数理解析研究所講究録 1329 巻 2003 年 115-120

COMPLEXITY OF THE WORD PROBLEM FOR SOME 3-MANIFOLD GROUPS

東京工業大学 情報理工学研究科 大山 洋史 (HIROSHI OOYAMA)
DEPARTMENT OF MATHEMATICAL AND COMPUTING SCIENCES,
TOKYO INSTITUTE OF TECHNOLOGY

ABSTRACT. In this paper, we show that the word problem for fundamental groups of torus bundles over the circle is solvable in quadratic time by finding explicit embeddings of them in $\mathrm{GL}(n,\mathbb{Q})$.

1. INTRODUCTION

Let G be a group with a finite presentation $\langle\mathcal{A}|\mathcal{R}\rangle$. We assume that the set of relators $\mathcal{R}$ is closed under inversion and cyclic shifts. A word $w\in(\mathcal{A}\cup\mathcal{A}^{-1})^*$ represents the identity element of G if and only if w can be rewritten to null word ϵ with following rules:

(1) Reduce if $a\in\mathcal{A}$ and a^{-1} are adjacent.

$$\alpha aa^{-1}\beta\rightarrow\alpha\beta,\ \alpha a^{-1}a\beta\rightarrow\alpha\beta.$$

(2) Insert a relator $r\in\mathcal{R}$.

$$\alpha\beta\rightarrow\alpha r\beta.$$

The minimum number of inserted relators to rewrite w to ϵ is called the area of w. The Dehn function $f(n)$ is defined as the maximum area of words whose length are at most n. The number of reduction is bounded by a constant multiple of the area of w plus the length of the word. The constant is determined by the maximum length of all relators in $\mathcal{R}$. Hence, the length of the optimal rewriting process is $O(f(n)+n)$.

If a Dehn function of a group is computable, the word problem of the group is solvable.

A group which has a linear Dehn function is called a word-hyperbolic group. It is well known that a word problem of a word-hyperbolic group is solvable in linear time with string rewriting on $(\mathcal{A}\cup\mathcal{A}^{-1})^*$ style algorithm. There is the class of automatic groups, which is larger than the class of word-hyperbolic groups. Automatic groups have quadratic Dehn functions, and their word problems are solvable in quadratic time with string rewriting on $(\mathcal{A}\cup\mathcal{A}^{-1})^*$ manner [4].

The classes of nilpotent and solvable groups are not contained in the class of automatic groups. In these classes, fundamental groups of torus bundles over the circle are of interest for 3-dimensional geometry. These groups do not have quadratic isoperimetric inequalities except virtually abelian ones [3, 4]. So their word problems may not be solved in quadratic time with string rewriting on $(\mathcal{A}\cup\mathcal{A}^{-1})^*$.

On the other hand, the word problem of a finitely generated subgroup of $\mathrm{GL}(n,\mathbb{Q})$ is solvable in quadratic time.

2000 *Mathematics Subject Classification.* Primary 20F10; Secondary 20F16, 20F18.

In this paper, we prove that the word problem for some nilpotent and solvable groups arising as fundamental groups of torus bundles over the circle is solvable in quadratic time by finding explicit embeddings of them in $\mathrm{GL}(n,\mathbb{Q})$.

Theorem 1.1. *The word problem for the fundamental group of a torus bundle over the circle is solvable in quadratic time.*

2. Dehn functions and areas of relators

Let G be a group with a finite presentation $\langle \mathcal{A}|\mathcal{R}\rangle$. Then there is an exact sequence

$$1 \to N \to F(\mathcal{A}) \xrightarrow{p} G \to 1$$

where $F(\mathcal{A})$ is the free group generated by $\mathcal{A}$ and N is the normal closure of $\mathcal{R} = \{r_1, \dots, r_n\}$ in $F(\mathcal{A})$. For each $w \in F(\mathcal{A})$ there is a unique way of writing w as a reduced word $w = a_1 \cdots a_k \in (\mathcal{A} \cup \mathcal{A}^{-1})^*$. We denote the length of w by $|w| = k$. The element w is called a *relator* for the presentation $\langle \mathcal{A}|\mathcal{R}\rangle$ if $p(w) = 1 \in G$. In this case, w can be written in the form

$$w = \prod_{i=1}^{m} u_i r_{k_i}^{e_i} u_i^{-1}$$

where $u_i \in F(\mathcal{A})$, $r_{k_i} \in \mathcal{R}$, and $e_i \in \{1, -1\}$. We define Area(w) to be the smallest value of m among all expressions of the form.

$$\mathrm{Area}(w) = \min\{m | w = \prod_{i=1}^{m} u_i r_{k_i}^{e_i} u_i^{-1}\}.$$

A function $f : \mathbb{N} \to \mathbb{N}$ is an isoperimetric function if

$$\max\{\mathrm{Area}(w) | w \in F(\mathcal{A}), |w| \leq n\} \leq f(n)$$

for all $n \in \mathbb{N}$. The smallest isoperimetric function is called the Dehn function.

Definition 2.1. We consider a preorder $\preceq$ on the set of functions $\mathbb{N} \to \mathbb{N}$. $f \preceq g$ if there exist positive constants α, β, γ such that $f(n) \leq \alpha g(\beta n) + \gamma n$ for all $n \in \mathbb{N}$. We say that f and g are *equivalent* if $f \preceq g$ and $g \preceq f$. We denote by $\simeq$ the equivalence relation.

Dehn functions corresponding to different finite presentations of the same group are equivalent. The Dehn function of a finitely presented group is well defined up to equivalence.

Let $\mathcal{R}'$ be the closure of $\mathcal{R}$ under inversion and cyclic shifts. Then the presentation $\langle \mathcal{A}|\mathcal{R}'\rangle$ is another presentation of the group with a presentation $\langle \mathcal{A}|\mathcal{R}\rangle$, and the area Area$'(w)$ of w which associates to $\mathcal{R}'$ is equal to Area(w) which associates to $\mathcal{R}$. We assume that $\mathcal{R}$ is closed under inversion and cyclic shifts.

Dehn function measures the complexity of word problem for G. We consider a string rewriting system whose set of rewriting rules is

$$\{aa^{-1} \to \epsilon, a^{-1}a \to \epsilon | a \in \mathcal{A}\} \cup \{\epsilon \to r | r \in \mathcal{R}\}$$

where ϵ is the null string in $(\mathcal{A} \cup \mathcal{A}^{-1})^*$. For each word w, if w is trivial in G, then there is a derivation $w \to w_1 \to \cdots \to \epsilon$ and its length is at most constant multiple of Area$(w) + |w|$. There is a nondeterministic Turing machine simulates this derivation.

For every finitely presented group G with the Dehn function $f(n)$, there exists a nondeterministic Turing machine which solves the word problem in time $O(f(n)+n)$.

3. LINEAR GROUPS HAVE QUADRATIC WORD PROBLEMS

In this section we prove the following theorem.

Theorem 3.1. *Let F be a finite extension of $\mathbb{Q}$. Then the word problem of every finitely generated subgroup of $\mathrm{GL}(n,F)$ can be solved in quadratic time.*

For matrices $A=(a_{ij})\in M(n,\mathbb{C})$, we denote $\max_{i,j}|a_{ij}|$ by $\|A\|$.

Since the product and sum of two integers a and b, written in binary, can be computed in time $O(\log|a|\log|b|)$, the product AB of integer matrices A,B can be computed in time $O(\log\|A\|\log\|B\|)$ and $\|AB\|\leq n\|A\|\|B\|$. p

Proof of Theorem 3.1. Let G be a finitely generated subgroup of $\mathrm{GL}(n,F)$ and $X=\{x_1,\dots,x_m\}$ be a set of semigroup generators. Let $A_i (i=1,\dots,m)$ be a $n\times n$ matrix over F which corresponds to x_i. Then we can reduce the word problem to the following.

Problem. For each word $w=x_{i_1}\cdots x_{i_l}$, decide whether the product $A_{i_1}\cdots A_{i_l}$ is equal to the identity matrix I.

We first solve the problem in the case $F=\mathbb{Q}$.

Let λ be the least common multiple of the denominators of all the entries in all the generating matrices. Multiplying the generating matrices by λ, we have integer matrices $\lambda A_1,\dots,\lambda A_m$. We can compute the product $(\lambda A_{i_1})\cdots(\lambda A_{i_l})$ of integer matrices in time $O(l^2)$, and compare it with $(\lambda^l)I$ in time $O(l)$.

When F is a finite extension of $\mathbb{Q}$, we can reduce the problem to the case $F=\mathbb{Q}$. F is a simple algebraic extension $\mathbb{Q}(\theta)$ of $\mathbb{Q}$. Let $f(x)=x^m-c_{m-1}x^{m-1}-\cdots-c_1x-c_0\in\mathbb{Q}[x]$ be the minimum polynomial of θ.

There exist a (associative $\mathbb{Q}$-algebra) monomorphism $\rho:\mathbb{Q}(\theta)\to M_m(\mathbb{Q})=\mathrm{End}(\mathbb{Q}^m)$([5], chapter 7)

$$\theta\mapsto\begin{pmatrix}0&0&\dots&0&c_0\\1&0&\dots&0&c_1\\0&1&\dots&0&c_2\\\vdots&&\ddots&\vdots&\vdots\\0&\dots&0&1&c_{n-1}\end{pmatrix}.$$

Let $\bar\rho=\mathrm{id}_{M(n,\mathbb{Q})}\otimes\rho: M(n,\mathbb{Q}(\theta))\to M(n,\mathbb{Q})\otimes_{\mathbb{Q}}M(m,\mathbb{Q})$. Then $\bar\rho$ embeds $\mathrm{GL}(n,\mathbb{Q}(\theta))$ into $\mathrm{GL}(nm,\mathbb{Q})$. Applying $\bar\rho$ to generating matrices, we obtain a set $\{\bar\rho(A_1),\dots,\bar\rho(A_k)\}$ of $mn\times mn$ matrices over $\mathbb{Q}$ as a new set of generating matrices. Thus the problem can be solved in quadratic time. □

4. FUNDAMENTAL GROUPS OF TORUS BUNDLES OVER THE CIRCLE

Consider the split extension $1\to\mathbb{Z}^n\to G\to\mathbb{Z}\to 1$. Let $e_1,e_2,\dots,e_n$ be a basis for $\mathbb{Z}^n$ and let t be a generator for $\mathbb{Z}$. There exists $A\in\mathrm{GL}(n,\mathbb{Z})$ which admits a presentation $G=\mathbb{Z}^n\rtimes_A\mathbb{Z}$

$$\langle e_1,\dots e_n,t|[e_i,e_j],te_it^{-1}A(e_i)^{-1}(i,j=1,\dots n)\rangle.$$

The fundamental group G of a T^n bundle over S^1 with gluing automorphism $A: T^n \to T^n$ is a semidirect product $G = \mathbb{Z}^n \rtimes_A \mathbb{Z}$.

It is well known that fundamental groups of closed 3-manifolds modelled on Sol or Nil geometry are not automatic [4]. A 3-manifold M which is expressed as a torus bundle over S^1 with reducible or Anosov gluing map $g: T^2 \to T^2$ is modelled on Nil or Sol, respectively. The fundamental group G of M is isomorphic to a semidirect product of $\mathbb{Z} = \pi_1(S^1)$ by $\mathbb{Z}^2 = \pi_1(T^2)$.

$$\pi_1(M) = G = \mathbb{Z}^2 \rtimes_A \mathbb{Z}.$$

The fundamental groups of torus bundles over the circle with Anosov gluing maps have Dehn functions which are equivalent to exponential functions. Hence, the lengths of rewriting processes of their words to the null word grow exponentially. However, we can embed these groups in $\mathrm{GL}(n, \mathbb{Q})$, and the word problems of linear groups over the rational numbers are solvable in (deterministic) quadratic time.

4.1. **Dehn functions.** Dehn function of $\mathbb{Z}^n \rtimes_A \mathbb{Z}$ is studied in [1, 2, 3].

The Dehn function $f(k)$ of $\mathbb{Z}^n \rtimes_A \mathbb{Z}$ is characterized by growth of the matrix A^k.

Theorem 4.1 ([3], Theorem 3.1). *Let $G = \mathbb{Z}^n \rtimes_A \mathbb{Z}$ where $A \in \mathrm{GL}(n, \mathbb{Z})$. If $f: \mathbb{N} \to \mathbb{N}$ is the Dehn function of any finite presentation of G then*

$$f(k) \simeq k^2 \|A^k\|.$$

Sketch of proof. The upper bound of $f(k)$ is obtained by combing argument [1].

To obtain the lower bound for f, we consider relators

$$w_k = t^k e_j^k t^{-k} e_{i+n}^k t^k e_j^{-k} t^{-k} e_{i+n}^{-k}.$$

Analyzing the geometry of van Kampen diagrams of w_k, we have

$$\mathrm{Area}(w_k) \geq k^2 \|A^k\|.$$

Hence $k^2 \|A^k\| \preceq f(k)$ [2, 3]. □

For $A \in \mathrm{SL}(2, \mathbb{Z})$, the growth of $\|A^k\|$ is as following:

- If $|\operatorname{tr} A| < 2$ or $A = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ then there is $m \in \mathbb{Z}$ such that $A^m = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Hence, $\|A^k\| \simeq 1$. And $\mathbb{Z}^2 \rtimes_A \mathbb{Z}$ is virtually abelian.
- If $|\operatorname{tr} A| = 2$ and $A \neq \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ then $\|A^k\| \simeq k$. And $\mathbb{Z}^2 \rtimes_A \mathbb{Z}$ is a nilpotent group.
- If $|\operatorname{tr} A| > 2$ then A has an eigenvalue λ whose absolute value is greater than 1. $\|A^k\| \simeq |\lambda|^k$. And $\mathbb{Z}^2 \rtimes_A \mathbb{Z}$ is a solvable group.

Corollary 4.2 ([2]). *The Dehn functions of cocompact lattices in Nil are equivalent to cubic polynomials. The Dehn functions of cocompact lattices in Sol are equivalent to exponential functions.*

4.2. **Linear representations.** We shall give an embedding of $G = \mathbb{Z}^2 \rtimes_A \mathbb{Z}$ in $\mathrm{GL}(n, F)$ where F is a finite extension of $\mathbb{Q}$. Applying Theorem 3.1, we can solve the word problem of G in quadratic time.

We consider the presentation of G

$$\langle x, y, t | xyx^{-1}y^{-1}, txt^{-1}A(x)^{-1}, tyt^{-1}A(y)^{-1} \rangle$$

where x, y are generators for $\mathbb{Z}^2$. Remark that all element in G has a representation in the normal form $x^a y^b t^c (a, b, c \in \mathbb{Z})$.

When $\operatorname{tr} A = 2$, there is an integer K and $P \in \mathrm{SL}(2,\mathbb{Z})$ such that

$$A = P^{-1}\begin{pmatrix}1 & 0\\ K & 1\end{pmatrix}P.$$

Changing generators, G is finitely presented by

$$\langle x, y, t | xyx^{-1}y^{-1}, txt^{-1}x^{-1}y^{-K}, tyt^{-1}y^{-1}\rangle$$

and it is linearly represented by the assignment,

$$x^a y^b t^c \mapsto \begin{pmatrix}1 & 0 & 0\\ a & 1 & 0\\ b & cK & 1\end{pmatrix} \in \mathrm{GL}(3,\mathbb{Z}).$$

Notice that the map defined as above is actually a homomorphism, because it maps all relators in the presentation to the identity matrix. And the map is obviously injective.

When $|\operatorname{tr} A| \neq 2$, ${}^t\!A$ has an eigenvector $\begin{pmatrix}\alpha\\ 1\end{pmatrix}$ and an eigenvalue λ.

$$\lambda\begin{pmatrix}\alpha\\ 1\end{pmatrix} = {}^t\!A\begin{pmatrix}\alpha\\ 1\end{pmatrix}.$$

λ is algebraic over $\mathbb{Q}$, and α is in $\mathbb{Q}(\lambda)$. The abelian group $\mathbb{Z}^2$ is embedded into $\mathbb{Q}(\lambda)$ by a map $\varphi : \begin{pmatrix}a\\ b\end{pmatrix} \mapsto a\alpha + b$ if we denote an element $x^a y^b \in \mathbb{Z}^2$ by $\begin{pmatrix}a\\ b\end{pmatrix}$. Notice that

$$\varphi(A\begin{pmatrix}a\\ b\end{pmatrix}) = \lambda(a\alpha + b).$$

Let μ be a square root of λ. We define a linear representation $\rho : G \to \mathrm{SL}(2,\mathbb{Q}(\mu))$ by

$$x \mapsto \begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix}, y \mapsto \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, t \mapsto \begin{pmatrix}\mu & 0\\ 0 & \mu^{-1}\end{pmatrix}.$$

ρ is well defined, because

- $\rho(x)\rho(y) = \rho(y)\rho(x)$ and
$$\rho(x^a y^b) = \begin{pmatrix}1 & \varphi(\begin{pmatrix}a\\ b\end{pmatrix})\\ 0 & 1\end{pmatrix},$$
- $\rho(t)\rho(x)\rho(t)^{-1} = \rho(A(x))$, $\rho(t)\rho(y)\rho(t)^{-1} = \rho(A(y))$:
$$\begin{pmatrix}\mu & 0\\ 0 & \mu^{-1}\end{pmatrix}\begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix}\begin{pmatrix}\mu & 0\\ 0 & \mu^{-1}\end{pmatrix}^{-1} = \begin{pmatrix}1 & \lambda\alpha\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & \varphi(A(x))\\ 0 & 1\end{pmatrix},$$
$$\begin{pmatrix}\mu & 0\\ 0 & \mu^{-1}\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}\mu & 0\\ 0 & \mu^{-1}\end{pmatrix}^{-1} = \begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & \varphi(A(y))\\ 0 & 1\end{pmatrix}.$$

Proposition 4.3. *If* $|\operatorname{tr} A| > 2$, *$\rho$ is injective.*

Proof. We show that the kernel of ρ is trivial.

Notice that

$$\rho(x^a y^b t^c) = \begin{pmatrix}\mu^c & \mu^{-c}(a\alpha + b)\\ 0 & \mu^{-c}\end{pmatrix}.$$

If $x^a y^b t^c$ is mapped to the identity matrix, $\mu^c = 1$ and $a\alpha + b = 0$. Since $|\mu| \neq 1$ and $\alpha \notin \mathbb{Q}$, $a = b = c = 0$. $\square$

If $|\operatorname{tr} A| < 2$, then $\mu^c = 1$ for some integer $c \neq 0$. Since $t^c \in G$ is not the identity if $c \neq 0$, the representation ρ is not injective in this case. But we can define an injection $\rho' : G \to \mathrm{GL}(3, \mathbb{Q}(\mu))$ by

$$x^a y^b t^c \mapsto \begin{pmatrix} \rho(x^a y^b t^c) & \\ & 2^c \end{pmatrix}.$$

Thus we have proved Theorem 1.1.

References

[1] M.R. Bridson, *Combings of semidirect products and 3-manifold groups*, Geom.Funct.Anal. **3**(3) (1993), 263-278.

[2] M.R. Bridson and Ch. Pittet, *Isoperimetric inequalities for the fundamental groups of torus bundles over the circle*, Geom. Dedicata **49**(2) (1994), 203-219.

[3] M.R. Bridson and S.M. Gersten, *The optimal isoperimetric inequalities for torus bundles over the circle*, Quart. J. Math. Oxford (2) **47**(185) (1996),1-23.

[4] D.B.A. Epstein, J.W. Cannon, D.F. Holt, S.V.F. Levy, M.S. Paterson and W.P. Thurston, *Word processing in groups*, Bartlett and Jones, 1992.

[5] N. Jacobson, *Basic Algebra I*, W.H. Freeman, 1985.

Department of Mathematical and Computing Sciences, Tokyo Institute of Technology, 2-12-1, O-okayama, Meguro-ku, Tokyo, 152-8550, Japan

E-mail address: `Hiroshi.Oyama@is.titech.ac.jp`