Nilpotent Groups Have Polynomial Growth

January 15, 2020

Theorem 1. *Let G be a finitely generated nilpotent group. Then G has polynomial growth.*

Proof. We proceed by induction on the length of the lower central series. If G is abelian on m generators $\{g_1, \dots, g_m\}$ then the elements in the ball of radius x around the identity are the elements made of n_i g_is for each i with $n_1 + \ldots + n_m \leq x$. Padding out with the identity element, which we say there are n_0 of, this is the number of ways of picking nonnegative integers $n_0, n_1, \dots, n_m$ with $n_0 + \cdots + n_m = x$. This is the same as the number of ways of picking positive integers with $n_i + 1$ with $(n_0 + 1) + \cdots + (n_m + 1) = x + m$. This is the number of ways of breaking up the distance $x + m$ with m fenceposts into positive integer distance lengths, which is $\binom{x+m}{m}$. We have not yet considered relations, so what we have is an upper bound:

$$\beta_G(x) \leq \binom{x+m}{m} = \frac{(x+m)!}{m!x!} \asymp x^m.$$

Let's do an example of how the induction step works.

Suppose G, generated by $\{g_1, \dots, g_m\}$ is a 2-step nilpotent group, that is, $[G, G]$ lies in the centre of the group. Take a product g of at most x generators, and add occurences of the identity to the start of the element until it is a word of length x in $\{1, g_0, \dots, g_m\}$. Exchanging two elements of this set may produce a commutator on the right:

$$gh = hg[g^{-1}, h^{-1}]$$

and this commutator lies in the center. So we can take our group element, and "move left" all occurences of g_1 over until all of the occurences of g_1 occur immediately after all occurences of the identity, and then do the same with g_2 and keep going. There are at most x generators to move to a new place, and they have to be commuted with at most x other generators, and the produced commutators. They commute with the produced commutators, so there are at most x^2 commutators produced by this process. So, we may write our group element in the form

$$g = 1^{n_0} g_1^{n_1} \cdots g_m^{n_m} C$$

where $n_0 + \cdots + n_m = x$ and C is a product of at most m^2 commutators.

In this case $[G,G]$ is generated by $[g_i^{\pm 1}, g_j^{\pm 1}]$ for $1 \le i < j \le m$ and the commutators are words of length 1 in the generators of $[G,G]$. By induction, the derived subgroup has polynomial growth. Let the degree of this growth be D.

We then have a bound of $\binom{x+m}{m} \asymp x^m$ elements of the form $1^{n_0} g_1^{n_1} \cdots g_m^{n_m}$ as above, and C is a word of length at most m^2 in an abelian group of polynomial growth degree D. Therefore, there are $\asymp (x^2)^D = x^{2D}$ words of this form in $[G,G]$, and the total number of possible elements is $\asymp x^{m+2D}$.

Now let's do the full induction step. Suppose G is a group with derived series having length n, so that $[G,[G,G]]$ has polynomial growth by induction and derived series length $n-1$.

Take a product g of at most x generators, and multiply on the left by the identity until we have a word of length x in the alphabet $\{1, g_1, \ldots, g_m\}$.

Again, rewrite this so that g has all occurrences of 1, then all occurrences of g_1, etc. This involves:

- producing at most x^2 commutators $[g_i, g_j]$ moving generators of low index to the left;
- moving all x generators past each of these x^2 commutators at most once, leaving x^3 elements of the form $[x_i,[x_j,x_k]]$;
- $\ldots$
- moving x generators past $\le x^{n-2}$ elements of the form $[g_{i_1}[\cdots[g_{i_{n-3}}, g_{i_{n-2}}]]\cdots]$, producing at most x^{n-1} elements of the form $[g_{j_1}[\cdots[g_{j_{n-2}}, g_{j_{n-1}}]]\cdots]$ on the right.
- nothing else, because elements of the form $[g_{i_1}[\cdots[g_{i_{n-2}}, g_{i_{n-1}}]]\cdots]$ lie in the centre.

So we can rewrite g in the form

$$1^{i_0} g_1^{i_1} \cdots g_m^{i_m} C$$

. C is a product of at most $x^n + x^{n-1} + \cdots + x^2 \le ax^n$ elements of $[G,G]$, all of which are of the form $[g_{j_1}[\cdots[g_{j_{k-1}}, g_{j_k}]\cdots]]$. These are in a subgroup generated by the commutators of depth at most $n-1$, and in these generators C is a word of length at most ax^n.

Since $[G,G]$ has polynomial growth of degree D, there are at most $(ax^n)^D \asymp x^n D$ such elements possible. As previously, there are at most $\binom{x+m}{m} \asymp x^m$ elements of the form $1^{i_0} g_1^{i_1} \cdots g_m^{i_m}$ so overall we have $\prec x^{m+nD}$ elements of the form $1^{i_0} g_1^{i_1} \cdots g_m^{i_m} C$ with $i_0 + \cdots + i_m = x$. So, $\beta_G(x) \prec x^{m+nD}$. $\square$