Journal of Algebra 408 (2014) 115–137

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Normal forms of random braids

Volker Gebhardt *,[1,2], Stephen Tawn [1]

University of Western Sydney, Centre for Research in Mathematics, Locked Bag 1797, Penrith NSW 2751, Australia

ARTICLE INFO

Article history:
Received 27 May 2013
Available online 5 November 2013
Communicated by Derek Holt

Keywords:
Random braids
Garside monoid
Normal form
Penetration distance
Expected value
Regular language

ABSTRACT

Analysing statistical properties of the normal forms of random braids, we observe that, except for an initial and a final region whose lengths are uniformly bounded (that is, the bound is independent of the length of the braid), the distributions of the factors of the normal form of sufficiently long random braids depend neither on the position in the normal form nor on the lengths of the random braids. Moreover, when multiplying a braid on the right, the expected number of factors in its normal form that are modified, called the *expected penetration distance*, is uniformly bounded.

We explain these observations by analysing the growth rates of two regular languages associated to normal forms of elements of Garside groups, respectively to the modification of a normal form by right multiplication.

A universal bound on the expected penetration distance in a Garside group yields in particular an algorithm for computing normal forms that has linear expected running time.

1. Introduction

Explicit computations play an increasingly important role in most areas of algebra; the study of braids is no exception. In many situations, computations with braids involve choosing braids at random: Some algorithms explicitly require a random braid to be generated; this is the case, for instance, in cryptographic protocols based on the braid group [1,12]. At other times, a large collection of typical

* Corresponding author.
E-mail addresses: v.gebhardt@uws.edu.au (V. Gebhardt), stephen@tawn.co.uk (S. Tawn).
URLs: http://www.uws.edu.au/crm (V. Gebhardt), http://www.stephentawn.info, http://www.uws.edu.au/crm (S. Tawn).

[1] Both authors acknowledge support under Australian Research Council's Discovery Projects funding scheme (project number DP1094072).
[2] Volker Gebhardt acknowledges support under the Spanish Project MTM2010-19355.

0021-8693/$ – see front matter
http://dx.doi.org/10.1016/j.jalgebra.2013.10.008

examples is to be generated; this is usually the case in computational experiments supporting theoretical research.

As B_n, the group of braids on n strands, is infinite, choosing braids at random is not a trivial task. There are various natural ways of choosing elements of B_n at random, and different approaches will yield different probability distributions on B_n. For both, computational experiments and applications (especially applications in cryptography), it is important to understand the statistical probabilities of samples of random elements generated using a particular method.

We consider in the following the *braid monoid* B_n^+ defined by the presentation

$$B_n^+ = \left\langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & (1 \leqslant i < j+1 \leqslant n) \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} & (1 \leqslant i < n-1) \end{array} \right\rangle^+, \tag{1}$$

which follows Artin's presentation for the braid group [2]. As the relations of B_n^+ are homogeneous, the number of generators occurring in any expression of $x \in B_n^+$ is well-defined; we call this number the *length* $|x|$ of x. We can then fix a non-negative integer k and generate an element $x \in B_n^+$ of length k. More specifically, there are two possibilities:

(A) For $i = 1, 2, \ldots, k$ independently choose $a_i \in \mathcal{A} = \{\sigma_1, \sigma_2, \ldots, \sigma_{n-1}\}$ with a uniform probability distribution on $\mathcal{A}$, or equivalently, consider the set $\mathcal{A}^*|_k$ of all *words* of length k over the alphabet $\mathcal{A}$, and choose an element of $\mathcal{A}^*|_k$ at random with a uniform probability distribution on this set.

(B) Consider the set $B_n^+|_k = \{x \in B_n^+ \colon\ |x| = k\}$ and choose an element of $B_n^+|_k$ at random with a uniform probability distribution on this set.

We will refer to (A) as *generating uniformly random words*, and to (B) as *generating uniformly random braids*. We will write Word_k, respectively URB_k, for the corresponding probability measures on B_n^+. Since the number of different words in $\mathcal{A}^*|_k$ that represent the same element x of $B_n^+|_k$ depends on x, generating uniformly random words results in a distribution of *braids* which is very far from being uniform on $B_n^+|_k$. Generating uniformly random braids is not easy; an algorithm whose time- and space-complexities are polynomial in both n and k was given in [11].

In this paper we analyse the generation of uniformly random braids and the generation of uniformly random words regarding some properties of the generated samples of braids. The *Garside normal form* defines a canonical way of expressing a braid as a sequence of permutations, so a probability distribution on the braid group induces a sequence of probability distributions on the symmetric group. We are particularly interested in how the resulting distributions on the symmetric group depend on the position in this sequence.

The structure of the paper is as follows: Section 2 recalls the Garside normal form; experts may skip this section. Section 3 contains our analysis of the normal forms of random braids. In Section 3.1 we observe that there is a "stabilisation" occurring in the normal forms of long random braids in the sense that for sufficiently long braids the distributions on the symmetric group induced by the factors of the normal form depend neither on the position in the normal form nor on the lengths of the random braids, except for an initial and a final region whose lengths are uniformly bounded. In Section 3.2, we give an explanation for this stabilisation phenomenon by demonstrating that the expected number of factors of the normal form of a braid that are modified when multiplying the braid on the right is uniformly bounded. Finally, in Section 4, we extend our analysis to general Garside groups and establish a criterion for deciding whether phenomena similar to the ones described above occur in a given Garside group.

2. Background

This section contains a brief summary of the main notions referred to in the paper. Specifically, we will recall Garside monoids and the Garside normal form. For details and proofs we refer to [9,8].

In a cancellative monoid M with unit $\mathbf{1}$, we can define the *prefix* partial order: For $x, y \in M$, we say $x \preccurlyeq y$ if there exists $c \in M$ such that $xc = y$. Similarly, we define the *suffix* partial order by saying