = \max\{d(U) : U \text{ is an open subgroup of } G \text{ of index } p^k\}.$$

*Then*

- (i)  $a_{p^k}(G) \geq p^{r_{k-1}(G)} - 1$ ;
- (ii)  $a_{p^k}(G) \leq a_{p^{k-1}}(G) \cdot (p^{r_{k-1}(G)} - 1)$ , and therefore  $a_{p^k}(G) \leq p^{\sum_{i=0}^{k-1} r_i(G)}$ .

*Proof.* (i) Let  $U$  be an open subgroup of index  $p^{k-1}$  with  $d(U) = r_{k-1}(G)$ . The quotient  $U/[U, U]U^p$  is a vector space over  $\mathbb{F}_p$  of dimension  $d(U)$  and therefore has  $p^{d(U)} - 1$  subspaces of codimension 1. These subspaces correspond to subgroups of index  $p$  in  $U$ , and each of those subgroups has index  $p^k$  in  $G$ .

(ii) follows from the same argument and the fact that each subgroup of index  $p^k$  in a pro- $p$  group is contained in a subgroup of index  $p^{k-1}$ .  $\square$

By the Schreier index formula, the sequence  $\{r_k(G)\}$  grows at most linearly in  $p^k$ . Hence, Lemma 8.1 shows that the subgroup growth of any finitely generated pro- $p$  group  $G$  is at most exponential, and the subgroup growth is exponential if and only if  $\inf_k r_k(G)/p^k > 0$ . In fact, there is an even more elegant characterization of exponential subgroup growth due to Lackenby [La3, Theorem 8.1].

**Definition.**

- (a) Let  $G$  be a finitely generated pro- $p$  group and  $\{G_n\}$  a strictly descending chain of open normal subgroups of  $G$ . We will say that  $\{G_n\}$  is an *LRG chain* (where LRG stands for linear rank growth) if  $\inf_n (d(G_n) - 1)/[G : G_n] > 0$ .
- (b) Let  $\Gamma$  be a finitely generated abstract group and  $\{\Gamma_n\}$  a strictly descending chain of normal subgroups of  $\Gamma$  of  $p$ -power index. We will say that  $\{\Gamma_n\}$  is an *LRG  $p$ -chain* if  $\inf_n (d_p(\Gamma_n) - 1)/[\Gamma : \Gamma_n] > 0$ . (Recall that  $d_p(\Lambda) = d(\Lambda/[\Lambda, \Lambda]\Lambda^p) = d(\Lambda_{\hat{p}})$  for an abstract group  $\Lambda$ .)

**Theorem 8.2** (Lackenby). *Let  $G$  be a pro- $p$  group. The following are equivalent.*

- (i)  $G$  has exponential subgroup growth
- (ii) There is  $c > 0$  such that  $r_k(G) > cp^k$  for all  $k$ .
- (iii) There is  $c > 0$  such that  $r_k(G) > cp^k$  for infinitely many  $k$ .
- (iv)  $G$  has an LRG chain.

*Proof.* The equivalence of (i) and (ii) has already been discussed. The implication “(iv) $\Rightarrow$ (iii)” is clear. The implication “(iii) $\Rightarrow$ (ii)” follows from the fact that the quantity  $(d(U) - 1)/[G : U]$  does not increase if  $U$  is replaced by its open subgroup, and hence the sequence  $\frac{r_k(G)-1}{p^k}$  is non-increasing. Finally, the implication “(ii) $\Rightarrow$ (iv)” is established by a Cantor diagonal argument (see [La3, Theorem 8.1] for details).  $\square$

**8.2. Subgroup growth of GGS groups.** As we will see later in the paper, many naturally occurring GS groups have LRG chains and therefore have exponential subgroup growth. It is very likely that there exist GS groups with subexponential subgroup growth, but to the best of our knowledge, this problem is still open. The best currently known lower bound on the subgroup growth of GS groups (which also applies to GGS groups) is due to Jaikin-Zapirain [EJ2, Appendix B] and is best stated in terms of the sequence  $\{r_k(G)\}$ .

**Theorem 8.3** (Jaikin-Zapirain). *Let  $G$  be a finitely generalized Golod-Shafarevich pro- $p$  group. Then there exists a constant  $\beta = \beta(G) > 0$  such that  $r_k(G) > p^{k\beta}$  for infinitely many  $k$ .*

*Proof.* Let  $(X, R)$  be a presentation of  $G$  and  $D$  an integer-valued degree function on  $F = F_{\hat{p}}(X)$  with respect to  $X$  such that  $H_{X,D}(\tau) - H_{R,D}(\tau) - 1 > 0$  for some  $\tau \in (0, 1)$ . Let  $\pi : F \rightarrow G$  be the natural projection, and for each  $n \in \mathbb{N}$  let

$$G_n = \{g \in G : g = \pi(f) \text{ for some } f \in F \text{ with } D(f) \geq n\} \text{ and } c_n = \log_p[G_n : G_{n+1}]$$

(Thus,  $G_n = G^{n,D}$  and  $c_n = c^{n,D}(G)$  in the notations of § 5.5).

By Theorem 5.13, there exists a presentation  $(X_n, R_n)$  of  $G_n$ , with  $X_n \subset F_{\hat{p}}(X)$ , such that  $H_{X_n,D}(\tau) - H_{R_n,D}(\tau) - 1 \geq (H_{X,D}(\tau) - H_{R,D}(\tau) - 1) \prod_{i=0}^{n-1} \left( \frac{1-\tau^{pi}}{1-\tau^i} \right)^{c_i}$ , whence

$\log_p(H_{X_n,D}(\tau) - H_{R_n,D}(\tau) - 1) \geq \log_p(H_{X,D}(\tau) - H_{R,D}(\tau) - 1) + c_{n-1} \log_p(1 + \tau^{n-1})$   
 By Lemma 5.14(a),  $d(G_n) \geq H_{X_n,D}(\tau) - H_{R_n,D}(\tau)$ , whence  
 $\log_p d(G_n) \geq c_{n-1} \log_p(1 + \tau^{n-1}) + \log_p(H_{X,D}(\tau) - H_{R,D}(\tau) - 1) \geq \frac{1}{2 \log p} c_{n-1} \tau^{n-1} - E$ ,  
 where  $E$  is a constant independent of  $n$ .

Now take  $0 < \tau_1 < \tau$  such that  $H_{X,D}(\tau_1) - H_{R,D}(\tau_1) - 1 > 0$ . By Theorem 5.10, the infinite product  $\prod_{i=0}^{\infty} \left( \frac{1 - \tau_1^{p^i}}{1 - \tau_1} \right)^{c_i}$  diverges, whence the series  $\sum_{i=0}^{\infty} c_i \tau_1^i$  also diverges. Thus if  $c = \limsup \sqrt[i]{c_i}$ , then  $c\tau_1 \geq 1$ , so  $c\tau > 1$ . Now choose any  $\alpha \in (1, c\tau)$ . Then  $\limsup \frac{c_{n-1} \tau^{n-1}}{\alpha^n} = \infty$ , whence

$$\log_p d(G_n) \geq \alpha^n \text{ for infinitely many } n. \quad (***)$$

On the other hand, the trivial upper bound  $c_n \leq |X|^n$  implies that  $\log_p[G : G_n] = \sum_{i=0}^{n-1} c_i < |X|^n$ . Thus, if we let  $k = \log_p[G : G_n]$  where  $n$  satisfies  $(***)$ , then

$$\log_p r_k(G) \geq \log_p d(G_n) \geq |X|^n \frac{\log \alpha}{\log |X|} > k^\beta \text{ for } \beta = \frac{\log \alpha}{\log |X|}.$$

□

**8.3. Subgroup growth of groups of non-negative deficiency.** In the proof of Theorem 8.3 we used Theorem 5.13 as a numerical inequality. The fact that it holds as inequality of power series also has a very interesting consequence.

**Notation.** Given positive integers  $n, m$  and  $p$ , define  $\binom{n}{m}_p$  to be the coefficient of  $t^m$  in the polynomial  $(1 + t + \dots + t^{p-1})^n$ . Thus,  $\binom{n}{m}_2 = \binom{n}{m}$  is the usual binomial coefficient.

**Proposition 8.4.** *Let  $G$  be a finitely presented pro- $p$  group and  $K$  an open subgroup of  $G$  containing  $\Phi(G) = [G, G]G^p$ , so that  $G/K \cong (\mathbb{Z}/p\mathbb{Z})^n$  for some  $n$ . Then for any integer  $0 \leq l < (p-1)n$  the following inequality holds:*

$$d(K) \geq d(G) \sum_{i=0}^l \binom{n}{i}_p - r(G) \sum_{i=0}^{l-1} \binom{n}{i}_p - \sum_{i=0}^{l+1} \binom{n}{i}_p.$$

*Proof.* Let  $(X, R)$  be a minimal presentation of  $G$  (so that  $|X| = d(G)$  and  $|R| = r(G)$ ). We shall apply Theorem 5.13 to this presentation and the standard degree function  $D$  on  $F_{\hat{p}}(X)$ . Since (in the notations of § 5.5)  $G^{2,D} = [G, G]G^p$ , we have  $G^{2,D} \subseteq K$ , so  $c^{1,D}(G/K) = n$  and  $c^{i,D}(G/K) = 0$  for  $i > 1$ . Thus, by Theorem 5.13,  $K$  has a presentation  $(X', R')$  such that

$$\frac{H_{X',D}(t) - H_{R',D}(t) - 1}{1 - t} \geq \frac{d(G)t - H_{R,D}(t) - 1}{1 - t} (1 + t + \dots + t^{p-1})^n. \quad (***)$$

Let us write  $H_{X',D}(t) = \sum d_i(K)t^i$ ,  $H_{R',D}(t) = \sum r_i(K)t^i$  and  $H_{R,D}(t) = \sum r_i t^i$ . Note that  $r_1 = 0$  by Lemma 3.5(i) since the presentation  $(X, R)$  is minimal and  $\sum_{i \geq 2} r_i = r(G)$ .

Computing the coefficient of  $t^{l+1}$  on both sides of  $(***)$ , we obtain

$$\sum_{i \leq l+1} d_i(K) - \sum_{i \leq l+1} r_i(K) - 1 \geq d(G) \sum_{i=0}^l \binom{n}{i}_p - r(G) \sum_{i=0}^{l-1} \binom{n}{i}_p - \sum_{i=0}^{l+1} \binom{n}{i}_p.$$

To finish the proof it suffices to show that  $d(K) \geq \sum_{i \leq l+1} d_i(K) - \sum_{i \leq l+1} r_i(K)$ . To prove the latter we take  $\tau \in (0, 1)$  and apply Lemma 5.14(b) to the weighted presentation



$(X, R, W)$  where  $W$  is the uniform weight function on  $F_{\widehat{p}}(X)$  with respect to  $X$  such that  $W(x) = \tau$  for all  $x \in X$ . The desired inequality follows by letting  $\tau$  tend to 1.  $\square$

The inequality in Proposition 8.4 was proved by Lackenby [La2, Theorem 1.6] for  $p = 2$ , and in a slightly weaker form for arbitrary  $p$ . Lackenby's proof was based on clever topological arguments, and it is remarkable that the finitary Golod-Shafarevich inequality (5.4) yields the same result for  $p = 2$ .<sup>4</sup>

There are many different ways in which Proposition 8.4 may be used. A very important application, discovered by Lackenby for  $p = 2$ , deals with the case when  $r(G) \leq d(G)$  and  $K = \Phi(G)$ .

**Corollary 8.5.** *Let  $G$  be a finitely presented pro- $p$  group with  $r(G) \leq d(G)$  and  $d(G) \geq 36p^2$ . Then  $d(\Phi(G)) \geq \frac{1}{6}\sqrt{d(G)}p^{d(G)-1}$ .*

*Proof.* Applying Proposition 8.4 with  $K = \Phi(G)$  (so that  $n = d(G)$ ) and  $l = [(p-1)n/2]$ , we get  $d(\Phi(G)) \geq n \cdot \binom{n}{l}_p - \sum_{i=0}^{l+1} \binom{n}{i}_p$ . Note that  $\sum_{i=0}^{l+1} \binom{n}{i}_p \leq \sum_{i=0}^{n(p-1)} \binom{n}{i}_p = p^n$ . We claim that

$$(8.1) \quad \binom{n}{l}_p \geq \frac{1}{3\sqrt{n}}p^{n-1}.$$

If  $p = 2$ , this is an easy consequence of Stirling formula, and for  $p > 2$  this could be proved, for instance, as follows. Consider independent identically distributed random variables  $X_1, \dots, X_n$  which take on integer values  $0, 1, \dots, p-1$  with equal probabilities  $1/p$ , and let  $S_n = X_1 + \dots + X_n$ . Then  $\binom{n}{l}_p = p^n \cdot \text{Prob}(S_n = l)$ , and note that  $l = (p-1)n/2$  is the expected value of  $S_n$ .

Each  $X_i$  has variance  $\sigma = \sqrt{(p-1)(2p-1)/6}$ , so by the central limit theorem we have

$$\text{Prob}\left(|S_n - l| < \frac{1}{2}\sigma\sqrt{n}\right) \geq \frac{1}{\sqrt{2\pi}} \int_{-1/2}^{1/2} e^{-x^2/2} \geq \frac{e^{-1/8}}{\sqrt{2\pi}}.$$

On the other hand, an easy induction on  $n$  shows that  $\binom{n}{i}_p$  is increasing as a function of  $i$  for  $0 \leq i \leq l$  and (by symmetry) decreasing for  $l \leq i \leq 2l = (p-1)n$ . Hence

$$\text{Prob}(S_n = l) \geq \frac{e^{-1/8}}{\sqrt{2\pi}(1 + \sigma\sqrt{n})} \geq \frac{1}{3 + 2p\sqrt{n}} \geq \frac{1}{3p\sqrt{n}},$$

which yields (8.1). Hence

$$d(\Phi(G)) \geq \frac{(\sqrt{n} - 3p)p^{n-1}}{3} \geq \frac{1}{6}\sqrt{np}p^{n-1}.$$

$\square$

**Remark:** The inequality  $d(G) \geq 36p^2$  can be significantly weakened using a more careful estimate. In particular, if  $p = 2$ , it is enough to assume that  $d(G) \geq 4$ , as proved in [La2].

Note that if  $G$  is a free pro- $p$  group, then  $d(\Phi(G)) - 1 = (d(G) - 1)p^{d(G)}$ , so the ratio  $d(\Phi(G))/d(G)$  guaranteed by Corollary 8.5 is not far from the best possible. In particular, it yields a very good bound on the subgroup growth of groups  $G$  for which  $d(U) \geq r(U)$  for every open subgroup  $U$  and  $d(U) > p^3$  for some open subgroup  $U$ , and this class includes pro- $p$  completions of all hyperbolic 3-manifold groups (see § 11 for details).

<sup>4</sup>The above proof of Proposition 8.4 was outlined by Kassabov during an informal discussion at the workshop ‘‘Lie Groups, Representations and Discrete Mathematics’’ at IAS, Princeton in February 2006, before Theorem 5.13 was formally proved in [EJ2].

9. GROUPS OF POSITIVE POWER  $p$ -DEFICIENCY

In this short section we will briefly discuss groups of positive power  $p$ -deficiency which are close relatives of Golod-Shafarevich groups. These groups provide very simple counterexamples to the general Burnside problem, and it is quite amazing that they had been discovered just two years ago by Schlage-Puchta [SP] and in a slightly different form by Osin [Os2].

**Definition.** Let  $p$  be a fixed prime number.

- (i) Let  $F$  be a free abstract group. Given  $f \in F$ , we let  $\nu_p(f)$  be the largest non-negative integer such that  $f = h^{p^{\nu_p(f)}}$  for some  $h \in F$ .
- (ii) If  $(X, R)$  is an abstract presentation, with  $|X| < \infty$ , we define its *power  $p$ -deficiency*, denoted by  $def_p(X, R)$  by

$$def_p(X, R) = |X| - 1 - \sum_{r \in R} p^{-\nu_p(r)}.$$

- (iii) If  $G$  is an abstract group, its power  $p$ -deficiency  $def_p(G)$  is defined to be the supremum of the set  $\{def_p(X, R)\}$  where  $(X, R)$  runs over all presentations of  $G$ .

The key property of power  $p$ -deficiency is the inequality in part (b) of the following theorem which is analogous to the corresponding inequalities for usual deficiency (Theorem 5.6(b)) and weighted deficiency (Theorem 5.7(b)).

Recall that for a finitely generated abstract group  $G$  we set  $d_p(G) = d(G/[G, G]G^p)$  and that  $d_p(G) = d(G_{\hat{p}})$  where  $G_{\hat{p}}$  is the pro- $p$  completion of  $G$ .

**Theorem 9.1.** *Let  $G$  be a finitely generated abstract group. The following hold:*

- (i)  $d_p(G) \geq def_p(G) + 1$
- (ii) *Let  $H$  be a subnormal subgroup of  $G$  of  $p$ -power index. Then*

$$def_p(H) \geq def_p(G)[G : H]$$

and therefore

$$\frac{d_p(H) - 1}{[G : H]} \geq def_p(G). \quad (***)$$

*Proof.* Relations which are  $p$ -powers do not affect  $d_p(G)$ , so (i) follows from the fact that if  $G = \langle X | R \rangle$ , then  $d_p(G) \geq |X| - |R|$ . To establish (ii), by multiplicativity of index it is enough to consider the case when  $H$  is a normal subgroup of index  $p$ . This case is covered by [SP, Theorem 2], and the proof of this result is quite short unlike Theorem 5.7(b).  $\square$

An immediate consequence of Theorem 9.1 is that groups of positive  $p$ -deficiency are infinite; in fact they must have infinite pro- $p$  completion. Indeed, suppose that  $def_p(G) > 0$ , but the pro- $p$  completion of  $G$  is finite. Then there exists a minimal subnormal subgroup of  $p$ -power index, call it  $H$ ; then  $d_p(H) = 0$  which contradicts (\*\*\*). On the other hand, it is clear that there exist torsion groups of positive power  $p$ -deficiency, so in this way one obtains a short elementary self-contained proof of the existence of infinite finitely generated torsion groups.

As suggested by the titles of both [SP] and [Os2], the original motivation for introducing groups of positive power  $p$ -deficiency was to find examples of torsion finitely generated groups with positive rank gradient.

**Definition.**

- (i) Let  $G$  be a finitely generated abstract or pro- $p$  group. The *rank gradient* of  $G$  is defined as  $RG(G) = \inf_H \frac{d(H)-1}{[G:H]}$  where  $H$  runs over all finite index subgroups of  $G$ .
- (ii) Let  $G$  be a finitely generated abstract group. The  *$p$ -gradient* (also known as mod  $p$  homology gradient)  $RG_p(G)$  is defined as  $RG_p(G) = \inf_H \frac{d_p(H)-1}{[G:H]}$  where  $H$  runs over all finite index subnormal subgroups of  $p$ -power index in  $G$ .

**Remark:** Since subnormal subgroups of  $p$ -power index are precisely the subgroups open in the pro- $p$  topology, it is easy to show that if  $G$  is an abstract group, then  $RG_p(G) = RG(G_{\widehat{p}})$ , that is, the  $p$ -gradient of  $G$  is equal to the rank gradient of its pro- $p$  completion. This also implies that  $RG_p(G) = RG_p(G')$  if  $G'$  is the image of  $G$  in its pro- $p$  completion.

Theorem 9.1(ii) asserts that groups of positive power  $p$ -deficiency have positive  $p$ -gradient. Combining this result with theorems from [La3] and [AJN], one obtains the following corollary:

**Corollary 9.2** ([SP]). *Let  $G$  be an abstract group of positive power  $p$ -deficiency. The following hold:*

- (a)  $G$  is non-amenable. Moreover, the image of  $G$  in its pro- $p$  completion is non-amenable.
- (b) If  $G$  is finitely presented, then  $G$  is large, that is, some finite index subgroup of  $G$  maps onto a non-abelian free group.

*Proof.* (a) Note that  $G$  has a  $p$ -torsion quotient  $Q$  with  $def_p(Q) > 0$  (this is proved in the same way as the analogous result for Golod-Shafarevich groups – see Theorem 6.2). Let  $Q'$  be the image of  $Q$  in its pro- $p$  completion. We claim that

$$RG(Q') \geq RG_p(Q') = RQ_p(Q) \geq def_p(Q) > 0.$$

Indeed,  $RG(Q') \geq RG_p(Q')$  since  $Q'$  is  $p$ -torsion, so every finite index normal subgroup of  $Q'$  is of  $p$ -power index, and therefore every finite index subgroup of  $Q'$  is subnormal of  $p$ -power index. The equality  $RG_p(Q') = RQ_p(Q)$  holds by the remark following the definition of  $p$ -gradient and  $RQ_p(Q) \geq def_p(Q)$  by Theorem 9.1(ii).

Thus,  $Q'$  is a residually finite group with positive rank gradient and therefore cannot be amenable as proved in [AJN]. If  $G'$  is the image of  $G$  in its pro- $p$  completion, then  $Q'$  is a quotient of  $G'$ , so  $G'$  is also non-amenable.

(b) follows from a theorem of Lackenby [La4, Theorem 1.18], which asserts that a finitely presented group with positive  $p$ -gradient is large.  $\square$

**Corollary 9.3.** *There exist residually finite torsion non-amenable groups.*

*Proof.* If  $G$  is any torsion group of positive power  $p$ -deficiency, the image of  $G$  in its pro- $p$  completion has the desired property by Corollary 9.2.  $\square$

Another construction of residually finite torsion non-amenable groups will be given in § 12. Recall that the first examples of torsion non-amenable groups (which were not residually finite) were Tarski monsters constructed by Ol'shanskii [Ol1] (with their non-amenability proved in [Ol2]).

We finish this section with a brief comparison of GS groups and groups of positive power  $p$ -deficiency. As suggested by the definitions, the latter class should be smaller than that of GS groups since in the definition of power  $p$ -deficiency only relators of the form  $f^{p^k}$ , with  $k$  large, are counted with small weight, while in the definition of GS groups the set of relators counted with small weight also includes long commutators (in addition to relators

of the form  $f^{p^k}$ , with  $k$  large). This heuristics suggests that groups of positive power  $p$ -deficiency may always be Golod-Shafarevich, and this turns out to be almost true:

**Theorem 9.4.** [BuTh] *Let  $G$  be an abstract or a pro- $p$  group of positive power  $p$ -deficiency. Then  $G$  has a finite index Golod-Shafarevich subgroup. Moreover, if  $p \geq 7$ , then  $G$  itself must be Golod-Shafarevich.*

While being a smaller class than GS groups, groups of positive power  $p$ -deficiency satisfy much stronger “largeness” properties, as we saw in this section. It would be interesting to find some intermediate condition on groups which is significantly weaker than having positive power  $p$ -deficiency, but has stronger consequences than being Golod-Shafarevich.

## 10. APPLICATIONS IN NUMBER THEORY

**10.1. Class field tower problem.** Let us begin with the following natural number-theoretic question:

**Question 10.1.** *Let  $K$  be a number field. Does there exist a finite extension  $L/K$  such that the ring of integers  $O_L$  of  $L$  is a PID?*

If  $K$  is a number field, the extent to which  $O_K$  fails to be a PID is measured by the ideal class group  $Cl(K)$ . In particular,  $O_K$  is a PID if and only if  $Cl(K)$  is trivial. The group  $Cl(K)$  is always finite and by class field theory,  $Cl(K)$  is isomorphic to the Galois group  $Gal(\mathbb{H}(K)/K)$  where  $\mathbb{H}(K)$  is the maximal abelian unramified extension of  $K$ , called the *Hilbert class field* of  $K$ .

**Definition.** Let  $K$  be a number field. The *class field tower*

$$K = \mathbb{H}^0(K) \subseteq \mathbb{H}^1(K) \subseteq \mathbb{H}^2(K) \subseteq \dots$$

of  $K$  is defined by  $\mathbb{H}^i(K) = \mathbb{H}(\mathbb{H}^{i-1}(K))$  for  $i \geq 1$ .

The class field tower of  $K$  is called finite if it stabilizes at some step and infinite otherwise.

**Lemma 10.2.** *Let  $K$  be a number field. Then the class field tower of  $K$  is finite if and only if there is a finite extension  $L/K$  with  $Cl(L) = \{1\}$ .*

*Proof.* Let  $\{K_i = \mathbb{H}^i(K)\}$  be the class field tower of  $K$ .

“ $\Rightarrow$ ” By assumption  $K_n = K_{n+1}$  for some  $n$ , so  $Cl(K_n) = \{1\}$  whence we can take  $L = K_n$ .

“ $\Leftarrow$ ” Consider the tower of fields  $L = LK_0 \subseteq LK_1 \subseteq \dots$ . Since for each  $i$  the extension  $K_{i+1}/K_i$  is abelian and unramified, the same is true for the extension  $LK_{i+1}/LK_i$ . In particular,  $LK_1$  is an abelian unramified extension of  $L$ . But  $Cl(L) = \{1\}$ , so  $L$  does not have such non-trivial extensions, which implies that  $LK_1 = L$ . Repeating this argument inductively, we conclude that  $LK_i = L$  for each  $i$ , so each  $K_i$  is contained in  $L$ , whence the tower  $\{K_i\}$  must be finite.  $\square$

Thus, Question 10.1 is equivalent to the so called *class field tower problem*.

**Problem** (Class field tower problem). *Is it true that for any number field  $K$  the class field tower of  $K$  is finite?*

Computing the class field of a given number field is a rather difficult task. It is a little bit easier to control the  *$p$ -class field*, where  $p$  is a fixed prime.

**Definition.** Let  $p$  be a prime and  $K$  a number field.

- (a) The *p*-class field of  $K$ , denoted by  $\mathbb{H}_p(K)$ , is the maximal unramified Galois extension of  $K$  such the Galois group  $\text{Gal}(\mathbb{H}_p(K)/K)$  is an elementary abelian  $p$ -group.
- (b) The *p*-class field tower of  $K$  is the ascending chain  $\{\mathbb{H}_p^i(K)\}_{i \geq 0}$  defined by  $\mathbb{H}_p^0(K) = K$  and  $\mathbb{H}_p^i(K) = \mathbb{H}_p(\mathbb{H}_p^{i-1}(K))$  for  $i \geq 1$ .

It is easy to see that  $\mathbb{H}_p^i(K) \subseteq \mathbb{H}^i(K)$  for any  $K$  and  $p$ , so if the  $p$ -class field tower of  $K$  is infinite for some  $p$ , then its class field tower must also be infinite. Let  $\mathbb{H}_p^\infty(K) = \bigcup_{i \geq 0} \mathbb{H}_p^i(K)$  be the union of all fields in the  $p$ -class field tower of  $K$  – this is easily shown to be the maximal unramified pro- $p$  extension<sup>5</sup> of  $K$ . Let  $G_{K,p} = \text{Gal}(\mathbb{H}_p^\infty(K)/K)$ . Thus, to solve the class field tower problem in the negative it suffices to find an example where the group  $G_{K,p}$  is infinite. The latter problem can be solved using Golod-Shafarevich inequality since quite a lot is known about the minimal number of generators and relators for the groups  $G_{K,p}$ .

By definition of  $\mathbb{H}_p(K)$ , the Frattini quotient  $G_{K,p} = G_{K,p}/[G_{K,p}, G_{K,p}]G_{K,p}^p$  is isomorphic to  $\text{Gal}(\mathbb{H}_p(K)/K)$  which, by the earlier discussion, is isomorphic to  $Cl(K)[p] = \{x \in Cl(K) : px = 0\}$ , the elementary  $p$ -subgroup of  $Cl(K)$ . Let  $\rho_p(K) = \dim Cl(K)[p]$ . Then

$$d(G_{K,p}) = d(G_{K,p}/[G_{K,p}, G_{K,p}]G_{K,p}^p) = \rho_p(K).$$

The following relation between the minimal number of generators and the minimal number of relators of  $G_{K,p}$  was proved by Shafarevich [Sh, Theorem 6].

**Theorem 10.3** (Shafarevich). *Let  $K$  be a number field and  $\nu(K)$  the number of infinite primes of  $K$ . Then for any prime  $p$  we have*

$$0 \leq r(G_{K,p}) - d(G_{K,p}) \leq \nu(K) - 1.$$

Combining Theorem 10.3 with Theorem 3.4(a), we obtain the following criterion for the group  $G_{K,p}$  to be infinite:

**Corollary 10.4** (Golod-Shafarevich). *In the above notations, assume that*

$$(10.1) \quad \rho_p(K) > 2 + 2\sqrt{\nu(K) + 1}.$$

*Then the group  $G_{K,p}$  is Golod-Shafarevich and therefore infinite.*

To complete the negative solution to the class field tower problem it suffices to exhibit examples of number fields satisfying the number-theoretic inequality (10.1). As we explain below, for any prime  $p$  and  $n \in \mathbb{N}$  there exists a number field  $K = K(p, n)$  such that  $[K : \mathbb{Q}] = p$  and  $\rho_p(K) \geq n$ . Since  $\nu(K) \leq [K : \mathbb{Q}]$  by the Dirichlet unit theorem, such  $K$  satisfies (10.1) whenever  $n > 2 + 2\sqrt{p + 1}$ .

For  $p = 2$  one can simply take any set of  $n + 1$  distinct odd primes  $q_1, \dots, q_{n+1}$  and let  $K = \mathbb{Q}(\sqrt{\varepsilon q_1 \dots q_{n+1}})$  where  $\varepsilon = \pm 1$  so that  $\varepsilon q_1 \dots q_{n+1} \equiv 1 \pmod{4}$ . If we choose  $\varepsilon_i = \pm 1$  for  $1 \leq i \leq n + 1$  so that  $\varepsilon_i q_i \equiv 1 \pmod{4}$ , then the extension  $\mathbb{Q}(\sqrt{\varepsilon_1 q_1}, \dots, \sqrt{\varepsilon_{n+1} q_{n+1}})/K$  is unramified (which can be seen, for instance, by directly computing its discriminant). Since this extension is abelian with Galois group  $(\mathbb{Z}/2\mathbb{Z})^n$ , we have  $\rho_2(K) \geq n$  (it is not hard to show that in fact  $\rho_2(K) = n$ ).

For an arbitrary  $p$ , we take  $n + 1$  distinct primes  $q_1, \dots, q_{n+1}$  congruent to 1 mod  $p$ , let  $L_i = \mathbb{Q}(\zeta_{q_i})$  be the  $q_i^{\text{th}}$  cyclotomic field and  $K_i$  the unique subfield of degree  $p$  over  $\mathbb{Q}$  inside  $L_i$ . Let  $L = L_1 \dots L_{n+1}$  and  $M = K_1 \dots K_{n+1}$ . Then  $\text{Gal}(L/\mathbb{Q}) \cong \bigoplus \text{Gal}(L_i/\mathbb{Q})$ , so  $\text{Gal}(M/\mathbb{Q}) \cong \bigoplus \text{Gal}(K_i/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^{n+1}$ . Clearly,  $\text{Gal}(M/\mathbb{Q})$  has a subgroup of index  $p$  which does not contain  $\text{Gal}(K_i/\mathbb{Q})$  for any  $i$ . Equivalently, there exists a subfield

<sup>5</sup>We say that a Galois extension  $L/K$  is pro- $p$  if the Galois group  $\text{Gal}(L/K)$  is pro- $p$ .

$\mathbb{Q} \subset K \subset M$  such that  $[K : \mathbb{Q}] = p$  and  $K$  is not contained in the compositum of any proper subset of  $\{K_1, \dots, K_{n+1}\}$ . We claim that each extension  $KK_i/K$  is unramified. Indeed,  $KK_i/K$  may only be ramified at  $q_i$  since  $L_i/\mathbb{Q}$  (and hence  $K_i/\mathbb{Q}$ ) is only ramified at  $q_i$ . If  $KK_i/K$  is ramified at  $q_i$ , then  $M/K$  is ramified at  $q_i$ , which is impossible since  $M/K = K \prod_{j \neq i} K_j/K$  and  $K_j/\mathbb{Q}$  is unramified at  $q_i$  for  $j \neq i$ . Thus, each  $KK_i$  is unramified over  $K$ , so their compositum  $M$  is also unramified over  $K$ . Since  $M/K$  is abelian with  $\text{Gal}(M/K) \cong (\mathbb{Z}/p\mathbb{Z})^n$ , we conclude that  $\rho_p(K) \geq n$  (again, one can show that equality holds).

**10.2. Galois groups  $G_{K,p,S}$ .** The groups  $G_{K,p}$  which arose in the solution to the class field tower problem are very interesting in their own right and have been studied for almost a century, yet their structure remains poorly understood. In fact, it is more natural to consider a larger class of groups: given a number field  $K$ , a prime  $p$  and a finite set of primes  $S$  of  $K$ , denote by  $\mathbb{H}_{p,S}^\infty(K)$  the maximal pro- $p$  extension of  $K$  which is unramified outside of  $S$ , and let  $G_{K,p,S} = \text{Gal}(\mathbb{H}_{p,S}^\infty(K)/K)$  (so  $G_{K,p} = G_{K,p,\emptyset}$ ).

The structure of the group  $G_{K,p,S}$  depends dramatically on whether  $S$  contains a prime above  $p$  or not. In the sequel we shall only discuss the so called tame case when  $S$  contains NO primes above  $p$  – this is equivalent to saying that  $p \nmid N(s)$  for any  $s \in S$  where  $N : K \rightarrow \mathbb{Q}$  is the norm function. In this case, without loss of generality we can actually assume that  $N(s) \equiv 1 \pmod{p}$  for any  $s \in S$  since primes  $s$  with  $N(s) \not\equiv 0, 1 \pmod{p}$  cannot ramify in  $p$ -extensions.

In this setting, Theorem 10.3 is a special case of the following [Sh, Theorems 1,6]:

**Theorem 10.5.** *Let  $K$  be a number field,  $p$  a prime,  $S$  a finite set of primes of  $K$ , and assume that  $N(s) \equiv 1 \pmod{p}$  for every  $s \in S$ . Let  $G = G_{K,S,p}$ . Then*

- (i)  $d(G) \geq |S| + 1 - \nu(K) - \delta(K)$
- (ii)  $0 \leq r(G) - d(G) \leq \nu(K) - 1$

where  $\nu(K)$  is the number of infinite primes of  $K$  and  $\delta(K) = 1$  or  $0$  depending on whether  $K$  contains a primitive  $p^{\text{th}}$  root of unity or not.

In particular, if we fix  $K$  and  $p$ , the group  $G_{K,p,S}$  can be made Golod-Shafarevich if  $|S|$  is chosen to be large enough:

**Corollary 10.6.** ([NSW, Theorem 10.10.1]) *In the above notations assume that*

$$|S| > 1 + \nu(K) + 2\sqrt{\nu(K)} + \delta(K).$$

*Then the group  $G_{K,p,S}$  is Golod-Shafarevich.*

In general, if we fix  $K$  and  $p$ , the structure of the group  $G_{K,p,S}$  becomes more transparent as  $S$  gets larger. In particular, by choosing  $S$  sufficiently large, one can ensure that certain number-theoretically defined group  $V_{K,S}$  is trivial, in which case one can write down a (fairly) explicit presentation for  $G_{K,p,S}$  by generators and relations (see, e.g., [Kol, Chapters 11,12]). Further very interesting results in this direction have been recently obtained by Schmidt [Sch1, Sch2, Sch3].

Thus, in attempting to study the structure of the groups  $G_{K,p,S}$  one might want to concentrate on the case when  $S$  is sufficiently large, and in view of Corollary 10.6 one might hope to make use of Golod-Shafarevich techniques in this case. One important result of this flavor was obtained by Hajir [Haj] who proved that the group  $G_{K,p,S}$  has exponential subgroup growth for sufficiently large  $S$ . In the next subsection we present a group-theoretic version of Hajir's argument in the simplest case  $K = \mathbb{Q}$ .

**10.3. Examples with exponential subgroup growth.** The following presentation for the groups  $G_{\mathbb{Q},p,S}$  is a special case of a more general theorem of Koch (see [Ko1, § 11.4] and [Ko2, § 6]).

**Theorem 10.7.** *Let  $p > 2$  be a prime and  $S = \{q_1, \dots, q_d\}$  a finite set of primes congruent to 1 mod  $p$ . Then the group  $G = G_{\mathbb{Q},p,S}$  has a presentation*

$$(10.2) \quad \langle x_1, \dots, x_d \mid x_i^{a_i} = x_i^{q_i} \rangle$$

for some elements  $\{a_i\}_{i=1}^d$  in the free pro- $p$  group on  $x_1, \dots, x_d$  (where as usual  $g^h = h^{-1}gh$  for group elements  $g$  and  $h$ ).

Note that presentation (10.2) can be rewritten as  $\langle x_1, \dots, x_d \mid [x_i, a_i] = x_i^{q_i-1} \rangle$  and each  $q_i - 1$  is divisible by  $p$ . This implies that all relators in the presentation (10.2) of  $G$  lie in the Frattini subgroup, and so  $d(G) = d$ . We shall now show that any group with such presentation has an LRG chain (and therefore exponential subgroup growth) whenever  $d \geq 10$ .

**Proposition 10.8.** *Let  $G$  be a group given by a presentation of the form*

$$\langle x_1, \dots, x_d \mid [x_i, a_i] = x_i^{p\lambda_i} \rangle$$

where  $a_i \in F_{\hat{p}}(x_1, \dots, x_d)$  and  $\lambda_i \in \mathbb{Z}_p$  (note that  $d(G) = d$  and  $r(G) \leq d$ ). If  $d \geq 10$ , then  $G$  has an LRG chain.

*Proof.* Consider the group  $Q = G / \langle x_1, x_2, a_1, a_2 \rangle^G$ , the quotient of  $G$  by the normal subgroup generated by  $x_1, x_2, a_1$  and  $a_2$ . We claim that  $G$  is Golod-Shafarevich (hence infinite). Indeed, by construction  $d(Q) \geq d(G) - 4 = d - 4 \geq 6$ . Also note that  $Q$  has a presentation with  $d$  generators and  $d + 2$  relations, namely

$$Q = \langle x_1, \dots, x_d \mid x_1 = x_2 = a_1 = a_2 = 1, [x_i, a_i] = x_i^{p\lambda_i} \text{ for } i \geq 3 \rangle,$$

so  $r(Q) - d(Q) \leq 2$  by Lemma 3.5(ii). Therefore,  $r(Q) - d(Q)^2/4 \leq 2 + d(Q) - d(Q)^2/4 < 0$  since  $d(Q) \geq 6$ .

Now choose any infinite descending chain  $\{Q_i\}$  of open subgroups of  $Q$ , and let  $G_i$  be the full preimage of  $Q_i$  under the projection  $\pi : G \rightarrow Q$ . Let  $F = F_{\hat{p}}(x_1, \dots, x_d)$ , let  $N = \langle \{[x_i, a_i](x_i^{p\lambda_i})^{-1}, 1 \leq i \leq d\} \rangle^F$  (so that  $G = F/N$ ), and let  $F_i$  be the full preimage of  $G_i$  in  $F$ . Note that  $G_i = F_i/N$ . Let  $n_i = [G : G_i] = [F : F_i]$ . Then  $d(F_i) = (d-1)n_i + 1$  by the Schreier formula, and  $N$  is generated as a normal subgroup of  $F_i$  by the set  $R_i$  which consists of conjugates of elements of  $R$  by some transversal of  $F_i$  in  $F$ . By construction, each  $F_i$  contains the elements  $x_1, x_2, a_1, a_2$ . Hence the relators  $[x_i, a_i](x_i^{p\lambda_i})^{-1}$  for  $i = 1, 2$  and all their conjugates lie in  $\Phi(F_i)$ , the Frattini subgroup of  $F_i$ , and therefore do not affect  $d(G_i)$ . The number of remaining relations in  $R_i$  is  $(d-2)n_i$ . Hence  $d(G_i) \geq (d-1)n_i + 1 - (d-2)n_i = n_i + 1 = [G : G_i] + 1$ , so  $\{G_i\}$  is an infinite chain with linear rank growth.  $\square$

Hajir [Haj] actually proved something more interesting than exponential subgroup growth for  $G_{K,p,S}$  for sufficiently large  $S$  – he showed that exponential subgroup growth can be achieved in the group  $G_{K,p} = G_{K,p,\emptyset}$  for a suitably chosen number field  $K$  depending on  $p$ . We now briefly outline how to construct such examples using the above presentations of the groups  $G_{\mathbb{Q},p,S}$ .

Let  $S$  and  $G$  be as in the statement of Theorem 10.7. Let  $H$  be any index  $p$  subgroup of  $G = G_{\mathbb{Q},p,S}$  which does not contain any of the generators  $x_i$  (such  $H$  exists since all relators in the presentation (10.2) lie in the Frattini subgroup), and let  $K \subset \mathbb{H}_{p,S}^{\infty}(\mathbb{Q})$  be

the fixed field of  $H$ . Then it is not hard to show that each prime from  $S$  ramifies in  $K$ . Note that  $\mathbb{H}_p^\infty(K)$ , the maximal unramified pro- $p$  extension of  $K$ , is contained in  $\mathbb{H}_{p,S}^\infty(\mathbb{Q})$  by construction, and therefore, the Galois group  $\text{Gal}(\mathbb{H}_p^\infty(K)/\mathbb{Q})$  is a quotient of  $G_{\mathbb{Q},p,S}$ .

According to [Ko1, Theorem 12.1], the assumption that each prime from  $S$  ramifies in  $K$  ensures that  $G' = \text{Gal}(\mathbb{H}_p^\infty(K)/\mathbb{Q})$  is isomorphic to  $G/\langle x_1^p, \dots, x_d^p \rangle^G$  where  $x_1, \dots, x_d$  are as in (10.2), so

$$G' = \langle x_1, \dots, x_d \mid x_i^p = 1, [x_i, a_i] = 1 \text{ for } 1 \leq i \leq d \rangle.$$

One can show directly from this presentation that the group  $G'$  has an LRG chain whenever  $d \geq 12$  – this is achieved by combining the idea of the proof of Proposition 10.8 with the notion of power  $p$ -deficiency discussed in the previous section. Since  $G_{K,p} = \text{Gal}(\mathbb{H}_p^\infty(K)/K)$  is a subgroup of index  $p$  in  $G' = \text{Gal}(\mathbb{H}_p^\infty(K)/\mathbb{Q})$ , we conclude that  $G_{K,p}$  also has an LRG chain.

Finally, we remark that the existence of an LRG chain in the group  $G_{K,p}$  has a very natural number-theoretic interpretation: it is equivalent to the existence of an infinite ascending chain of finite unramified  $p$ -extensions  $K \subset K_1 \subset K_2 \subset \dots$  such that the sequence  $\{\rho_p(K_n)\}_{n \geq 1}$  of the  $p$ -ranks of the ideal class groups of  $K_n$  grows linearly with the degree  $[K_n : K]$ .

## 11. APPLICATIONS IN GEOMETRY AND TOPOLOGY

In this section we will discuss some applications of the Golod-Shafarevich theory to the study of hyperbolic 3-manifolds or rather their fundamental groups. By a hyperbolic 3-manifold we shall always mean a finite volume orientable hyperbolic 3-manifold without boundary. The fundamental groups of hyperbolic 3-manifolds are precisely the torsion-free lattices in  $PSL_2(\mathbb{C}) \cong SO(3,1)$ , with cocompact lattices corresponding to compact 3-manifolds. Arbitrary lattices in  $PSL_2(\mathbb{C})$  (which are always virtually torsion-free) correspond to hyperbolic 3-orbifolds.

If  $X$  is a compact (orientable) 3-manifold and  $\Gamma = \pi_1(X)$  its fundamental group, then by a result of Epstein [Ep],  $\Gamma$  has a presentation  $(X, R)$  with  $|X| \geq |R|$ . Thus  $\text{def}(\Gamma) \geq 0$ , and moreover the same is true if  $\Gamma$  is replaced by a finite index subgroup (since a finite cover of a compact 3-manifold is itself a compact 3-manifold). Note that by Theorem 3.4(b), a group  $\Gamma$  with non-negative deficiency is Golod-Shafarevich with respect to a prime  $p$  whenever  $d(\Gamma_{\hat{p}}) \geq 5$ .

Lubotzky [Lu2] proved that if  $\Gamma$  is a finitely generated group which is linear in characteristic different from 2 or 3 and not virtually solvable, then for any prime  $p$  the set  $\{d(\Delta_{\hat{p}}) : \Delta \text{ is a finite index subgroup of } \Gamma\}$  is unbounded. If  $X$  is hyperbolic, then  $\Gamma = \pi_1(X)$  is linear and not virtually solvable (being a lattice in  $PSL_2(\mathbb{C})$ ). Thus, the discussion in the previous paragraph implies the following:

**Proposition 11.1** ([Lu1]). *Let  $X$  be a hyperbolic 3-manifold and  $\Gamma = \pi_1(X)$ . Then for every prime  $p$ ,  $\Gamma$  has a finite index subgroup which is Golod-Shafarevich with respect to  $p$ .*

Proposition 11.1 was established in 1983 Lubotzky's paper [Lu1] as a tool for solving a major open problem, known at the time as Serre's conjecture. The conjecture (now a theorem) asserts that arithmetic lattices in  $SL_2(\mathbb{C})$  do not have the congruence subgroup property. The proof of this conjecture is a combination of three results:

- (a) Proposition 11.1.
- (b) If  $\Gamma$  is an arithmetic group with the congruence subgroup property, then for any prime  $p$ , the pro- $p$  completion  $\Gamma_{\hat{p}}$  is  $p$ -adic analytic.



(c) Golod-Shafarevich pro- $p$  groups are not  $p$ -adic analytic.

Lubotzky established part (c) using Lazard's theorem [Laz] which asserts that a pro- $p$  group is  $p$ -adic analytic if and only if the coefficients of the Hilbert series  $\text{Hilb}_{\mathbb{F}_p[[G]],d}(t)$  grow polynomially, where  $d$  is the standard degree function. By Corollary 4.3, this cannot happen in a Golod-Shafarevich group. Now one can give simple alternative proofs of (c) thanks to many new characterizations of  $p$ -adic analytic obtained after [Lu1]. For instance, a pro- $p$  group is  $p$ -adic analytic if and only if the set  $\{d(U) : U \text{ is an open subgroup of } G\}$  is bounded (see, e.g., [LuMn] or [DDMS, § 3,7]). This also prevents  $G$  from being Golod-Shafarevich, e.g., by Theorem 8.3.

Lubotzky's work provided the first (and very non-trivial) geometric application of Golod-Shafarevich groups and gave hope that even deeper problems about 3-manifolds could be tackled in the same way. Indeed, suppose one wants to prove that hyperbolic 3-manifold groups always have certain property (P) and (P) is inherited by finite index subgroups and overgroups. In view of Proposition 11.1, to prove such a result it is sufficient to show that every Golod-Shafarevich group has property (P).

One of the main open problems about 3-manifolds is the virtually positive Betti number (VPBN) conjecture due to Thurston and Waldhausen:

**Conjecture 11.2** (VPBN Conjecture). *Let  $M$  be a hyperbolic 3-manifold. Then  $M$  has a finite cover with positive first Betti number. Equivalently,  $\pi_1(M)$  does not have property (FAb), that is,  $\pi_1(M)$  has a finite index subgroup with infinite abelianization.*

This conjecture clearly cannot be settled just using Proposition 11.1 since there exist torsion Golod-Shafarevich groups. However, Golod-Shafarevich theory seemed to be a promising tool for attacking a weaker conjecture of Lubotzky and Sarnak.

**Conjecture 11.3** (Lubotzky-Sarnak). *Let  $M$  be a hyperbolic 3-manifold. Then  $\pi_1(M)$  does not have property  $(\tau)$ .*

**FIX** For the definition and basic properties of Kazhdan's property  $(T)$  and its weaker (finitary) version property  $(\tau)$  we refer the reader to the books [BHV] and [LuZ].

A finitely generated group with property  $(\tau)$  must have (FAb), so Conjecture 11.2 would imply Lubotzky-Sarnak Conjecture. The latter was originally posed not because of its intrinsic value, but with the hope that it may be easier to settle than VPBN conjecture, while its solution may shed some light on VPBN conjecture.

It seemed quite feasible that Lubotzky-Sarnak conjecture might be solved using Golod-Shafarevich approach, that is, it may be true that Golod-Shafarevich groups never have property  $(\tau)$ . The latter, however, turned out to be false, as explicit examples of Golod-Shafarevich groups with property  $(\tau)$  (actually, with property  $(T)$ ) were constructed in [Er1].

These examples still leave a possibility that Lubotzky-Sarnak conjecture (or even VPBN conjecture) could be solved by group-theoretic methods since it is easy to identify group-theoretic properties which hold for hyperbolic 3-manifold groups and which clearly fail for all known examples of Golod-Shafarevich groups with property  $(\tau)$ . Unfortunately, at present there seems to be no group-theoretic conjecture which would imply Lubotzky-Sarnak conjecture and which could be attacked with currently known methods.

Nevertheless, Golod-Shafarevich techniques did yield new important results about 3-manifold groups. Perhaps the most interesting of those are two results of Lackenby dealing with subgroup growth.

**11.1. Subgroup growth of 3-manifold groups.** In [La1] and [La2], Lackenby obtained strong lower bounds on the subgroup growth of hyperbolic 3-manifold groups. The first result asserts that for any hyperbolic 3-manifold group, the subgroup growth function is bounded below by an almost exponential function on an infinite subset of  $\mathbb{N}$ .

**Theorem 11.4.** ([La2]) *Let  $\Gamma$  be the fundamental group of a hyperbolic 3-manifold, and let  $a_n(\Gamma)$  be the number of subgroups of index  $n$  in  $\Gamma$ . Then  $a_n(\Gamma) \geq 2^{n/(\sqrt{\log n} \cdot \log(\log n))}$  for infinitely many  $n$ .*

This result follows by a direct (though not completely straightforward) computation from Corollary 8.5 and Lemma 8.1 for  $p = 2$  (see [La2, § 6, Claim 2] for details) applied to the pro- $p$  completion of  $\Gamma$ . (We note that by [Lu2], the assumption  $d_p(\Gamma) = d(\Gamma_{\hat{p}}) \geq 4$  can always be achieved replacing  $\Gamma$  by a finite index subgroup). The proof of Corollary 8.5 (which is an algebraic result) in [La2] uses topological techniques, but the alternative proof given in this paper is purely algebraic and based on the finitary Golod-Shafarevich inequality.

The second result of Lackenby asserts that for a large class of hyperbolic 3-manifolds the subgroup growth is at least exponential:

**Theorem 11.5** ([La1]). *Let  $M$  be a hyperbolic 3-manifold which is commensurable with an orbifold  $O$  with non-empty singular locus. Let  $p$  be any prime such that  $\pi_1(O)$  has an element of order  $p$ . Then  $\pi_1(M)$  has an LRG  $p$ -chain and hence has at least exponential subgroup growth.*

Unlike Theorem 11.4, it does not seem possible to give an entirely algebraic proof of Theorem 11.5 (although a substantial part of the argument in [La1] is group-theoretic). For this reason we do not discuss the proof of this result in this paper and refer the reader to a very clear exposition in [La1]. However, we do remark that there are many similarities between the proof of Theorem 11.5 and that of Proposition 10.8 (in fact, the latter was inspired by the former).

Another interesting application of Golod-Shafarevich inequality to 3-manifold groups (specifically, to the structure of their rational lower central series) was obtained by Freedman, Hain and Teichner [FHT].

## 12. GOLOD-SHAFAREVICH GROUPS AND KAZHDAN'S PROPERTY $(T)$

**12.1. Golod-Shafarevich groups with property  $(T)$ .** In the previous section we discussed why the question of the existence of Golod-Shafarevich groups with property  $(\tau)$  was important in topology, or rather, why the lack of such groups would have been very useful. This question, however, is quite natural from a purely group-theoretic point of view as well, and when the question was open, one could present natural heuristic arguments for both non-existence and existence of such groups. On the one hand, as we already saw, every Golod-Shafarevich group has a lot of quotients (including finite quotients), seemingly too many for such a group to have property  $(\tau)$ . On the other hand, Golod-Shafarevich groups behave similarly to hyperbolic groups in many ways, and there exist hyperbolic groups with property  $(T)$  (hence also property  $(\tau)$ ). A posteriori, it seems that the latter heuristics was the “right one”, at least it predicted the right answer, although the actual examples of Golod-Shafarevich groups with property  $(T)$  are completely different from the examples of hyperbolic groups with  $(T)$ .

The first examples of Golod-Shafarevich groups with property  $(T)$  were constructed in [Er1] as positive parts of certain Kac-Moody groups over finite fields. Property  $(T)$  for

such groups was established earlier by Dymara and Januskiewicz [DJ], while the Golod-Shafarevich condition was verified using certain optimization of the Tits presentation of such groups. We shall not discuss this construction since much simpler to describe examples of Golod-Shafarevich groups with (T) were given in [EJ1].

**Theorem 12.1.** [EJ1] *Let  $p$  be a prime and  $d \geq 2$  an integer, and consider the group*

$$G_{p,d} = \langle x_1, \dots, x_d \mid x_i^p = 1, [x_i, x_j, x_j] = 1 \text{ for } 1 \leq i \neq j \leq 9 \rangle.$$

*Then*

- (i) *The group  $G_{p,d}$  is Golod-Shafarevich whenever  $p \geq 3$  and  $d \geq 9$  or  $p = 2$  and  $d \geq 12$ .*
- (ii) *The group  $G_{p,d}$  has property (T) whenever  $p > (d-1)^2$ .*

*In particular, for any  $p \geq 67$ , there exists a Golod-Shafarevich group with property (T).*

Part (i) is established by direct verification: indeed, if  $(X, R)$  is the presentation of  $G_{p,d}$  given above, then  $1 - H_X(\tau) + H_R(\tau) = 1 - d\tau + d(d-1)\tau^3 + d\tau^p$ , which is negative for  $\tau = 2/d$  under the required conditions on  $p$  and  $d$ .

Part (ii) is proved using a general criterion for property (T) from [EJ1] (see Theorem 12.2 below).

**Definition.** Let  $H$  and  $K$  be subgroups of the same group. The *orthogonality constant*  $\text{orth}(H, K)$  is defined to be the smallest  $\varepsilon \geq 0$  with the following property: if  $V$  is a unitary representation of the group  $\langle H, K \rangle$  without nonzero invariant vectors,  $v \in V$  is  $H$ -invariant and  $w \in V$  is  $K$ -invariant, then  $|\langle v, w \rangle| \leq \varepsilon \|v\| \|w\|$ .

**Theorem 12.2.** ([EJ1, Theorem 1.2]) *Suppose that a group  $G$  is generated by  $n$  finite subgroups  $H_1, \dots, H_n$ , and for each  $1 \leq i \neq j \leq n$  we have  $\text{orth}(H_i, H_j) < \frac{1}{n-1}$ . Then  $G$  has property (T).*

The wonderful thing about this criterion is that the orthogonality constant  $\text{orth}(H, K)$  is completely determined by the representation theory of the subgroup  $\langle H, K \rangle$ ; in fact, it suffices to consider only irreducible representations. If  $G = G_{p,d}$  is a group from Theorem 12.1, we let  $H_i = \langle x_i \rangle$  for  $1 \leq i \leq d$ . For any  $i \neq j$ , the group  $\langle H_i, H_j \rangle$  is isomorphic to the Heisenberg group over  $\mathbb{F}_p$  which has very simple representation theory, and one easily shows that  $\text{orth}(H_i, H_j) = 1/\sqrt{p}$ . Therefore, by Theorem 12.2,  $G_{p,d}$  has (T) whenever  $p > (d-1)^2$ .

**Remark:** The “Kac-Moody examples” with property (T) from [Er1] are quotients of the groups  $G_{p,d}$ . These groups are Golod-Shafarevich under stronger assumptions on  $p$  and  $d$  than the ones given in Theorem 12.1, and it takes some work to verify the Golod-Shafarevich condition for these groups.

**12.2. Applications.** In terms of potential applications to 3-manifolds, the existence of Golod-Shafarevich groups with property (T) was a “negative result”. However, it turned out to be a very useful tool for constructing examples of groups with exotic finiteness properties. For instance, it immediately implies the existence of residually finite torsion non-amenable groups.

**Theorem 12.3.** [Er1] *There exist residually finite torsion non-amenable groups.*

*Proof.* Let  $G$  be a Golod-Shafarevich group with property (T). By Theorem 6.2,  $G$  has a torsion quotient  $G'$  which is also Golod-Shafarevich. Hence the image of  $G'$  in its pro- $p$  completion, call it  $G''$ , is infinite. Then  $G''$  is a torsion residually finite group which has

property  $(T)$  (being a quotient of  $G$ ). Since an infinite group with  $(T)$  is non-amenable, we are done.  $\square$

**Remark:** Recall that another construction of residually finite torsion non-amenable groups due to Schlage-Puchta and Osin was described in § 9.

Golod-Shafarevich groups with  $(T)$  also provide a very simple approach to constructing infinite residually finite groups which have  $(T)$  and some additional property  $(P)$  via the following observation.

**Observation 12.4.** *Let  $(P)$  be a group-theoretic property such that every Golod-Shafarevich group has an infinite residually finite quotient with  $(P)$ . Then there exists an infinite residually finite group which has  $(P)$  and  $(T)$ .*

Recall that several properties  $(P)$  satisfying the hypothesis of Observation 12.4 were stated in § 6. Applying Observation 12.4 to those properties, we obtain the following results:

**Proposition 12.5.** ([EJ3, Theorem 1.3]) *There exists an infinite LERF group with  $(T)$ .*

**Proposition 12.6.** [Er2] *There exists an infinite residually finite group with  $(T)$  whose FC-radical (the set of elements with finite conjugacy class) is not virtually abelian.*

Proposition 12.5 answers a question of Long and Reid [LR] which arose in connection with the study of property LERF for 3-manifold groups while Proposition 12.6 settled a question of Popa and Vaes [PV] coming from measurable group theory.

**12.3. Kazhdan quotients of Golod-Shafarevich groups.** In this subsection we discuss the proof of the following theorem:

**Theorem 12.7.** ([EJ2, Theorems 1.1, 4.6]) *Every generalized Golod-Shafarevich group has an infinite quotient with Kazhdan's property  $(T)$ .*

While the fact that Golod-Shafarevich groups with  $(T)$  exist was somewhat surprising, once it was established, it was natural to expect that the assertion of Theorem 12.7 is true, and this was explicitly conjectured by Lubotzky. The conjecture was partially motivated by the theory of hyperbolic groups where the analogous result was known to be true: every (non-elementary) hyperbolic group has an infinite quotient with property  $(T)$ , which follows directly from two deep theorems:

- (a) There exists a hyperbolic group with property  $(T)$ .
- (b) Any two hyperbolic groups have a common infinite quotient.

In fact, this analogy suggests a naive approach to Theorem 12.7: Theorem 12.7 would follow from Theorem 12.1, at least for  $p \geq 67$ , if one could show that any two GGS groups (with respect to the same  $p$ ) have a common infinite quotient. The latter is of course too much to expect, even if we consider GS groups instead of GGS groups (we do not know explicit counterexamples at this point, but there is little doubt that such counterexamples exist). Nevertheless, one could still try to show that for any GGS group  $G$  there is another GGS group  $H$  with  $(T)$  such that  $G$  and  $H$  have a common infinite quotient – if true, this would still imply Theorem 12.7.

In order to implement this approach, one needs to possess a large supply of GGS group with  $(T)$ . The class of groups described in Theorem 12.1 is way too small for this to work, but using essentially the same method one can construct more groups with this property.

**Theorem 12.8.** (see [EJ2, Theorem 4.2]) *Let  $p$  be a prime,  $d > 0$  an integer and  $n_1, \dots, n_d$  positive integers. Consider the group  $G$  given by the presentation  $(X_{KMS}, R_{KMS})$  where  $X_{KMS} = \{x_{i,k} : 1 \leq i \leq d, 1 \leq k \leq n_d\}$  and  $R_{KMS} = \{[x_{i,k}, x_{j,l}, x_{j,m}] \text{ for } i \neq j\} \cup \{[x_{i,k}, x_{i,l}]\} \cup \{x_{i,k}^p\}$ . If  $d \geq 9$  and  $p > (d-1)^2$ , then  $G$  is GGS and has property (T).*

**Remark:** The groups described in this theorem are called Kac-Moody-Steinberg groups in [EJ1] since they map onto suitable Kac-Moody groups over  $\mathbb{F}_p$  as well as certain Steinberg groups. This explains the notations  $X_{KMS}$  and  $R_{KMS}$  for the sets of generators and relators.

This class of groups is still insufficient to make the naive approach work, but a more convoluted scheme based on the same idea does work. We shall now outline the argument.

First we reduce the problem to the following:

**Theorem 12.9.** Every generalized Golod-Shafarevich group has a finite index subgroup which has an infinite quotient with Kazhdan's property (T).

The reduction is possible due to the following general statement:

**Proposition 12.10.** *Let  $(P)$  be a group-theoretic property, which is preserved by quotients, finite direct products, finite index subgroups and finite index overgroups. Let  $G$  be a group, and suppose that some finite index subgroup of  $G$  has an infinite quotient with  $(P)$ . Then  $G$  itself has an infinite quotient with  $(P)$ .*

Proposition 12.10 was proved by Jaikin-Zapirain in the case  $(P) = (T)$  (see [EJ2, Prop. 4.5]), but as observed in [BuTh, Prop. 3.5], the same argument applies to any property  $(P)$  as above.

*Proof of Theorem 12.9(sketch).* We shall restrict ourselves to the case  $p \geq 67$ ; the proof in the case  $p < 67$  is similar, but more technical. Let  $\Gamma$  be a generalized Golod-Shafarevich abstract group; without loss of generality we can assume that  $\Gamma$  is residually- $p$ . Let  $G = \Gamma_{\hat{p}}$  be the pro- $p$  completion of  $\Gamma$  and  $\overline{W}$  a valuation on  $G$  such that  $\text{def}_{\overline{W}}(G) > 0$ . The proof of Theorem 12.9 consists of four main steps.

*Step 1:* Given  $M \in \mathbb{R}$ , find an open subgroup  $H$  of  $G$  such that  $\text{def}_{\overline{W}}(H) > M$ . Then we can find a weighted presentation  $(X, R, W)$  of  $H$  (where  $W$  induces  $\overline{W}$ ) such that  $\text{def}_W(X, R) > M$ .

*Step 2:* Given real numbers  $w > 1$  and  $\varepsilon > 0$ , show that there is a real number  $f(w, \varepsilon)$  such that if in Step 1 we take  $M > f(w, \varepsilon)$ , then there is another weighted presentation  $(X', R', W')$  of  $H$ , with  $X' \subset F_{\hat{p}}(X)$ , such that  $W'(X') = w$ ,  $W'(R') < \varepsilon$ ,  $W'(x) < \varepsilon$  for all  $x \in X'$  and  $W'(h) \leq W(h)$  for all  $h \in F_{\hat{p}}(X')$ .

*Step 3:* Show that if  $w$  and  $\varepsilon$  in Step 2 are suitably chosen, then there is a KMS group  $\Lambda$  with (T) from the family described in Theorem 12.8 such that

- (i) the canonical set of generators  $X_{KMS} = \{x_{i,j}\}$  of  $\Lambda$  has the same cardinality as  $X'$  from Step 2, so there is a bijection (thought of as identification)  $\sigma : X_{KMS} \rightarrow X'$ .
- (ii) If  $R_{KMS}$  is the canonical set of relators of  $\Lambda$ , we can choose  $\sigma : X_{KMS} \rightarrow X'$  in such a way that  $\text{def}_{W'}(X', R' \cup R_{KMS}) > 0$ , so the pro- $p$  group  $Q = \langle X' \mid R' \cup R_{KMS} \rangle$  is GGS.

*Step 4:* Let  $\Delta$  be the image of  $\Gamma \cap H$  in  $Q$ , and let  $\Delta'$  be the subgroup of  $Q$  abstractly generated by  $X'$ . Note that  $\Delta'$  is a quotient of  $\Lambda$ . By Lemma 6.7 (Tails Lemma), we can find a GGS quotient  $Q'$  of  $Q$  in which the images of  $\Delta$  and  $\Delta'$  coincide; call their common image  $\Omega$ .

We claim that  $\Omega$  satisfies the conclusion of Theorem 12.9. Indeed, by construction,  $\Omega$  is a quotient of  $\Gamma \cap H$  (which is a finite index subgroup of  $\Gamma$ ) and has  $(T)$  being a quotient of  $\Lambda$ . Finally,  $\Omega$  is infinite being a dense subgroup of the GGS pro- $p$  group  $Q'$ .

We now comment briefly on the proof of each step. Step 4 has already been fully explained. Recall that  $\text{def}_{\overline{W}}(H) \geq \text{def}_{\overline{W}}(G) \cdot [G : H]_{\overline{W}}$  for any open subgroup  $H$  by Theorem 5.7(b) and the  $\overline{W}$ -index  $[G : H]_{\overline{W}}$  can be made arbitrarily large by Corollary 5.11. This justifies Step 1.

The key tool in Step 2 is the notion of contraction of weight functions.

**Definition.** Let  $F$  be a free pro- $p$  group,  $W$  a weight function on  $F$  and  $c \geq 1$  a real number. Choose a  $W$ -free generating set  $X$  of  $F$ , and let  $W'$  be the unique weight function on  $F$  with respect to  $X$  such that  $W'(x) = W(x)/c$  for all  $x \in X$ . We will say that the function  $W'$  is obtained from  $W$  by the  $c$ -contraction. (It is easy to see that  $W'$  does not depend on the choice of  $X$ ).

In order to understand better what a contraction does we go back to weight functions on power series algebras. By definition, the initial weight function  $W$  is given by  $W(f) = w(f - 1)$  where  $w$  is a weight function on  $\mathbb{F}_p[[F]]$  with respect to  $U = \{x - 1 : x \in X\}$ . Then the contracted weight function  $W'$  can be defined by  $W'(f) = w'(f - 1)$  where  $w'$  is the unique weight function on  $\mathbb{F}_p[[F]]$  with respect to  $U$  such that  $w'(u) = w(u)/c$  for all  $u \in U$ . Recall that  $\mathbb{F}_p[[F]] \cong \mathbb{F}_p\langle\langle U \rangle\rangle$ . It is clear that for any  $a \in \mathbb{F}_p[[F]]$  such that the degree of  $a$  as a power series in  $U$  is at least  $k$  we have  $w'(a) \leq w(a)/c^k$ . In particular this implies that

- (i)  $W'(f) \leq W(f)/c$  for all  $f \in F$ .
- (ii)  $W'(f) \leq W(f)/c^2$  for all  $f \in \Phi(F) = [F, F]F^p$ .

Let us now go back to the setting of Step 2. Assume first that all elements of  $R$  lie in  $\Phi(F)$ . If we obtain  $W'$  from  $W$  by the  $c$ -contraction for  $c = W(X)/w$ , then  $W'(X) = w$  and  $W'(R) \leq W(R)/c^2$  by (ii). Since  $W(R) < W(X)$  and  $W(X) > M$ , we get  $W'(R) \leq W(R)w^2/W(X)^2 < w^2/M$  and  $W'(x) < w/M$  for all  $x \in X$ . Thus in this case we can simply set  $X' = X$ ,  $R' = R$  and  $f(w, \varepsilon) = \max\{w^2/\varepsilon, w/\varepsilon\}$ .

In general, the situation is more complex. Note that starting with the presentation  $(X, R)$ , we can eliminate some of the relators together with the corresponding generators (using the procedure described in Lemma 3.5(ii)), so that in the new presentation all relators lie in the Frattini subgroup; unfortunately, during this operation the weighted deficiency may increase. In order to resolve this problem, one needs to apply a contraction, followed by elimination of some of the relators, followed for the second contraction. For the details we refer the reader to [EJ2, Theorem 3.15].

Finally, we turn to Step 3. Here the precise form of relators in  $R_{KMS}$  plays an important role. Let  $X_i = \{x_{i,j}\}_{j=1}^{n_i}$  for  $1 \leq i \leq 9$ , so that  $X_{KMS} = \sqcup X_i$ . The key property is that the presentation  $(X_{KMS}, R_{KMS})$  is very symmetric, and therefore  $\text{def}_V(X_{KMS}, R_{KMS}) > 0$  for many different weight functions  $V$ . A direct computation (see the proof of Theorem 4.3 in [EJ2]) shows that  $\text{def}_V(X_{KMS}, R_{KMS}) > 1/50$  whenever  $V(X_{KMS}) = \sum_{i=1}^9 V(X_i) = 3/2$  and all subsets  $X_1, \dots, X_9$  have approximately equal  $V$ -weights; more precisely, it is enough to assume that  $|V(X_i) - 1/6| < 1/100$  for  $1 \leq i \leq 9$ .

Now take  $w = 3/2$  and  $\varepsilon = 1/100$  in Step 2. Then we can divide the generators from  $X'$  into 9 subsets such that the total  $W'$ -weight in each subset differs from  $1/6 = (3/2)/9$  by less than  $1/100$ . Letting  $X_i$  be the  $i^{\text{th}}$  subset, we obtain an identification  $\sigma$  between  $X'$  and  $X_{KMS}$ . Then  $\text{def}_{W'}(X', R' \cup R_{KMS}) \geq \text{def}_{W'}(X_{KMS}, R_{KMS}) - W'(R') > 1/50 - \varepsilon > 0$ , so conditions (i) and (ii) from Step 3 are satisfied.  $\square$

## 13. RESIDUALLY FINITE MONSTERS

The following famous theorem was proved by Ol'shanskii in 1980:

**Theorem 13.1** (Ol'shanskii, [Ol1]). *For every sufficiently large prime  $p$  there exists an infinite group  $\Gamma$  in which every proper subgroup is cyclic of order  $p$ .*

Groups satisfying the above condition are called Tarski monsters, named after Alfred Tarski who first posed the question of their existence. Tarski monsters satisfy a number of extremely unusual properties. However, they are not residually finite (as they do not have any proper subgroups of finite index), and it is a common phenomenon in combinatorial group theory that residually finite finitely generated groups are much better behaved than arbitrary finitely generated groups. Thus it is interesting to find out how close a residually finite group can be to a Tarski monster. In particular, the following natural question was asked by several different people.

**Problem.** *Let  $p$  be a prime. Does there exist an infinite finitely generated residually finite  $p$ -torsion group in which every subgroup is either finite or of finite index?*

This problem remains completely open, except for  $p = 2$  when non-existence of such groups was known since 1970s and in fact can be proved by a very elementary argument (see [EJ3, § 8.1] and references therein). However, in [EJ3], Golod-Shafarevich techniques were used to prove the existence of residually finite groups which satisfy the condition in the above problem for all finitely generated subgroups:

**Theorem 13.2.** *For every prime  $p$  there exists an infinite finitely generated residually finite  $p$ -torsion group in which every **finitely generated** subgroup is either finite or of finite index. Moreover, every (abstract) generalized Golod-Shafarevich group (with respect to  $p$ ) has a quotient with this property.*

**13.1. Sketch of the proof of Theorem 13.2.** The basic idea behind constructing such groups is very simple. Let  $\Gamma$  be a generalized Golod-Shafarevich group. Without loss of generality, we can assume right away that  $\Gamma$  is  $p$ -torsion and residually- $p$ , so we can identify  $\Gamma$  with a subgroup of  $G = \Gamma_{\widehat{p}}$ . There are only countably many finitely generated subgroups of  $\Gamma$ , so we can enumerate them:  $\Lambda_1, \Lambda_2, \dots$ . At the first step we construct an infinite quotient  $G_1$  of  $G$  such that if  $\pi_1 : G \rightarrow G_1$  is the natural projection, then  $\pi_1(\Lambda_1)$  is either finite or has finite index in  $\pi_1(\Gamma)$ ; note that the latter condition will be preserved if we replace  $G_1$  by another quotient. Next we construct an infinite quotient  $G_2$  of  $G_1$  such that if  $\pi_2 : G \rightarrow G_2$  is the natural projection, then  $\pi_2(\Lambda_2)$  is either finite or of finite index in  $\pi_2(\Gamma)$ . We proceed in this way indefinitely. Let  $G_\infty = \varprojlim G_i$ ; in other words, if  $G_i = G/N_i$  (so that the chain  $\{N_i\}$  is ascending), we let  $N_\infty = \overline{\cup N_i}$ , the closure of  $\cup N_i$ , and  $G_\infty = G/N_\infty$ . Since each  $G_i$  is infinite,  $G_\infty$  must also be infinite (otherwise  $N_\infty$  is of finite index in  $G$ , hence it is a finitely generated pro- $p$  group, which easily implies that  $N_\infty = N_i$  for some  $i$ ). Let  $\Gamma_\infty$  be the image of  $\Gamma$  in  $G_\infty$ . By construction,  $\Gamma_\infty$  is  $p$ -torsion, and each of its finitely generated subgroups is finite or of finite index. Finally,  $\Gamma_\infty$  is residually finite being a subgroup of  $G_\infty$  and infinite being dense in  $G_\infty$ , so it satisfies the required properties.

So, we just have to make sure that a sequence  $\{G_i\}$  as above can indeed be constructed. Things would have been really nice if at each step we could make  $G_i$  a GGS group. We do not know how to achieve this, and in order to resolve the problem we have to extend the class of GGS groups even further.

**Definition.** A pro- $p$  group  $G$  will be called a *pseudo-GGS group* if there exist an open normal subgroup  $H$  of  $G$  and a finite valuation  $W$  on  $H$  such that

- (i)  $\text{def}_W(H) > 0$  (so, in particular,  $H$  is a GGS group).
- (ii) The function  $W$  is  $G$ -invariant, that is,  $W(h^g) = W(h)$  for all  $h \in H$  and  $g \in G$ .

**Remark:** Pseudo-GGS groups are called *groups of positive virtual weighted deficiency* in [EJ3].

We will need a simple lemma which generalizes Lemma 6.1:

**Lemma 13.3.** *Let  $G$  be a pseudo-GGS group, and let  $H$  and  $W$  satisfy conditions (i) and (ii) above. Let  $S$  be a subset of  $H$  and let  $G' = G/\langle S \rangle^G$ . If  $W(S) < \text{def}_W(H)/[G : H]$ , then  $G'$  is also a pseudo-GGS group.*

*Proof.* Let  $T$  be a transversal of  $H$  in  $G$  and  $H'$  be the image of  $H$  in  $G'$ . Then  $H' \cong H/\langle S' \rangle^H$  where  $S' = \{s^t : s \in S, t \in T\}$ . Since  $W$  is  $G$ -invariant,  $W(S') \leq W(S)|T| = W(S)[G : H]$ , so  $\text{def}_W(H') > 0$  by Lemma 6.1. Thus,  $G'$  is also a pseudo-GGS group with  $H'$  satisfying conditions (i) and (ii) above.  $\square$

The following result is a key step in the proof of Theorem 13.2:

**Theorem 13.4.** *Let  $G$  be a pseudo-GGS pro- $p$  group,  $\Gamma$  a finitely generated dense subgroup of  $G$  and  $\Lambda$  a finitely generated subgroup of  $\Gamma$ . Then there exists an epimorphism  $\pi : G \rightarrow Q$  such that*

- (i)  $Q$  is a pseudo-GGS pro- $p$  group;
- (ii)  $\pi(\Lambda)$  is either finite or has finite index in  $\pi(\Gamma)$ .

Theorem 13.4 ensures that we can make each step in the above iterated algorithm, and therefore we have now reduced Theorem 13.2 to Theorem 13.4.

*Sketch of the proof of Theorem 13.4.* Let  $H$  be an open normal subgroup of  $G$  and  $W$  a valuation on  $H$  from the definition of a pseudo-GGS group. By the Tails Lemma, we can assume that  $\Gamma \cap H$  is abstractly generated by  $X$ . Also, replacing  $\Lambda$  by its finite index subgroup, we can assume that  $\Lambda \subset H$ .

Let  $L$  be the closure of  $\Lambda$ . Which of the two alternatives in the conclusion of Theorem 13.4 will occur depends on whether the  $W$ -index  $[H : L]_W$  is infinite or finite.

*Case 1:*  $[H : L]_W < \infty$ . In this case, by multiplicativity of  $W$ -index (Proposition 5.8) and Continuity Lemma (Proposition 5.9), for any given  $\varepsilon > 0$  we can find an open subgroup  $U$  of  $H$  containing  $L$  such that  $[U : L]_W < 1 + \varepsilon$ . This easily implies that there exists a subset  $X_\varepsilon$  of  $U$  such that  $W(X_\varepsilon) < \varepsilon$  and  $U$  is generated by  $L$  and  $X_\varepsilon$ . The latter condition implies that if we let  $Q = G/\langle X_\varepsilon \rangle^G$  and let  $\pi : G \rightarrow Q$  be the natural projection, then  $\pi(L) = \pi(U)$ , so  $\pi(L)$  must be of finite index in  $Q$ . On the other hand, by Lemma 13.3, if we take  $\varepsilon < \text{def}_W(H)/[G : H]$ , then  $Q = \pi(G)$  is a pseudo-GGS group, as desired.

Note that if  $G$  was a GGS group, then  $Q = \pi(G)$  would also be a GGS group, so if Case 1 always occurred, we would not need to consider pseudo-GGS groups at all. It is Case 2 where such generalization is needed.

*Case 2:*  $[H : L]_W = \infty$ . In this case we start with an important subcase:

*Subcase:*  $\text{rk}_W(L) < 1$ . In this subcase we construct the desired quotient  $Q$  exactly as in the proof of Theorem 3.3. Note that the assumption  $[H : L]_W = \infty$  is not explicitly used in the proof; however, it is already implied by the assumption  $\text{rk}_W(L) < 1$ .

If  $\text{rk}_W(L) \geq 1$ , the first thing we can try is to replace  $W$  by the valuation  $W'$  obtained from  $W$  by  $c$ -contraction for some  $c > 1$  (recall that  $c$ -contractions were defined in Step 2



of the proof of Theorem 12.9). More precisely, we choose a weight function  $\widetilde{W}$  which induces  $W$ , let  $\widetilde{W}'$  be the  $c$ -contraction of  $\widetilde{W}$  and then induce the valuation  $W'$  from  $\widetilde{W}'$ . One can show that if  $\widetilde{W}$  is suitably chosen, the valuation  $W'$  will still be  $G$ -invariant (see [EJ3, Prop. 4.13]). If we take  $c > rk_W(L)$ , then clearly  $rk_{W'}(L) < 1$ ; the problem is that the deficiency  $def_{W'}(H)$  may become negative; more precisely, we can only guarantee that  $def_{W'}(H) > 0$  if  $def_W(H) > rk_W(L)$ .

To overcome this problem we proceed as follows. Using the assumption  $[H : L]_W = \infty$ , it is not hard to show that for any descending chain  $\{U_i\}$  of open subgroups of  $H$  with  $\cap U_i = \{1\}$ , the quantity  $\frac{def_W(U_i)}{rk_W(L \cap U_i)}$  goes to infinity. This follows from Theorem 5.7, Continuity Lemma and multiplicativity of  $W$ -index. In particular, we can find  $U \subseteq H$  which is open and normal in  $G$  for which  $rk_W(L \cap U) < def_W(U)$ . Thus, if we let  $W'$  be the valuation on  $U$  (not on  $H$ ) obtained from  $W$  by the  $c$ -contraction, where  $rk_W(L \cap U) < c < def_W(U)$ , then  $rk_{W'}(L \cap U) < 1$  and  $def_{W'}(U) > 0$ . Now we can finish the proof as in the above subcase with  $W$  replaced by  $W'$  and  $H$  replaced by  $U$ .  $\square$

#### 14. OPEN QUESTIONS

In this section we pose several open problems about Golod-Shafarevich groups. All these questions make sense for generalized Golod-Shafarevich groups as well, but with the exception of Problem 4, it does not seem that answering them for GGS groups would be easier or harder or more interesting than for GS groups. For each problem we provide brief motivation and discuss related works and conjectures. Our list has some overlap with the list of problems in a paper of Button [Bu].

**Problem 1.** *Let  $G$  be a finitely presented Golod-Shafarevich abstract group. Does  $G$  contain a non-abelian free subgroup?*

Recall that Golod-Shafarevich pro- $p$  groups contain non-abelian free pro- $p$  groups, even if not finitely presented. In the abstract case there exist Golod-Shafarevich torsion groups, so an additional assumption about the group is needed to ensure the existence of a non-abelian free subgroup. We conjecture that the answer to Problem 1 is positive, although we are unaware of any promising approach to it at the moment.

**Problem 2.** *Let  $G$  be a Golod-Shafarevich abstract group with a balanced presentation (a presentation with the same number of generators and relators). Is  $G$  necessarily large?*

The main motivation for this problem comes from 3-manifold topology. Lackenby posed a stronger form of the virtual positive Betti number conjecture asserting that if  $G$  is the fundamental group of a hyperbolic 3-manifold, then  $G$  must be large. As explained in § 11, such  $G$  must have a finite index subgroup which is Golod-Shafarevich and has a balanced presentation, so a positive answer to Problem 2 would settle Lackenby's conjecture. In fact, to settle the latter it is enough to answer Problem 2 in the positive under the stronger assumption that every finite index subgroup of  $G$  has a balanced presentation. Unfortunately, even in this form the problem remains wide open and there are no strong indications that the answer should be positive.

**Problem 3.** *Let  $G$  be a Golod-Shafarevich abstract group with a balanced presentation. Is it true that  $G$  does not have (FAB)?*

Recall that  $G$  is said to have (FAB) if every finite index subgroup of  $G$  has finite abelianization, so a positive answer to Problem 2 would, of course, imply the same for Problem 3. Settling Problem 3 in the affirmative would still be an amazing result – even

under the extra hypothesis that every finite index subgroup of  $G$  has balanced presentation, it would imply virtual positive Betti number conjecture.

We remark that the analogue of Problem 3 for pro- $p$  groups has negative answer – as explained in § 10, the Galois group  $G_{\mathbb{Q},p,S}$  has a balanced (pro- $p$ ) presentation and is Golod-Shafarevich, provided  $|S| \geq 5$  and all primes in  $S$  are congruent to 1 mod  $p$ , but also has (FAb) by class field theory. Note though that finite index subgroups of the groups  $G_{\mathbb{Q},p,S}$  do not necessarily have balanced presentations.

Finally, note that Problem 3 (and hence also Problem 2) would have negative answer if we only assumed that  $G$  is finitely presented (not assuming the existence of a balanced presentation). Indeed, the groups described in Theorem 12.1 are finitely presented Golod-Shafarevich groups which have property (T) and therefore (FAb) as well.

**Problem 4.** *Let  $G$  be a GGS pro- $p$  group and  $W$  a valuation on  $G$  such that  $\text{def}_W(G) > 0$ . Does  $G$  always have a closed subgroup  $H$  of finite  $W$ -index such that  $H$  can be mapped onto a non-abelian free pro- $p$  group?*

Problem 4 should be considered as a fancy pro- $p$  analogue of Baumslag-Pride theorem, as we now explain.

Baumslag-Pride theorem [BP] asserts that if  $G$  is an abstract group of deficiency at least two (that is,  $G$  has a presentation with two more generators than relators), then  $G$  is large. Several people independently asked if Baumslag-Pride theorem remains true for pro- $p$  groups, that is, if a pro- $p$  group of deficiency at least two has an open subgroup mapping onto a non-abelian free pro- $p$  group. It is clear that the proof of Baumslag-Pride theorem in the abstract case cannot possibly be adapted to pro- $p$  groups. The reason is that if  $G$  is an abstract group with  $\text{def}(G) \geq 2$ , the index of a finite index subgroup  $H$  of  $G$ , which is guaranteed to map onto a non-abelian free group, depends on the word length of relators of  $G$ , and in the pro- $p$  case relators may be words of infinite length. In fact, most experts believe that the analogue of Baumslag-Pride theorem for pro- $p$  groups should be false, although no counterexamples (or even potential counterexamples) have been constructed.

Problem 4 is a “weighted substitute” for Baumslag-Pride theorem for pro- $p$  groups: we consider a larger class of groups replacing the condition  $\text{def}(G) \geq 2$  by its weighted analogue  $\text{def}_W(G) > 0$ , but also relax the assumption on the subgroup  $H$ , only requiring finite  $W$ -index.

We remark that a positive answer to Problem 4 would yield a new solution to Zelmanov’s theorem about the existence of non-abelian free pro- $p$  subgroups in Golod-Shafarevich pro- $p$  groups.

**Problem 5.** *Let  $G$  be a Golod-Shafarevich pro- $p$  group. Is  $G$  SQ-universal, that is, does every countably based pro- $p$  group embed into some (continuous) quotient of  $G$ ?*

Recall that an abstract group is called SQ-universal if any finitely generated group (and hence any countable group) embeds into some quotient of  $G$ . If  $G$  is an abstract (resp. pro- $p$ ) group which maps onto a non-abelian free (resp. free pro- $p$ ) group, then  $G$  is obviously SQ-universal. A result of Hall and Neumann [Ne] shows that in the abstract case SQ-universality extends to overgroups of finite index (we expect that the same is true for pro- $p$  groups), and therefore abstract groups of deficiency at least two are SQ-universal by Baumslag-Pride theorem.

While the validity of Baumslag-Pride theorem for pro- $p$  groups is highly questionable, it is reasonable to conjecture that pro- $p$  groups of deficiency at least two are still SQ-universal. It is less likely that SQ-universality holds for all Golod-Shafarevich groups,

but we do not see any obvious indications of why this should be false. We note that the existence of torsion Golod-Shafarevich abstract groups means that Problem 5 would have negative answer in the category of abstract groups.

**Problem 6.** *Find a Golod-Shafarevich group of subexponential subgroup growth.*

There is almost no doubt that such groups exist. In fact, we expect that Golod-Shafarevich groups with property (T) described in Theorem 12.1 have subexponential subgroup growth. In any case, it would be interesting to compute (or at least estimate) subgroup growth for these groups. In the unlikely case that their subgroup growth is (at least) exponential, these groups would provide the first examples of Kazhdan groups with (at least) exponential subgroup growth.

**Problem 7.** *Find an interesting intermediate condition between being virtually Golod-Shafarevich and having positive power  $p$ -deficiency.*

This problem has already been discussed at the end of § 9.

**Problem 8.** *Establish new results about Golod-Shafarevich groups in characteristic zero.*

Let  $\Omega$  be the class of (abstract) groups which are Golod-Shafarevich in characteristic zero (see § 3.4 for the definition). Recall that every group in  $\Omega$  is also Golod-Shafarevich with respect to  $p$  for every prime  $p$ , and it seems that all known results about groups in  $\Omega$  follow from that fact. One obvious consequence is that given a group  $G$  in  $\Omega$ , for every  $n \in \mathbb{N}$  and every prime  $p$  there exists a finite index subgroup  $H = H(n, p)$  of  $G$  s.t.  $d_p(H) = d(H/[H, H]H^p) \geq n$ . It is natural to ask whether one can find such  $H(n, p)$  which is independent of  $p$ . Equivalently, is it true that for every  $n \in \mathbb{N}$ , there exists a subgroup  $H = H(n)$  of  $G$  s.t.  $d(H^{ab}) = d(H/[H, H]) \geq n$ ; in other words, does  $G$  have infinite virtual first Betti number?

The latter question is particularly interesting for free-by-cyclic groups  $F \rtimes \mathbb{Z}$  (with  $F$  free non-abelian). As mentioned at the end of § 3.4, a group  $G$  of this form is GS in characteristic zero whenever its first Betti number is at least two (this is equivalent to saying that  $G$  maps onto  $\mathbb{Z}^2$ ).

**Problem 9.** *Find a “direct” proof of non-amenability of Golod-Shafarevich groups.*

Recall that in [EJ2], non-amenability of GS groups follows from the fact that they possess infinite quotients with property (T) which, in turn, depends on the existence of a very concrete family of groups with property (T) (described in Theorem 12.8) which happen to be GGS with respect to many different weight functions. While the fact that an infinite group with property (T) is non-amenable is not a deep one, it does not seem that the groups from Theorem 12.8 provide the “real reason” for non-amenability of GS groups.

Finding a proof of non-amenability of GS groups which does not use property (T) is also of interest because it may shed some light on the following question of Vershik [Ve] which is still open.

**Question 14.1.** *Let  $G$  be a finitely generated group, let  $p$  be a prime, let  $M$  be the augmentation ideal of the group algebra  $\mathbb{F}_p[G]$ , and assume that the graded algebra  $\text{gr}_{\mathbb{F}_p}[G] = \bigoplus_{n=0}^{\infty} M^n/M^{n+1}$  has exponential growth. Does it follow that  $G$  is non-amenable?*

Corollary 4.3 implies that GS groups satisfy the above hypothesis, so a positive answer to Question 14.1 would provide a new proof of non-amenability of GS groups.

Our last problem deals with the Galois groups  $G_{K,p,S}$  defined in § 10. As explained in § 10.3, many such groups have an LRG (linear rank growth) chain, and it is natural to ask whether every chain is an LRG chain in those groups. Assuming that  $K, p$  and  $S$  are such that  $G_{K,p,S}$  is infinite, the following conditions are easily seen to be equivalent:

- (a)  $G_{K,p,S}$  has positive rank gradient.
- (b) Any (strictly) descending chain of open normal subgroups of  $G_{K,p,S}$  is an LRG chain.
- (c) Let  $K = K_0 \subset K_1 \subset \dots$  be a (strictly) ascending chain of finite Galois  $p$ -extensions of  $G$  unramified outside of  $S$ . Then the sequence  $\{\rho_p(K_n)\}$  of  $p$ -ranks of the ideal class groups of  $K_n$  grows linearly in  $[K_n : K]$ .

**Problem 10.** Assume that the group  $G_{K,p,S}$  is infinite and hypotheses of Theorem 10.5 hold. Determine whether the equivalent conditions (a), (b) and (c) above hold or fail (depending on the triple  $(K, p, S)$ ).

We are not aware of a single example where the answer to this question is known. We conjecture that conditions (a), (b), (c) always fail, that is, the group  $G_{K,p,S}$  always has zero rank gradient (under the above restrictions). This conjecture is based on the various known analogies between the groups  $G_{K,p,S}$  and hyperbolic 3-manifold groups (see, e.g., [Rez] and [Mo]). In particular, similarly to the groups  $G_{K,p,S}$ , many hyperbolic 3-manifold groups have LRG  $p$ -chains by Theorem 11.5. At the same time, very deep recent work of Wise on quasi-convex hierarchies combined with a theorem of Lackenby [La4, Theorem 1.18] implies that for every hyperbolic 3-manifold group  $G$  and every prime  $p$ , the  $p$ -gradient of  $G$  (equal to the rank gradient of  $G_{\widehat{p}}$ ) is zero.

## REFERENCES

- [An1] D. J. Anick, *Noncommutative graded algebras and their Hilbert series*. J. Algebra 78 (1982), no. 1, 120-140.
- [An2] D. J. Anick, *Generic algebras and CW complexes*. Algebraic topology and algebraic K-theory (Princeton, N.J., 1983), 247-321, Ann. of Math. Stud., 113, Princeton Univ. Press, Princeton, NJ, 1987.
- [AJN] M. Abert, A. Jaikin-Zapirain and N. Nikolov, *The rank gradient from a combinatorial viewpoint*, Groups Geom. Dyn. 5 (2011), no. 2, 213-230.
- [BL] Y. Barnea, M. Larsen, *A non-abelian free pro- $p$  group is not linear over a local field*. J. Algebra 214 (1999), no. 1, 338-341.
- [BaGr] L. Bartholdi and R. Grigorchuk, *Lie methods in growth of groups and groups of finite width*. Computational and geometric aspects of modern algebra (Edinburgh, 1998), 1-27, London Math. Soc. Lecture Note Ser., 275, Cambridge Univ. Press, Cambridge, 2000.
- [BP] B. Baumslag and S. Pride, *Groups with two more generators than relators*. J. London Math. Soc. (2) 17 (1978), no. 3, 425-426.
- [BHV] B. Bekka, P. de la Harpe and A. Valette, *Kazhdan's property (T)*. New Math. Monogr. 11, Cambridge Univ. Press, Cambridge, 2008.
- [Bu] J. Button, *Largeness of LERF and 1-relator groups*. Groups Geom. Dyn. 4 (2010), no. 4, 709-738.
- [BuTh] J. Button and A. Thillaisundaram, *Applications of  $p$ -deficiency and  $p$ -largeness*, Internat. J. Algebra Comput. 21 (2011), no. 4, 547-574.
- [DDMS] J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic pro- $p$  groups*. Second edition. Cambridge Studies in Advanced Mathematics, 61. Cambridge University Press, Cambridge, 1999.
- [DJ] J. Dymara and T. Januszkiewicz, *Cohomology of buildings and their automorphism groups*. Invent. Math. 150 (2002), no. 3, 579-627.
- [Ep] D.B.A. Epstein, *Finite presentations of groups and 3-manifolds*. Quart. J. Math. Oxford Ser. (2) 12 (1961), 205-212.
- [EJ1] M. Ershov and A. Jaikin-Zapirain, *Property (T) for noncommutative universal lattices*. Invent. Math. 179 (2010), no. 2, 303-347.

- [EJ2] M. Ershov, *Kazhdan quotients of Golod-Shafarevich groups*, with appendices by A. Jaikin-Zapirain, Proc. Lond. Math. Soc. 102 (2011), no. 4, 599-636.
- [EJ3] M. Ershov and A. Jaikin-Zapirain, *Groups of positive weighted deficiency*, to appear in J. Reine Angew. Math., arXiv:1007.1489.
- [Er1] M. Ershov, *Golod-Shafarevich groups with property (T) and Kac-Moody groups*, Duke Math. J. 145 (2008), no. 2, 309-339.
- [Er2] M. Ershov, *Kazhdan groups whose FC-radical is not virtually abelian*, preprint (2010).
- [FHT] M. Freedman, R. Hain and P. Teichner, *Betti number estimates for nilpotent groups*. Fields Medalists' lectures, 413-434, World Sci. Ser. 20th Century Math., 5, World Sci. Publ., River Edge, NJ, 1997.
- [GS] E. Golod and I. Shafarevich, *On the class field tower. (Russian)* Izv. Akad. Nauk SSSR Ser. Mat. 28 (1964), 261-272.
- [Go1] E. Golod, *On nil algebras and finitely approximable groups. (Russian)* Izv. Akad. Nauk SSSR Ser. Mat. 28 (1964), 273-276.
- [Go2] E. Golod, *Some problems of Burnside type. (Russian)* 1968 Proc. Internat. Congr. Math. (Moscow, 1966) pp. 284-289. Izdat. "Mir", Moscow.
- [Gr] R. I. Grigorchuk, *On Burnside's problem on periodic groups. (Russian)* Funktsional. Anal. i Prilozhen. 14 (1980), no. 1, 53-54.
- [Hab] K. Haberland, *Galois cohomology of algebraic number fields*, VEB Deutscher Verlag der h: Wissenschaften, Berlin, 1978.
- [Haj] F. Hajir, *On the growth of  $p$ -class groups in  $p$ -class field towers*. J. Algebra 188 (1997), no. 1, 256-271.
- [Ha] P. de la Harpe, *Uniform growth in groups of exponential growth*. Proceedings of the Conference on Geometric and Combinatorial Group Theory, Part II (Haifa, 2000). Geom. Dedicata 95 (2002), 1-17.
- [IySh1] N. Iyudu and S. Shkarin, *The Golod-Shafarevich inequality for Hilbert series of quadratic algebras and the Anick conjecture*. Proc. Roy. Soc. Edinburgh Sect. A 141 (2011), no. 3, 609-629.
- [IySh2] N. Iyudu and S. Shkarin, *Finite dimensional semigroup quadratic algebras with minimal number of relations*, preprint (2011), arXiv:1104.2029, accepted by Monatshefte für Mathematik.
- [KaMe] M. I. Kargapolov and Yu. I. Merzlyakov, *Osnovy teorii grupp. (Russian) [Fundamentals of group theory] Fourth edition*. Fizmatlit "Nauka", Moscow, 1996. 288 pp.
- [Ka] M. Kassabov, *On pro-unipotent groups satisfying the Golod-Shafarevich condition*. Proc. Amer. Math. Soc. 131 (2003), no. 2, 329-336.
- [Ko1] H. Koch, *Galois theory of  $p$ -extensions*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002. xiv+190 pp.
- [Ko2] H. Koch, *On  $p$ -extensions with restricted ramification*. Appendix 1 in [Hab].
- [Kos] A. I. Kostrikin, *On defining groups by means of generators and defining relations. (Russian)* Izv. Akad. Nauk SSSR Ser. Mat. 29 (1965), 1119-1122.
- [La1] M. Lackenby, *Covering spaces of 3-orbifolds*. Duke Math. J. 136 (2007), no. 1, 181-203.
- [La2] M. Lackenby, *New lower bounds on subgroup growth and homology growth*. Proc. Lond. Math. Soc. (3) 98 (2009), no. 2, 271-297.
- [La3] M. Lackenby, *Large groups, property  $(\tau)$  and the homology growth of subgroups*. Math. Proc. Cambridge Philos. Soc. 146 (2009), no. 3, 625-648.
- [La4] M. Lackenby, *Detecting large groups*. J. Algebra 324 (2010), no. 10, 2636-2657.
- [Laz] M. Lazard, *Groupes analytiques  $p$ -adiques. (French)* Inst. Hautes Études Sci. Publ. Math. 26 (1965), 389-603.
- [LR] D. D. Long and A. Reid, *Subgroup separability and virtual retractions of groups*, Topology 47 (2008), 137-159.
- [Lu1] A. Lubotzky, *Group presentation,  $p$ -adic analytic groups and lattices in  $SL_2(C)$* . Ann. of Math. (2) 118 (1983), no. 1, 115-130.
- [Lu2] A. Lubotzky, *On finite index subgroups of linear groups*. Bull. London Math. Soc. 19 (1987) 325-328.
- [LuMa1] A. Lubotzky and A. R. Magid, *Cohomology of unipotent and prounipotent groups*. J. Algebra 74 (1982), no. 1, 76-95.
- [LuMa2] A. Lubotzky and A. R. Magid, *Free prounipotent groups*. J. Algebra 80 (1983), no. 2, 323-349.
- [LuMa3] A. Lubotzky and A. R. Magid, *Cohomology, Poincaré series, and group algebras of unipotent groups*. Amer. J. Math. 107 (1985), no. 3, 531-553.

- [LuMn] A. Lubotzky and A. Mann, *Powerful  $p$ -groups. II.  $p$ -adic analytic groups*. J. Algebra 105 (1987), no. 2, 506-515.
- [LuS] A. Lubotzky and D. Segal, *Subgroup growth*. Progress in Mathematics, 212. Birkhäuser Verlag, Basel, 2003.
- [LuZ] A. Lubotzky and A. Zuk, *On property  $(\tau)$* , unpublished book, available at <http://www.ma.huji.ac.il/~alexclub/>
- [Ma] W. Magnus, *Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring*. (German) Math. Ann. 111 (1935), no. 1, 259-280.
- [Mo] M. Morishita, *On certain analogies between knots and primes*. J. Reine Angew. Math. 550 (2002), 141-167.
- [MyaOs] A. Myasnikov and D. Osin, *Algorithmically finite groups*. J. Pure and Appl. Alg. 215 (2011), no. 11, 2789-2796.
- [NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields. Second edition*. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 323. Springer-Verlag, Berlin, 2008. xvi+825 pp
- [Ne] W. Neumann, *The SQ-universality of some finitely presented groups*. Collection of articles dedicated to the memory of Hanna Neumann, I. J. Austral. Math. Soc. 16 (1973), 1-6.
- [NS] N. Nikolov and D. Segal, *On finitely generated profinite groups I, II*. Ann. of Math. (2) 165 (2007), no. 1, 171-238 and 239-273
- [NA] P. S. Novikov and S. I. Adyan, *Infinite periodic groups. I, II, III*. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 32 (1968), 212-244, 251-524, 709-731.
- [Ol1] A. Yu. Ol'shanskii, *An infinite group with subgroups of prime orders*, Izvestia Akad. Nauk SSSR, Ser. Matem., 44 (1980), N 2, 309-321 (in Russian); English translation: Math. USSR-Izv. 16 (1981), no. 2, 279-289.
- [Ol2] A. Yu. Ol'shanskii, *On the question of the existence of an invariant mean on a group*. (Russian) Uspekhi Mat. Nauk 35 (1980), no. 4(214), 199-200.
- [Ol3] A. Yu. Ol'shanskii, *Geometry of defining relations in groups*. Translated from the 1989 Russian original by Yu. A. Bakhturin. Mathematics and its Applications (Soviet Series), 70. Kluwer Academic Publishers Group, Dordrecht, 1991. xxvi+505 pp.
- [Os1] D. Osin, *Small cancellations over relatively hyperbolic groups and embedding theorems*. Ann. of Math. (2) 172 (2010), no. 1, 1-39.
- [Os2] D. Osin, *Rank gradient and torsion groups*. Bull. Lond. Math. Soc. 43 (2011), no. 1, 10-16.
- [Pi] D. I. Piontovskii, *Hilbert series and relations in algebras*. (Russian) Izv. Ross. Akad. Nauk Ser. Mat. 64 (2000), no. 6, 205-219; translation in Izv. Math. 64 (2000), no. 6, 1297-1311.
- [PP] A. Polishchuk and L. Positselski, *Quadratic algebras*. University Lecture Series, 37. American Mathematical Society, Providence, RI, 2005. xii+159 pp.
- [PV] S. Popa and S. Vaes, *On the fundamental group of  $\mathrm{II}_1$  factors and equivalence relations arising from group actions*. Quanta of maths, 519-541, Clay Math. Proc., 11, Amer. Math. Soc., Providence, RI, 2010.
- [Rez] A. Reznikov, *Three-manifolds class field theory (homology of coverings for a nonvirtually  $b_1$ -positive manifold)*. Selecta Math. (N.S.) 3 (1997), no. 3, 361-399.
- [Ro] P. Roquette, *On class field towers*. 1967 Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965) pp. 231-249.
- [Sch1] A. Schmidt, *Circular sets of prime numbers and  $p$ -extensions of the rationals*. J. Reine Angew. Math. 596 (2006), 115-130.
- [Sch2] A. Schmidt, *Rings of integers of type  $K(\pi, 1)$* . Doc. Math. 12 (2007), 441-471.
- [Sch3] A. Schmidt, *Über pro- $p$ -fundamentalgruppen markierter arithmetischer kurven*. (German) [On pro- $p$  fundamental groups of marked arithmetic curves] J. Reine Angew. Math. 640 (2010), 203-235, English translation available at arXiv:0806.1863
- [Sh] I. Shafarevich, *Extensions with prescribed ramification points*. (Russian) Inst. Hautes Études Sci. Publ. Math. No. 18 (1963), 71-95.
- [SP] J.-C. Schlage-Puchta, *A  $p$ -group with positive rank gradient*. J. Group Th. 15 (2012), no. 2, 261-270.
- [Uf] V. Ufnarovskii, *Combinatorial and asymptotic methods in algebra* (Russian), Current problems in mathematics. Fundamental directions 57, 5-177, Itogi Nauki i Tekhniki, Akad. Nauk SSSR, Moscow, 1990
- [Ve] A. Vershik, *Amenability and approximation of infinite groups*. Selected translations. Selecta Math. Soviet. 2 (1982), no. 4, 311-330.

- [Vi] E. B. Vinberg, *On the theorem concerning the infinite-dimensionality of an associative algebra. (Russian)* Izv. Akad. Nauk SSSR Ser. Mat. 29 (1965), 209-214.
- [Vo] T. Voden, *Subalgebras of Golod-Shafarevich algebras.* Internat. J. Algebra Comput. 19 (2009), no. 3, 423-442.
- [Wi1] J. Wilson, *Finite presentations of pro- $p$  groups and discrete groups.* Invent. Math. 105 (1991), no. 1, 177-183.
- [Wi2] J. Wilson, *Profinite groups.* London Mathematical Society Monographs. New Series, 19. The Clarendon Press, Oxford University Press, New York, 1998.
- [Wis1] J. Wisliceny, *Zur Darstellung von Pro- $p$ -Gruppen und Lieschen Algebren durch Erzeugende und Relationen. (German) [On the presentation of pro- $p$ -groups and Lie algebras by generators and relations]* Math. Nachr. 102 (1981), 57-78
- [Wis2] J. Wisliceny, *Konstruktion nilpotenter assoziativer Algebren mit wenig Relationen. (German) [Construction of nilpotent associative algebras with few relations]* Math. Nachr. 147 (1990), 75-82
- [Zel1] E. Zelmanov, *On groups satisfying the Golod-Shafarevich condition.* New horizons in pro- $p$  groups, 223-232, Progr. Math., 184, Birkhäuser Boston, Boston, MA, 2000
- [Ze2] E. Zelmanov, *Some open problems in the theory of infinite dimensional algebras.* J. Korean Math. Soc. 44 (2007), no. 5, 1185-1195.

UNIVERSITY OF VIRGINIA

*E-mail address:* `ershov@virginia.edu`