İSTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

GROWTH OF GROUPS

M.Sc. Thesis by
Ulaş KARADAĞ

Department : Mathematics

Programme: Mathematics Engineering

Supervisor : Prof. Dr. Ulviye BAŞER

JANUARY 2008

İSTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

GROWTH OF GROUPS

M. Sc. Thesis by
Ulaş KARADAĞ
(509051008)

Date of submission : 24 December 2007
Date of defence examination: 21 January 2008

Supervisor : Prof. Dr. Ulviye BAŞER
Members of the Examining Committee: Prof. Dr. Vahap ERDOĞDU (İ.T.Ü.)
Assoc. Prof. Dr. İlhan İKEDA (İ.B.Ü.)

JANUARY 2008

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

GRUPLARIN BÜYÜMESİ

YÜKSEK LİSANS TEZİ

Ulaş KARADAĞ
(509051008)

Tezin Enstitüye Verildiği Tarih : 24 Aralık 2007
Tezin Savunulduğu Tarih : 21 Ocak 2008

Tez Danışmanı : **Prof. Dr. Ulviye BAŞER**
Diğer Jüri Üyeleri: **Prof.Dr. Vahap ERDOĞDU (İ.T.Ü.)**
Yrd. Doç. Dr. İlhan İKEDA (İ.B.Ü.)

OCAK 2008

ACKNOWLEDGMENTS

I would like to pay my gratitude to my advisors Prof. Dr. Oleg Belegradek and Prof. Dr. Ulviye Başer for their support and encouragement during the preparation of this work.

January, 2008 Ulaş Karadağ

CONTENTS **Page No**

FIGURE LIST **Page No**

SYMBOL LIST

G: A finitely generated group

S : A generating set of a group

l_S: Length function

γ_G: Growth function

$[G : H]$: Index of subgroup

$\times$: Cartesian or direct product

$\oplus$: Direct sum

$\sim$: Equivalence of functions

F_m: Free group

$\mathbb{Z}$: The set of integers

$\rtimes$: Semi-direct product

$\leqslant$: Subgroup

$\triangleleft$: Normal subgroup

$\wr$: Wreath product

$[g, h]$: Commutator of g and h

G^n: Derived series of G

$Z(G)$: Center of G

GROWTH OF GROUPS

SUMMARY

In this study we consider basic notions and examples in the theory of growth of finitely-generated groups. In particular, we find the growth rate in case of important examples of finitely-generated nonabelian free groups, finitely generated abelian groups, the Heisenberg group(which is a finitely generated nilpotent group), and the group $\mathbb{Z}_2 \wr \mathbb{Z}$ (which is a finitely generetad solvable non-nilpotent group). This notion, growth of a group, was introduced by John Milnor in journal of differential geometry in 1968.
Firstly, we define the Cayley graph of a finitely-generated group G with respect to a generating set S. Then we introduce a metric on the Cayley graph of G. After that we define the length function on G by using this metric. Then we define the growth function of G. The growth function has some basic properties: it is always submultiplicative and it is monotone increasing under the assumption that G is infinite. After giving the definition of the equivalence of functions over the natural numbers we show that growth functions are equivalent for any generating set.
There are three types of groups according to their growth functions: groups of polynomial growth, groups of exponential growth, and groups of intermediate growth. In 1968 John Milnor possed a problem of existence of finitely generated groups of intermediate growth, that is, of growth strictly between exponential growth and polynomial growth. This question was open for many years. In 1983, this problem was positively solved by Rostivlav Grigorchuk, i.e. he constructed a group that has intermediate growth. At the end of this work we give construction.

GRUPLARIN BÜYÜMESİ

ÖZET

Bu çalışmada sonlu üreteci var olan grupların büyüme fonksiyonları teorisindeki temel kavramlar ve örnekler üzerinde duruyoruz. Özellikle sonlu üreteci var olan değişmeli olmayan özgür grupların, sonlu üreteci var olan değişmeli grupların, Heisenberg grubunun(sonlu üreteci var olan nilpotent grup) ve $\mathbb{Z}_2 \wr \mathbb{Z}$ grubunun (sonlu üreteci var olan nilpotent olmayan çözülebilir grup) büyüme oranlarını hesaplıyoruz.
Bu kavram, grupların büyümesi, ilk olarak 1968 yılında John Milnor tarafından diferansiyel geometri alanındaki bir dergide yer almıştır.
İlk olarak sonlu üreteci var olan bir grubun G bir üreteç kümesine bağlı olarak grubun Cayley çizelgesinin tanımını veriyoruz. Sonra G grubunun Cayley çizelgesi üzerinde bir metrik tanımlıyoruz. Daha sonra bu metrik yardımıyla G grubunun uzunluk fonksiyonunun tanımını veriyoruz. Uzunluk fonksiyonunu kullanarak G grubunun büyüme fonksiyonunu tanımlıyoruz. Büyüme fonksiyonları bazı temel özelliklere sahiptir: Büyüme fonksiyonları herzaman alt çarpımsaldır ve G grubunun sonsuz çoklukta elemena sahip olması durumunda sürekli artan bir fonksiyondur. Doğal sayılar kümesi üzerinde tanımlı fonksiyonların birbirilerine denk olma koşulunun tanımını verdikten sonra sonlu çoklukta üreteci var olan bir grubun büyüme fonksiyonlarının birbirilerine denk olduğunu gösteriyoruz. Büyüme fonksiyonlarına göre üç farklı grubun varlığı söz konusudur: Büyüme fonksiyonu polinom derecesinde olan gruplar, büyüme fonksiyonu üstel fonksiyon derecesinde olan gruplar ve büyüme fonksiyonu orta büyüklüğe sahip olan gruplar. 1968 yılında John Milnor orta büyüklüğe sahip olan grupların varlığını sorguladı, yani orta büyüklüğe sahip gruplar var mıydı? Bu sorunun cevabı uzun yıllar boyunca yanıtsız kaldı. Nihayet Rostislav Grigorchuk 1983 yılında bu soruyu olumlu olarak cevapladı. Grigorchuk orta büyüklüğe sahip bir grup inşaa etti. Bu çalışmanın sonunda Grigorchuk'un bu inşaasını ele almaktayız.

1. INTRODUCTION

The notion of the growth of a finitely generated group was introduced by John Milnor in [7] in journal of differential geometry in 1968.

For a finite set of generators A of a group G and a positive integer n, the ball of radius n with the center in 1 in the Cayley graph of G with respect to the generating set A is a finite set; let $\gamma_A^G(n)$ denote its cardinality. It is easy to see that the growth rate of the function $n \longmapsto \gamma_A^G(n)$ at infinity does not depend on the choice of the finite generating set A.

The initial observations were that the growth of any finitely generated group is at most exponential, and any finitely generated nonabelian free group is of exponential growth. On the other hand, any finitely generated abelian group is of polynomial growth.

John Milnor and Joseph Wolf showed in 1968 that any finitely generated solvable group either has exponential growth or is virtually nilpotent. H. Bass proved in 1971 that any virtually nilpotent group is of polynomial growth. M. Gromov in 1981 proved the converse of that result: any finitely generated group of polynomial growth is virtually nilpotent.

These results of J. Milnor, J. Wolf and H. Bass show that any finitely generated solvable group has either exponential or polynomial growth. Already in 1968 J. Milnor[8] posed a problem of existence of finitely generated groups of intermediate growth, that is, of growth strictly between exponential growth and polynomial growth. The problem was positively solved by Rostislav Grigorchuk[6] in 1983.

In this work we consider basic notions and examples in the theory of growth of groups, and give proofs of their properties. In particular, we find the growth rate in case of important examples of finitely generated nonabelian free groups, finitely generated abelian groups, the Heisenberg group (which is a finitely generated nilpotent group), the wreath product of $\mathbb{Z}_2$ and $\mathbb{Z}$ (which is a finitely generated solvable non-nilpotent group).

2. GROWTH OF A FINITELY GENERATED GROUP

2.1 Length Function

Let G be a group generated by a fixed finite set S. Elements of the form $w = a_1 a_2 ... a_n$, where each a_i is s or s^{-1} for some $s \in S$, are called group words over S. We denote n by $|w|$ and we call it the word length of the group word w. Any such word w represents an element of the group G. Since S generates G, any element g of G is represented by some such w (not in a unique way). Among the the words representing g in G there is a group word w with the smallest length $|w|$; we call the word w the shortest decomposition of g in generators S. In general, the shortest decomposition of g in generators S is not unique, but clearly the lengths of all shortest decomposition of g in generators S are the same.

Definition 2.1.1: Let G be a finitely generated group with generating set $S = \{s_1, ..., s_k\}$. For each element $g \in G$, we define the length of g with respect to the generating set S to be the length of the shortest decomposition

$$g = s_{i_1}^{\varepsilon_1} s_{i_2}^{\varepsilon_2} ... s_{i_n}^{\varepsilon_n} \tag{2.1}$$

where $\varepsilon_k = \pm 1$ and $s_{i_j} \in S$ for all $k, j = 1, ..., n$. We denote this length function by $l_S(g)$.

For example, if $S = \{a, b\}$, and $g = a^{-2}bab$ then $l_S(g) = 5$.

2.2 Cayley Graphs

Definition 2.2.1: Let G be a finitely generated group. The Cayley graph of G with respect to the generating set $X = \{g_1, g_2, ..., g_n\}$ is the graph $\Gamma = (V, E)$ whose vertices V are the elements of G and whose edges determined by the following condition: if $x, y \in V = G$, then $(x, y) \in E$ if and only if either $y = g_i x$ or $x = g_i y$ for some $i = 1, ..., n$.

Example: Let $G = S_3 = \langle s_1, s_2 \rangle$ where $s_1 = (12)$ and $s_2 = (23)$. Then the Cayley graph of G with respect to $X = \{s_1, s_2\}$ is

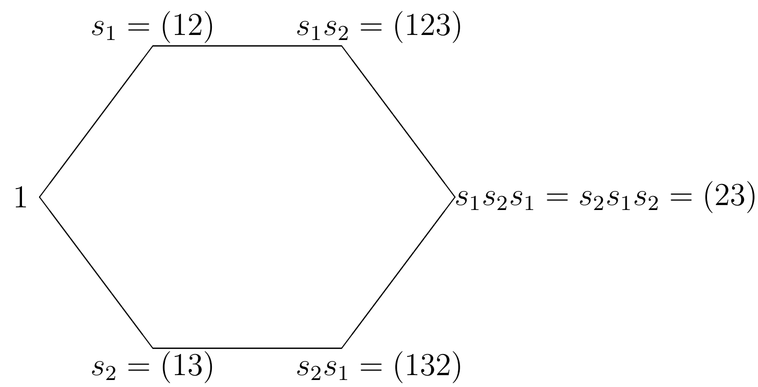

Figure 1: The Cayley graph of S_3

Example: Let $G = \mathbb{Z}_n = \langle \bar{1} \rangle$. Then the Cayley graph of G is

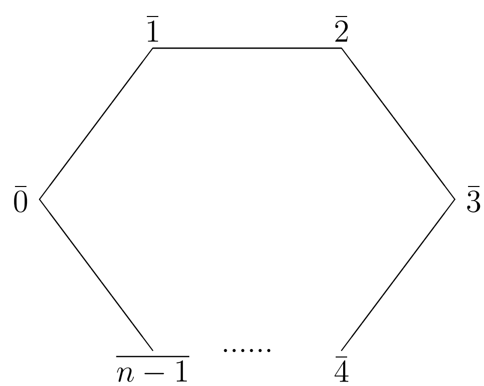

Figure 2: The Cayley graph of $\mathbb{Z}_n$

A Cayley graph of a group G can be considered as a metric space with $d(x, y), x, y \in G$, being the minimum of number of edges that one must traverse to get x from y. Thus, if G is a finitely generated group with generating set S, then we have $l_S(g) = d(e, g)$ for any $g \in G$.

In the Cayley graph of $S_3 = \langle s_1, s_2 \rangle$ we see that $l(1) = d(1, 1) = 0$, and the element $s_2 s_1$ can be obtained by either multiplying s_2 from the right with s_1 or multiplying $s_1 s_2 s_1$ from the right with s_1. But $l(s_2 s_1) = d(1, s_2 s_1) = 2$.

2.3 Growth Function:

For a finite set of generators S of a group G and a positive integer n, the ball of radius n with the center in 1 in the Cayley graph of G with respect to the generating set S is finite.

Definition 2.3.1: For each $n \in \mathbb{N}$ we define the growth function of a finitely generated group G with respect to the generating set S, denoted by $\gamma(n) = \gamma_G^S(n)$, to be the number of elements of $g \in G$ such that $l_S(g) \leq n$ i.e.,

$$\gamma_G^S(n) = \sharp\{g \in G : l_S(g) \leq n\} \tag{2.2}$$

the cardinality of the ball with radius n centered at 1.

The growth rate of this function $n \longmapsto \gamma_G^S(n)$ at infinity does not depend on the choice of the finite generating set S.

Lemma 2.3.1: Let G be a finitely generated infinite group. Then the growth function is monotone increasing: $\gamma(n+1) > \gamma(n)$ for all $n \geq 1$.

Proof 2.3.1: Suppose not. So there exists $m \in \mathbb{N}$ such that $\gamma(m+1) \leq \gamma(m)$. Since

$$\begin{aligned}\gamma(m+1) &= \sharp\{g \in G : l(g) \leq m+1\} \\ &= \gamma(m) + \sharp\{g \in G : l(g) = m+1\}\end{aligned}$$

we have $\gamma(m+1) = \gamma(m)$. So $\{g \in G : l(g) = m+1\} = \emptyset$. Now I claim that $\{g \in G : l(g) = m+k\} = \emptyset$ for all $k \in \mathbb{N}^+$.

We prove this by induction on k. If $k = 1$, we already know this.

Assume it is true for k, I will show that it is true for $k+1$ (i.e. assume $\{g \in G : l(g) = m+k\} = \emptyset$, show that $\{g \in G : l(g) = m+k+1\} = \emptyset$). If there were an element $g \in G$ such that $l(g) = m+k+1$, then we would have

$$g = s_{i_1}^{\varepsilon_1} s_{i_2}^{\varepsilon_2} ... s_{i_{m+k}}^{\varepsilon_{m+k}} s_{i_{m+k+1}}^{\varepsilon_{m+k+1}}$$

with $\varepsilon_i = \pm 1$ and $s_{i_j} \in S$. Then $h = s_{i_1}^{\varepsilon_1} s_{i_2}^{\varepsilon_2} ... s_{i_{m+k}}^{\varepsilon_{m+k}}$ is an element of G that has length $m+k$. This is a contradiction to induction assumption.

So we have $\{g \in G : l(g) = m+k+1\} = \emptyset$.

Thus the group G only contains elements that have length at most n. But there are at most $(2k)^n + 1$ such many elements. This gives rise to a contradiction to the assumption that G is infinite.

Lemma 2.3.2: The growth function γ is submultiplicative: $\gamma(m+n) \leq \gamma(m)\gamma(n)$ for all $n, m \geq 1$.

Proof 2.3.2: Claim: If $l(g) \leq m+n$, then $g = ab$ where $l(a) \leq m$ and $l(b) \leq n$. Suppose that we proved the claim. Let $a_1, ..., a_{\gamma(m)}$ be all distinct elements of length at most m, and let $b_1, ..., b_{\gamma(n)}$ be all distinct elements of length at most n. Then the set

$$A = \{a_i b_j : 1 \leq i \leq \gamma(m), \quad 1 \leq j \leq \gamma(n)\}$$

consists of all the elements of length $\leq m+n$, maybe with repetitions. Now if $l(g) \leq m+n$, then by the claim we have $g \in A$. Therefore, $\gamma(m+n) \leq |A|$. But $|A| \leq \gamma(m)\gamma(n)$. Thus, we get

$$\gamma(m+n) \leq \gamma(m)\gamma(n). \tag{2.3}$$

Proof of the Claim: Suppose that $l(g) \leq m+n$.

I will show $g = ab$ for some a, b with $l(a) \leq m$ and $l(b) \leq n$. Consider the shortest decomposition $g = s_{i_1}^{\varepsilon_1} s_{i_2}^{\varepsilon_2} ... s_{l(g)}^{\varepsilon_{l(g)}}$. Since $l(g) \leq m+n$, represent $l(g) = t+r$ such that $t \leq n$ and $r \leq m$.

Now $g = \underbrace{s_{i_1}^{\varepsilon_1} s_{i_2}^{\varepsilon_2} ... s_{i_t}^{\varepsilon_t}}_{t-times} \underbrace{s_{i_{t+1}}^{\varepsilon_{t+1}} ... s_{l(g)}^{\varepsilon_{l(g)}}}_{r-times}$.

Take $a = \underbrace{s_{i_1}^{\varepsilon_1} s_{i_2}^{\varepsilon_2} ... s_{i_t}^{\varepsilon_t}}_{t-times}$ and $b = \underbrace{s_{i_{t+1}}^{\varepsilon_{t+1}} ... s_{l(g)}^{\varepsilon_{l(g)}}}_{r-times}$.

3. DOMINATION RELATION FOR SEQUENCES OF REAL NUMBERS

Definition 3.1: Let $f, g : \mathbb{N} \longrightarrow \mathbb{R}_+$ be two functions. By Grigorchuk[5], we define $f \preceq g$ if and only if

$$f(n) \leq Cg(\alpha n). \tag{3.1}$$

for all $n > 0$ and for some real number $C > 0$ and for some natural number $\alpha > 0$.

We say that f and g are equivalent, denoted by $f \sim g$, if $f \preceq g$ and $g \preceq f$.

Example: $n^e \preceq n^\pi$ and $a^n \sim b^n$ for any $a, b > 1$.

Definition 3.2: A function $f : \mathbb{N} \longrightarrow \mathbb{R}_+$ is called polynomial if $f(n) \sim n^\alpha$ for some $\alpha > 0$. A function f is called exponential if $f(n) \sim e^n$, and it is called subexponential if there exists a limit $\lim \dfrac{\ln f(n)}{n} = 0$ as $n \longrightarrow \infty$.

Example: n^π is polynomial, $n^e e^n$ is exponential, and $e^{n/\ln(n)}$ is subexponential.

Definition 3.3: A function f is called subadditive if $f(n+m) \leq f(n) + f(m)$ and it is called submultiplicative if $f(n+m) \leq f(n)f(m)$.

Example: The square root function is subadditive since for any $x, y \geq 0$ we have $\sqrt{x+y} \leq \sqrt{x} + \sqrt{y}$.

Definition 3.3: A sequence $(a_n)_{n\in\mathbb{N}}$ is called subadditive if it satisfies the inequality $a_{n+m} \leq a_n + a_m$ for all n and m.

Example: For $n \in \mathbb{N}$ let $a_n = n$.

Theorem 3.1(Fekete's Lemma): Let $(a_n)_n$ be a subadditive sequence of nonnegative numbers. Then (a_n/n) is bounded from below and it converges to $\inf a_n/n$.

Proof 3.1: To see that the sequence (a_n/n) is bounded below, just not that $a_n \geq 0$ so $a_n/n \geq 0$ for all n. Let $l = \inf(a_n : n \in \mathbb{N})$. We will prove that $a_n/n \longrightarrow l$. So we must show that for each $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that

$|a_n/n - l| < \varepsilon$ for all $n > N$.

Let $\varepsilon > 0$ be given.

Let $K \in \mathbb{N}$ be such that $|\frac{a_K}{K} - l| < \varepsilon/2$. There exists such K, otherwise $l + \varepsilon/2$ would also be a lower bound, contradicting the fact that l is the greatest lower bound.

Let $M \in \mathbb{N}$ be such that $\frac{a_r}{KM} < \frac{\varepsilon}{2}$ for all $r = 0, 1, ..., K-1$. To find such M just find $R = max(a_r/K : r < K)$ and choose M so that $R/M < \varepsilon/2$.

Let $N = KM$. Let $n > N$ be arbitrary.

Let $r, s \in \mathbb{N}$ such that $n = sK + r$ with $r < K$. So $s \geq M$. Then $\frac{a_n}{n} = \frac{sa_K}{sK+r} + \frac{a_r}{sK+r} \leq \frac{sa_K}{sK} + \frac{a_r}{KM} \leq \frac{a_K}{K} + \frac{a_r}{KM} < (l + \varepsilon/2) + \varepsilon/2$ since $a_K/K < l + \varepsilon/2$. This means that $|a_n/n - l| < \varepsilon$ since $a_n/n \geq l$ by the definition of l. Therefore, $|a_n/n - l| < \varepsilon$ for all $n > N$.

Lemma 3.2: Let G be a finitely generated group with a generating set S, and let $\gamma = \gamma_G^S$ be its growth function. Then the limit $\lim_{n\to\infty} \frac{\ln \gamma(n)}{n}$ always exists. This limit is called the growth rate of G.

Proof 3.2: From (2.3) we know that the growth function is submultiplicative. So $\ln \gamma(n)$ is subadditive. Then by Fekete's lemma this limit $\lim_{n\to\infty} \frac{\ln \gamma(n)}{n}$ exists.

4. EQUIVALENCE OF GROWTH FUNCTIONS

Lemma 4.1: Let S and S' be two different generating sets of a group G. Then the corresponding growth functions γ_S and $\gamma_{S'}$ are equivalent.

Proof 4.1:[10] I will show that there exist constants $C, D, \alpha, \beta > 0$ such that $\gamma_{S'}(n) \leq C\gamma_S(\alpha n)$ and $\gamma_S(n) \leq D\gamma_{S'}(\beta n)$ for all $n > 0$.
Since S and S' are two generating sets of G, every element of S' can be written as a finite product of elements of S. Thus, there exists a constant $\alpha > 0$ such that the $l_S(s') \leq \alpha$ for all $s' \in S'$ (Take $\alpha = max\{l_S(s') : s' \in S'\}$).
If $g \in G$ is a product of m elements of S', then g can be written as a product of at most αm elements of S. So $l_S(g) \leq \alpha m$. Thus, if $l_{S'}(g) \leq n$, then $l_S(g) \leq \alpha n$. Hence, $\gamma_{S'}(n) \leq \gamma_S(\alpha n)$.
Similarly, we get $\gamma_S(n) \leq \gamma_{S'}(\beta n)$ for some $\beta > 0$.

Lemma 4.2: Let G be a group and let H be a subgroup of G of finite index. Then their growth functions γ_G and γ_H are equivalent.
Proof 4.2: Clearly, $\gamma_H \preceq \gamma_G$.
Assume $[G : H] = k < \infty$. Choose generators $S = \{s_1, s_2, ..., s_m\}$ of H. Assume $S = S^{-1}$, if not add the elements. Choose representatives of left cosets of H and add their inverses: $a_1, a_2, ..., a_{2k}$. Then $s_1, ..., s_m, a_1, ..., a_{2k}$ generate G. Assume that 1 is one of them. Then we have

$$s_i a_j = a_{t(i,j)} w_{ij}(s_1, ..., s_m) \quad (4.1)$$

$$a_i a_j = a_{r(i,j)} v_{ij}(s_1, ..., s_m) \quad (4.2)$$

Now choose D such that $|w_{ij}|,\ |v_{ij}| \leq D$ for all i, j.
Claim: For any word $u(\bar{s}, \bar{a})$ in G there are words $v(\bar{s}),\ a_i$ such that $u(\bar{s}, \bar{a}) = a_i v(\bar{s})$ with $|v(\bar{s})| \leq D|u(\bar{s}, \bar{a})|$.
Suppose we proved the claim. Then we show that if $l(g) \leq n$, then g can be represented as $g = a_i h$ with $h \in H$ and $l(h) \leq Dn$. Suppose $l(g) = k \leq n$.

Let $g = u(\bar{s},\bar{a})$ be a representative of length k. Then $u(\bar{s},\bar{a}) = a_i v(\bar{s})$ with $|v(\bar{s})| \leq Dk$. So $l_H(v(\bar{s})) \leq |v(\bar{s})| \leq Dk \leq Dn$. Take $h = v(\bar{s})$.

Then the set

$$\{a_i h : i = 1, ..., 2k, h \in H, l(h) \leq Dn\}$$

contains, maybe with repetitions, all the elements of G of length at most n.

So $\gamma_G(n) \leq 2k\gamma_H(Dn)$.

Proof of Claim: We proceed by induction on the number n of the occurrences of a_i's in $u(\bar{s},\bar{a})$. If $n = 0$, this means $u(\bar{s},\bar{a})$ does not contain any a_i.

So $u(\bar{s},\bar{a}) = v(\bar{s})$. By assumption we know that there exists i such that $a_i = 1$.

Thus, we get the desired equality $u(\bar{s},\bar{a}) = a_i v(\bar{s})$. Clearly, $|v(\bar{s})| \leq D|u(\bar{s},\bar{a})|$.

Assuming it is true for $k < n$, we will show that it is true for $k = n$.

Write $u(\bar{s},\bar{a}) = u_1(\bar{s},\bar{a})a_j u^{'}(\bar{s})a_l u^{''}(\bar{s})$, where a_j and a_l are the first two occurrences from the right.

From (4.1) we know that exchanging a s_i in $u^{'}(\bar{s})a_l$ with a_l, it produces a word $w_{(i,l)}$ such that $|w_{(i,l)}| \leq D$. So $u^{'}(\bar{s})a_l = a_l w(\bar{s})$ with $|w(\bar{s})| \leq D|u^{'}(\bar{s})a_l|$.

Then $u^{'}(\bar{s})a_l u^{''}(\bar{s}) = a_l v(\bar{s})$ with $|v(\bar{s})| \leq D|u^{'}(\bar{s})| + |u^{''}(\bar{s})|$.

Now from (4.2) we know that $a_j a_l = a_k w(\bar{s})$, $|w(\bar{s})| \leq D$

So $a_j a_l v(\bar{s}) = a_k w(\bar{s})v(\bar{s})$ and

$$\begin{aligned}|w(\bar{s})v(\bar{s})| = |w(\bar{s})| + |v(\bar{s})| \leq D + D|u^{'}(\bar{s})| + |u^{''}(\bar{s})| = \\ = D(1 + |u^{'}(\bar{s})| + |u^{''}(\bar{s})|) = D|u^{'}(\bar{s})a_l u^{''}(\bar{s})|.\end{aligned}$$

So $u(\bar{s},\bar{a}) = u_1(\bar{s},\bar{a})a_k w(\bar{s})v(\bar{s})$ with $|w(\bar{s})v(\bar{s})| \leq D|u^{'}(\bar{s})a_l u^{''}(\bar{s})|$.

By induction assumption we have $u_1(\bar{s},\bar{a})a_k = a_t v^{'}(\bar{s})$ with $|v^{'}(\bar{s}) \leq D|u_1(\bar{s},\bar{a})a_k|$.

Therefore, we get $u(\bar{s},\bar{a}) = a_t v^{'}(\bar{s})w(\bar{s})v(\bar{s})$.

$$\begin{aligned}|v^{'}(\bar{s})w(\bar{s})v(\bar{s})| = |v^{'}(\bar{s})| + |w(\bar{s})v(\bar{s})| &\leq D|u_1(\bar{s},\bar{a})a_k| + D|u^{'}(\bar{s})a_l u^{''}(\bar{s})| \\ &= D(|u_1(\bar{s},\bar{a})a_k| + |u^{'}(\bar{s})a_l u^{''}(\bar{s})|) \\ &= D|u(\bar{s},\bar{a})|.\end{aligned}$$

5. GROUPS OF EXPONENTIAL GROWTH

Lemma 5.1: Any group is either of exponential growth or subexponential growth.

Proof 5.1: We know that the limit $\lim_{n\to\infty} \dfrac{\ln \gamma(n)}{n}$ always exists.

Case1: If $\lim_{n\to\infty} \dfrac{\ln \gamma(n)}{n} = 0$, then by definition the group has subexponential growth.

Case2: Suppose $\lim_{n\to\infty} \dfrac{\ln \gamma(n)}{n} = L \neq 0$. Let $\varepsilon > 0$ be arbitrary.

Then there exists $N \in \mathbb{N}$ such that $|\ln \gamma(n)^{\frac{1}{n}} - L| < \varepsilon$ for all $n > N$. So $e^{L-\varepsilon} < \gamma(n)^{\frac{1}{n}} < e^{L+\varepsilon}$. Then $e^{(L-\varepsilon)n} < \gamma(n) < e^{(L+\varepsilon)n}$ for all $n > N$. Now for $\varepsilon = L$ there exists $N_1 \in \mathbb{N}$ such that if $n > N_1$, then $\gamma(n) < e^{2Ln}$. Taking $C = \gamma(N)$ and $\alpha = 2L$ we get $\gamma(n) < Ce^{\alpha n}$ for all $n > 0$.

Now I will show that there exist $D, \beta > 0$ such that $e^n < D\gamma(\beta n)$ for all $n > 0$. Choose $\varepsilon > 0$ such that $e^n < e^{(L-\varepsilon)n}$ for all $n > 0$. Then there exists $N \in \mathbb{N}$ such that $e^n < \gamma(n)$ for all $n > N$. Take $D = 1$ and $\beta = N$. Then $e^n < D\gamma(\beta n)$ for all $n > 0$.

Therefore, we have $\gamma(n) \sim e^n$.

5.1 Free Groups

Definition 5.1.1: A group F is called free if there exists a generating set X of F such that for any map $\varphi : X \longrightarrow G$ where G is a group, there exists a homomorphism $\psi : F \longrightarrow G$ that extends φ.

Example: The trivial group is free.

Example: $\mathbb{Z} =< 1 >$ is free. If G is an arbitrary group and $\varphi(1) = g$, then define $\psi : \mathbb{Z} \longrightarrow G$ as $\psi(n) = g^n$.

Let X be an arbitrary set. Let $W(X)$ be the set of all finite words over $X \cup X^{-1}$ where $X^{-1} = \{x^{-1} : x \in X\}$. For example, if $X = \{a, b\}$, then $W(X)$ is the set of all words over a, b, a^{-1}, b^{-1}. Eg. $a^{-1}bb^{-1}abaa^{-1}bba \in W(X)$.

We call $w \in W$ irreducible if it has no subwords of the form xx^{-1} or $x^{-1}x$ where $x \in X$. For $w \in W$ we define $w^{'} = x_n^{-\varepsilon_n} x_{n-1}^{-\varepsilon_{n-1}} ... x_1^{-\varepsilon_1}$ where $w = x_1^{\varepsilon_1} x_1^{\varepsilon_1} ... x_{n-1}^{\varepsilon_{n-1}} x_n^{\varepsilon_n}$ and $\varepsilon_i = \mp 1$. Eg. $(bbba)^{'} = a^{-1}b^{-1}b^{-1}b^{-1}$.

Let $F(X) = \{w \in W(X) : w \text{ is irreducible}\}$.

For $u, v \in F(X)$, let w be the word of maximal length such that $u = u_1 w$ and $v = w^{'} v_1$. Eg. $u = \underbrace{aab}_{u_1}\underbrace{a^{-1}b^{-1}}_{w}$, $v = \underbrace{ba}_{w^{'}}\underbrace{bba^{-1}b}_{v_1}$.

On $F(X)$ define an operation "$\cdot$" as $u \cdot v = u_1 v_1$.

$(F(X), \cdot)$ is a group and it is free. We call it the free group generated by X.

Lemma 5.1.1: The free group F_m with m generators $X = \{x_1, ..., x_m\}$ is of exponential growth .

Proof 5.1.1: For any $k \geq 1$ there are exactly $(2m)(2m-1)^{k-1}$ elements in F_m of length k with respect to X. Therefore,

$$\gamma_{F_m}(n) = 1 + \sum_{k=1}^{n} (2m)(2m-1)^{k-1}$$

If $m = 1$, then $\gamma_{F_m}(n) = 1 + 2n$. If $m > 1$, then

$$\gamma_{F_m}(n) = 1 + \sum_{k=1}^{n} (2m)(2m-1)^{k-1} = 1 + m\frac{(2m-1)^n - 1}{m-1}.$$

Since $a^n \sim b^n$ for any $a, b > 1$, we get $\gamma_{F_m}(n) \sim e^n$.

5.2 Semi-direct Product

Let H and X be two groups.

Let $\varphi : X \longrightarrow Aut(H)$ be a homomorphism denoted by $\varphi(x) = \varphi_x$.

The semi-direct product $H \rtimes_{\varphi} X$ is defined to be the group with underlying set $H \rtimes_{\varphi} X = \{(h, x) : h \in H, x \in X\}$ and group operation defined by $(h_1, x_1)(h_2, x_2) := (h_1 \varphi_{x_1}(h_2), x_1 x_2)$. This group $G = H \rtimes_{\varphi} X$ has the following properties:

1. $H \times \{1_X\} \lhd G$ is isomorphic to H,
2. $\{1_H\} \times \ X \leqslant G$ is isomorphic to X,
3. $G = (H \times \{1_X\})(\{1_H\} \times X)$.

5.3 Wreath Product

Let A and B be two groups.

Let $Fun(B, A) = \{f \mid f : B \longrightarrow A\}$.

Let $fun(B, A) = \{f \in Fun(B, A) : \{b \in B : f(b) \neq 1_A\}$f is finite$\}$.

Let $\Phi \leqslant Sym(B)$. For any $\varphi \in Sym(B)$, define $\bar{\varphi} \in Aut(fun(B, A))$ as $\bar{\varphi} : f \mapsto f \circ \varphi$. Then $^{-} : \Phi \longrightarrow Aut(fun(B, A))$ is a homomorphism. We define the wreath product of A and B to be $A \wr B = fun(B, A) \rtimes B$.

Lemma 5.2.1: The group $G = \mathbb{Z}_2 \wr Z = (\cdots \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots) \rtimes \mathbb{Z}$ is of exponential growth.

Proof 5.2.1: Let a be a generator of $\mathbb{Z}_2$, and b be a generator of $\mathbb{Z}$. Then any element of G can be uniquely represented in the form

$$b^k a^{b^{k_1}} ... a^{b^{k_q}},$$

where $q \geq 0$, and $k, k_1, ..., k_q$ are integers with $k_1 > k_2 > ... > k_q$. We call such a representation of an element canonical.

Let n be a positive integer, and $\tau = (t_1, ..., t_n)$, where each t_i is 1 or 2. Denote by g_τ the element

$$ab^{t_1} ab^{t_2} ... ab^{t_n}$$

of the group G. We show that for different tuples τ the elements g_τ are different. Using that in G

$$ab^t = b^t a^{b^t}, \quad a^{b^t} a^{b^s} = a^{b^s} a^{b^t}$$

for any integers t, s. It is easy to show by induction on n that in G

$$g_\tau = b^{t_1+t_2+\cdots+t_n} a^{b^{t_1+t_2+\cdots+t_n}} a^{b^{t_2+\cdots+t_n}} ... a^{b^{t_n}}.$$

This representation of g_τ is canonical because for all $i = 1, ..., n-1$

$$t_i + \cdots + t_n > t_{i+1} + \cdots + t_n.$$

It is clear that for different τ the corresponding tuples

$$t_1 + \cdots + t_n,\ t_2 + \cdots + t_n, ...,\ t_{n-1} + t_n,\ t_n$$

are different. Now uniqueness of the canonical representation easily implies that if $\tau \neq \tau'$, then g_τ and $g_{\tau'}$ are different elements of G.

We have

$$l(g_\tau) \leq |ab^{t_1}ab^{t_2}...ab^{t_n}| = n + t_1 + t_2 + \cdots + t_n \leq 3n.$$

Since the number of possible τ is equal to 2^n, and all g_τ are distinct, it follows that for any $n > 0$

$$\gamma(3n) \geq 2^n.$$

Hence, $\gamma(n)$ is of exponential growth.

6. GROUPS OF POLYNOMIAL GROWTH

Recall that a group G has polynomial growth if $\gamma_G \sim n^\alpha$ for some $\alpha > 0$.

Example: $\mathbb{Z}$ has polynomial growth since $\gamma_{\mathbb{Z}}(n) = 2n+1$ for all $n \geq 0$.

Lemma 6.1: Let G and H be two infinite groups of polynomial growth. Then their direct product $G \times H$ has also polynomial growth. But $\gamma_G \nsim \gamma_{G\times H}$.

Proof 6.1: Suppose $\gamma_G \sim n^{\alpha_1}$ and $\gamma_H \sim n^{\alpha_2}$ for some $\alpha_1, \alpha_2 > 0$.

Now if $(g,h) \in G \times H$ such that $l(g,h) \leq n$, then $l(g) \leq n$ and $l(h) \leq n$. But there are at most $\gamma_G(n)$ such $g \in G$ and $\gamma_H(n)$ such many $h \in H$.

Thus, $\gamma_{G\times H}(n) \leq \gamma_G(n)\gamma_H(n)$. Then $\gamma_{G\times H}(n) \leq C_1(\beta_1 n)^{\alpha_1} C_2(\beta_2 n)^{\alpha_2}$ for some $C_1, C_2, \beta_1, \beta_2 > 0$. Therefore,

$$\gamma_{G\times H}(n) \leq C n^{\alpha_1+\alpha_2} \tag{6.1}$$

where $C = C_1 C_2 \beta_1^{\alpha_1} \beta_2^{\alpha_2}$.

Clearly, $\gamma_G(n) \leq \gamma_{G\times H}(n)$ and $\gamma_H(n) \leq \gamma_{G\times H}(n)$. Since $\gamma_G \sim n^{\alpha_1}$ and $\gamma_H \sim n^{\alpha_2}$, we know that $n^{\alpha_1} \leq C_1 \gamma_G(\beta_1 n)$ and $n^{\alpha_2} \leq C_2 \gamma_H(\beta_2 n)$ for some $C_1, C_2, \beta_1, \beta_2 > 0$. Then $n^{\alpha_1} \leq C\gamma_G(\beta n)$ and $n^{\alpha_2} \leq C\gamma_H(\beta n)$ with $C = max\{C_1, C_2\}$, $\beta = max\{\beta_1, \beta_2\}$. Thus, we have the following inequality

$$n^{\alpha_1+\alpha_2} \leq C^2 \gamma_G(\beta n)\gamma_H(\beta n). \tag{6.2}$$

Now if $g \in G$ with $l(g) \leq \beta n$ and $h \in G$ with $l(h) \leq \beta n$, then the element (g,h) in $G \times H$ has length at most $2\beta n$.

Therefore, $\gamma_G(\beta n)\gamma_H(\beta n) \leq \gamma_{G\times H}(2\beta n)$.

By (6.2) we get

$$n^{\alpha_1+\alpha_2} \leq C^2 \gamma_{G\times H}(2\beta n). \tag{6.3}$$

From (6.1) and (6.32) we get $\gamma_{G\times H} \sim n^{\alpha_1+\alpha_2}$.

Hence, $G \times H$ has polynomial growth. And $\gamma_G \nsim \gamma_{G\times H}$ follows by the fact that polynomials of different degree are not equivalent.

Example: $\mathbb{Z}^d$ has polynomial growth for any $d \geq 1$.

Example: Any finitely generated abelian group is of polynomial growth. We know that such a group is isomorphic to $\mathbb{Z}^d \oplus \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \oplus \mathbb{Z}_{p_k}$ for some $d \geq 0$ and some numbers $p_1, p_2, ..., p_k$ (not necessarily distinct) of powers of prime numbers.

6.1 Nilpotent Groups

Let G be a group. For $g, h \in G$, we define $[g, h] = ghg^{-1}h^{-1}$ and call it the commutator of g and h. If A and B are two subgroups of G, define $[A, B] = \langle [a, b] \ : \ a \in A, b \in B \rangle$.

Claim: G is abelian if and only if $[G, G] = \{1\}$.

Proof:

$$\begin{aligned} G \text{ is abelian} &\Leftrightarrow gh = hg \text{ for all } g, h \in G \\ &\Leftrightarrow ghg^{-1}h^{-1} = 1 \text{ for all } g, h \in G \\ &\Leftrightarrow [g, h] = 1 \text{ for all } g, h \in G \\ &\Leftrightarrow [G, G] = \{1\}. \end{aligned}$$

Definition 6.1.1: A series of normal subgroups $1 = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_n = G$ of a group G is called central if

$$G_{i+1}/G_i \leqslant Z(G/G_i) \tag{6.4}$$

for any $i = 0, ..., n-1$.

Condition (6.4) is equivalent to $[G_{i+1}, G] \leqslant G$ because for any $x \in G_{i+1}$ and $y \in G$, xG_i and yG_i commute in G/G_i if and only if $[x, y] \in G_i$ if and only if $[G_{i+1}, G] \leqslant G$.

Definition 6.1.2: We define the derived series G^n of a group G inductively:

- $G^0 = G$,
- $G^{n+1} = [G, G^n]$.

The derived series is also called the lower central series.

Lemma 6.1.1: A group G is nilpotent if and only if $G^n = \{1\}$ for some n.

If n is the smallest natural number such that $G^n = \{1\}$, then we say that G is nilpotent of class n or G has nilpotent length $n - 1$ for $n \geq 1$.

Example: Every abelian group is nilpotent of class 1, except for the trivial group which is nilpotent of class 0.

Proposition 6.1.2: If G is nilpotent, then $Z(G) \neq 1$.

Proof 6.1.2: Suppose $1 = G_0 \leqslant G_1 \leqslant ... \leqslant G_n = G$ is the lower central series. Suppose $Z(G) = 1$. I will show that $G = 1$.

Claim: $G_i = 1$ for all $i = 0, 1, ..., n$.

Proof: If $i = 0$, then $G_i = 1$.

Suppose $G_0 = G_1 = ... = G_i = 1$. I will show that $G_{i+1} = 1$.

Since $G_{i+1} \simeq G_{i+1}/G_i \leqslant Z(G/G_i) \simeq Z(G) = 1$, we have $G_{i+1} = 1$.

Then $G = 1$, a contradiction.

Lemma 6.1.3: If $G/Z(G)$ is nilpotent, then so is G.

Proof 6.1.3: Suppose $1 = G_0/Z(G) \leqslant G_1/Z(G) \leqslant ... \leqslant G_n/Z(G) = G/Z(G)$ is central in $G/Z(G)$. I claim that $1 \leqslant Z(G) \leqslant G_1 \leqslant ... \leqslant G_n = G$ is central in G. By the assumption know that $[G_{i+1}/Z(G), G/Z(G)] \leqslant G_i/Z(G)$.

But $[G_{i+1}/Z(G), G/Z(G)] = [G_{i+1}, G]/Z(G)$. Then $[G_{i+1}, G] \leqslant G_i$.

Theorem 6.1.4: Any finite p-group is nilpotent for any prime p.

Proof 6.1.4: We proceed by induction on $|G|$.

If $|G| = 1$, then G is the trivial group. Suppose $|G| > 1$. We know that $Z(G) \neq 1$.

Then $|G/Z(G)| < |G|$. So by induction assumption, $G/Z(G)$ is nilpotent.

Hence, G is nilpotent by Lemma 6.1.3.

Theorem 6.1.5: Any finitely generated nilpotent group has polynomial growth.

Proof 6.1.5[11]: Let G be a finitely-generated nilpotent group. Assume G is nilpotent of class s. I will show that G has polynomial growth.

We proceed by induction on s.

If $s = 0$, then G is the trivial group. If $s = 1$, then G is an abelian group.

We prove it for the case $s = 2$ to understand the ideas and then we generalize it.

Groups of Nilpotent Class Two: Let G be nilpotent of class two. Suppose that $g_1, g_2, ..., g_m$ generate G. Then $[G, G]$ is abelian and it belongs to the center of G. Now consider a product of n generators. Exchanging any two generators produces a commutator on the right i.e.

$$g_j g_i = g_i g_j [g_j^{-1}, g_i^{-1}] \text{ for all } 1 \leq i, j \leq m.$$

Since commutators are in the center $Z(G)$, they can be moved to the right. So if we want to put generators into a canonical order, we need at most n^2 interchanges. Then, we get an element of the form $g_1^{k_1} g_2^{k_2} ... g_m^{k_m} C$, where C is a product of at most n^2 commutators of the generators. These commutators are words of bounded length with respect to any system of generators in the abelian group $[G, G]$ with polynomial growth, say $\gamma_{[G,G]} \sim n^k$. So the total number of such C is

$$\gamma_{[G,G]}(n^2) \leq (n^2)^k = n^{2k}$$

and the total number of $g_1^{k_1} g_2^{k_2} ... g_m^{k_m}$ is at most n^m since $k_1 + k_2 + ... + k_m = n$. Thus, the number of elements in G which are products of n generators is at most $n^m n^{2k} = n^{m+2k}$, i.e. $\gamma_G(n) \leq n^{m+2k}$.

Inductive Step: Assuming that the theorem holds for groups of nilpotent of class $< s$, I will show that it holds for s. Assume G is of nilpotent class s. Let $g_1, g_2, ..., g_m$ generate G. Then $[G, G]$ is nilpotent of class $\leq s - 1$. Hence, by induction assumption it has polynomial growth, say n^k.

Now consider a product of n generators and bring it to a form $g_1^{k_1} g_2^{k_2} ... g_m^{k_m} C$ where $C \in [G, G]$. Exchanging a pair of generators produces a commutator on the right. We know that there will be no more than n^2 such commutators in the process of rearranging the generators. But this time when we move generators to the left we need to exchange them with the commutators thus producing elements of the form $[g_{i_1}, [g_{i_2}, g_{i_3}]] \in [G, [G, G]]$. The total number of these elements is at most n^3 and so on. Since G is nilpotent of class s, this process of generating new terms will stop at s-th level i.e. moving generators through commutators of s-th order will not produce any new terms. Thus, the total length of C is estimated from above by Mn^s for some constant $M > 0$ since there are at most $n^2 + n^3 + ... + n^s$ commutators of different orders and each of them is a word of bounded length. Thus, we get $\gamma_G(n) \leq n^{m+sk}$. ■

Example: $UT_3(\mathbb{Z})$ has polynomial growth. Since $UT_3(\mathbb{Z})$ is finitely generated and nilpotent we know that it has polynomial growth. But we will show that it is of polynomial growth of degree 4, i.e.$\gamma_{UT_3(\mathbb{Z})} \sim n^4$.

Let $s = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $t = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, $u = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

It can be easily verified that $us = su$, $ut = tu$, $sts^{-1}t^{-1} = u$ and

$$s^k = \begin{pmatrix} 1 & k & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ t^l = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & l \\ 0 & 0 & 1 \end{pmatrix},\ u^m = \begin{pmatrix} 1 & 0 & m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

for all $k, l, m \in \mathbb{Z}$.

Then we have

$$\begin{pmatrix} 1 & k & m \\ 0 & 1 & l \\ 0 & 0 & 1 \end{pmatrix} = u^m t^l s^k$$

for all $k, l, m \in \mathbb{Z}$.

Thus, $UT_3(\mathbb{Z}) = \langle s, t, u \rangle$.

And for any $k, l, m \in \mathbb{Z}$, we have

$$s(u^m t^l s^k) = u^{m+l} t^l s^{k+1},$$
$$t(u^m t^l s^k) = u^m t^{l+1} s^k,$$
$$u(u^m t^l s^k) = u^{m+1} t^l s^k.$$

Lemma 6.1.6(Harpe, 197): With the above notation,

1. $|u^m t^l s^k| \leq |k| + |l| + 6\sqrt{|m|}$ for all $k, l, m \in \mathbb{Z}$,
2. $|u^m t^l s^k| \leq r \Rightarrow \begin{cases} |k| + |l| \leq r \\ |m| \leq r^2. \end{cases}$

Proof 6.1.6: For any $k, l \in \mathbb{Z}$ we have $t^l s^{-k} t^{-l} s^k = u^{kl}$.

Now consider an integer m.

Let i be the integral part of $\sqrt{|m|}$, and $j = m - i^2$. Since $0 \leq \sqrt{|m|} - i \leq 1$, we get $j = (\sqrt{|m|} - i)(\sqrt{|m|} + i) \leq (\sqrt{|m|} + i) \leq 2\sqrt{|m|}$.

Now $u^m = u^{j+i^2} = u^j u^{i^2} = u^j u^{ii} = u^j t^i s^{-i} t^{-i} s^i$.

Thus, we have

$$|u^m| = |u^j t^i s^{-i} t^{-i} s^i| \leq |u^j| + |t^i| + |s^{-i}| + |t^{-i}| + |s^i|$$
$$\leq j + 4i \leq 6\sqrt{m}.$$

Therefore, $|u^m t^l s^k| \leq |u^m| + |t^l| + |s^k| \leq |k| + |l| + 6\sqrt{|m|}$ for all $u^m t^l s^k \in UT_3(\mathbb{Z})$.■

Proposition 6.1.7(Harpe, 198): Let $\gamma(r)$ be the growth function of $UT_3(\mathbb{Z})$. Then there exist constants $A, B > 0$ such that $Ar^4 \leq \gamma(r) \leq Br^4$ for all $r \geq 1$.

Proof 6.1.7: Let $r \geq 1$.

If $|k| \leq \frac{r}{8}$, $|l| \leq \frac{r}{8}$, and $|m| \leq (\frac{r}{8})^2$, then by part 1 of Lemma 6.1.6, we see that $|u^m t^l s^k| \leq r$.

But there are exactly $(2[\frac{r}{8}] + 1)$ many such k and l, and $(2[\frac{r^2}{64}] + 1)$ many such m. Thus, we have

$$\gamma(r) \geq (2[\frac{r}{8}] + 1)^2 (2[\frac{r^2}{64}] + 1)$$

i.e. $\gamma(r) \geq Ar^4$ for an appropriate $A > 0$ and for all $r \geq 1$.

From part 2 of Lemma 6.1.6 and using the same argument above we get

$$\gamma(r) \leq (2r + 1)^2 (2r^2 + 1) \leq 12r^4$$

for all $r \geq 1$. ■

Let G be a finitely generated group with generating set S.

If there exist polynomials P and Q with positive leading coefficients such that

$$P(n) \leq \gamma_S(n) \leq Q(n)$$

for sufficiently large $n > 0$, then there are constants $A, B > 0$ such that

$$An^d \leq \gamma_S(n) \leq Bn^e \tag{6.5}$$

for almost all $n > 0$, where $d = deg(P)$ and $e = deg(Q)$.

Now if T is another finite generating set of G, then by Lemma 4.1 we know that there are integers $a, b > 0$ such that

$$\gamma_T(n) \leq \gamma_S(an) \;\text{ and }\; \gamma_S(n) \leq \gamma_T(bn). \tag{6.6}$$

So from (6.5) and (6.6) we get

$$\gamma_T(n) \leq \gamma_S(an) \leq B(an)^e = (Ba^e)n^e$$

and

$$\gamma_T(n) \geq \gamma_T(b[\frac{n}{b}]) \geq \gamma_S([\frac{n}{b}]) \geq A[\frac{n}{b}]^d \geq (\frac{A}{b^d})(m-b)^d.$$

Therefore, γ_T is bounded above and below by polynomials of the same degree with positive leading coefficients (Bass[4]).

Definition 6.1.3:(Bass[4]) We say that a group G has polynomial growth of degree $d > 0$ if there exist constants $A, B > 0$ such that

$$An^d \leq \gamma_S(n) \leq Bn^d$$

for all $n > 0$.

Let G be a finitely generated nilpotent group with lower central series $G = G_1 \geqslant G_2 \geqslant \cdots \geqslant G_n = 1$. Let r_n denote the (torsion-free) rank of the finitely generated abelian group G_n/G_{n+1} (The rank of an abelian group A is the largest cardinal d such that A contains a copy of direct sum of d copies of the integers $\mathbb{Z}$).
Let $d(G) = \sum_{k=1}^{n} nr_n$ and $e = \sum_{k=1}^{n} 2^{n-1}r_n$.
Wolf[10] shows that there are constants $A, B > 0$ such that

$$Am^d \leq \gamma_G(n) \leq Bm^e \tag{6.7}$$

for all $m \geq 1$. But Bass[4] shows that the inequality still holds if e is replaced by $d = d(G)$.

Theorem 6.1.8 (Bass[4]): Any finitely generated nilpotent group G has polynomial growth of degree $d(G)$ i.e. there are constants $A, B > 0$ such that $Am^d \leq \gamma_G(n) \leq Bm^d$ for all $m \geq 1$.
Plan of Proof 6.1.8: To prove this it is enough to show that there are polynomials P and Q of degrees $d(G)$ such that

- $P(n) \leq \gamma_S(n)$,
- $\gamma_S(n) \leq Q(n)$.

for all $n > 0$. (For more see Bass[4]).

Definition 6.1.4: A group is called virtually nilpotent if it has a nilpotent subgroup of finite index.

Example: Any finite p-group is virtually nilpotent.

Theorem 6.1.9 (Gromov, 1981): A group G has polynomial growth if and only if G is virtually nilpotent.

6.2 Solvable Groups

We define the commutator series of a group G inductively

- $G^{(0)} = G$,
- $G^{(n+1)} = [G^{(n)}, G^{(n)}]$.

Definition 6.2.1: A group G is called solvable if $G^{(n)} = \{1\}$ for some $n \in \mathbb{N}$.

Example: Any nilpotent group is solvable.

Example: S_3 and S_4 are solvable.

Theorem 6.2.1 (Milnor, Wolf 1968): A finitely generated solvable group is either virtually nilpotent or has exponential growth.

7. GROUPS OF INTERMEDIATE GROWTH

Grigorchuk's Construction:

Let T be an infinite binary tree rooted at $r = \emptyset$.

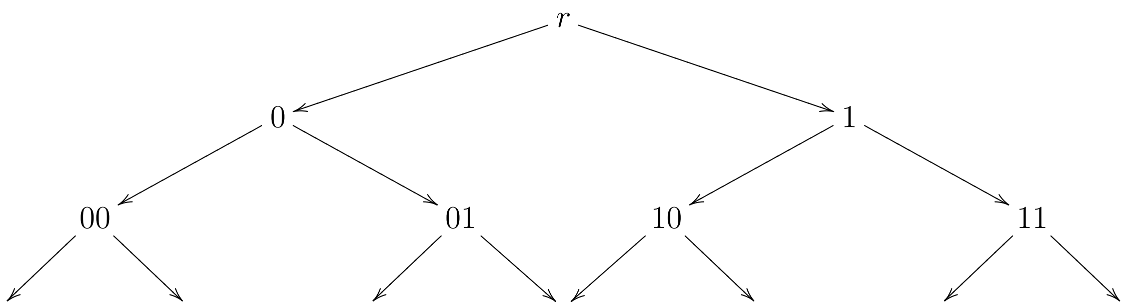

Figure 3: The graph of binary tree T

We consider the group $Aut(T)$ of automorphisms of T i.e. the set of all bijections $\tau : V \longrightarrow V$ which preserve edges where V is the set of all vertices in T, the set of all finite words in $\{0, 1\}$.

Let T_0 and T_1 be the subtrees of T rooted at 0 and 1, respectively. For $x \in \{0, 1\}$ define $\bar{x} : \{0, 1\} \longrightarrow \{0, 1\}$ by $\bar{x}(0) = 1$ and $\bar{x}(1) = 0$. Now we define four automorphisms a, b, c, and d of T as follows (Grigorchuk[5], Harpe[2] p.218):

$$a(x_1, x_2, ..., x_n) = (\bar{x}_1, x_2, ..., x_n),$$

and b, c, are defined recursively:

$$b = (a, c), \quad c = (a, d), \quad d = (Id, b)$$

i.e. b behaves as a on T_0 and c on T_1, c behaves as a on T_0 and d on T_1, and d behaves as identity on T_0 and b on T_1.

$$\begin{cases} b(0, x_2, x_3, ..., x_n) = & (0, \bar{x}_2, x_3, ..., x_n) \\ b(1, x_2, x_3, ..., x_n) = & (1, c(x_2, x_3, ..., x_n)) \end{cases}$$

$$\begin{cases} c(0, x_2, x_3, ..., x_n) = & (0, \bar{x}_2, x_3, ..., x_n) \\ c(1, x_2, x_3, ..., x_n) = & (1, d(x_2, x_3, ..., x_n)) \end{cases}$$

$$\begin{cases} d(0, x_2, x_3, ..., x_n) = & (0, x_2, x_3, ..., x_n) \\ d(1, x_2, x_3, ..., x_n) = & (1, b(x_2, x_3, ..., x_n)) \end{cases}$$

Example: $b(0, 1, 1, 0, 1) = (0, \bar{1}, 1, 0, 1) = (0, 0, 1, 0, 1)$.

$$\begin{aligned} b(1, 1, 1, 0, 1) &= (1, c(1, 1, 0, 1)) = (1, 1, d(1, 0, 1)) \\ &= (1, 1, 1, b(0, 1)) = (1, 1, 1, 0, \bar{1}) \\ &= (1, 1, 1, 0, 0) \end{aligned}$$

These automorphisms have the following properties:

1. They are involutions,
2. b, c, and d commute with each other,
3. $b \cdot c \cdot d = Id$.

Let $\mathbb{G} = \langle a, b, c, d \rangle$.

$\mathbb{G}$ is called first Grigorchuk group which is a $3-$generated, infinite group.

Theorem 7.1: $\mathbb{G}$ has intermediate growth i.e. $n^d \precnsim \gamma_{\mathbb{G}}(n) \precnsim e^n$ for any $d \in \mathbb{N}$.

8. CONCLUSION

In this study, we consider growth functions of finitely generated groups and we give some properties of this function. Then we introduce some groups that have different type of growth functions such as groups of exponential growth, groups of polynomial growth, and groups of intermediate growth. The existence of groups of intermediate growth was not known for a long time. In 1983, Rostislav Grigorchuk constructed such a group. At the end of this study we give this construction.

REFERENCES

[1] **Grillet, P.**, 1999. Algebra, John Wiley & Sons. Inc.

[2] **Harpe, P.**, 2000. Topics in Geometric Group Theory, Chicago University Press.

[3] **Lang, S.**, 1993. Algebra, Addison-Wesley Publishing Company

[4] **Bass H.**, 1971. The Degree of Polynomial Growth of Finitely Generated Nilpotent Groups, Proc. London Math. Soc. 3 (603-614)

[5] **Grigorchuk R., Pak I.**, 2006. Groups of Intermediate Growth: An Introduction for Beginners, Arxiv:math.GR/0607384 v1

[6] **Grigorchuk R. I.**, 1983. On The Milnor Problem of Group Growth, Soviet Math. Dokl. 28 no. 1 (23-26)

[7] **Milnor J.**, 1968. A Note On Curvature and The Fundamental Group, J. Differential Geometry 2 (1-7)

[8] **Milnor J.**, 1968. Problem 5603, Amer. Math. Monthly 75 (685-686)

[9] **Nathanson M. B.**, 1999. Number Theory and Semigroups of Intermediate Growth, Amer. Math. Monthly 106 (666-669)

[10] **Wolf, J.**, 1968. Growth of Finitely Generated Solvable Groups and Curvature of Riemannian Manifolds, J. Differential Geometry 2 (421-446)

[11] http://www.math.psu.edu./katok_a/Nilpotent.pdf

CURRICULUM VITAE

Ulaş Karadağ was born in 1980 in Erzincan. He educated from Çatalca High School and then he studied mathematics at İstanbul Bilgi University. He studies mathematics engineering at İstanbul Technical University and he has been working as a teaching assistant at İstanbul Bilgi University since 2005.