GROUP PRESENTATIONS AND p-ADIC ANALYTIC GROUPS

GAL PORAT

In this talk, I will first present the Golod-Shafarevich theorem about finite p-groups; then I will present a generalization of the theorem to to p-adic analytic pro p-groups. Finally I will show some applications to presentations of discrete groups. This talk is based in full on the article "Group presentation, p-adic analytic groups and lattices in $SL_2(\mathbb{C})$" by Alex Lubtozky.

1 Notation and preliminaries

Recall that a pro-p group is an inverse limit of finite p-groups. When given a discrete group Γ, taking the inverse limit $\underset{\leftarrow}{lim}\Gamma/N$ where N is a normal subgroup of index a finite power of p yields pro-p group called the pro-p completion of Γ. We denote it by $\Gamma_{\hat{p}}$. It is characterized by a universal property: every homomorphism from Γ to a pro-p group G factors uniquely through $\Gamma_{\hat{p}}$ to a continuous homomorphism.

For a finitely generated group, $d(G)$ denotes the minimal number of topological generators. The Frattini subgroup $\Phi(G)$ is defined as the intersection of all the maximal open subgroups of G. It is elementary to show that $d(G) = d(G/\Phi(G))$. If G is a pro-p group, then $\Phi(G) = \overline{[G,G]G^p}$ so that $d(G) = dim_{\mathbb{F}_p}(G/\Phi(G))$.

A presentation of a finitely generated pro-p group G is a pair $<X;R>$ where $|X|$ is finite and $\hat{F_p}/«R» \simeq G$ for the pro-p completion of the free group on $|X|$ generators, i.e. $\hat{F_p} = (F[X])_{\hat{p}}$.

Finally, a pro-p group is said to be p-adic analytic if it has the structure of a manifold over $\mathbb{Q}_p$ that is compatible with the group structure. A finite p-group is p-adic analytic, and so is $\mathbb{Z}_p$.

2 The Golod-Shafarevich Theorem and its generalization

Theorem (Golod-Shafarevich). *Let G be a finite p-group with minimal presentation $<X;R>$(in the usual sense). Then $|R| \geq \frac{|X|^2}{4}$.*

Remark: the inequality is in fact strict whenever $G \neq 1$.

I will not present here the proof of this theorem, but we will discuss a certain portion of it when we talk about the generalization. The proof I know of mainly uses cohomology of groups.

Side note: the originial motivation for this theorem is from number theory. It can be used to construct an infinite tower of Hilbert class field extensions, thus answering to the negative a conjecture of Furtwangler.

The following is a generaliztaion of the previous theorem for p-adic analytic groups.

Theorem (Lubotzky). *Let G be a p-adic analytic pro-p group different from the p-adic integers $\mathbb{Z}_p$. If $<X;R>$ is a minimal presentation of G then*

$$|R| \geq \frac{|X|^2}{4}$$

It can also be shown that that is inequality is strict except for three exceptional cases.

(very) Partial proof: we set some notation. Put $d = |X|, r = |R|$. Let $G = \lim_{\leftarrow} G_i$ where the G_i are finite p-groups. Define $B = \mathbb{F}_p[[G]] = \underset{\leftarrow}{lim}\mathbb{F}[G_i]$. Let $I(G) = Ker(B \overset{sum}{\to} \mathbb{F}_p)$ (the augmentation ideal) and $C_n(G) = dim_{\mathbb{F}_p} B/\overline{I(G)^n}$. We will take it as a fact that if $\sum C_n(G)t^n$ is absolutely convergent for $0 \leq t < 1$ then $\varphi(t) = 1 - dt + rt^2 > 0$ for $0 \leq t < 1$. In the proof for the Golod-Shafarevich theorem, it is shown that the series $\sum C_n(G)t^n$ satisfies the convergence condition by commenting that $C_n(G) = |G|$ for large enough n. By a result of Lazard, a finitely generated pro-p group is p-adic analytic if and only if $C_n(G)$ has polynomial growth. Hence the convergence condition is still satisfied for a general p-adic analytic group, so we have $\varphi(t) = 1 - dt + rt^2 > 0$ for $0 \leq t < 1$ (the reader may now safely forget about the origin of this $\varphi(t)$).

Setting $t = 1$ we see that $1 - d + r \geq 0$, i.e. $r \geq d - 1$. If $r = 0$,$d = 1$ this is the case $\mathbb{Z}_p$. If $r = 0, d = 0$ this clearly satisfies the theorem. We can now assume that $r > 0$. Suppose by contradiction that $r < \frac{d^2}{4}$. Plugging $t_0 = \frac{d}{2r}$ into $\varphi(t)$ gives $t_0 \leq 0$, which is possible only if $t_0 \geq 1$, i.e. $d \geq 2r$. But we also have that $r \geq d - 1$, so we must have $d = 2, r = 1$. But in this case $r = \frac{d^2}{4}$, so this is a contradiction, and we're done.

3 Presentations of pro-p completions

For the next theorem, we first prove two Lemmas.

Lemma 1. *Let G be a finitely generated pro-p group and let $<X;R>$ be a presentation of G. Then there is a minimal presentaion $<Y;S>$ of G such that $|S| - |Y| = |R| - |X|$. (we can change a given presentation to a minimal presentation without changing the difference between the number of relations and generators).*

Proof. Let $F = \hat{F} < X >$ be the free pro-p group on the elements of $|X|$. Then there is an epimorphism $\varphi : F \twoheadrightarrow G$ with kernel «R». This induces a map $\overline{\varphi} : F/\Phi(F) \to G/\Phi(G)$ (it is easy to see that $\varphi([F,F]F^p) = [G,G]G^p$, with or without closures). Let $M/\Phi(F)$ be the kernel of $\overline{\varphi}$. Notice that this is then a subspace of the $\mathbb{F}_p$ vector space $F/\Phi(F)$.

I claim that this subspace is generated by the image of R. To see this, consider the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Phi(F) & \longrightarrow & F & \longrightarrow & F/\Phi(F) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \varphi|_{\Phi(F)}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \overline{\varphi}} & & \\ 1 & \longrightarrow & \Phi(G) & \longrightarrow & G & \longrightarrow & G/\Phi(G) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 1 & & 1 & & 1 & & \end{array} \qquad (1)$$

This has exact rows and columns (the left map is onto because $\varphi([F,F]F^p) = [G,G]G^p$). The snake lemma is valid in the category of groups whenever the vertical maps have cokernels (the proof is the same). We then have an exact sequence $1 \to ker\varphi|_{\Phi(F)} \to ker\varphi \to ker\overline{\varphi} \to 1$, so $ker\varphi$ surjects onto $ker\overline{\varphi}$ which is the same as saying that R generates $M/\Phi(F)$.

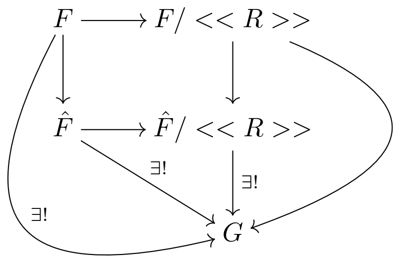
Now let $r_1\Phi(F), ..., r_k\Phi(F)$ be a basis for $M/\Phi(F)$ where $r_1, ..., r_k \in R$. By linear algebra $k = d(F) - d(G)$. Extend $r_1\Phi(F), ..., r_k\Phi(F)$ to a basis $r_1\Phi(F), ..., r_k\Phi(F), y_1\Phi(F), ..., y_m\Phi(F)$ of $F/\Phi(F)$. Then $r_1, ..., r_k, y_1, ..., y_m$ generate F by the property of $\Phi(F)$, and since a finitely generated free group is Hopfian this must be a free basis for F. Hence we have a free pro-p group $F' = \hat{F} < y_1, ..., y_m >= F/<r_1, ..., r_k>$, so that $d(F') = d(F) - k = d(G)$, and F' surjects on G. Take S as the image of $R \backslash \{r_1, ..., r_k\}$ in F'; then $|S| \leq |R| - k$, and we can add trivial relations to make this an equality. Then $F' \to G$ is a minimal presentation and by construction $|S| - d(F') = |R| - k - (d(F) - k) = |R| - d(F)$.

□

Lemma 2. *Let Γ be a discrete group, $<X;R>$ a presentation of Γ with $|X|$ finite. Then $<X;R>$ is also a presentation for its pro-p completion $\Gamma_{\hat{p}}$.*

Proof. We check this has the universal property of the completion. To see this, we write $F = F(X)$ as the discrete free group on the elements of X, and $\hat{F}$ for its pro-p completion. We can then write $\Gamma = F/ << R >>$. Suppose G is a pro-p group and we have a map F/«R» $\to G$. One has a commutative diagram consisting of $F \to F/$«R» $\to G$, thus giving a unique map from $\hat{F}$ and hence a unique map from $\hat{F}/$«R», which is what we wanted to prove.

In a diagram this looks like this:



(2)

∎

Theorem. *Let Γ be a discrete group with a finite presentation $< X; R >$. Assume $\Gamma_{\hat{p}}$ is p-adic analytic but not isomorphic to $\mathbb{Z}_p$. Then*

$$|R| - (|X| - d(\Gamma_{\hat{p}})) \geq d(\Gamma_{\hat{p}})^2/4$$

Proof. By Lemma 2, the given presentation is also a presentation for $\Gamma_{\hat{p}}$. By Lemma 1, we can replace the given presentation by a minimal presentation of $\Gamma_{\hat{p}}$ with $s = |R| - (|X| - d(\Gamma_{\hat{p}}))$ relations.
The extension of the Golod-Shafarevich theorem now gives

$$|R| - (|X| - d(\Gamma_{\hat{p}})) = s \geq \frac{d(\Gamma_{\hat{p}})^2}{4}$$

∎

4 Minimal presentations of finitely generated nilpotent groups

Proposition 1. *For any finitely generated group Γ there is a prime p such that $d_{ab}(\Gamma) = d(\Gamma_{\hat{p}})$.*

Proof. First we claim that $d(\Gamma_{\hat{p}}) = d(\Gamma/[\Gamma,\Gamma]\Gamma^p)$.
Let H be the Frattini subgroup of $\Gamma_{\hat{p}}$, i.e. $H = [\Gamma_{\hat{p}}, \Gamma_{\hat{p}}]\Gamma_{\hat{p}}^p$. We then have $\Gamma_{\hat{p}}/H \simeq (\Gamma/[\Gamma,\Gamma]\Gamma^p)_{\hat{p}}$, because completion commutes with the quotient by a normal subgroup. Notice now that $\Gamma/[\Gamma,\Gamma]\Gamma^p$ is just a finite abelian p-group, so its completion is isomorphic to itself. It follows that $d(\Gamma_{\hat{p}}) = d(\Gamma_{\hat{p}}/H) = d((\Gamma/[\Gamma,\Gamma]\Gamma^p)_{\hat{p}}) = d(\Gamma/[\Gamma,\Gamma]\Gamma^p)$.
Now write $\Gamma/[\Gamma,\Gamma] \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus ... \oplus \mathbb{Z}/d_r\mathbb{Z} \oplus \mathbb{Z}^k$, where $d_1 \mid ... \mid d_r$ so $d_{ab}(\Gamma) = r + k$. Let p be such that $p|d_1$ (or $p = 2$ if $\Gamma/[\Gamma,\Gamma]$ is torsion free), then clearly $\Gamma/[\Gamma,\Gamma]\Gamma^p$ is a vector space of dimension $r+k$ over $\mathbb{F}_p$, hence also $d(\Gamma/[\Gamma,\Gamma]\Gamma^p) = r + k$.
So in conclusion, we have $d(\Gamma_{\hat{p}}) = d(\Gamma/[\Gamma,\Gamma]\Gamma^p) = r + k = d_{ab}(\Gamma)$.

∎

We want to say something strong on nilpotent groups. For this we will do two things: to show that in that case every $\Gamma_{\hat{p}}$ is p-adic analytic and to relate $d_{ab}(\Gamma)$ with $d(\Gamma)$.

Lemma (without proof). *If* $1 \to \Gamma' \to \Gamma \to \Gamma'' \to 1$ *is an exact sequence with* $\Gamma'_{\hat{p}}, \Gamma''_{\hat{p}}$ *p-adic analytic, then so is* $\Gamma_{\hat{p}}$.

Proposition 2. *Let* Γ *be a finitely generated solvable noetherian group (every subgroup is finitely generated). Then* $\Gamma_{\hat{p}}$ *is p-adic analytic for every p.*

Proof. Since Γ is solvable, there is a series of subgroups $1 \lhd N_1 \lhd ..., \lhd N_k \lhd \Gamma$, with each N_{i+1}/N_i abelian. Since Γ is noetherian, each N_{i+1}/N_i is finitely generated, so we can refine this enough so that each N_{i+1}/N_i is cyclic. For a cyclic group it is clear that its pro-p completion is always p-adic analytic, so by the previous lemma we get that if for N_k the pro-p completion is p-adic analytic then so is $\Gamma_{\hat{p}}$. Now use induction on the length of the composition series.

□

Lemma 3. *Let* Γ *be a finitely generated nilpotent group, then* $d(\Gamma) = d_{ab}(\Gamma)$.

Proof. Since $d(\Gamma) = d(\Gamma/\Phi(\Gamma)), d(\Gamma^{ab}) = d(\Gamma^{ab}/\Phi(\Gamma^{ab}))$, it is enough to show that $\Gamma/\Phi(\Gamma) \simeq \Gamma^{ab}/\Phi(\Gamma^{ab})$. Recall that an epimorphism $G \to H$ always factors to a map $G/\Phi(G) \to H/\Phi(H)$. It is known that for a nilpotent group, $[\Gamma, \Gamma] \subset \Phi(\Gamma)$. Therefore there is an epimorphism $\Gamma^{ab} \to \Gamma/\Phi(\Gamma)$ which factors to a map $\Gamma^{ab}/\Phi(\Gamma^{ab}) \to \Gamma/\Phi(\Gamma)$. On the other hand, the epimorphism $\Gamma \to \Gamma^{ab}$ factors to a map $\Gamma/\Phi(\Gamma) \to \Gamma^{ab}/\Phi(\Gamma^{ab})$, and these two maps are clearly inverses.

□

Theorem. *If* Γ *is a finitely generated nilpotent group different from* $\mathbb{Z}$, *and* $< X; R >$ *is a minimal presentation for* Γ, *then* $|R| \geq \frac{|X|^2}{4}$.

Proof. It is known that a finitely generated nilpotent group is solvable and noetherian. Hence by the previous propsition each $\Gamma_{\hat{p}}$ is p-adic analytic. Moreover, there is some p such that $d(\Gamma_{\hat{p}}) = d_{ab}(\Gamma)$, which equals $d(\Gamma)$ by the previous lemma. Moreover, if $\Gamma_{\hat{p}} = \mathbb{Z}_p$, then $d(\Gamma_{\hat{p}}) = d(\Gamma) = 1$, which is possible only if Γ is cyclic. In that case we can't have $\Gamma = \mathbb{Z}$, so Γ is finite and cyclic in which case the inequality clearly holds. Otherwise, by the previous theorem we have $|R| - (|X| - d(\Gamma)) \geq d(\Gamma)^2/4$. But $d(\Gamma) = |X|$ by definition, so $|R| \geq \frac{|X|^2}{4}$.

□