Journal of Algebra 407 (2014) 178–200

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Algorithmic theory of free solvable groups: Randomized computations

Alexander Ushakov [1,2]

Stevens Institute of Technology, Hoboken, NJ 07030, USA

ARTICLE INFO

Article history:
Received 23 January 2013
Available online 1 April 2014
Communicated by Derek Holt

MSC:
03D15
20F65
20F10

Keywords:
Solvable groups
Metabelian groups
Word problem
Cyclic subgroup membership
Power problem
Conjugacy problem
Randomized algorithms

ABSTRACT

We design new deterministic and randomized algorithms for computational problems in free solvable groups. In particular, we prove that the word problem and the power problem can be solved in quasi-linear time and the conjugacy problem can be solved in quasi-quartic time by Monte Carlo type algorithms.

1. Introduction

The study of algorithmic problems in free solvable groups can be traced to the work [11] of Magnus, who in 1939 introduced an embedding (now called the *Magnus embedding*) of an arbitrary group of the type $F/[N,N]$ into a matrix group of a particular

E-mail address: aushakov@stevens.edu.

[1] This work was partially supported by NSA Mathematical Sciences Program grant number H98230-14-1-0128.

[2] The author would like to thank Andrey Nikolaev for his helpful and insightful comments.

http://dx.doi.org/10.1016/j.jalgebra.2014.02.014

type with coefficients in the group ring of F/N (see Section 1.5 below). Since the word problem in free abelian groups is decidable in polynomial time, by induction, this embedding gives a polynomial time decision algorithm for a fixed free solvable group $S_{r,d}$. However the degree of the polynomial here grows together with d. An algorithm polynomial in both: the length of a given word and the class d of the free solvable group was found later in [15]. It was proved that the word problem has time complexity $O(r|w|\log_2|w|)$ in the free metabelian group $S_{r,2}$, and $O(rd|w|^3)$ in a free solvable group $S_{r,d}$ for $d \geqslant 3$.

The general approach to the conjugacy problem in wreath products was suggested by Matthews in [14] who also described the solution to the conjugacy problem in free metabelian groups. The first solution to the conjugacy problem in free solvable groups was given by Remeslennikov and Sokolov in [20] who proved that the conjugacy in $S_{r,d}$ can be reduced to the conjugacy in a wreath product of $S_{r,d-1}$ and a free abelian group. Later Vassileva showed in [24] that the power problem in free solvable groups can be solved in $O(rd(|u| + |v|)^6)$ time and used that result to show that the Matthews–Remeslennikov–Sokolov approach can be transformed into a polynomial time $O(rd(|u|+|v|)^8)$ algorithm. In this paper we improve the results of [15] and [24], namely we prove that:

Theorem 2.6. *There exists a quasi-quadratic time $\tilde{O}(|w|^2)$ deterministic algorithm solving the word problem in $S_{r,d}$.*

Theorem 5.1. *There exists a quasi-quadratic time $\tilde{O}((|u|+|v|)^2)$ deterministic algorithm solving the power problem in $S_{r,d}$.*

Theorem 6.5. *There exists a quasi-quintic time $\tilde{O}((|u| + |v|)^5)$ deterministic algorithm solving the conjugacy problem in $S_{r,d}$.*

We can improve these results further if we grant our machine an access to a random number generator. The price of that improvement is an occasional incorrectness of the result. Fortunately, we can control the probability of an error: for any fixed polynomial p we can adjust some internal parameter in the algorithm to guarantee that the probability of an error converges to 0 as fast as $O(1/p(n))$.

Theorem 4.5. *There exists a quasi-linear time $\tilde{O}(|w|)$ false-biased randomized algorithm solving the word problem in $S_{r,d}$.*

Theorem 5.2. *There exists a quasi-linear time $\tilde{O}(|u|+|v|)$ unbiased randomized algorithm solving the power problem in $S_{r,d}$.*

Theorem 6.6. *There exists a quasi-quartic time $\tilde{O}((|u| + |v|)^4)$ unbiased randomized algorithm solving the conjugacy problem in $S_{r,d}$.*

Also, we want to mention Theorem 6.4 which gives a geometric approach to the conjugacy problem in free solvable groups.