Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Advances in Applied Mathematics 35 (2005) 323–334
ADVANCES IN Applied Mathematics
www.elsevier.com/locate/yaama

# Probabilistic solutions of equations in the braid group ☆

David Garber [a,b], Shmuel Kaplan [c], Mina Teicher [c], Boaz Tsaban [d,*], Uzi Vishne [c]

[a] *Einstein Institute of Mathematics, The Hebrew University, Givat-Ram 91904, Jerusalem, Israel*
[b] *Department of Sciences, Holon Academic Institute of Technology, 52 Golomb Street, Holon 58102, Israel*
[c] *Department of Mathematics and Statistics, Bar-Ilan University, Ramat-Gan 52900, Israel*
[d] *Department of Applied Mathematics and Computer Science, The Weizmann Institute of Science, Rehovot 76100, Israel*

Received 30 August 2004; accepted 4 March 2005

Available online 14 June 2005

**Abstract**

Given a system of equations in a "random" finitely generated subgroup of the braid group, we show how to find a small ordered list of elements in the subgroup, which contains a solution to the equations with a significant probability. Moreover, with a significant probability, the solution will be the first in the list. This gives a probabilistic solution to: the conjugacy problem, the group membership problem, the shortest presentation of an element, and other combinatorial group-theoretic problems in random subgroups of the braid group.

We use a memory-based extension of the standard length-based approach, which in principle can be applied to any group admitting an efficient, reasonably behaving length function.


☆ This paper is a part of the PhD thesis of the second named author at Bar-Ilan University.

* Corresponding author.
*E-mail addresses:* garber@math.huji.ac.il, garber@hait.ac.il (D. Garber), kaplansh@math.biu.ac.il (S. Kaplan), teicher@math.biu.ac.il (M. Teicher), boaz.tsaban@weizmann.ac.il (B. Tsaban), vishne@math.biu.ac.il (U. Vishne).
*URL:* http://www.cs.biu.ac.il/~tsaban (B. Tsaban).

0196-8858/$ – see front matter 
doi:10.1016/j.aam.2005.03.002

## 1. The general method

### 1.1. Systems of equations in a group

Fix a group $G$. A *pure equation* in $G$ with variables $X_i$, $i \in \mathbb{N}$, is an expression of the form

$$X_{k_1}^{\sigma_1} X_{k_2}^{\sigma_2} \cdots X_{k_n}^{\sigma_n} = b, \tag{1}$$

where $k_1, \ldots, k_n \in \mathbb{N}$, $\sigma_1, \ldots, \sigma_n \in \{1, -1\}$, and $b$ is given. A *parametric equation* is one obtained from a pure equation by substituting some of the variables with given (known) parameters. By *equation* we mean either a pure or a parametric one. Since any probabilistic method to solve a system of equations implies a probabilistic mean to check that a given system has a solution, we will confine attention to systems of equations which possess a solution.

Given a system of equations of the form (1), it is often possible to use algebraic manipulations (taking inverses and multiplications of equations) in order to derive from it a (possibly smaller) system of equations all of which share the same leading variable, that is, such that all equations have the form

$$X W_i = b_i, \tag{2}$$

where $X$ is one of the variables appearing in the original system. The task is to find the leading variable $X$ in the system (2). Having achieved this, the process can be iterated to recover all variables appearing in the original system (1). In the sequel we confine our attention to systems consisting of one or more equations of the form (2).

### 1.2. Solving equations in a finitely generated group

The following general scheme is an extension of one suggested by Hughes and Tannenbaum [6] and examined in [2]. Our new scheme turns out dramatically more successful (compare the results of Section 2 to those in [2]).

It is convenient to think of each of the variables as an unknown element of the group $G$. Assume that the group $G$ is generated by the elements $a_1, \ldots, a_m$, and that there exists a "reasonable" length function $\ell : G \to \mathbb{R}^+$, that is, such that the expected length tends to increase with the number of multiplied generators.

Assume that equations of the form (2), $i = 1, \ldots, k$, are given. We propose the following algorithm: Since $X \in G$, it has a (shortest) form

$$X = a_{j_1}^{\sigma_1} a_{j_2}^{\sigma_2} \cdots a_{j_n}^{\sigma_n}.$$

The algorithm generates an ordered list of $M$ sequences of length $n$, such that with a significant probability, the sequence

$$\big((j_1, \sigma_1), (j_2, \sigma_2), \ldots, (j_n, \sigma_n)\big)$$