Lecture 8 – Wed Mar 8

<u>Elrifai & Morton's (1994) sol^{n} to word & conj. problems</u>

(fundamentally similar to Garside, but vastly improved)

<u>Recall</u>: B_n^+ = semigroup of positive braids (embeds into B_n by Garside)

- $\Delta = (\sigma_1 \cdots \sigma_{n-1})(\sigma_1 \cdots \sigma_{n-2}) \cdots (\sigma_1\sigma_2)\sigma_1$ Garside elt (180° rotation)
- Will introduce an <u>order relation</u> on B_n^+, for which the interval $[e, \Delta]$ consists precisely of <u>permutation braids</u>
- Every elt of B_n has a <u>normal form</u> ("left-canonical form")

$$B = \Delta^r A_1 \cdots A_k, \quad \begin{cases} r \in \mathbb{Z} \\ A_i \text{ permutation braids } \neq e, \Delta \end{cases}$$

with property that $(A_1, \dots, A_k)$ maximal wrt lexicographic order

Call $r = \underline{\inf(B)}$, $r+k = \underline{\sup(B)}$

<u>NB</u>: # braids with given inf & sup is <u>finite</u>!! – this will be key to conj. problem.

- <u>Def</u>: For $A, B \in B_n$, write $A \le B$ if $\exists C_1, C_2 \in B_n^+ / B = C_1 A C_2$.

(in particular $B \in B_n^+ \iff e \le B$)

<u>Rmk</u>: • $A \le B \iff B^{-1} \le A^{-1}$

<u>Lemma</u>:
- $A \le \Delta^s \Rightarrow \exists D_1, D_2 \in B_n^+$ s.t. $\Delta^s = D_1 A = A D_2$
- $\Delta^r \le A \Rightarrow \exists E_1, E_2 \in B_n^+$ s.t. $A = E_1 \Delta^r = \Delta^r E_2$
- $\Delta^{r_1} \le A_1 \le \Delta^{s_1}$, $\Delta^{r_2} \le A_2 \le \Delta^{s_2} \Rightarrow \Delta^{r_1+r_2} \le A_1 A_2 \le \Delta^{s_1+s_2}$

<u>Def</u>: $\tau : B_n \to B_n$, $\sigma_i \mapsto \sigma_{n-i}$
- τ is an order-preserving involution of B_n
- $\Delta \sigma_i = \sigma_{n-i} \Delta \Rightarrow \Delta A = \tau(A) \Delta$, ie. τ = conj by Δ.

<u>Pf lemma</u>: • $A \le \Delta^s \Rightarrow \Delta^s = C_1 A C_2 = \underbrace{(C_1 A C_2)}_{\Delta^s} C_2 \underbrace{(C_1 A C_2)^{-1}}_{\Delta^{-s}} C_1 A = \tau^s(C_2) C_1 A$

$C_1, C_2 \in B_n^+$

similarly, $\Delta^s = A C_2 \tau^s(C_1)$.

- $\Delta^r \le A \Rightarrow A = B_1 \Delta^r B_2 = \Delta^r \tau^r(B_1) B_2 = B_1 \tau^r(B_2) \Delta^r$.
- under assumption: $A_1 = D_1 \Delta^{r_1}$, $A_2 = \Delta^{r_2} D_2 \to A_1 A_2 = D_1 \Delta^{r_1+r_2} D_2 \ge \Delta^{r_1+r_2}$

same with other half

<u>Prop</u>: $\forall B \in B_n$, $\exists r, s \in \mathbb{Z}$ s.t. $\Delta^r \le B \le \Delta^s$

<u>Pf</u>: $1 \le \sigma_i \le \Delta$, $\Delta^{-1} \le \sigma_i^{-1} \le 1$, & apply lemma to bound $B = \prod \sigma_{k_i}^{\pm 1}$

Def:
- $[r,s] = \{ B \in B_n \mid \Delta^r \leq B \leq \Delta^s \}$
- $\inf(B) := \max\{ r \mid \Delta^r \leq B \}$ $\leftarrow$ well def^d because $\deg: B_n \to \mathbb{Z}$, $\sigma_i \mapsto 1$
- $\sup(B) := \min\{ s \mid B \leq \Delta^s \}$ $\leftarrow$
- $\ell(B) := \sup(B) - \inf(B)$ <u>canonical length</u>

$A \leq B \Rightarrow \deg A \leq \deg B$
in particular $r\frac{n(n-1)}{2} \leq \deg B \leq s\frac{n(n-1)}{2}$

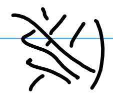
NB:
- $[r,s] = \Delta^r \cdot [0, s-r]$
- this is a <u>finite</u> set! indeed, every elt of $[0,s-r]$ is a positive braid (word in σ_i only) of degree $\leq (s-r)\frac{n(n-1)}{2}$, so <u>wordlength</u> $\leq \ldots$
- $\inf(B^{-1}) = -\sup(B)$
- $[r_1,s_1]\cdot[r_2,s_2] \subseteq [r_1+r_2, s_1+s_2]$ — actually <u>equal</u>!

Def: $S_n^+ = \{\text{permutation braids}\} = \{ A \in B_n^+ \mid \text{any two strings cross at most once} \}$

Recall $\mathfrak{S}_n \xrightarrow{1-1} S_n^+$, $\pi \longmapsto A_\pi$ given by bubble sort decomp. of π into $(i\ i{+}1)$ and replacing by σ_i

$\deg(A_\pi) = \#$<u>inversions</u> of $\pi = \#\{ i<j \mid \pi(i) > \pi(j) \}$

Prop: $[0,1] = S_n^+$.

Pf: – $\Delta \in S_n^+$ (any 2 strings cross once 

– $\Delta = AB$, $A, B \in B_n^+ \Rightarrow$ any 2 strings cross at most once in A (can't uncross in B!)
so $A \in S_n^+$; so $[0,1] \subseteq S_n^+$

– if $A_\pi \in S_n^+$: let $\delta = i \mapsto n-i$ permutation of Δ
$\rho \in \mathfrak{S}_n$ s.t. $\pi\rho = \delta$

$A_\pi A_\rho$ is a positive braid, induces permutation δ
$\Rightarrow$ if we show $A_\pi A_\rho$ is a permutation braid then $A_\pi A_\rho = \Delta$ and hence $A_\pi \in [0,1]$.

Any pair of strings in $A_\pi A_\rho$ crosses at most twice (once in A_π, once in A_ρ), but crosses an odd # times to induce δ $\Rightarrow$ crosses just once ✓ ∎

Def: $B \in B_n^+ \Rightarrow$ <u>starting set</u> $S(B) = \{ i \mid B = \sigma_i B_i \text{ for some } B_i \in B_n^+ \}$
<u>finishing set</u> $F(B) = \{ i \mid B = B_i \sigma_i \text{ ——— } \}$

Def: A decomposition $P = A\cdot B$, $A, B \in B_n^+$ is <u>left-weighted</u> if $S(B) \subseteq F(A)$

Prop: $\forall P \in B_n^+$, $\exists$ <u>unique</u> left-weighted decomp. $P = A_1 B_1$, $A_1 \in [0,1]$
Every other decomp. $P = AB$, $A \in [0,1]$ has the prop that $\exists Q \in B_n^+ / A_1 = AQ$
(i.e. A_1 is <u>maximal</u>)

Lemma:
- If $A = A_\pi \in [0,1]$, $\pi \in \mathfrak{S}_n$ then $S(A) = \{i \,/\, \pi(i) > \pi(i+1)\}$ (i.e. strings i & $i+1$ cross)
- if $A \in [0,1]$ then $\sigma_i A \in [0,1] \iff i \notin S(A)$.
- if $A \in [0,1]$ then $S(A) = \{1, \dots, n-1\} \iff A = \Delta$.

<u>Pf:</u>
- if $i \in S(A)$ then $A = \sigma_i A'$, $A' \geq e \Rightarrow i$ & $i+1$ cross (at least once, hence exactly once).
- conversely, if $\pi(i) > \pi(i+1)$, can draw a diagram for A where this crossing happens first (and the rest is $\pi \circ (i, i+1)$ which has one fewer inversions)
- upon adding σ_i at beginning of A the property that any 2 strings cross at most once is preserved iff i&$(i+1)$ didn't cross in A ie. iff $i \notin S(A)$.
- $S(A_\pi) = \{1, \dots, n-1\} \iff \pi(1) > \dots > \pi(n) \iff A_\pi = \Delta$. ▲

- $\exists$ similar statement about finishing sets: $F(A) = \{i \,/\, \pi^{-1}(i) > \pi^{-1}(i+1)\}$, $A\sigma_i \in [0,1] \iff i \notin F(A)$.

<u>Pf. prop:</u>
- consider all decomps. $P = AB$, $A \in [0,1]$, $B \in B_n^+$ & choose one where $\deg(A)$ is maximal.

  If $S(B) \not\subset F(A)$ then take $i \in S(B)$, $i \notin F(A)$: $A' = A\sigma_i \in [0,1]$ by lemma, $B = \sigma_i B'$ by def. of $S(B)$

  $\to P = A'B'$, $\deg(A') > \deg(A)$, contradiction

  Hence $\exists$ left-weighted decomp! Call it $A_1 B_1$.
- now we show any other decomp $P = AB$ has $A_1 = AQ$, $B = QB_1$ for some $Q \in B_n^+$

  Assume not & start taking off letters from A's right until it becomes a subfactor of A_1 in this sense $\rightsquigarrow \exists$ decomp. $P = C\sigma_i B'$, $C\sigma_i \in [0,1]$, C initial factor of A_1 but $C\sigma_i$ not.

  choose such a decomp. with $\deg(C)$ maximal, & write $A_1 = CQ$

  since $\underset{\substack{\uparrow \\ \text{choice of } A_1 \,:\, \text{max. degree}}}{\deg(A_1) \geq} \deg(C\sigma_i) > \deg C$, $Q \neq e$; $\Rightarrow$ take $j \in S(Q)$ $(\neq \emptyset)$

  $\Rightarrow$ can also write $P = C\sigma_j B''$ ($C\sigma_j \in [0,1]$ since $C\sigma_j \leq CQ = A_1$). $B'' = (\sigma_j^{-1} Q) B_1 \in B_n^+$

  Apply left-cancellation lemma to $\sigma_i B' = \sigma_j B''$ in B_n^+ (by assumption $i \neq j$ since $C\sigma_i$ not an initial factor of A_1)

  $\Rightarrow \begin{cases} |i-j| \geq 2: & \text{can rewrite } P = C\sigma_i\sigma_j B''' \\ |i-j| = 1: & P = C\sigma_i\sigma_j\sigma_i B''' \end{cases}$

  also, $C\sigma_i, C\sigma_j \in [0,1] \Rightarrow i, j \notin F(C) \Rightarrow$ easy to check $\begin{matrix} C\sigma_i\sigma_j & |i-j| \geq 2 \\ C\sigma_i\sigma_j\sigma_i & |i-j| = 1 \end{matrix} \in [0,1]$

Now we get that $P = C\sigma_j\sigma_i B'''$ $\quad C\sigma_j$ initial factor of A_1,

or $C\sigma_j\sigma_i\sigma_j B''$ $\quad C\sigma_j\sigma_i$ or $C\sigma_j\sigma_i\sigma_j$ isn't (since $C\sigma_i$ isn't),

contradicts maximality of $\deg(C)$.

Hence really any other A is an initial factor of A_1.

– this implies $P = AB$, $A \neq A_1 \Rightarrow \deg A < \deg A_1$. Implies uniqueness of A_1 ✓.

Rmk: $P = A_1 B_1$ left-weighted $\Rightarrow S(A_1) = S(P)$

(• clearly $S(A_1) \subset S(P)$ since $A_1 = \sigma_i A' \Rightarrow P = \sigma_i A' B_1$

• $i \in S(P) \Rightarrow P = \sigma_i B'$; but $\text{Prop}^{\underline{n}} \Rightarrow \sigma_i$ is an initial factor of A_1 ✓)

Thm: $\forall P \in B_n^+$, $\exists!$ decomp. $P = A_1 \cdots A_k$, $A_i \in [0,1]$, $A_i \neq e$, $S(A_{i+1}) \subset F(A_i)$ $\forall i$

("left-canonical decomposition").

Pf: • $\exists$: $P = A_1 B_1$ as in proposition, & iterate $B_i = A_{i+1} B_{i+1}$ until we get $B_k = e$. (happens in finitely many steps since $\deg \downarrow$ strictly each time).

• By downward induction on i, given decomp. where $S(A_{i+1}) \subset F(A_i) \Rightarrow$ $A_i \cdot (A_{i+1} \cdots A_k)$ is left-weighted and $S(A_i A_{i+1} \cdots A_k) = S(A_i)$.

• This gives uniqueness (using uniqueness in $\text{Prop}^{\underline{n}}$).

Rmk: • $P \geq \Delta$ iff $A_1 = \Delta$

Pf: – $A_1 = \Delta \Rightarrow P \geq \Delta$ clear

– if $P \geq \Delta \underset{\text{old lemma}}{\Rightarrow} P = \Delta Q$ for some $Q \in B_n^+$ $\Rightarrow S(P) = \{1 \ldots n-1\}$
$\Rightarrow S(A_1) = $ ——
$\Rightarrow A_1 = \Delta$.

• if a factor is Δ then all previous ones as well

So: $\inf(P) = \max\{i \,/\, A_i = \Delta\}$.

Prop: if $P = A_1 \cdots A_k$ (left canonical) then $\sup(P) = k$ (won't prove yet).

Corollary: $\forall P \in B_n$, $\exists!$ decomp. $P = \Delta^r A_1 \cdots A_k$, $r \in \mathbb{Z}$, $A_i \in S_n^+ \setminus \{e, \Delta\}$, $S(A_{i+1}) \subset F(A_i)$

This normal form gives a solution to the word problem, given algorithm to compute it.

- start with expression $P = \Delta^r P'$, $P' \in B_n^+$ given as $B_1 \dots B_k$ (permutation braids)

  [e.g.: stupid way from expr. as $\prod \sigma_i^{\pm 1}$: replace each σ_i^{-1} by $\Delta^{-1} U_i$ (perm braid) & collect all Δ^{-1}'s to the left

  $\exists$ smarter ways to collect more letters into a same B_i when obviously possible]

- if $S(B_{i+1}) \subset F(B_i)$ $\forall i$ we're done! (simply the first few B_i might be Δ, the last few might be e, collect appropriately)

- otherwise, pick $j \in S(B_{i+1}) \setminus F(B_i)$, replace $B_i \leftarrow B_i \sigma_j$
  $B_{i+1} \leftarrow \sigma_j^{-1} B_{i+1}$

  (gives something with $(\deg B_1, \dots, \deg B_k)$ lexicographically larger) & repeat.

  $\rightsquigarrow$ terminates in finite # steps

  (not too large if we do things in the right order...).

Machine representation = a bunch of permutation tables ($\pi_i \in \mathfrak{S}_n$ corresp. to the factors).

$\exists$ efficient ways to manipulate them (and starting/finishing sets easy to read off!).

‖ For a word of length ℓ in B_n, can compute the normal form in $O(\ell^2 n \log n)$.

(if improve a bit on above algorithm by passing as much as possible $B_{i+1} \rightsquigarrow B_i$ in a single step & doing these operations in sequence in a particular order.)