The alternating normal form of braids

Patrick Dehornoy

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen, France

Friday Seminar, Osaka State University, May 15, 2015

- New normal form(s) for braid groups (and other Garside groups), suitable for investigating order properties, and for applications to unprovability statements.
- An introduction for T. Ito's talk in IDLT...

Plan:

- 1. The alternating normal form
- 2. Connection with the standard braid order
- 3. Application to unprovability statements
- 4. The rotating normal form

Plan:

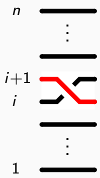
- 1. The alternating normal form
- 2. Connection with the standard braid order
- 3. Application to unprovability statements
- 4. The rotating normal form

- Definition (Artin 1925/1948): The braid group B_n is the group with presentation

$$\left\langle \sigma_1, \dots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & \text{for } |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{for } |i-j| = 1 \end{array} \right\rangle.$$

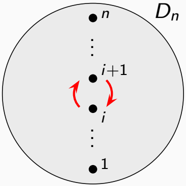
$\simeq$ { braid diagrams } / isotopy:

$\sigma_i \quad \leftrightarrow$



$\simeq$ mapping class group of D_n (disk with n punctures):

$\sigma_i \quad \leftrightarrow$



- Definition: $B_n^+ :=$ submonoid of B_n generated by $\sigma_1, \dots, \sigma_{n-1}$ (positive braids).

- Proposition: B_n *is a group of (left and right) fractions for* B_n^+.

$\uparrow$

every element of B_n can be expressed as $\beta\gamma^{-1}$ and $\beta'^{-1}\gamma'$ with $\beta, \gamma, \beta', \gamma' \in B_n^+$

Garside's half-turn braid: $\Delta_1 = 1, \;\; \Delta_n = \Delta_{n-1}\sigma_{n-1}\cdots\sigma_1$

$\downarrow$

- Proposition: B_n^+ *is a Garside monoid with Garside element* Δ_n*: every* β *in* B_n^+ *has a unique expression* $\beta_p \cdots \beta_1$ *with* β_i *maximal right-divisor of* $\beta_p \cdots \beta_i$ *lying in Div*(Δ_n).

$\uparrow$

β is a right-divisor of γ if $\exists\gamma' \; (\gamma = \gamma'\beta)$

- Corollary: *Every* β *in* B_n *has a unique expression* $\beta_p \cdots \beta_1\gamma_1^{-1} \cdots \gamma_q^{-1}$ *with* β_1, ..., β_p *and* γ_1, ..., γ_q *in Div*(Δ_n) *and gcd*$(\beta_1, \gamma_1) = 1$.

- This (right) "greedy normal form" gives a bi-automatic structure on B_n, etc.

- Other normal forms on B_n or B_n^+
  that are not—or not directly—connected with the greedy normal form:

  - Type 1: Normal forms coming from combing (Artin, Markov–Ivanovsky).

  - Type 2: Normal forms coming from relaxation strategies
    (Dynnikov–Wiest, Bressaud).

  - Type 3: Normal forms coming from an order on braid words:
    $\mathrm{NF}(x)$ defined to be the least word representing x.
    - Example 1 (Bronfman): lexicographical order of braid words;
    - Example 2 (Burckel): associate with every braid word w
      a certain finite tree, and use a well-ordering on trees.

  - Type 4: Alternating (and rotating) normal forms
    coming from parabolic submonoids

- Recall: β right-divisor of γ —equivalently: γ left-multiple of β— if $\exists\gamma'(\gamma = \gamma'\beta)$.

- Proposition (Garside, 1969): *Under (left- and right-) division, B_n^+ is a lattice: least common multiples (lcms) and greatest common divisors (gcds) exist.*

- Lemma: *If $S \subseteq B_n^+$ is closed under left-lcm and right-divisor, then every β in B_n^+ admits a unique decomposition $\beta = \beta'\,\beta_1$ with β_1 a maximal right-divisor of β in S.*

- If S generates B_n^+, iterating gives a unique normal form.

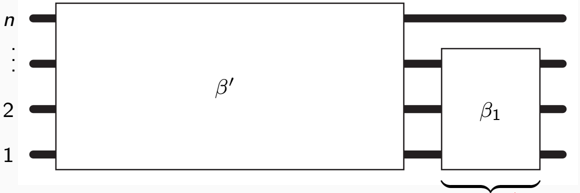
  for instance, $S = \mathrm{Div}(\Delta_n)$ gives the (right) greedy normal form

- Lemma (variant): *If S is a submonoid of B_n^+ closed under left-lcm and right-divisor, then every β in B_n^+ admits a unique decomposition $\beta = \beta'\,\beta_1$ such that the only right-divisor of β' lying in S is 1.*

  "β' right-coprime to S"

- Definition: In the above framework, call β_1 the S-tail of β.

- Example: $S = B^+_{n-1}$:

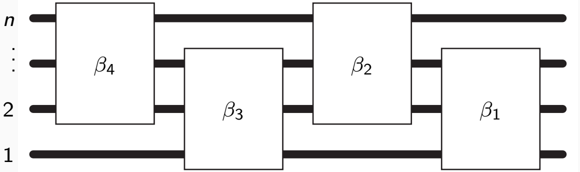


B^+_{n-1}-tail of β

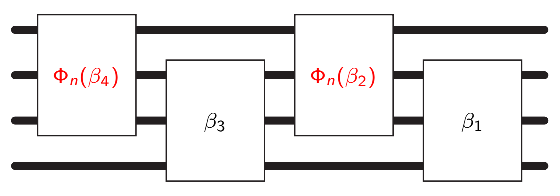
... stuck after one step.

- Use two submonoids S_1, S_2 that, together, generate B^+_n,

typically: $S_1 = B^+_{n-1} = \langle \sigma_1, ..., \sigma_{n-2} \rangle^+$, $S_2 = \langle \sigma_2, ..., \sigma_{n-1} \rangle^+$.



- Fact: B_n admits an automorphism Φ_n that exchanges σ_i and σ_{n-i} for each i.
  - A horizontal symmetry in braid diagrams
  - The monoid $\langle \sigma_2, ... \sigma_{n-1} \rangle^+$ is the image of B^+_{n-1} under Φ_n.
  - Hence a decomposition $\cdots \beta_4 \beta_3 \beta_2 \beta_1$ with $\beta_1, \beta_3, ...$ in B^+_{n-1} and $\beta_2, \beta_4, ...$ in $\langle \sigma_2, ... \sigma_{n-1} \rangle^+$ can also be written



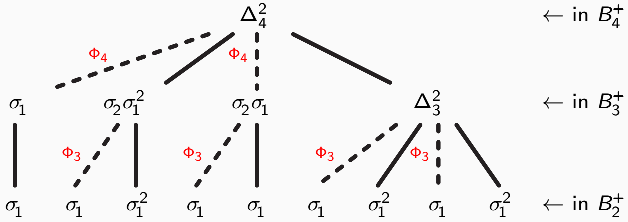
with all β_i in B^+_{n-1}.

- Proposition: *Every braid β in B^+_n admits a unique decomposition*

$$\beta = \cdots \Phi_n(\beta_4) \cdot \beta_3 \cdot \Phi_n(\beta_2) \cdot \beta_1 \qquad \leftarrow \text{the } \Phi\text{-splitting of } \beta$$

with $\beta_i \in B^+_{n-1}$ s.t., for $i \geqslant 2$, no σ_k with $k \geqslant 2$ right-divides $\cdots b_{i+2} \Phi_n(\beta_{i+1}) \beta_i$.

- Iterate to obtain a unique normal form: construct a tree for each positive braid



after flipping: σ_3 σ_2 σ_1^2 σ_2 σ_3 σ_2 σ_1^2 σ_2 σ_1^2

- ▶ the alternating normal form of Δ_4^2 is $\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_3\sigma_2\sigma_1^2\sigma_2\sigma_1^2$.

• Proposition: *Every braid in B_n^+ admits a unique alternating normal form, which can be computed in quadratic time. Alternating normal words are recognized by a finite state automaton.*

• A "bizarre" normal form, very different from the greedy normal form:

- Example: the greedy NF of Δ_3^p is $\Delta_3|\cdots|\Delta_3$ (p entries) its alternating NF is

$$\underbrace{\sigma_1|\sigma_2^2|\cdots|\sigma_2^2|\sigma_1^2|\sigma_2|\sigma_1^p}_{p+3\text{ entries}} \text{ for odd } p, \qquad \underbrace{\sigma_2|\sigma_1^2|\cdots|\sigma_2^2|\sigma_1^2|\sigma_2|\sigma_1^p}_{p+3\text{ entries}} \text{ for even } p.$$

• Proposition: *A positive 3-strand braid word $\sigma_i^{e_p}\cdots\sigma_1^{e_3}\sigma_2^{e_2}\sigma_1^{e_1}$ is alternating-normal iff*

$$e_p \geqslant 1,\ e_{p-1} \geqslant 2,\ \ldots,\ e_3 \geqslant 2,\ e_2 \geqslant 1,\ e_1 \geqslant 0.$$

• Remarks:

- The normal form can be extended to B_n using fractions.
- Works in every "locally Garside" monoid, in particular every Artin–Tits monoid.
- NB: The alternating normal form is not connected with an automatic structure.

Plan:

- 1. The alternating normal form
- 2. Connection with the standard braid order
- 3. Application to unprovability statements
- 4. The rotating normal form

• Definition: For x, x' in B_∞, declare $x <_D x'$ if, among all braid words that represent $x^{-1}x'$, at least one is such that the generator σ_i with highest index appears positively only.

↑
σ_i occurs, σ_i^{-1} does not

• Example: $\sigma_2 <_D \sigma_1\sigma_2$ holds, because $\sigma_2^{-1}\sigma_1\sigma_2 = \sigma_1\sigma_2\sigma_1^{-1}$,
and, in the latter word, σ_2 appears positively only.

• Theorem
(i) (D, 1992): The relation $<_D$ is a left-invariant linear order on B_∞.
(ii) (Laver, 1994): The restriction of $<_D$ to B_∞^+ is a well-order;
(iii) (Burckel, 1997): The restriction of $<_D$ to B_n^+
is the initial interval $[1, \sigma_n)$ of $(B_\infty^+, <_D)$ and has length $\omega^{\omega^{n-2}}$.

• Remark: replacing "maximal index" with "minimal index" in the definition
amounts to flipping the order: for β, γ in B_n, $\beta <'_D \gamma$ iff $\Phi_n(\beta) <_D \Phi_n(\gamma)$.

- The braid order is effective (there is an algorithm deciding $<_D$), but complicated.

- In particular: The well-order property gives a distinguished element ($<_D$-smallest elt) in every nonempty subset of B_n^+ (e.g., in each conjugacy class) but cannot be computed in practice (?).

- Typically: $<_D$ is not well connected with the greedy normal form:
  - If β, γ are divisors of Δ_n, then $\beta <_D \gamma$ iff $\mathrm{perm}(\beta) <^{\mathrm{Lex}} \mathrm{perm}(\gamma)$, (good!)
  - ... but does not extend to arbitrary positive braids, viewed as sequences of divisors of Δ_n. (bad!)

• Theorem (D., 2007): *The order $<_D$ on B_n^+ is a ShortLex-extension of the order $<_D$ on B_{n-1}^+ via the Φ-splitting:*
For β, γ in B_n^+ with Φ-splittings

$$\beta = \Phi_n^{p-1}(\beta_p) \cdots \beta_3 \cdot \Phi_n(\beta_2) \cdot \beta_1, \quad \gamma = \Phi_n^{q-1}(\gamma_q) \cdots \gamma_3 \cdot \Phi_n(\gamma_2) \cdot \gamma_1,$$

$\beta <_D \gamma$ holds iff either $p < q$,
or $p = q$ and there exists r s.t. $\beta_i = \gamma_i$ for $i > r$ and $\beta_r <_D \gamma_r$.

• Proof: The flip normal form coincides with the Burckel normal form. □

• Corollary: *The braid order can be read from the alternating normal form.*

Plan:

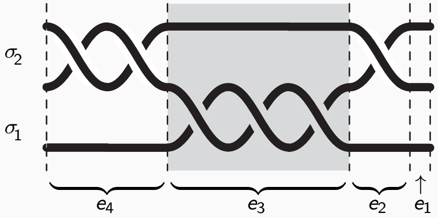
- 1. The alternating normal form
- 2. Connection with the standard braid order
- 3. Application to unprovability statements
- 4. The rotating normal form

- Aim: Construct (very) long sequences of braids using a simple inductive rule. (reminiscent of Goodstein's sequences and Hydra battles)

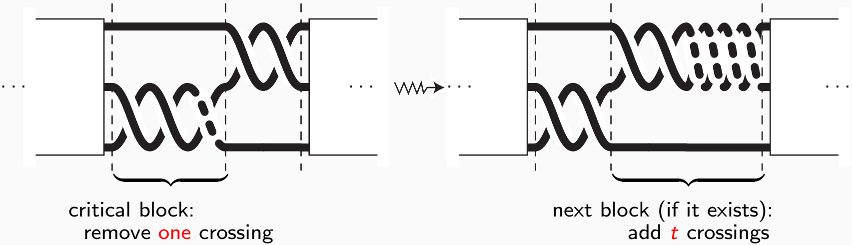
- Recall: A 3-strand braid word $\sigma_{[p]}^{e_p} \dots \sigma_2^{e_2} \sigma_1^{e_1}$ ($[p] = 1$ or 2) is normal iff

$$e_p \geqslant 1, \quad e_{p-1} \geqslant 2, \ \dots, \quad e_3 \geqslant 2, \quad e_2 \geqslant 1, \text{ and } e_1 \geqslant 0.$$

- Definition: The critical position in a positive 3-strand braid word: smallest k (= rightmost) s.t. e_k does not have the minimal legal value, if it exists, p otherwise.



- Definition: The $\mathcal{G}_3$-sequence from a positive 3-braid x:
  - Start with the alternating normal form of x;
  - At step t: remove one crossing in the critical block;
    add t new crossings in the next block, if it exists;
  - The sequence stops when (if) one reaches the braid 1.



- Example: $\sigma_2^2\sigma_1^2$, $\sigma_2^2\sigma_1$, σ_2^2, $\sigma_2\sigma_1^3$, $\sigma_2\sigma_1^2$, $\sigma_2\sigma_1$, σ_2, σ_1^7, σ_1^6, σ_1^5, σ_1^4, σ_1^3, σ_1^2, σ_1, 1.

- More examples:
  - The $\mathcal{G}_3$-sequence from $\sigma_1\sigma_2\sigma_1$ has length 30.
  - The $\mathcal{G}_3$-sequence from $\sigma_1^2\sigma_2^2\sigma_1^2$ has length 90,159,953,477,630...

Nevertheless:

- Proposition A: *Every $\mathcal{G}_3$-sequence (resp. $\mathcal{G}_\infty$-sequence) is finite.*

↑ similar with B_∞^+ instead of B_3^+...

- Proof: The sequences are descending in the braid well-order. □

But:

- Theorem (joint with L.Carlucci and A.Weiermann, 2010):
  Proposition A cannot be proved in $I\Sigma_1$ (resp. $I\Sigma_2$).

↑ ↑ the subsystem of Peano arithmetic in which induction is restricted to formulas with one ∃ (resp. ∃∀) unbounded quantifier

Contrasting with the folklore result:

- Proposition: All usual (algebraic) properties of braids can be proved in $I\Sigma_1$.

- Proof of the unprovability of the finiteness of $\mathcal{G}_3$-sequences in $I\Sigma_1$:
  - Principle: Assign ordinals to braids, and compare with the Hardy hierarchy.
  - Main lemma: *For β a 3-braid with normal form $\sigma_{[p]}^{e_p} \dots \sigma_2^{e_2} \sigma_1^{e_1}$, put*

$$ord(\beta) := \omega^{p-1} \cdot e_p + \sum_{p>k\geqslant 1} \omega^{k-1} \cdot (e_k - e_k^{min}),$$

(with $e_k^{min} = 2$ for $k \geqslant 3$, $e_2^{min} = 1$, $e_1^{min} = 0$). Then

$$ord(\beta) = \xi \quad \Rightarrow \quad \forall k \; (T(\beta\sigma_1^k) \geqslant H_\xi(k)).$$

T ↑ the length of the $\mathcal{G}_3$-sequence from...

H_ξ ↑ "Hardy hierarchy" of functions:
$H_r(x) := x + r$,
$H_{\omega+r}(x) := 2(x+r)$,
$H_{\omega\cdot 2}(x) := 4x$,
H_{ω^ω} = Ackerman function,...

  - Hence: $T(\sigma_{[k]}\sigma_{[k-1]}^2 \dots \sigma_1^2\sigma_2\sigma_1^k) \geqslant H_{\omega^\omega}(k)$.
  - $I\Sigma_1$ does not prove that the Ackermann function is defined everywhere, hence it cannot prove that T is defined everywhere, that is, that all $\mathcal{G}_3$-sequences of braids are finite □

- So far, particular sequences of braids ($\mathcal{G}_3$-sequences); now, arbitrary sequences.

- Definition: For $f : \mathbb{N} \to \mathbb{N}$, let WO_f be the combinatorial principle:
"For each k, there exists m s.t. no descending sequence $(\beta_0, \beta_1, ...)$ in B_3^+ satisfying $\forall i\ (\|\beta_i\| \leqslant k + f(i))$ has length larger than m" (with $\|\beta\| :=$ least k s.t. β divides Δ_3^k)

  "There is no infinite descending sequence of braids with complexity bounded by f"

- Trivially: $WO_{constant}$ true. Actually: WO_f true for every f (provable from ZF).

- Theorem (Carlucci–D.–Weiermann, 2010): *For $r \leqslant \omega$, put $f_r(x) := \lfloor \sqrt[Ack_r^{-1}(x)]{x} \rfloor$. Then:*
  (i) WO_{f_r} is provable from $I\Sigma_1$ for each finite r.
  (ii) WO_{f_ω} is not provable from $I\Sigma_1$.

- Key point for the proof: Fine counting arguments in B_3^+, namely evaluating

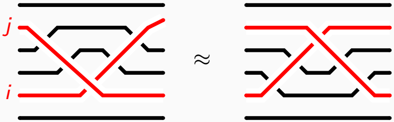
$$\#\{\beta \in B_3^+ \mid \|\beta\| \leqslant \ell \quad \text{and} \quad \beta <_{\mathrm{D}} \Delta_3^k\}.$$

Plan:

- 1. The alternating normal form
- 2. Connection with the standard braid order
- 3. Application to unprovability statements
- 4. The rotating normal form

- Another family of generators for B_n: the Birman–Ko–Lee generators

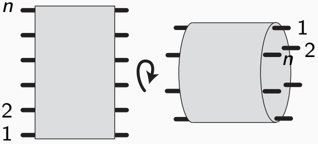
$$a_{i,j} := \sigma_{j-1} \cdots \sigma_{i+1} \sigma_i \sigma_{i+1}^{-1} \cdots \sigma_{j-1}^{-1} \text{ for } 1 \leqslant i < j \leqslant n.$$



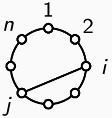
- Definition: (dual braid monoid) B_n^{+*}:= the submonoid of B_n generated by the $a_{i,j}$s.

- Remark= $B_n^+ \subseteq B_n^{+*}$, since $\sigma_i = a_{i,i+1}$; $\neq$ for $n \geqslant 3$, since $a_{1,3} = \sigma_2 \sigma_1 \sigma_2^{-1} \notin B_3^+$.

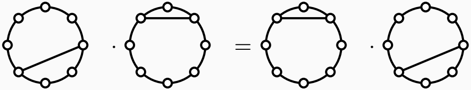
- Chord representation of the Birman–Ko–Lee generators:



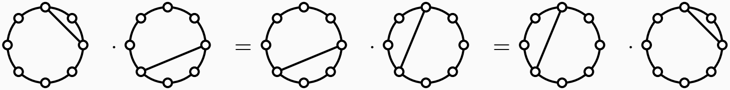
$a_{i,j} \mapsto$



- Lemma: *In terms of the $a_{i,j}$s, the group B_n and the monoid B_n^{+*} are presented by*



for disjoint chords,



for adjacent chords enumerated in clockwise order.

- Remember: flip automorphism Φ_n of B_n^+ = conjugating under Δ_n
  = symmetry in the braid diagram.

- Lemma: *Conjugating by* $\Delta_n^* := a_{1,2}a_{2,3} \cdots a_{n-1,n}$ *gives an automorphism* Φ_n^* *of* B_n^{+*}*;*
For all i, j, one has

$$\Phi_n^*(a_{i,j}) = a_{i+1 \bmod n, j+1 \bmod n}.$$

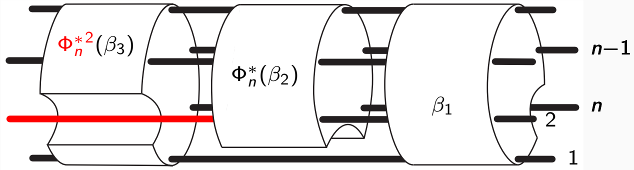
↑

= rotating by $2\pi/n$ in the chord representation

• Proposition (Fromentin): Every braid β in B_n^{+*} admits a unique decomposition

$$\beta = \Phi_n^{*\,p-1}(\beta_p) \cdot \ldots. \cdot \Phi_n^{*\,2}(\beta_3) \cdot \Phi_n^{*}(\beta_2) \cdot \beta_1, \qquad \leftarrow \text{the } \Phi^*\text{-splitting of } \beta$$

with $\beta_i \in B_{n-1}^{+*}$ s.t. $\Phi_n^{*\,p-k}(\beta_p) \cdot \ldots \cdot \beta_k$ is right-divisible by no $a_{i,j}$ with $i, j \neq n-1$.



• Theorem (Fromentin 2008): For β, γ in B_n^{+*} with Φ^*-splittings

$$\beta = \Phi_n^{*\,p-1}(\beta_p) \cdot \ldots. \cdot \Phi_n^{*}(\beta_2) \cdot \beta_1, \quad \gamma = \Phi_n^{*\,q-1}(\gamma_q) \cdot \ldots. \cdot \Phi_n^{*}(\gamma_2) \cdot \gamma_1,$$

$\beta <_D \gamma$ holds iff either $p < q$,

or $p = q$ and there exists r s.t. $\beta_i = \gamma_i$ for $i > r$ and $\beta_r <_D \gamma_r$.

• Iterating: the rotating normal form... and applications.

- P. Dehornoy, *Alternating normal forms for braids and locally Garside monoids*, J. Pure Appl. Algebra 212-11 (2008) 2416-2439.

- L. Carlucci, P. Dehornoy, A. Weiermann, *Unprovability statements involving braids*, Proc. London Math. Soc. 102-1 (2011) 159-192.

- P. Dehornoy, with I. Dynnikov, D. Rolfsen, B. Wiest, Ordering braids, Math. Surveys and Monographs vol. 148, Amer. Math. Soc. (2008)

- J. Fromentin, *The well-order on dual braid monoids* J.Knot Th. Ramif. 19-5 (2010) 631-654.

- J. Fromentin, *Every braid admits a short sigma-definite expression*, J. Europ. Math. Soc. 13 (2011) 1591-1631.

- T. Ito, *On finite Thurston-type orderings on braid groups*, Groups, Complexity Cryptol. 2 (2010) 123-155.

- T. Ito, *Finite Thurston-type orderings on dual braid monoids*, J. Knot Th. Ramif. 20 (2011) 995-1019.