Uniform Generation of Braids

Samy Abbes[1], Sébastien Gouëzel[2,3], Vincent Jugé[1,4] & Jean Mairesse[2,4]

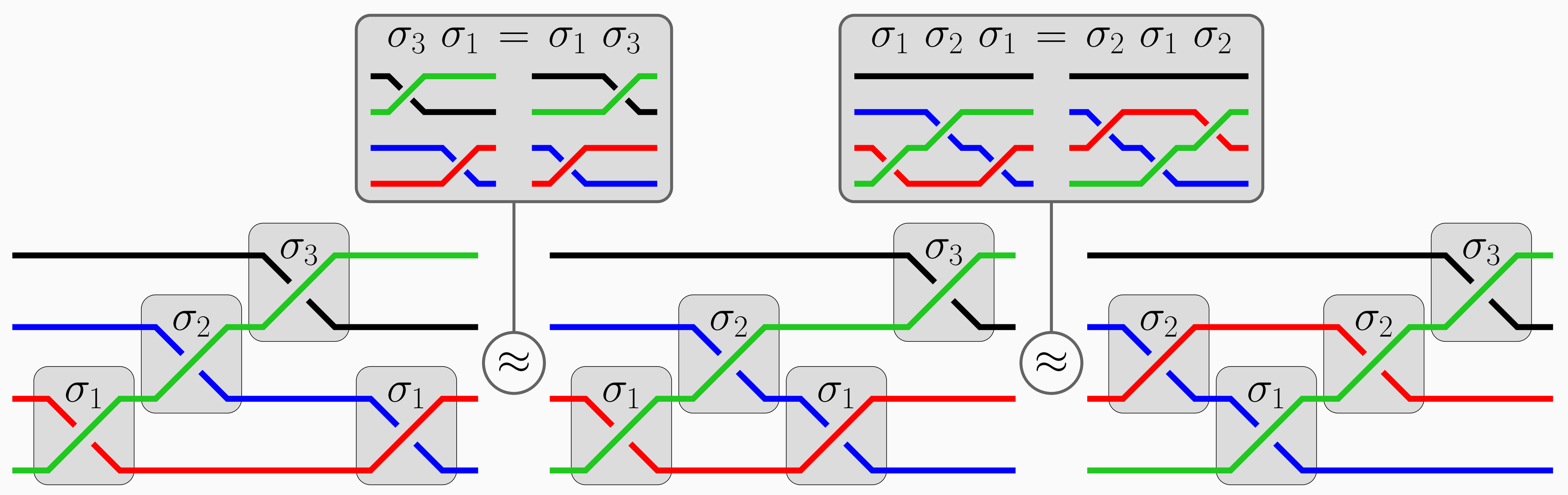
1 : Université Paris 7   2 : CNRS   3 : Université de Nantes   4 : Université Paris 6

Monoid of positive braids

Positive braids with n strands are elements of the monoid

$$B_n^+ = \langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ and } \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } |i-j| \geq 2\rangle^+.$$

Braids represent **isotopy** classes of **braid diagrams**.



Isotopic braid diagrams associated with the braid $\sigma_1\sigma_2\sigma_1\sigma_3$

Uniform sampling of n-strand braids of length k

Simple 3-step algorithm:

1. Enumerate the elements of the set $B_n^k := \{n\text{-strand braids of length } k\}$;
2. Draw some integer $i \in \{1, 2, \ldots, \#B_n^k\}$ uniformly at random;
3. Pick the i^{th} element of your enumeration of B_n^k.

⚠ Step 1 is **computationally difficult**!

Example ($n = 4$ and $0 \leq k \leq 2$):

$$B_4^0 = \{\mathbf{1}\},\ B_4^1 = \{\sigma_1, \sigma_2, \sigma_3\} \text{ and } B_4^2 = \{\sigma_1^2, \sigma_1\sigma_2, \sigma_1\sigma_3, \sigma_2\sigma_1, \sigma_2^2, \sigma_2\sigma_3, \sigma_3\sigma_2, \sigma_3^2\}.$$

There exists an **efficient variant** [5] that works in time $\mathcal{O}(k^2n^4)$.

Garside normal form

Theorem & Definitions [2]: The monoid B_n^+, endowed with the **division** ordering $\preccurlyeq$ (i.e. $\alpha \preccurlyeq \alpha\beta$ for all $\alpha, \beta \in B_n^+$), is a **lattice**. Furthermore, we call

- **Garside element** of B_n^+ the braid $\Delta := \sigma_1 \vee \sigma_2 \vee \ldots \vee \sigma_{n-1}$.
- **Garside normal form** of a positive braid $\alpha \in B_n^+$ the smallest word $a_1 \cdot a_2 \cdot \ldots \cdot a_k$ such that $a_1a_2\ldots a_k = \alpha$ and $a_i = \Delta \wedge (a_ia_{i+1}\ldots a_k)$ for all $i \in \{1, \ldots, k\}$.

Consequence: Uniform sampling of braids in B_n^k can be performed in time $\mathcal{O}(n! + n^2 2^{2n} k)$ by constructing **inductively** the sets

$$B_n^{k,\alpha} := \{n\text{-strand braids } \beta \text{ of length } k \text{ and such that } \alpha = \Delta \wedge \beta\}$$

for all divisors α of Δ, via the recursion formulæ:

$$B_n^{k,\alpha} = \bigsqcup_{\substack{\beta\,:\,\beta \preccurlyeq \Delta \text{ and} \\ \alpha = \Delta \wedge (\alpha\beta)}} B_n^{k-length(\alpha),\beta}.$$

Inconsistent samplings

Given oracles for drawing elements of B_n^k, can we draw elements of B_n^{k+1}?

With the above algorithms, we need to start again **from scratch**! Is there a better way?

Naive (and incorrect) **idea:**

To draw an element of B_n^{k+1}, begin by drawing some prefix of length k, i.e.

1. Draw some element $\alpha \in B_n^k$;
2. For all $\beta \in B_n^{k+1}$ such that $\alpha \preccurlyeq \beta$, compute an **extension probability** $p_{\alpha,\beta}$;
3. Draw β with probability $p_{\alpha,\beta}$.

⚠ **Issue:** This approach fails for $n = 4$ and $k = 1$: drawing $\beta \in \{\sigma_2\sigma_1, \sigma_2^2, \sigma_2\sigma_3\}$ (with probability 3/8) amounts to drawing $\alpha = \sigma_2$ (with probability 1/3) in the first place!

Let us find other ways to generate large random braids...

A new approach on consistent samplings

Idea: Let us smoothen measures on the "spheres" B_n^k by taking averages!

1. Choose p such that the sum $Z_n(p) := \sum_{k \geq 0} \#B_n^k p^k$ converges;
2. Choose $\mu_p : \alpha \mapsto \frac{1}{Z_n(p)} p^{length(\alpha)}$.

Key results:

1. We have $\mu_p(\alpha B_n^+) = p^{length(\alpha)}$ for all $\alpha \in B_n^+$, where $\alpha B_n^+ := \{\alpha\beta : \beta \in B_n^+\}$;
2. **Möbius inversion formulæ** allow computing $\mu_p\left(\mathbf{A}^{\mathbf{Gar}}\right)$ for all finite words $\mathbf{A}$, where

$$\mathbf{A}^{\mathbf{Gar}} := \{\beta : \text{ the Garside normal form of } \beta \text{ begins with the prefix } \mathbf{A}\}.$$

Möbius inversion formulæ

For all $\alpha \in B_n^+$, we have

1. $\alpha B_n^+ = \bigsqcup_{\beta : \alpha \preccurlyeq \beta \preccurlyeq \Delta^{\|\alpha\|}} \mathbf{GNF}(\beta)^{\mathbf{Gar}}$;
2. $\mu_p\left(\mathbf{GNF}(\alpha)^{\mathbf{Gar}}\right) = \sum_{I \subseteq \{1,\ldots,n-1\}} \mathbf{1}_{\|\alpha\| = \|\alpha\Delta_I\|} (-1)^{\#I} \mu_p(\alpha\Delta_I B_n^+)$, where

$\mathbf{GNF}(\alpha)$ is Garside normal form of α, $\|\alpha\|$ is the length of $\mathbf{GNF}(\alpha)$, and $\Delta_I := \vee_{i \in I}\sigma_i$.

Example ($n = 4$ and $\mathbf{A} = \sigma_1 \cdot \sigma_1$) **:**

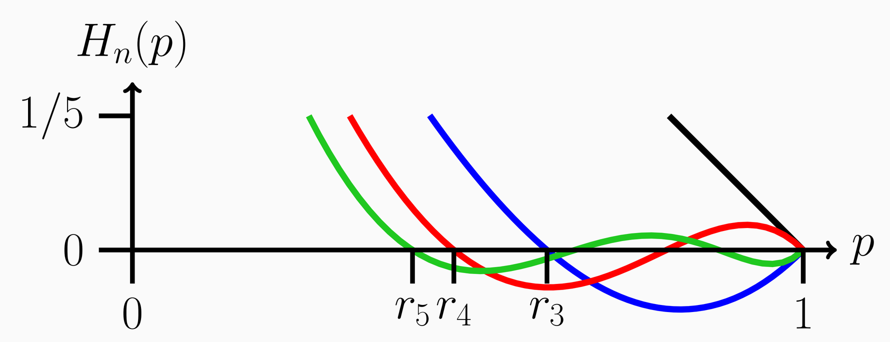
$$\mu_p\left(\mathbf{A}^{\mathbf{Gar}}\right) = \mu_p(\sigma_1^2 B_4^+) - \mu_p\left(\sigma_1^2\sigma_2 B_4^+\right) - \mu_p\left(\sigma_1^2\sigma_3 B_4^+\right) + \mu_p\left(\sigma_1^2\sigma_2\sigma_3\sigma_2 B_4^+\right) = p^2 - 2p^3 + p^5.$$

Möbius polynomial

Theorem [3, 4]: Let $H_n(X)$ be the **Möbius polynomial** of the monoid B_n^+, i.e.

$$H_n(X) = \sum_{I \subseteq \{1,\ldots,n-1\}} (-1)^{\#I} X^{length(\Delta_I)}.$$

The power series $Z_n(X)$ and $H_n(X)$ are inverses of each other, i.e. $Z_n(X)H_n(X) = 1$.



$r_2 = 1$
$r_3 \approx 0.61803$
$r_4 \approx 0.47920$
$r_5 \approx 0.41756$

Möbius polynomials $H_2(p)$, $H_3(p)$, $H_4(p)$ and $H_5(p)$ and their smallest positive roots

Theorem: Using Möbius inversion formulæ and Möbius polynomials, we derive a

Markov realisation of μ_p

There exists an explicit Markov chain $(\Theta_k^p)_{k \geq 1}$ over the set $\{\beta : \beta \preccurlyeq \Delta\}$ such that, for all finite words $\mathbf{A} = a_1 \cdot a_2 \cdot \ldots \cdot a_k$,

$$\mu_p\left(\mathbf{A}^{\mathbf{Gar}}\right) = \mathbb{P}[\Theta_1^p = a_1 \wedge \Theta_2^p = a_2 \wedge \ldots \wedge \Theta_k^p = a_k].$$

Critical behaviour: What happens when $p \to r_n$?

Adding infinite braids:

1. Endow B_n^+ with a **topology** generated by sets αB_n^+ and consider its **completion** $\overline{B_n^+}$;
2. Extend Garside normal forms to **infinite** braids (i.e. elements of $\partial B_n^+ := \overline{B_n^+} \setminus B_n^+$).

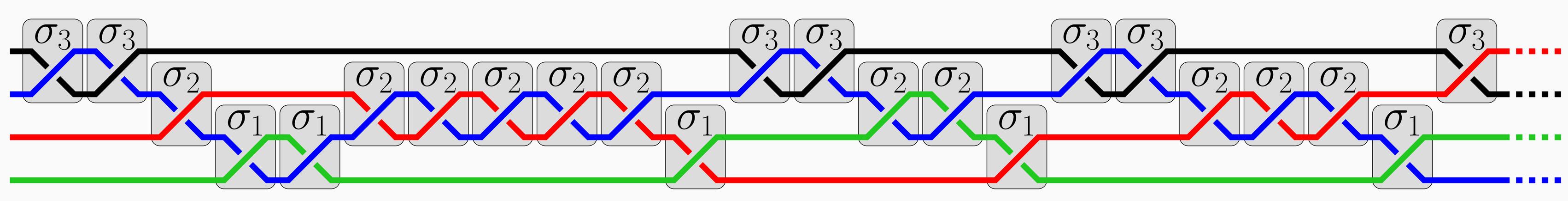
Increasing p:

1. Both μ_p and $(\Theta_k^p)_{k \geq 1}$ have **limits** μ_∞ and $(\Theta_k^\infty)_{k \geq 1}$ when $p \to r_n$;
2. $(\Theta_k^\infty)_{k \geq 1}$ is still a **Markov realisation** of μ_∞.

Theorems:

1. The support of μ_∞ is ∂B_n^+;
2. Uniform probability measures on B_n^k converge weakly towards μ_∞ when $k \to +\infty$.

Hence, we say that **μ_∞ is a uniform probability measure on infinite braids!**



An infinite braid chosen uniformly at random

This work was inspired by the similar case of **trace monoids** [1].

References

1. S. Abbes and J. Mairesse. Uniform and Bernoulli measures on the boundary of trace monoids. *J. Combin. Theory Ser. A*, 135:201–236, 2015.
2. S. Adian. Fragments of the word Δ in the braid group. *Matematicheskie Zametki*, 36(1):25–34, 1984.
3. M. Albenque. Bijective combinatorics of positive braids. *Electron. Notes Discrete Math.* 29:225–229, 2007.
4. A. Bronfman. Growth functions of a class of monoids. *Preprint*, 2001.
5. V. Gebhardt and J. González-Meneses. Generating random braids. *J. Combin. Theory Ser. A*, 120(1):111–128, 2013.