

COMPUTATIONS OVER INFINITE GROUPS

Jin-yi Cai

CS-TR-325-91

June 1991

Computations Over Infinite Groups

*Jin-yi Cai**

Department of Computer Science
Princeton University
Princeton, New Jersey 08544

Abstract

We propose the study of a wide variety of infinite groups from a computational complexity point of view. We raise some important structural questions on these groups from a computational aspect. The purpose of this paper is to invite the attention of both the theoretical computer science community and the combinatorial group theorists that a fruitful area of cross fertilization may be offering itself. As a specific problem, we consider randomly generated groups and their isomorphism problem.

1 Introduction

A rich class of groups have been identified recently as having significant computational aspects to them. They are called automatic groups. Certain extensions of these groups have also been considered, but are not known to be distinct from these.

These groups attained their recognition, among other reasons, because they include a wide variety of groups most commonly encountered in topology, and because they have a solvable, in fact algorithmically fairly fast solvable, word problem. Thus topologists working on classification theory of three-dimensional manifolds would like to actually compute in these groups, and their structure does allow a reasonably fast computation process.

We will only consider finitely generated groups, and in most cases we will use the representation of group elements as words. In a most informal sense, a group is called automatic, if there is a finite state automaton operating in the background, so that various questions concerning group operation can be carried out in terms of the operations of the finite state automaton. As we expect from our experience with lexicographic analysis, this affords a fast algorithm to resolve a variety of problems for the automatic groups.

In this note, I intend to lead a leisurely tour of some of the topics that might interest

*Research supported by NSF grant CCR-9057486 and a grant from MITL.

the readers. No attempt is made to be comprehensive and rigorous in my treatment. Most results mentioned are due to others, please see the reference. We propose the study of this rich class of infinite groups from a computational complexity point of view. We raise some important structural questions on these groups from a computational aspect. The purpose of this paper is to invite the attention of both the theoretical computer science community and the combinatorial group theorists that a fruitful area of cross fertilization may be offering itself. There is a Chinese saying: "Cast a brick to attract jade". It is my hope that this note may incite interest in this area and more beautiful results may be obtained by the readers.

As a problem that came up in this research on infinite groups, we consider randomly generated groups in a suitable sense, and consider their isomorphism problem. It is noted that although the Novikov-Boone theorem on the unsolvability of group word problem rules out any general algorithm for finitely presented groups, it is nonetheless possible to make general statements for *almost all* groups.

2 Definitions and basic properties

We start with the definition of the automatic groups.

Let G be a finitely generated group, with generators a, b, c, \dots . We will use these letters as alphabet symbols as well as group elements. For technical reasons, we will introduce A, B, C, \dots in upper case letters to represent inverse elements of these group elements. We do not assume that these elements $a, b, c, \dots, A, B, C, \dots$ are distinct group elements, but we take this as our alphabet set Σ of distinct letters. In other words, we consider a semigroup generator set for G . The group G will be called an automatic group if the following conditions are satisfied.

1. There is a regular language L_0 over Σ^* such that the natural map from L_0 to G is onto. In other words, every group element has a word representative in a regular language L_0 .
2. The multiplication by a generator of the group can be carried out by a finite automaton. More specifically, for each generator $g \in \Sigma$, there is a finite state automaton M_g over the alphabet set of cross product $(\Sigma \cup \$) \times (\Sigma \cup \$)$, (here $\$$ is a padding symbol), such that if $a_1 a_2 \dots a_n, b_1 b_2 \dots b_m \in \Sigma$ represent group elements $\overline{a_1 a_2 \dots a_n} = g_1$ and $\overline{b_1 b_2 \dots b_m} = g_2$ (wolog we assume $n \leq m$), then our finite automaton M_g accepts

$$\begin{array}{ccccccc} a_1 & a_2 & \dots & a_n & \dots & \$ & \\ b_1 & b_2 & \dots & b_n & \dots & b_m & \end{array} \text{ iff } a_1 a_2 \dots a_n, b_1 b_2 \dots b_m \in L_0 \text{ and } g_1 = g_2 \cdot g \text{ in } G.$$

Thus automatic groups have finite state automata acting on their chosen representatives, and the automata recognize right multiplications by generators. We can always

assume that the empty word is in L_0 and it represents the identity element.

We enumerate some immediate consequences of this definition. First of all, equality of group elements, given by its representatives, can be checked by a finite state automaton using finite automata corresponding to a and $A = a^{-1}$ linked up together. Secondly, given a word over the alphabet representing a group element, not necessarily in the form sanctioned by the regular language L_0 , one can get a representative for the same group element in L_0 . This can be accomplished by working one step at a time to obtain representatives in L_0 for group elements corresponding to all initial segments of the given word, starting with the empty word for the identity element.

In some sense, this notion of automaticity only makes sense for infinite groups; all finite groups are automatic in a trivial way, by making the group itself the generating set, $L_0 = \Sigma^*$, all elements of the group the states of the finite automata, and the multiplication table supplies the transition of the automata. But it will be interesting to investigate for large finite groups with a given (and small) set of generators, whether, and for which class of groups, one can avoid the exponential blow-up in the size of the set of states of finite automata.

A fruitful approach to finitely generated groups is to consider its Cayley graph. We will consider only finitely presented groups; these are usually infinite groups. Given such a group, its Cayley graph gives us a geometric structure on the group. One can speak of the shortest paths (geodesics) in the group between two group elements, triangles which are geodesics connecting three distinct points in the Cayley graph. These notions are particularly important as they are usually related to certain geometric objects on which the group naturally acts. For example, many automatic groups are obtained as the fundamental group acting on an underlying manifold; thus the Cayley graph can be viewed as sitting inside of the universal covering of the manifold. In such a case, the combinatorial distance induced by the geometric structure of the Cayley graph is closely related to the underlying geometry of the manifold and its covering, often they are pseudo-isometric. A familiar example of this rich interplay is the modular group

$$PSL(2, \mathbf{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbf{Z}, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1 \right\} / \{\pm I\}$$

acting on the hyperbolic upper plane \mathbf{H}^2 .

The notion of a discrete group acting properly discontinuously and with compact quotient has been a very fruitful idea. It had its origin in the work of Max Dehn. It was very successful in the hands of Margulis and Mostow, and has played a fundamental role in the work of Gromov and Thurston.

Let's look at the definition of automatic groups from the geometry of the Cayley graph. Suppose we have two group elements represented by two vertices in the graph that differ by a generator a , $g_1 = g_2 a$. the words representing g_1 and g_2 give us two paths

in the graph from the origin e . Let's imagine we travel along these paths at unit speed (one letter per unit time). (The padding symbol $\$$ can be viewed as stationary, while the other path is unfinished.) Then one would like to know how far can two corresponding points get during this traverse. The answer is that they must stay close, within a constant distance k , independent of the path (only depend on the group). This is called the *k-fellow travelers property*. The reason is simple: As the automaton has only finite number of states, if they get too far, the finite state machine can be fooled, much like the proof of the pumping lemma.

In some sense, this is the essential part of the geometry of automatic groups. Together with a regular set of geodesic representatives of groups elements, one can show that this *k-fellow travelers property* for some constant k implies that the group is automatic. The proof is essentially the following: We keep track in the states the difference of the initial segments of the words representing the elements in terms of right multiplication, up to a distance k ; if the two paths attempts to deviate by more than a distance k the machine gives up and enters a failure state.

Groups with just this *k-fellow travelers property* without regard to the regularity of its representative set is called a combable group. No example is known that is combable but not automatic.

As examples of automatic groups, one can take any cyclic group, and since the class of automatic groups is closed under direct product, all finitely generated abelian groups. Another easy example is the free group (of finite rank). For the free group of rank 2, we take all words over $\{a, b, A, B\}$ which do not have consecutive a and A , and consecutive b and B . The class of automatic groups is also closed under free product of groups, thus many matrix groups such as the modular group are automatic. Many more interesting examples are given by fundamental groups in topology.

It is curious that the following is an open problem: Suppose $G \times H$ is automatic, does it follow that G and H are automatic?

3 Hyperbolic groups and isoperimetric inequality

A class of groups have been introduced by Gromov, called hyperbolic groups. They generalize free groups in some sense and is closely related to manifolds with hyperbolic structures. A group is called hyperbolic, if it is δ -thin, i.e., for some constant δ (only depending on the group), any geodesic triangle ABC has the property that the geodesic path AB lies within the δ -neighborhood of the union of the two other geodesics BC and CA . (Note that the free group is 0-thin). The classical modular group is hyperbolic (from which the name came) since it sits nicely inside a hyperbolic space.

Given any finite presentation of a group

$$G = \langle a_1, a_2, \dots, a_k \mid r_1, r_2, \dots, r_\ell \rangle,$$

if k and ℓ are fixed but r_1, r_2, \dots, r_ℓ are chosen randomly as words over the letters a_1, a_2, \dots, a_k , then naturally one expects that there will be very little common segments in the relators r_1, r_2, \dots, r_ℓ , as the length $n = |r_i| \rightarrow \infty$. More specifically, with probability approaching 1, the longest common substring will be no more than $O(\log n)$ in the symmetric words of r_1, r_2, \dots, r_ℓ (obtained by cyclically reducing and permuting them). It will be no longer than $O(n^\epsilon)$ with exponentially small exceptional probability. Thus they define small cancellation groups (i.e., the smallest number of pieces a relator can be divided into segments which appear in other symmetric relators is more than 7, in fact here it goes to ∞). When this is true the group it defined is hyperbolic. Thus almost all group presentations are hyperbolic. This observation was made by Gromov. However, the more interesting question is the following: Among these randomly generated groups (not presentations) is it the case that almost all groups are hyperbolic? Thus we are interested in the question of these groups up to isomorphism. This is still open.

In a group presentation

$$G = \langle a_1, a_2, \dots, a_k \mid r_1, r_2, \dots, r_\ell \rangle,$$

an element represented by a word is the identity element in G if and only if it can be written as a finite product of conjugates of the relators in the free group. The minimal number of relators for any word equal to 1 in G , maximized over all words of length n is called the isoperimetric function. The name comes from the fact that in the Cayley graph, the word and its product of conjugates of relators form a disk with the word as the perimeter and the conjugated relators as translated basic regions in the graph to cover the disk. And the isoperimetric function refers to the relationship between the perimeter and the area estimate (in terms of the basic regions.) Clearly a group has a solvable word problem *iff* it has a recursive isoperimetric function.

In the case of our randomly presented group, with high probability, the group has a linear isoperimetric function. If the small cancellation property holds, then any such disk will have geometrically increasing number of basic regions in the outer layer, and thus the length of perimeter dominates the area.

Thurston proved that every hyperbolic group is automatic. As hyperbolic groups obviously have the k -fellow traveler's property, the only non-trivial part is to show a regularity structure for its elements. The idea here is to consider all geodesic words up to a constant distance k , and let the states of the finite automaton be the set of all subsets in this "ball" $B_k(1)$ around the origin 1. the initial state is $\{1\}$. The regular set will capture precisely the geodesic paths. Let S be such a subset, and $x \in \Sigma$. Define the transition $\tau(S, x)$ be the failure state if $x \in S$. The point is that in case $x \in S$ we can't

be reading a geodesic path. In case $x \notin S$, define

$$\tau(S, x) = \{ \overline{x^{-1}ga} \mid g \in S, a \in \Sigma \cup \{\epsilon\} \} \cap B_k(1).$$

Automatic groups satisfy quadratic isoperimetric inequality, i.e., every automatic group has its isoperimetric function bounded by a quadratic polynomial. The proof is relatively simple. Suppose a word $w = x_1 \dots x_n = 1$ in an automatic group G , thus bounds a disk in the Cayley graph of G . We get a representative path in the regular set L_0 for each $w_i = x_1 \dots x_i$. Clearly each representative path is linearly bounded in length as they can only be up to a distance k longer than its previous one, for some constant k . And between the successive two paths they stay close within a constant distance. Therefore the area bounded by w as its perimeter can be cut up into a quadratic number of small disks, each of which have a constant perimeter. Since there are only a constant number of such words of length bounded by a constant, defining the identity element in G , each of which can be written as a product of bounded number of conjugates of relators. This completes the proof.

We note that this proof gives us a $O(n^2)$ time algorithm to decide the word problem for automatic groups. Successively find the representative word for w_i , using w_{i-1} , and check finally if it is the empty word. It takes only $O(n^2)$ time, since we need to iterate only n times, and each time we are running a partially specified word on a finite automaton (the top track of the input tape), and trying to find a word, which if we supply to the bottom track of the input tape, our finite state automaton will accept. This can be done in real time, as we basically guess and label the finite number of states in the automaton as we go along.

An interesting question is the following: Can this be parallelized? In other words is the word problem for automatic groups in \mathcal{NC} or is it \mathcal{P} -hard under logspace reductions? Using parallel prefix search, each step of the algorithm can be parallelized to time $O(\log n)$, thus the entire algorithm can be speeded up to time $O(n \log n)$, using $n^{O(1)}$ processors. On the other hand, the mere fact that the successive words can be checked by a finite state automaton does not seem strong enough to ensure membership in \mathcal{NC} , as the successive ID's in a generic \mathcal{P} computation has this property as well. This leads to my conjecture that the word problem for automatic groups is \mathcal{P} -hard under logspace reductions.

4 Nilpotent groups

The significance of the quadratic isoperimetric inequality is that it is pretty much the only tool to prove certain groups are not automatic.

Another computationally important class of groups is the nilpotent groups. As an

example, we can consider the Heisenberg group. It has the presentation $\langle a, b, c \mid [a, b] = c, [a, c] = [b, c] = 1 \rangle$. More concretely, we can consider the upper triangular matrices with integral entries and 1's on the diagonal. It is generated by a and b where

$$a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, c = aba^{-1}b^{-1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

It can be shown that the Heisenberg group does not satisfy the quadratic isoperimetric inequality, and thus it is not automatic. An offending word can be chosen as $a^n b^n a^{-n} b^{-2n} a^{-n} b^n a^n$.

Nonetheless (finitely generated) nilpotent groups are extremely amenable to computation. In fact they resemble in some sense finitely generated abelian groups, and have a canonical representation similar to ordinary integer representations in binary, say.

It has been recognized in the combinatorial group theory community that problems on nilpotent groups, say the word problem, can be solved quickly. However the computational complexity of a problem should not be obscured by a particular representation scheme. What combinatorial group theorists meant by fast they refer to the word representation, which is similar to unary representation of an integer. Many problems are “fast” under the unary representation, as many computationally (probably) intractable problems in number theory are also “fast” under unary representation, such as factoring, discrete logarithm. But that is not honest complexity theory. The time is really exponential, compared to a more “reasonable” representation scheme of the information, such as in binary.

We can show that for a nilpotent group of class c , the canonical form takes space $O((\phi + 1)^c \cdot \log n)$ for a word in unary representation of length n , where $\phi \approx 1.618$ is the golden ratio. And this is sharp, in the sense that some nilpotent group of class c attains this bound. As a consequence, nilpotent groups also satisfy a polynomial isoperimetric inequality of the form $n^{O((\phi+1)^c)}$.

Thus, the canonical form and any further manipulations, such as to solve the word problem, multiplication of two elements, finding the inverse, conjugation, ..., can all be computed in almost linear time (linear in the binary length!) using polynomial arithmetic computation such as the Schönhage-Strassen algorithm.

A challenging problem is to devise a uniform framework that includes the automatic groups and nilpotent groups.

5 Random groups and knot polynomials

We consider in this section the following problem on random groups. We want to estimate the probability that a pair of randomly generated groups are isomorphic. We claim that

this probability is exponentially small. Here we deal with the simplest case, namely groups with two free generators modulo a single random word in the generators and their inverses.

$$G = \langle a, b \mid R \rangle.$$

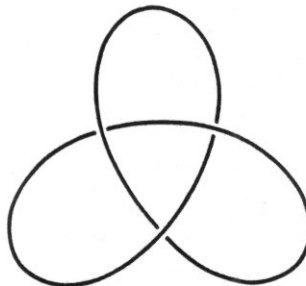
We will omit most proofs, only indicating the proof idea and techniques. A more detailed presentation of these results will be given in a separate paper.

The first idea is to abelianize the group G , thus we consider G/G' , where G' is the commutator subgroup of G . It is clear that in the group G , G' is generated as a normal subgroup by the commutator of a and b , i.e., $G' = \langle [a, b] \rangle_G$. Thus, with the help of second isomorphism theorem, $G/G' \cong \mathbf{Z} \times \mathbf{Z}/\bar{R}$, where $\mathbf{Z} \times \mathbf{Z}$ is the free abelian group of rank 2 and \bar{R} is the image of R in $\mathbf{Z} \times \mathbf{Z}$. Hence, \bar{R} can be taken as the word $a^i b^j$ where i and j are the exponent sums of a and b respectively in the word R .

Suppose we randomly generate two such groups G and G_1 , clearly if the greatest common divisor $\gcd(i, j) \neq \gcd(i_1, j_1)$ then the abelianization of G and G_1 are non-isomorphic, and thus *a fortiori* $G \not\cong G_1$. The problem is that the probability of $\gcd(i, j) = \gcd(i_1, j_1)$ is non-trivial. In fact, as the numbers i, j are independently distributed essentially according to the Gaussian distribution in the range of $O(-\sqrt{n})$ to $O(\sqrt{n})$, the so called *visibility probability* of $\gcd(i, j) = 1$ tends to be around $\frac{6}{\pi^2}$. Thus we must handle the case $\gcd(i, j) = \gcd(i_1, j_1) = 1$ with much more care. (The case $\gcd(i, j) = \gcd(i_1, j_1) \neq 1$ will not be discussed here.)

The idea is to consider the second commutator subgroup G'' . In fact the factor group G'/G'' will be investigated. It turns out that we will be better off not to just consider the group structure of the abelian group G'/G'' , but instead, making it into a suitable module over an operator ring. The intuitive idea is that we are not going to forget the order in which a and b appear in the random word, as we did in the previous paragraph when we abelianized the whole thing, but rather we will think of an appearance of $a^i b^j a^{-i}$ as the conjugate action of a^i on b^j ; and then we will forget (and forgive) any order in which these actions themselves appeared in R .

This idea is due to the topologist Alexander when he considered fundamental groups of 3-dimensional knots. So let's consider the *Mother of All Knots*, the *trefoil* (also known as the *clover leave*) knot pictured below.



The fundamental group of this knot has the presentation

$$T = \langle a, b \mid a^2 = b^3 \rangle.$$

In order to facilitate the consideration of T'/T'' , we would like to transform the free generators a, b to a new set of free generators, where T' has a easier form for us to handle. We will write down the following matrix representing the exponent sums of a and b in the relator a^2b^{-3}

$$\begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} 2 \\ -3 \end{pmatrix}.$$

Now we will perform a two-dimensional basis reduction, which is just the Euclidean algorithm on the matrix while keeping track of the new free generators.

$$\begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} 2 \\ -3 \end{pmatrix} \longrightarrow \begin{pmatrix} ab^{-1} \\ b \end{pmatrix} \begin{pmatrix} 2 \\ -1 \end{pmatrix} \longrightarrow \begin{pmatrix} ab^{-1} \\ b(ab^{-1})^{-2} \end{pmatrix} \begin{pmatrix} 0 \\ -1 \end{pmatrix}.$$

Let $\alpha = ab^{-1}$ and $\beta = b(ab^{-1})^{-2} = b^2a^{-1}ba^{-1}$. Thus the trefoil group T has the following presentation as well:

$$T = \langle \alpha, \beta \mid W \rangle,$$

where

$$\begin{aligned} W &= a^2b^{-3} = (\alpha\beta\alpha^2)^2(\beta\alpha^2)^{-3} \\ &= \alpha\beta\alpha\beta^{-1}\alpha^{-2}\beta^{-1} \\ &= \beta^{-1}B(\alpha, \beta), \end{aligned}$$

where the word $B = \beta\alpha\beta\alpha\beta^{-1}\alpha^{-2}\beta^{-1}$ has zero exponent sums for α and β .

What about T' ? Surely $B \in T'$ as it has zero exponent sums. Thus $\beta^{-1} \in T'$. Therefore all the conjugates and inverses of β are in T' , $\beta_n = \alpha^n\beta\alpha^{-n}$, for $n = 0, \pm 1, \pm 2, \dots$

It can be easily verified that these elements β_n generate T' and the abelian group T'/T'' has the following (not finitary) presentation:

$$T'/T'' = \langle \beta_n, n = 0, \pm 1, \pm 2, \dots \mid [\beta_n, \beta_m], \beta^{-1}B \rangle,$$

where B is a word over β_n 's, namely

$$B = \beta_0\beta_1\beta_2^{-1}\beta_0^{-1}.$$

Now we are going to define an action on the abelian group T'/T'' to make it into a module over a suitable ring, and derive an invariant which is very hard to duplicate by another random word \tilde{W} .

The action we define is the natural one, namely conjugation by α , thus,

$$\beta_n^\theta = \beta_{n+1}, n = 0, \pm 1, \pm 2, \dots,$$

and

$$\beta_n^{\theta^{-1}} = \beta_{n-1}, n = 0, \pm 1, \pm 2, \dots$$

This naturally extends to an action on T'/T'' by the ring generated by θ and θ^{-1} over the integers

$$\mathcal{L}(\theta) = \{\theta^{-n}f(\theta), n = 0, 1, 2, \dots\}$$

where $f(\theta)$ is any polynomial with integral coefficients. That this action is well-defined follows from the fact that T'/T'' is abelian.

Now $\beta^{-1}B = \beta^{(-1+1+\theta-\theta^2-1)}$, and the polynomial $1 - \theta + \theta^2$ is called the Alexander polynomial of the trefoil knot.

For our random group G , one can carry out the similar procedure, and arriving at a polynomial $f(\theta)$ which annihilates the generator β in the module G'/G'' . Thus the polynomial characterizes the order in which the α 's and β 's appeared in R but forgets the order of the conjugated version of the β 's.

Why is this a good invariant? Suppose the word B is more or less randomly generated with the condition that the exponent sums are zero,

$$B = \alpha^{i_1} \beta^{j_1} \alpha^{i_2} \beta^{j_2} \dots \alpha^{i_k} \beta^{j_k},$$

then clearly the corresponding polynomial will be

$$f(\theta) = j_1 \theta^{i_1} + j_2 \theta^{i_1+i_2} + \dots + j_{k-1} \theta^{i_1+i_2+\dots+i_{k-1}} + j_k.$$

We note that $\sum_{\ell} i_{\ell} = \sum_{\ell} j_{\ell} = 0$. Clearly two such polynomials corresponding to randomly chosen two words could coincide with only exponentially small probability.

Of course we should verify that the polynomial so obtained is an invariant of the group G . This is relatively easy to see. Suppose $G \cong G_1$. Since $G/G' \cong \langle \alpha \rangle$ is an infinite cyclic group, the isomorphism σ from G to G_1 must take α to α_1 modulo G'_1 , or α_1^{-1} modulo G'_1 , since they are the only generators for G_1/G'_1 . Suppose $\sigma(\alpha) = \alpha_1 k_1'$, then the action by $\sigma(\alpha)$ on β_1 is the action by α_1 followed by the conjugation by k_1' . But since G'/G'' is abelian and $k_1' \in G'_1$, this last one is inner and thus trivial. Thus, up to a change of θ^{-1} for θ , the induced polynomial is the minimal polynomial that annihilates the generator and thus the module. Therefore, up to a change of θ^{-1} for θ , $f(\theta)$ is an invariant of the group.

Acknowledgement

I wish to thank Laci Babai, Benson Farb, Laci Lovasz, Miki Simonovits, Bill Thurston, Andy Yao for many interesting conversations on the subject.

References

- [1] G. Baumslag, S.M.Gersten, M.Shapiro, and H. Short. Automatic groups and amalgams, Unpublished.
- [2] J.W. Cannon, D.B.A. Epstein, D.F.Holt, M.S.Paterson, and W.P.Thurston, Word processing and group theory, Preprint, University of Warwick, 1990.
- [3] J.E.Hopcroft and J.D.Ullman, Introduction to automata theory, languages and computation. Addison Wesley, 1979.
- [4] W.Magnus, A. Karrass and D.Solitar, Combinatorial group theory. Interscience Publishers, 1966.
- [5] M. Gromov, Hyperbolic groups, in "Essays in group theory", MSRI series vol 8, S.M.Gersten, editor, Springer Verlag, 1987.