修士論文

Braid群のconjugacy algorithmについて

上村 恭子
奈良女子大学大学院　人間文化研究科　数学専攻

2007年

目 次

1 Introduction

Braid 群は 1926 年に Artin[1] によって導入され，その有限表示が与えられた．n 次の braid 群 B_n の元は，直観的には上下に水平に置かれた 2 本の棒の間を上から下へ n 本のひもが単調に下がっているような図形 (図 1.1) で，その積は 2 つの braid を上下に重ねてひもをつなげてやることに対応している．

図 1.1: braid

一般に，有限表示群 G の 2 つの元 a, b が word の表示によって与えられたとき，

(1) a と b が同じ元を表しているかどうか判定せよ (word problem)

(2) a と b は conjugate (すなわち，ある $t \in G$ で $b = t^{-1}at$ となるものが存在する) かどうか判定せよ (conjugacy problem)

という問題は，非常に難しい問題である．

Braid 群に関する上の 2 つの問題は 1960 年代後半に Garside[6] によって解決されたが，後に Thurston[9]，Elrifai-Morton[5]，Birman-Ko-Lee[4] らによってより効率的に解く algorithm が発見されている．これらの algorithm では，braid に対して「よい」標準形を定義することが基本的なアイディアとなっている．この修士論文では，これらのうち left-canonical form (l.c.f.) と呼ばれる標準形を用いた Elrifai-Morton の algorithm を紹介する．

現在 braid 群は，数学に限らず様々な分野に現れて広く研究されている．特に韓国のグループ [7] は braid 群を用いた公開鍵暗号を提案し，一連の研究を行っている．この暗号は「braid 群の conjugacy problem を解く効率的な algorithm がまだ見つかっていない」ことによって，その安全性が保障されている．このように braid 群の conjugacy problem を解く効率的な algorithm の発見は，実用の面でも大きな意味があることを注意しておく．

この論文の構成は以下のとおりである．まず第 2 節で群を定義し，その基本的性質と概念を紹介する．中でも Elrifai-Morton の algorithm において重要な役割を果たす置換群については 2.2 節で紹介する．次に第 3 節で braid 群を定義してその上

に半順序 $\leq$ を導入する．また，ひもを全体的に 180° ひねって得られる braid を Δ (図 1.2) で表すとき，任意の braid B に対して $\Delta^r \leq B \leq \Delta^s$ となる $r, s \in \mathbb{Z}$ が存在することを示す (定理 3.9)．これは Elrifai-Morton の algorithm の基礎となっている標準形を求めるための第一段階にあたる．第 4 節では braid を positive braid に限って議論を進める．ここでは positive braid が positive permutation braid と呼ばれる基本的な positive braid の積に分解できることを示す (命題 4.3)．これと第 3 節の結果を併せることにより，任意の braid は次のような形 (l.c.f.) に一意的に表されることがわかる (定理 4.13)．

$$\Delta^r A_1 A_2 \cdots A_k \quad (A_i : \text{positive permutation braid})$$

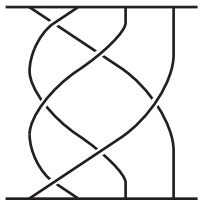


図 1.2: Δ

Braid 群の word problem と conjugacy problem は，こうして得られた l.c.f. の性質を用いることで解決される．まず第 5 節では l.c.f. の求め方 (すなわち，word problem を解く方法) について紹介する．次いで第 6 節では，conjugacy problem を解く方法について紹介する．このときに基本となるアイディアは，l.c.f. $\Delta^r A_1 A_2 \cdots A_k$ において A_1 を positive permutation braid の積の最後尾 (A_k の後ろ) に送る cycling と呼ばれる word の変換を braid に対して行うことである．

謝辞

ここでこの論文を作成するにあたり，ご多忙中にもかかわらずご指導くださいました小林毅先生に心よりお礼申し上げます．2 年前，何の計画もないまま奈良へ来た私ですが，先生はそんな私に対して様々な資料を提示し，丁寧にご指導くださいました．また日々の生活の中で講義や地域貢献事業に取り組まれる先生のお姿は，社会に対する姿勢として私の大きな目標となりました．微力ながらお手伝いできたこと，その経験を今後に活かしたいと思います．

最後に，奈良女子大学数学教室の諸先生方をはじめ，院生のみなさん，そしてこの 2 年間でかかわったすべての方々に心から感謝いたします．

2 Group

ここでは後で必要となる群の基本的な事柄と有限表示について紹介する.

2.1 Finite presentation of groups

集合 S の元の順序対 (a, b) の各々に対して，対応する元 c を定めることを**演算**という．演算の結果として a, b から c が決まるとき，演算の記号，例えば $\circ$ を用いて $c = a \circ b$ (あるいは単に ab) で表す.

注意 2.1 この演算を形式的に**乗法**ということもある．このとき，演算の結果を**積**という.

定義 演算 $\circ$ の定義された集合 S において，任意の元 a, b, c に対して次が成り立つとき，S は演算 $\circ$ に関して**半群** (**semi-group**) であるという.

$$(a \circ b) \circ c = a \circ (b \circ c) \tag{2.1}$$

注意 2.2 演算が乗法で表される半群を**乗法半群**という.

注意 2.3 任意の元 $a \in S$ に対して，$a \circ e = e \circ a = a$ となる元 e を S の**単位元**という．また $a \circ b = b \circ a = e$ となる元 b を a の**逆元**といい，a^{-1} で表す.

乗法半群 S おいて元 a の n 個の積 $\overbrace{aa\cdots a}^{n}$ を a^n で表す．特に $a^1 = a$ である．このとき，任意の自然数 m, n に対して

$$a^m a^n = a^{m+n} \tag{2.2}$$

$$(a^m)^n = a^{mn} \tag{2.3}$$

が成り立つ．また， $ab = ba$ のとき

$$(ab)^n = a^n b^n \tag{2.4}$$

が成り立つことは容易にわかる.

定義 集合 G が演算 $\circ$ に関して半群をつくり，かつ G に単位元が存在し，G の任意の元に対して逆元が存在するとき，G は演算 $\circ$ に関して**群** (**group**) であるという.

注意 2.4 群 G に属する元の個数を G の**位数**という．また位数が有限である群を**有限群**といい，そうでない群を**無限群**という.

定義 群 G のすべての元が G のある元 a のベキ乗になっているとき，G は a で生成された**巡回群**であるといい，$< a >$ で表す．また a をその**生成元**という．

注意 2.5 特に有限群でない巡回群を**無限巡回群**という．無限巡回群 $\{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$ は整数 $\mathbb{Z}$ に足し算で演算を定義した群と同型である．

$M = \{G_\lambda\}$ を群 G_λ の集合とし，λ はある有限集合の上にわたるものとする．M に属する群はどの 2 つも単位元 e のみを共通にもつとする．また $A = (a_1, a_2, \ldots, a_n)$ を G_λ の和集合 $\cup_\lambda G_\lambda$ から任意に有限個の元をとって並べた重複順列とする．

n 項の順列 $A = (a_1, a_2, \ldots, a_n)$ において，隣り合った 2 つの項 a_i と a_{i+1} が同じ群 G_λ に属するとき，この 2 項を積 $a_i a_{i+1}$ に置き換えて $n-1$ 項の順列 $(a_1, \ldots, a_i a_{i+1}, \ldots, a_n)$ をつくる．特に a_i (または a_{i+1}) が単位元の場合には，単位元を 1 つ取り除いてやる．これを A を**簡約**するという．簡約を繰り返すと，ついには簡約のできない順列を得る．この最後の結果は，途中の簡約の順序に依らずに定まることが知られている．

いま順列 $(a_1, a_2, \ldots, a_n)$ で，もうこれ以上簡約できないものすべての集合を G とする．A, B が G の元のとき，順列 $(A, B) = (a_1, \ldots, a_n, b_1, \ldots, b_m)$ を簡約して得られる G の元を AB で表すと，この結合によって G は群をつくることが知られている．このとき，群 G を M **に属する群の自由積**という．

定義 $M = \{x_\lambda\}$ を x_λ の集合とする．このとき，無限巡回群 $G_\lambda =< x_\lambda >$ の自由積 F を M **で生成された自由群**という．

注意 2.6 F の単位元以外の元は $x_{\lambda_1}^{v_1} x_{\lambda_2}^{v_2} \cdots x_{\lambda_n}^{v_n}$ $(v_i \neq 0)$ の形で一意的に表される．ただし，ここでは n 項の列 $x_{\lambda_1}, x_{\lambda_2}, \ldots, x_{\lambda_n}$ において同じ G_λ に属するものは隣り合わせていない．

定義 群 G の部分集合 H が G の演算に関して群をつくるとき， H を G の**部分群** (**subgroup**) という．

定義 M を群 G の部分集合とする．このとき

$$a_1^{v_1} a_2^{v_2} \cdots a_r^{v_r} \quad (v_i = \pm 1,\ a_i \in M,\ i = 1, 2, \ldots, r) \tag{2.5}$$

の形の元全体は群をつくる．この部分群を M **から生成された** G **の部分群**といい，$< M >$ で表す．

注意 2.7 $< M >$ は M を含む G の最小の部分群である．

注意 2.8 M が有限集合 $\{a_1, a_2, \ldots, a_n\}$ の場合には，群 $< M >$ は**有限生成**であるといい，$< M >$ を $< a_1, a_2, \ldots, a_n >$ で表す．またこの $a_1, a_2, \ldots, a_n$ を**生成元**といい，M を $< M >$ の**生成系**という．

定義 群 G の元 a,b に対して，ある元 $t \in G$ で $b = t^{-1}at$ となるものが存在するとき，b は a に**共役** (**conjugate**) であるという．

定義 群 G の各元 x と可換な G の元全体の集合 $\{c \in G : cx = xc, \forall x \in G\}$ は G の部分群である．これを群 G の**中心** (**center**) という．

定義 集合 M を互いに共通な元をもたない (空でない) 部分集合 $A, B, C, \ldots$ に分けることを M を**類別**するといい，その各部分集合を**類** (**class**) という．また，1つの類 (例えば A) から任意に取り出した元 a はその類を代表することができる．この a を A の**代表元**という．

群 G の部分群 H と G の元 a に対して，G の部分集合 aH, Ha を次のように定める．

$$aH = \{ah : h \in H\}, \quad Ha = \{ha : h \in H\} \tag{2.6}$$

群 G の部分群 H と G の元 a,b に対して，$aH = bH$ が成り立つとき a と b は H を法として**左合同**であるという．同様に，$Ha = Hb$ が成り立つとき a と b は H を法として**右合同**であるという．

定義 H を群 G の部分群，a を G の元とする．このとき，H を法として a と左合同である G の元全体の集合を a の H を法とする**左剰余類**という．また，H を法として a と右合同である G の元全体の集合を a の H を法とする**右剰余類**という．

定義 群 G の各元 a に対して $aH = Ha$ が成り立つとき，H を G の**正規部分群**という．

注意 2.9 このとき ($aH = Ha$ のとき) 左剰余類と右剰余類の区別はしなくてもよい．よって単に**剰余類**という．H を法とする G の剰余類全体の集合を G/H で表す．また G/H は乗法に関して群をつくることが知られている (ここで単位元は H，元 aH の逆元は $(aH)^{-1} = a^{-1}H$ である)．この群を G の H を法とする**剰余類群** (あるいは単に**剰余群**) といい，剰余類全体の集合と同じ記号 G/H で表す．

定義 F を $\{x_1, x_2, \ldots, x_n\}$ で生成された自由群，M を F の部分集合とする．このとき

$$\prod_{i=1}^{t} P_i(x)^{-1} Q_i(x)^{\mu_i} P_i(x) \quad (P_i(x) \in F,\ Q_i(x) \in M,\ \mu_i \pm 1) \tag{2.7}$$

の形の元全体は F の正規部分群 N' をつくる．この N' を M **から生成された** F **の正規部分群**という．

定義 群 G から群 G' への写像 f が次の条件を満たすとき，f を G から G' への**準同型写像** (あるいは単に**準同型**) という．

$$f(ab) = f(a)f(b) \quad (\forall a, b \in G) \tag{2.8}$$

注意 2.10 f が準同型写像のとき G の像 G' は群をつくる．G' の単位元は $e' = f(e)$ である．また $\{e'\}$ の原像

$$N = f^{-1}(\{e'\}) = \{x \in G : f(x) = e'\} \tag{2.9}$$

は G の正規部分群である．これを準同型写像 f の**核**という．

定義 群 G から群 G' への準同型写像 f が $f(G) = G'$ を満たすとき，f を G から G' の**上への準同型写像**という．

注意 2.11 N を群 G の正規部分群とし，f は G の元 a を G/N の元 $A = Na$ に写す写像とする．このとき次が成り立つから，f は G から G/N の上への準同型写像である．

$$\begin{aligned} f(ab) &= Nab = NNab = NaNb = f(a)f(b) \\ f(G) &= G/N \end{aligned}$$

定義 群 G から群 G' への写像 f が一対一，かつ準同型写像であるとき，G と G' は**同型**であるという．

G をある群の元の有限集合 $S = \{a_1, a_2, \ldots, a_n\}$ から生成される群とする．いま，これとは別に n 個の元 $\{x_1, x_2, \ldots, x_n\}$ で生成された自由群 F を考える．このとき F の単位元 e 以外の元は

$$P(x) = x_{i_1}^{v_1} x_{i_2}^{v_2} \cdots x_{i_r}^{v_r} \quad (v_i \pm 1,\ i = 1, 2, \ldots, r) \tag{2.10}$$

の形で一意的に表される．ただし，この表示は簡約されているとする．

このとき F から G への準同型写像 f が次のように構成される．f は x_i を a_i に写し，簡約された F の任意の元 $P(x) = x_{i_1}^{v_1} x_{i_2}^{v_2} \cdots x_{i_r}^{v_r}$ を G の元 $P(a) = a_{i_1}^{v_1} a_{i_2}^{v_2} \cdots a_{i_r}^{v_r}$ に写す．このとき f の核 N は次のようになる．

$$N = \{R(x) \in F : R(a) = e\} \tag{2.11}$$

いま M を N の部分集合とすると，

$$Q(a) = e \quad (\forall Q(x) \in M) \tag{2.12}$$

が成り立つ．この M を用いて

$$R(x) = \prod_{i=1}^{t} P_i(x)^{-1} Q_i(x)^{\mu_i} P_i(x) \quad (P_i(x) \in F,\ Q_i(x) \in M,\ \mu_i \pm 1) \tag{2.13}$$

の形の元をつくれば，$Q_i(a)$ は単位元なので次が成り立つ．

$$\begin{aligned} R(a) &= \prod_{i=1}^{t} P_i(a)^{-1} Q_i(a)^{\mu_i} P_i(a) \\ &= \prod_{i=1}^{t} P_i(a)^{-1} P_i(a) \\ &= e \end{aligned}$$

注意 2.12 N の任意の元が M の元を用いて (2.13) のような形で表示されるとき，(2.12) を G の**基本関係**という．

定理 2.13 M を自由群 $F =< x_1, x_2, \ldots, x_n >$ の部分集合とする．n 個の元から生成される群 $G =< s_1, s_2, \ldots, s_n >$ で，次を満たし，かつこれを基本関係とするものが存在する．

$$Q_i(s) = e \quad (\forall Q_i(x) \in M) \tag{2.14}$$

定義 定理2.13の M を G の**基本関係式**という．特に M が有限個の元 $Q_1, Q_2, \ldots, Q_m$ からなるときには次のように表し，これを G の**有限表示**という．

$$G = < x_1, x_2, \ldots, x_n \mid Q_1, Q_2, \ldots, Q_m > \tag{2.15}$$

2.2 Permutation group

集合 M から M への写像を M の**自己写像**という．M の自己写像 f によって M の元 x に対応する元を積 xf で表すことにする．f, g が M の自己写像のとき，M の元 x は f によって xf に写り，xf はさらに g によって $(xf)g$ に写る．ここで M の各元 x に $(xf)g$ を対応させると M の自己写像 $x \mapsto (xf)g$ が得られる．これを f と g の積といい，fg で表す．

$$x(fg) = (xf)g \quad (\forall x \in M) \tag{2.16}$$

M の自己写像の積をこのように定義すると，自己写像全体の集合 S は単位元をもつ半群をつくることがわかる．実際，M の任意の元 x に対して

$$\begin{aligned} x((fg)h) &= (x(fg))h = ((xf)g)h \\ x(f(gh)) &= (xf)(gh) = ((xf)g)h \end{aligned}$$

となるから，$x((fg)h) = x(f(gh))$，すなわち $(fg)h = f(gh)$ (結合法則) が成り立つ．また $xI = x$ となる写像 I (M の単位写像) が S の単位元である．

定義 M の自己写像のうち，M から M の上への一対一写像を M の**置換**という．また単位元に対応する置換 I を**単位置換**という．

置換の積は明らかに置換であるから，M の置換全体の集合は I を含む半群をつくる．φ を M の置換とすると，

$$x \mapsto x' = x\varphi \quad (\forall x \in M) \tag{2.17}$$

は M から M の上への一対一の対応であるから，逆の対応 $x' \mapsto x$ を考えることができる．この置換を φ' とすると，

$$\varphi\varphi' = \varphi'\varphi = I \tag{2.18}$$

となる．したがって φ' は φ の逆元 φ^{-1} で，これを φ の**逆置換**という．このようにして，集合 M の置換全体は置換の積に関して群をつくる．この群を S^M で表す．

注意 2.14 S^M の単位元は単位置換 $I : x \mapsto x$ である．また置換 $\varphi : x \mapsto x'$ の逆元は逆置換 $\varphi^{-1} : x' \mapsto x$ である．

M が有限集合の場合には，M の元に番号 $1, 2, \ldots, n$ を付け，この番号によって M の元を表すことができる．

記号　置換 $i \mapsto p_i$ $(i = 1, 2, \ldots, n)$ を次のように表す.

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix} \tag{2.19}$$

2 つの置換 σ, τ に対し，σ によって i $(= 1, 2, \ldots, n)$ が p_i に写り，さらに τ によって p_i が r_i に写るとする．このとき積として次を得る.

$$\sigma\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix} \tag{2.20}$$

例　$n = 3$ とする．このとき,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

とすれば

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

を得る.

定義　集合 $\{1, 2, \ldots, n\}$ の置換全体がつくる群を n 次の**置換群**といい，S_n で表す.

S_n は有限群で，その位数は $n!$ である．また S_n は次のような有限表示をもつことが知られている.

$$\left\langle s_1, s_2, \ldots, s_{n-1} \;\middle|\; \begin{array}{rcll} s_i s_j s_i & = & s_j s_i s_j, & |i-j| = 1 \\ s_i s_j & = & s_j s_i, & |i-j| \geq 2 \\ s_i^2 & = & 1, & i = 1, 2, \ldots, n-1 \end{array} \right\rangle \tag{2.21}$$

ここで s_i は i と $i+1$ を入れ換える置換になっている．このような置換を**互換**といい，$(i, i+1)$ で表す.

3 Artin's braid group

ここでは Artin [1] によって与えられた n 次の braid 群 B_n について紹介する．まず braid の定義から始める．

3.1 Braid

図 3.1 のような箱を考える．箱の上の面に n 個の異なる点 $P_1, P_2, \ldots, P_n$ をとり，箱の下の面にもこれらの真下にあたる場所に点 $Q_1, Q_2, \ldots, Q_n$ をとる．

いま時刻 0 において点 P_i $(i = 1, 2, \ldots, n)$ を出発した n 個の点が，高さが単調に減少するように箱の中を動き回って，時刻 1 にそれぞれ点 Q_j $(j = 1, 2, \ldots, n)$ のいずれかに到達するとする．特にここではこれらの点が通った軌跡は互いに交わらないとする．このとき，これらの軌跡は箱の中の上下にある点を結び，箱の内側を通る n 本のひもになっている．このようにしてできる n 本のひもがつくる図形を **geometric braid** という．ここで 2 つの geometric braids が上下の点を止めて geometric braid の状態を保ちつつ移り合うならば，それらは同じものであるとみなす．

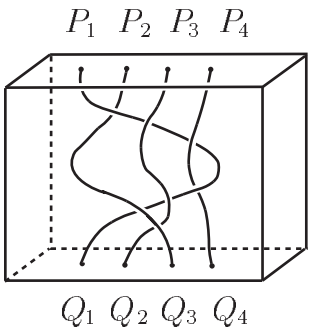


図 3.1: $n = 4$ の geometric braid

Geometric braid を表示するには，箱の正面 (ただし，箱の正面は光を通すことができるとする) に光をあて，箱の一番奥の平面に映る影を描いてやると便利である．このとき，図 3.2 のように下にあるひもを切れたように描くことで，交点をつくる 2 本のひもの上下がわかるようにする．

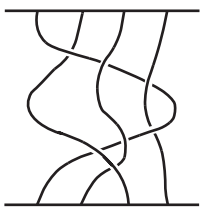


図 3.2: geometric braid の平面表示

n 本のひもからなる 2 つの geometric braids A, B が与えられたとき，その積 AB を A を B の上に置いてひもをつなげることによって得られる geometric braid と定める．このとき，n 本のひもからなる geometric braid 全体はこの積に関して群をつくることが証明できる．この群を n 次の **braid 群**といい，B_n で表す．また braid 群の元のことを単に braid という．以下では geometric braid と braid を必要に応じて同一視することにする．

注意 3.1 B_n の単位元は，n 本の真っ直ぐで垂直なひもからなる braid である．また A の逆元は，A を水平な線で鏡映をとって得られる braid である．

いま σ_i $(i = 1, 2, \ldots, n-1)$ を図 3.3 のような geometric braid で表される B_n の元とする．

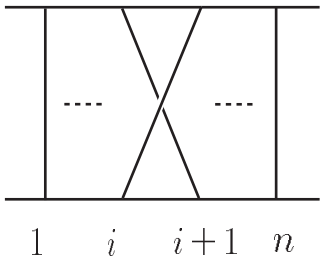


図 3.3: σ_i

このとき Artin は，B_n が次のような有限表示をもつことを示した ([1][3]).

$$B_n = \left\langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{rcll} \sigma_i\sigma_j\sigma_i & = & \sigma_j\sigma_i\sigma_j, & |i-j| = 1 \\ \sigma_i\sigma_j & = & \sigma_j\sigma_i, & |i-j| \geq 2 \end{array} \right\rangle \tag{3.1}$$

またこの表示に関係式 $\sigma_i^2 = 1$ $(i = 1, 2, \ldots, n-1)$ を加えたものは 2.2 節で紹介した置換群 S_n の表示になる．したがって，自然な上への準同型 $\rho : B_n \to S_n$ が存在することがわかる．

注意 3.2 このとき各 $\rho(\sigma_i)$ は互換 $(i, i+1)$ になっている．

B_n の自己同型写像 τ を次で定める．

$$\tau(\sigma_i) = \sigma_{n-i} \quad (i = 1, 2, \ldots, n-1) \tag{3.2}$$

このとき τ は，幾何的には図 3.4 で表される 'turning over' になっている．

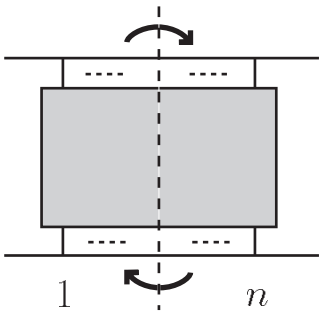


図 3.4: turning over

また B_n の自己写像 rev を $\mathrm{rev}(\sigma_i) = \sigma_i$ $(i = 1, 2, \ldots, n-1)$ で定まる B_n の anti automorphism (すなわち $A, B \in B_n$ に対して $\mathrm{rev}(AB) = \mathrm{rev}(B)\mathrm{rev}(A)$ が成り立つような自己写像) とする．これは B を $\{\sigma_i\}$ の word で表したときに，その word を後ろから読むことに対応している．

例 $\mathrm{rev}(\sigma_1\sigma_2\sigma_3) = \mathrm{rev}(\sigma_2\sigma_3)\mathrm{rev}(\sigma_1) = \mathrm{rev}(\sigma_3)\mathrm{rev}(\sigma_2)\mathrm{rev}(\sigma_1) = \sigma_3\sigma_2\sigma_1$

このとき rev は，幾何的には図 3.5 で表される 'reversing' になっている．

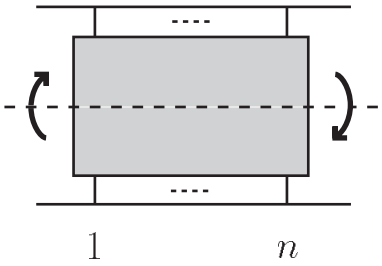


図 3.5: reversing

記号 次のように帰納的に定義される B_n の元 Δ_{n-1} を **fundmental braid** という．

$$\Delta_1 = \sigma_1 \quad (\in B_2) \tag{3.3}$$

$$\Delta_{n-1} = \Delta_{n-2}\sigma_{n-1}\cdots\sigma_1 \quad (\in B_n) \tag{3.4}$$

Δ_{n-1} は横棒から n 本のひもが下がった状態を positive 方向に 180° ひねって得られる geometric braid (図 3.6) に対応している．以下では紛らわしくない限り Δ_{n-1} を Δ で表すことにする．

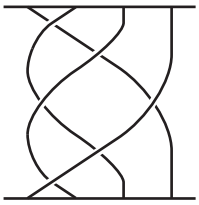


図 3.6: Δ_3

注意 3.3 Δ^2 は B_n の center の生成元であることが知られている．特に次が成り立つ．

$$\Delta^2 B = B\Delta^2 \quad (\forall B \in B_n) \tag{3.5}$$

これは幾何的には図 3.7 のように表される．

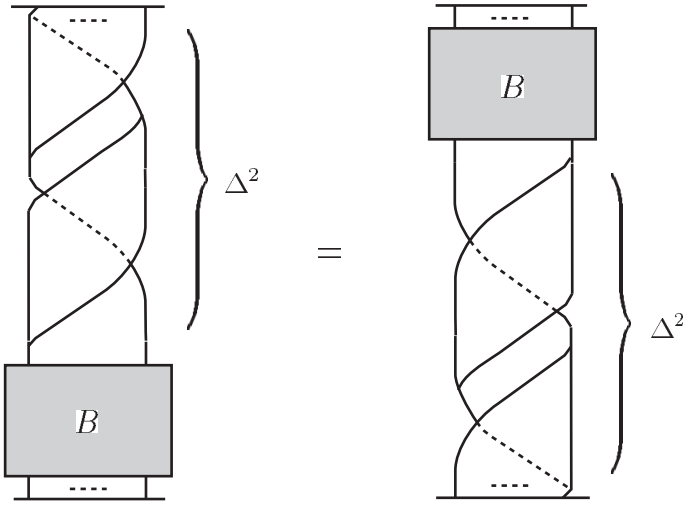


図 3.7: center

また図 3.8 からわかるように，τ は Δ (または Δ^{-1}) による conjugate である．すなわち，次が成り立つ．

$$\tau(B) = \Delta^{-1} B \Delta, \quad \tau(B) = \Delta B \Delta^{-1} \quad (\forall B \in B_n) \tag{3.6}$$

したがって，次のことがわかる．

$$\Delta\tau(B) = B\Delta, \quad \tau(B)\Delta = \Delta B \quad (\forall B \in B_n) \tag{3.7}$$

$$\Delta^{-1}\tau(B) = B\Delta^{-1}, \quad \tau(B)\Delta^{-1} = \Delta^{-1} B \quad (\forall B \in B_n) \tag{3.8}$$

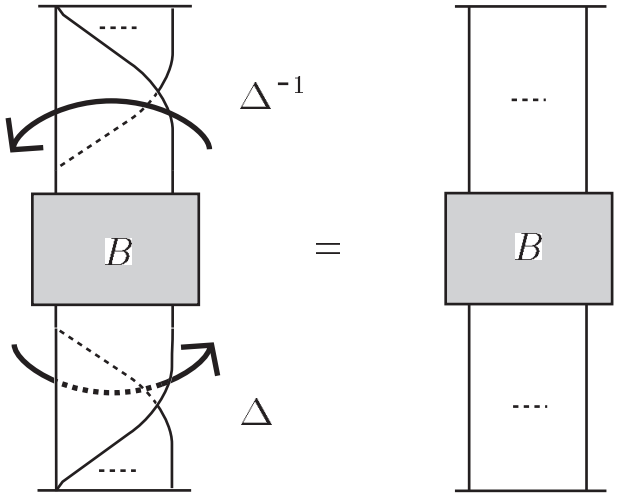


図 3.8: conjugate

3.2 Partial order

ここでは positive braid B_n^+ を用いて B_n の上に半順序を導入し，その性質を紹介する．

定義 B_n の元 B が **positive braid** であるとは，B が成元 $\{\sigma_i\}$ の positive word (すなわち σ_i^{-1} の形の元を含まない word) で表示できることである．

記号 B_n の positive braid 全体の集合を B_n^+ で表す．

B_n から $\mathbb{Z}$ への準同型写像 wt を $\mathrm{wt}(\sigma_i) = 1$ $(i = 1, 2, \ldots, n-1)$ で定める．これは B_n^+ の元 B に対し，B を表す positive braid word の長さを与える．

いま，次のようにして B_n の上に半順序を導入する．

記号 B_n の元 A, B に対して，ある $C_1, C_2 \in B_n^+$ で $B = C_1 A C_2$ となるものが存在するとき，$A \leq B$ で表す．

注意 3.4 次が成り立つ．

$$B \in B_n^+ \ \Leftrightarrow \ e \leq B \tag{3.9}$$

$$A \leq B \ \Leftrightarrow \ B^{-1} \leq A^{-1} \tag{3.10}$$

実際これは，次のようにして証明できる．
[(3.9) について] $B \in B_n^+$ とする．ここで $C_1 = B$，$C_2 = e$ とすると $B = Bee$ とかける．よって $e \leq B$ を得る．逆に $e \leq B$ のとき $B \in B_n^+$ となることは定義より明らか．
[(3.10) について] $A \leq B$ とする．このとき定義より，ある $C_1, C_2 \in B_n^+$ が存在して $B = C_1 A C_2$ とかける．ここで両辺の逆元をとると $B^{-1} = C_2^{-1} A^{-1} C_1^{-1}$ となる．さらに両辺の左から C_2 を，右から C_1 を掛けると $C_2 B^{-1} C_1 = A^{-1}$，よって $B^{-1} \leq A^{-1}$ を得る．逆に $B^{-1} \leq A^{-1}$ のとき $A \leq B$ となることも同様にして示される．

以下では (3.9) に従い，B が positive braid であることを $B \geq e$ で表すことにする．

命題 3.5 B_n の各生成元 σ_i $(i = 1, 2, \ldots, n-1)$ に対して $e \leq \sigma_i \leq \Delta$ が成り立つ．

証明 $e \leq \sigma_i$ は明らか．また定義より $\Delta = \Delta_{n-2}\sigma_{n-1} \cdots \sigma_{i+1}\sigma_i\sigma_{i-1} \cdots \sigma_1$ とかける．ここで $C_1 = \Delta_{n-2}\sigma_{n-1} \cdots \sigma_{i+1}$，$C_2 = \sigma_{i-1} \cdots \sigma_1$ とすれば $\sigma_i \leq \Delta$ を得る．□

命題 3.6 $s \in \mathbb{Z}$ に対して $A \leq \Delta^s$ とする．このとき，ある $D_1, D_2 \geq e$ で $\Delta^s = D_1 A = A D_2$ となるものが存在する．

証明 $A \leq \Delta^s$ であるから，定義より，ある $C_1, C_2 \geq e$ が存在して $\Delta^s = C_1 A C_2$ とかける．よって $\Delta^s C_2^{-1} = C_1 A$ が成り立つ．これに (3.7) または (3.8) を繰り返し適用して $\tau^s(C_2^{-1})\Delta^s = C_1 A$ を得る．τ の定義より任意の $C \geq e$ に対して $\tau(C^{-1}) = (\tau(C))^{-1}$ がわかるから，$(\tau^s(C_2))^{-1}\Delta^s = C_1 A$，よって $\Delta^s = \tau^s(C_2) C_1 A$ を得る．ここで $D_1 = \tau^s(C_2) C_1$ とすればよい．また $A D_2 = \Delta^s$ となるような $D_2 \geq e$ の存在も同様にして示される． □

命題 3.7 $r \in \mathbb{Z}$ に対して $\Delta^r \leq A$ とする．このとき，ある $E_1, E_2 \geq e$ で $A = E_1 \Delta^r = \Delta^r E_2$ となるものが存在する．

証明 $\Delta^r \leq A$ であるから，定義より，ある $C_1, C_2 \geq e$ が存在して $A = C_1 \Delta^r C_2$ とかける．これに (3.7) または (3.8) を繰り返し適用して $A = C_1 \tau^r(C_2) \Delta^r$ を得る．ここで $E_1 = C_1 \tau^r(C_2)$ とすればよい．また $\Delta^r E_2 = A$ となるような $E_2 \geq e$ の存在も同様にして示される． □

命題 3.8 $r_1, r_2, s_1, s_2 \in \mathbb{Z}$ に対して $\Delta^{r_1} \leq B \leq \Delta^{s_1}$，$\Delta^{r_2} \leq C \leq \Delta^{s_2}$ とする．このとき $\Delta^{r_1+r_2} \leq BC \leq \Delta^{s_1+s_2}$ が成り立つ．

証明 $\Delta^{r_1} \leq B \leq \Delta^{s_1}$ であるから，命題 3.6 と命題 3.7 より，ある $D_1, E_1 \geq e$ が存在して $\Delta^{s_1} = D_1 B$，$B = E_1 \Delta^{r_1}$ とかける．また $\Delta^{r_2} \leq C \leq \Delta^{s_2}$ であるから $\Delta^{s_2} = C D_2$，$C = \Delta^{r_2} E_2$ とかける．よって $BC = E_1 \Delta^{r_1+r_2} E_2$ $(E_1, E_2 \geq e)$，ゆえに $\Delta^{r_1+r_2} \leq BC$ を得る．また $\Delta^{s_1+s_2} = D_1 BC D_2$ $(D_1, D_2 \geq e)$，ゆえに $BC \leq \Delta^{s_1+s_2}$ を得る． □

定理 3.9 B_n の元 B に対して，ある $r, s \in \mathbb{Z}$ で $\Delta^r \leq B \leq \Delta^s$ となるものが存在する．

証明 $B \in B_n$ を表す $\{\sigma_i^{\pm}\}$ $(i = 1, 2, \ldots, n-1)$ の word w をひとつ固定する．命題 3.5 と (3.10) より $e \leq \sigma_i \leq \Delta$，$\Delta^{-1} \leq \sigma_i^{-1} \leq e$ がわかる．ここで命題 3.8 を適用すると $\Delta^r \leq B \leq \Delta^s$ がわかる (ただし $-r$ は w の中に現れる σ_i^{-1} の個数，s は w の中に現れる σ_i の個数とする)． □

記号 $r, s \in \mathbb{Z}$ に対して $r < s$ とする．このとき B_n の部分集合 $[r, s]$ を次のように定める．

$$[r, s] = \{B \in B_n : \Delta^r \leq B \leq \Delta^s\} \tag{3.11}$$

一般に，S, T を群 G の部分集合とする．このとき G の部分集合 ST を次のように定める．

$$ST = \{st \in G : s \in S, t \in T\} \tag{3.12}$$

注意 3.10 命題3.8より $[r_1, s_1][r_2, s_2] \subset [r_1 + r_2, s_1 + s_2]$ がわかるが，実はこれらは一致している．この証明は付録Aで与える．

注意 3.11 $[r, s] = \Delta^r[0, s - r]$ が成り立つ．

実際これは，次のようにして証明できる．
$[\subset]$ $B \in [r, s]$，すなわち $\Delta^r \leq B \leq \Delta^s$ が成り立つとする．このとき命題3.6より，ある $D \geq e$ が存在して $\Delta^s = BD$ とかける．また命題3.7より，ある $E \geq e$ が存在して $B = \Delta^r E$ とかけるから，$\Delta^s = \Delta^r ED$ を得る．よって $\Delta^{s-r} = ED\,(E, D \geq e)$，ゆえに $e \leq E \leq \Delta^{s-r}$ (i.e. $E \in [0, s - r]$) がわかる．いま $B = \Delta^r E$ であるから，$B \in \Delta^r[0, s - r]$ を得る．
$[\supset]$ $B \in \Delta^r[0, s - r]$ とする．このとき，ある $E \in [0, s - r]$ が存在して $B = \Delta^r E$ とかける．よって $\Delta^r \leq B$ がわかる．また $E \leq \Delta^{s-r}$ であるから，命題3.6より，ある $D \geq e$ が存在して $\Delta^{s-r} = ED$ とかける．いま $B = \Delta^r E$ であるから $BD = \Delta^r ED = \Delta^s$，ゆえに $B \leq \Delta^s$ がわかる．したがって $\Delta^r \leq B \leq \Delta^s$，すなわち $B \in [r, s]$ を得る．

定理3.9より，次の定義が導かれる．

定義 B_n の元 B に対して $\inf B$，$\sup B$ を次のように定める．

$$\inf B = \max\{r : \Delta^r \leq B\} \tag{3.13}$$
$$\sup B = \min\{s : B \leq \Delta^s\} \tag{3.14}$$

このとき B の **canonical length** $l(B)$ を $l(B) = \sup B - \inf B$ と定める．

注意 3.12 命題3.8より，$l(AB) \leq l(A) + l(B)$ が成り立つことがわかる．

注意 3.13 $-\sup B = \inf B^{-1}$ が成り立つ．

実際これは，次のようにして証明できる．$m = \sup B$ とすると $B \leq \Delta^m$，よって $B^{-1} \geq \Delta^{-m}$ を得る (3.10)．ゆえに $\inf B^{-1} \geq -m = -\sup B$，すなわち $\inf B^{-1} \geq -\sup B$ を得る．また $n = \inf B^{-1}$ とおいて同様にしてやると $\sup B \leq -n = -\inf B^{-1}$，すなわち $-\sup B \geq \inf B^{-1}$ を得る．以上より与式は成り立つ．

4 Positive braid

ここでは positive braids の集合 B_n^+ を取り扱う.

4.1 Positive permutation braid

いま positive braid を標準的な方法で基本的な positive braid (positive purmutation braid と呼ばれる) に分解することを考える. そのためにまず次を準備する.

記号 次のように記号 $*$ を定める.

$$\sigma_i * \sigma_j = \begin{cases} \sigma_i, & i = j \\ \sigma_i\sigma_j, & |i-j| > 1 \\ \sigma_i\sigma_j\sigma_i, & |i-j| = 1 \end{cases} \tag{4.1}$$

次の Garside の補題 ([6] 定理 1.2) は認めることにする.

補題 4.1 (Garside) $P_1, P_2 \geq e$ に対して $P = \sigma_i P_1 = \sigma_j P_2$ とする. このとき次が成り立つ.

ある $P_3 \geq e$ で $P = (\sigma_i * \sigma_j)P_3$ となるものが存在する.

定義 $P \geq e$ に対し, P の **starting set** $S(P)$ と **finishing set** $F(P)$ を次のように定める.

$$S(P) = \{i : P = \sigma_i P_i,\ P_i \geq e\} \tag{4.2}$$
$$F(P) = \{i : P = P_i \sigma_i,\ P_i \geq e\} \tag{4.3}$$

注意 4.2 このとき, 次が成り立つことは容易にわかる.

$$F(P) = S(\mathrm{rev}(P)) \tag{4.4}$$

定義 $P \geq e$ に対して分解 $P = AB$ $(A, B \geq e)$ を考える. いま $S(B) \subset F(A)$ が成り立つときこの分解を **left-weighted**, $S(B) \supset F(A)$ が成り立つときこの分解を **right-weighted** という.

次に $P \geq e$ に対し, left-weighted factorization (以下では l.w.f. とかく) $P = A_1 P_1$ で $A_1 \in [0, 1]$ となるようなものを考える. これに関して次が成り立つ.

命題 4.3 $P \geq e$ に対し, 次を満たすような l.w.f. $P = A_1 P_1$ $(A_1 \in [0, 1])$ がただ 1 つ存在する.

任意の分解 $P = AB$ $(A \in [0,1])$ に対し，ある $Q \geq e$ が存在して
$A_1 = AQ$ が成り立つ $(*)$.

命題 4.3 の証明を与える前に，$[0,1]$ に属する braid の特徴付けを与える．まず次のことに注意する．

2 つの geometric braids B_1, B_2 は同じ braid を表しているとする．このとき，B_1 の中の 2 本のひもがつくる交点の数と，B_2 の中の対応する 2 本のひもがつくる交点の数は一般には一致しない (図 4.1).

図 4.1: 一致しない

しかし B_1, B_2 がともに positive braid のときには，B_n の基本関係式を利用することで，これらの値が常に等しいことがわかる (図 4.2).

図 4.2: 常に一致する

定義 任意の 2 本のひもが高々1 回しか交差しないような positive braid として描ける braid を **positeive permutation braid** という.

記号 Positive permutation braids の集合を S_n^+ で表す.

注意 4.4 Δ は S_n^+ の元である．実際 Δ は横棒から n 本のひもが下がった状態を positive 方向に $180°$ ひねった geometric braid で表される．よって任意の 2 本のひもはちょうど 1 回交差している.

注意 4.5 $P \in S_n^+$ とする．このとき $A, B \geq e$ に対して次が成り立つ.

$$P = AB \;\Rightarrow\; A, B \in S_n^+ \tag{4.5}$$

実際 $P \in S_n^+$ であるから，P $(= AB)$ の任意の 2 本のひもは高々1 回しか交差しない．よって A (または B) の中の任意の 2 本のひもは高々1 回しか交差しない．ゆえに A, B は S_n^+ の元である．

定理 4.10 で S_n^+ が $[0,1]$ と等しいことを示す．まず S_n^+ と S_n が全単射で対応することを示す．

補題 4.6 S_n^+ の元 A_1, A_2 が同じ置換を導くとき，$A_1 = A_2$ が成り立つ．また S_n の元 π に対して，π を導くような S_n^+ の元 A_π が存在する．

証明 [前半] A_1 と A_2 が同じ置換を導くとする．まず各々の braid のひもの上端点に左から順に番号 $1, 2, \ldots, n$ を付け，i 番目のひもを「ひも i」と呼ぶことにする．次に braid の入っている箱の中に，手前の面と平行な n 枚の平面で braid よりも奥に位置するようなものを固定する．

いま A_1, A_2 は positive permutation braid であるから，ひも i とひも j は高々 1 回しか交差せず，$i < j$ のときにひも i はひも j の奥を通ることがわかる．よってひも 1 に注目すると，ひも 1 は他のひもと交差しないように箱の奥方向へ押し込んで，一番奥の平面に乗せることができる．そこで，ひも 1 をこの位置に移しておく．次にひも 2 に注目する．同様の議論により，ひも 2 は他のひもと交差しないように箱の奥方向へ押し込み，奥から 2 番目の平面に乗せることができる．よって，ひも 2 をこの位置に移しておく．さらに ひも $3, \ldots,$ ひも n についても順に同様の操作を繰り返す．その結果，ひも 1 は箱の一番奥に位置する平面に乗っていて，その他のひもは番号順に 1 枚ずつ手前の平面に 1 本ずつ乗っている．

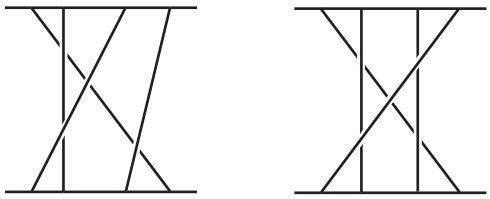
いま A_1 と A_2 が同じ置換を導くから，各々の braid のひも i は同じ下端点につながっている．よって A_1 の中の任意のひもは A_2 の中の対応するひもに垂直平面の isotopy で移り合うことがわかる．したがって $A_1 = A_2$ を得る．

[後半] $\pi \in S_n$ とする．A_π を構成するには，π を実現するような positive braid で任意の 2 本のひもが高々1 回しか交差しないようなものを見つければよい．よって以下でこのような geometric braid の作り方を紹介する．

まず長方形の上辺と下辺に n 個の点をとり，左から順に番号 $1, 2, \ldots, n$ を付ける．次に上辺の点 i から下辺の点 $\pi(i)$ に線分を引く (これは置換を視覚化するよく知られた方法である)．このとき，これらの線分の任意の 2 本は高々1 回しか交差しないことに注意する．次にこの図の交点を positive に描き直す (これは $i < j$ のときに，点 i から出発する直線を点 j から出発する直線の下を潜って交差させることで実現できる)．こうして得られる braid が求める A_π になっていることは明らかである． □

以下では補題 4.6 に従い，置換 $\pi \in S_n$ を導く positive permutation braid を A_π で表すことにする．

例 $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$, $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$ とする．これらを導く braid A_{π_1}, A_{π_2} を図 4.3 に示す.



A_{π_1}　　A_{π_2}

図 4.3: A_{π_1}, A_{π_2}

これらは $\{\sigma_i\}$ の word を使って表示できる (例えば $A_{\pi_1} = \sigma_1\sigma_2\sigma_3\sigma_1$, $A_{\pi_2} = \sigma_1\sigma_3\sigma_2\sigma_3\sigma_1$ というように具体的にかける)．しかし補題 4.6 は，与えられた positive permutation braid を表示するためには実は $\{\sigma_i\}$ の word を知る必要はなく，その braid が導く置換さえわかれば十分であることを示している．

以下では，B_n の元を表す geometric braid に対して補題 4.6 の証明の中で述べたのと同様にしてひも i $(= 1, 2, \ldots, n)$ を定めることにする．

命題 4.7 S_n^+ の元 A_π に対して次は同値である．

(1) $i \in S(A_\pi)$

(2) A_π に対応する geometric braid の中で，ひも i とひも $i+1$ は交差する．

(3) $\pi(i+1) < \pi(i)$

証明 (3) $\Rightarrow$ (2) は明らか．(2) $\Rightarrow$ (3) を示す．$A_\pi \in S_n^+$ より，ひも i とひも $i+1$ はちょうど 1 回交差する．よって $\pi(i+1) < \pi(i)$ を得る．(1) $\Rightarrow$ (2) を示す．$i \in S(A_\pi)$ であるから，ある $A' \geq e$ が存在して $A_\pi = \sigma_i A'$ とかける．よって，ひも i とひも $i+1$ は交差する．(2) $\Rightarrow$ (1) を示す．ひも i とひも $i+1$ がつくる交差は，その他のすべての交差を positive に保ったまま A_π の一番上まで持ち上げることができる (図 4.4)．よって A_π は σ_i から始まる positive word でかくことができる．□

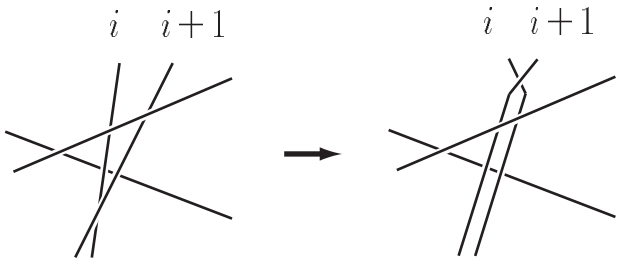


図 4.4: σ_i と他の交差の位置関係

例 前の例の A_{π_1}, A_{π_2} とそれぞれの reverse に命題 4.7 を適用することで，次のことがわかる．

$$\begin{aligned} S(A_{\pi_1}) &= \{1,2\} \\ F(A_{\pi_1}) &= \{1,3\} \\ S(A_{\pi_2}) &= F(A_{\pi_2}) = \{1,3\} \end{aligned}$$

命題 4.8 S_n^+ の元 A に対して次が成り立つ．

$$i \notin S(A) \Leftrightarrow \sigma_i A \in S_n^+ \tag{4.6}$$

証明 $[\Rightarrow]$ $i \notin S(A)$ であるから，A の中でひも i とひも $i+1$ は交差しない (命題 4.7 (2) $\Rightarrow$ (1))．よって $\sigma_i A$ の中でひも i とひも $i+1$ はちょうど 1 回交差する．一方，$\sigma_i A$ の中でその他の任意の 2 本のひもは高々1 回しか交差しない．ゆえに $\sigma_i A \in S_n^+$ がわかる．
$[\Leftarrow]$ $\sigma_i A \in S_n^+$ であるから，$\sigma_i A$ の中で任意の 2 本のひもは高々1 回しか交差しない．一方，σ_i でひも i とひも $i+1$ は交差している．よって A の中でひも i とひも $i+1$ は交差しない．ゆえに $i \notin S(A)$ がわかる (命題 4.7 (1) $\Rightarrow$ (2))． □

注意 4.9 命題 4.8 の証明と同様の議論により次が示せる．

$$i, j \notin S(A) \Leftrightarrow (\sigma_i * \sigma_j)A \in S_n^+ \tag{4.7}$$

さらに $\mathrm{rev}(A)$ に命題 4.8 を適用することで finishing set に対しても同様の結果が得られる．

$$i \notin F(A) \Leftrightarrow A\sigma_i \in S_n^+ \tag{4.8}$$
$$i, j \notin F(A) \Leftrightarrow A(\sigma_i * \sigma_j) \in S_n^+ \tag{4.9}$$

定理 4.10 $[0,1] = S_n^+$ が成り立つ．

証明 $[\subset]$ $A \in [0,1]$，すなわち $A \leq \Delta$ が成り立つとする．このとき命題 3.6 より，ある $B \geq e$ が存在して $\Delta = AB$ とかける．いま注意 4.4 より $\Delta \in S_n^+$ であるから，注意 4.5 において $P = \Delta$ とみなすと $A \in S_n^+$ が成り立つ．

[$\supset$] $A = A_\pi \in S_n^+$ とする．δ を Δ に対応する置換とし，ρ を $\pi\rho = \delta$ となるような置換とする．このとき $A_\pi A_\rho \in S_n^+$ となる．実際 $A_\pi, A_\rho \in S_n^+$ であるから，$A_\pi A_\rho$ の中の任意の 2 本のひもは高々2 回しか交差しない．またその交差はすべて positive である．一方 $\pi\rho = \delta$ より，$A_\pi A_\rho$ の中の任意の 2 本のひもは奇数回交差する．ゆえに $A_\pi A_\rho$ の中の任意の 2 本のひもはちょうど 1 回交差して，すべて positive，すなわち $A_\pi A_\rho \in S_n^+$ がわかる．いま $\pi\rho = \delta$ であるから $A_\pi A_\rho$ が導く置換は A_δ $(= \Delta)$ が導く置換に等しい．よって補題 4.6 より $A_\pi A_\rho = A_\delta$ $(= \Delta)$ がわかる．ゆえに $A_\pi \leq \Delta$ を得る．また明らかに $e \leq A_\pi$ であるから，$A_\pi \in [0, 1]$ が成り立つ． □

命題 4.7 と (4.8) より，Δ に対して次が成り立つことがわかる．

$$S(\Delta) = F(\Delta) = \{1, 2, \ldots, n-1\} \tag{4.10}$$

補題 4.11 S_n^+ の元 A に対し，$S(A) = \{1, 2, \ldots, n-1\}$ のとき $A = \Delta$ が成り立つ．

証明 π を A が導く置換とする．このとき任意の i $(= 1, 2, \ldots, n-1)$ に対して $i \in S(A)$ であるから，命題 4.7 より $\pi(i+1) < \pi(i)$ が成り立つ．よって，$i < j$ となる任意のひも i, j に対して $\pi(j) < \pi(i)$ が成り立つ．特に，任意の $i > 1$ に対して $\pi(i) < \pi(1)$ が成り立つ．このことより $\pi(1) = n$ がわかる．次に $\pi(2)$ について考える．任意の $i > 2$ に対して $\pi(i) < \pi(2)$ が成り立つ．これと上の事実 $(\pi(1) = n)$ より，$\pi(2) = n-1$ となることがわかる．同様にして $\pi(3) = n-2, \ldots, \pi(n) = 1$ がわかる．以上より，A が導く置換は Δ が導く置換に等しい．よって補題 4.6 より $A = \Delta$ を得る． □

次に定理 4.10 と S_n^+ の性質を用いて命題 4.3 を証明する．そのために用語を 1 つ準備しておく．

定義 S_n^+ の元 A, A_1 に対し，ある $Q \geq e$ で $A_1 = AQ$ となるものが存在するとき，A は A_1 の **subfactor** であるという．

命題 4.3 の 証明 [l.w.f. $P = A_1 P_1$ $(A_1 \in S_n^+)$ の存在] P の分解で $P = AB$ $(A \in S_n^+)$ の形をしたものについて考える．すべてのこのような分解の中で $\mathrm{wt}(A)$ が最大となるものを 1 つ固定し，それを改めて $P = AB$ とかくことにする．このとき $S(B) \subset F(A)$ が成り立つ．

実際 $S(B) \not\subset F(A)$ とすると，ある $i \in S(B)$ が存在して $i \notin F(A)$ が成り立つ．ここで $i \in S(B)$ より，ある $B' \geq e$ が存在して $B = \sigma_i B'$ とかける．また $i \notin F(A)$ であるから (4.8) より $A\sigma_i \in S_n^+$ がわかる．ゆえに $A' = A\sigma_i$ とおくと $P = A'B'$ とかける．このとき $A' \in S_n^+$, $\mathrm{wt}(A') = \mathrm{wt}(A) + 1$ となり，$\mathrm{wt}(A)$ の

最大性に矛盾する．以下ではこのようにして得られた $\mathrm{wt}(A)$ が最大となる分解を $P = A_1P_1$ とかくことにする．
[条件 $(*)$ について] 次にこの分解 $P = A_1P_1$ が条件 $(*)$ を満たすことを背理法で示す．P のある分解 $P = AB$ $(A \in S_n^+)$ で，A は A_1 の subfactor でないようなものが存在すると仮定する．このとき次のことが成り立つ．

> P のある分解 $P = C\sigma_iB'$ $(C\sigma_i \in S_n^+)$ で，C $(\in S_n^+)$ は A_1 の subfactor であるが $C\sigma_i$ は A_1 の subfactor でないようなものが存在する $(**)$.

実際に，$i_1 \in F(A)$ のとき $A = C_1\sigma_{i_1}$ $(C_1 \in S_n^+)$ とおいて C_1 が A_1 の subfactor かどうかを調べる．もし C_1 が A_1 の subfactor ならば $C = C_1,\ \sigma_i = \sigma_{i_1},\ B' = B$ とすればよい．そうでないなら，$C_1 = C_2\sigma_{i_2}$ $(C_2 \in S_n^+,\ i_2 \in F(C_1))$ とおいて C_2 が A_1 の subfactor かどうかを調べる．もし C_2 が A_1 の subfactor ならば $C = C_2,\ \sigma_i = \sigma_{i_2},\ B' = \sigma_{i_1}B$ とすればよい．そうでないなら，$C_2 = C_3\sigma_{i_3}$ $(C_3 \in S_n^+,\ i_3 \in F(C_2))$ とおいて C_3 が A_1 の subfactor かどうかを調べる．この操作を繰り返すと，最終的に $(**)$ を満たすような分解

$$P = C\sigma_iB' \tag{4.11}$$

が見つかる．

次にこのような分解の中で $\mathrm{wt}(C)$ が最大となるものを 1 つ固定する．C は A_1 の subfactor であるから，ある $Q \geq e$ が存在して

$$A_1 = CQ \tag{4.12}$$

とかける．このとき $Q \neq e$ である．実際 $Q = e$ とすると $A_1 = C$ となる．一方 $P = C\sigma_iB' = A_1\sigma_iB'$ $(A_1\sigma_i \in S_n^+)$ とかけるが，これは $\mathrm{wt}(A_1)$ の最大性に矛盾する．よって $j \in S(Q)$ がとれて，(4.12) より $C\sigma_j \leq A_1$ がわかる．ゆえに，ある $D \geq e$ が存在して

$$A_1 = C\sigma_jD \tag{4.13}$$

とかける．ここで $B'' = DP_1$ とおくと，$P = A_1P_1$ より

$$P = C\sigma_jB'' \tag{4.14}$$

とかける．このとき (4.11) と (4.14) より $\sigma_iB' = \sigma_jB''$ がわかるが，この元を B とかくことにする．$B = \sigma_iB' = \sigma_jB''$ に対して補題 4.1 を適用すると，ある $B''' \geq e$ が存在して $B = (\sigma_i * \sigma_j)B'''$ とかける．よって $P = C(\sigma_i * \sigma_j)B'''$ を得る．一方 $C\sigma_i \in S_n^+$ であるから，(4.8) より $i \notin F(C)$ がわかる．また $A_1 \in S_n^+$ であるから，(4.13) に注意 4.5 を適用して $C\sigma_j \in S_n^+$ を得る．よって (4.8) より $j \notin F(C)$ がわかる．このとき (4.9) より，$C(\sigma_i * \sigma_j) \in S_n^+$ となる．以下では次の 3 つの Case に分けて考える．
Case 1: $i = j$ のとき

$P = C\sigma_j B'''$ を考える．$(**)$ より $C\sigma_i$ は A_1 の subfactor でないから，$C\sigma_j$ $(= C\sigma_i)$ も subfactor ではない．一方，(4.13) より $C\sigma_j$ は A_1 の subfactor である．よって $i = j$ に矛盾する．

Case 2: $|i - j| > 1$ のとき

$P = C\sigma_j\sigma_i B'''$ を考える．$(**)$ より $C\sigma_i$ は A_1 の subfactor でないから，$C\sigma_j\sigma_i$ $(= C\sigma_i\sigma_j)$ も subfactor ではない．また (4.13) より $C\sigma_j$ は A_1 の subfactor である．よって，$C\sigma_j$ は $(**)$ を満たしていることがわかる．一方，$\mathrm{wt}(C\sigma_j) = \mathrm{wt}(C) + 1$ となり，$\mathrm{wt}(C)$ の最大性に矛盾する．

Case 3: $|i - j| = 1$ のとき

$P = C\sigma_j\sigma_i\sigma_j B'''$ を考える．$(**)$ より $C\sigma_i$ は A_1 の subfactor でないから，$C\sigma_j\sigma_i\sigma_j$ $(= C\sigma_i\sigma_j\sigma_i)$ も subfactor ではない．このとき，さらに 2 つの場合に分けて考える．(i) $C\sigma_j\sigma_i$ が A_1 の subfactor のときには，$C\sigma_j\sigma_i$ は $(**)$ を満たしていることがわかる．一方，$\mathrm{wt}(C\sigma_j\sigma_i) = \mathrm{wt}(C) + 2$ となり，$\mathrm{wt}(C)$ の最大性に矛盾する．(ii) そうでない ($C\sigma_j\sigma_i$ が A_1 の subfactor でない) とする．いま，(4.13) より $C\sigma_j$ は A_1 の subfactor である．ゆえに $C\sigma_j$ は $(**)$ を満たしていることがわかる．一方，$\mathrm{wt}(C\sigma_j) = \mathrm{wt}(C) + 1$ となり，$\mathrm{wt}(C)$ の最大性に矛盾する．

以上で $(*)$ が示せた．
[一意性] 最後に一意性を背理法で示す．いま $P = AB$ を別の l.w.f. とする．このとき $(*)$ より，ある $Q \geq e$ が存在して

$$A_1 = AQ \tag{4.15}$$

とかける．ここで $Q = e$ ならば $A_1 = A$ を得る．よって $Q \neq e$ と仮定して矛盾を導く．このとき $i \in S(Q)$ がとれて，(4.15) より $A\sigma_i \leq A_1 \in S_n^+$ がわかる．よって (4.8) より $i \notin F(A)$ を得る．一方，$(AB =)$ $P = A_1P_1 = AQP_1$ であるから，$B = QP_1$ がわかる．いま $i \in S(Q)$ だから $i \in S(B)$ を得る．また $i \notin F(A)$ だから $S(B) \not\subset F(A)$，すなわち $P = AB$ は left-weighted ではない． □

系 4.12 $P \geq e$ とする．$P = A_1P_1$ $(A_1 \in S_n^+)$ を命題 4.3 で得られた P の l.w.f. とする．このとき $S(A_1) = S(P)$ が成り立つ．

証明 $[\subset]$ $i \in S(A_1)$ とすると，ある $A' \geq e$ が存在して $A_1 = \sigma_i A'$ とかける．よって $P = A_1P_1 = \sigma_i A'P_1$ となり $i \in S(P)$ がわかる．
$[\supset]$ $i \in S(P)$ とすると，ある $B \geq e$ が存在して $P = \sigma_i B$ とかける．このとき命題 4.3 より，ある $Q \geq e$ が存在して $A_1 = \sigma_i Q$ とかける．よって $i \in S(A_1)$ がわかる． □

4.2 Left-canonical form

ここでは 4.1 節で導入した l.w.f. を用いて，braid を $[0,1]$ $(= S_n^+)$ の元の積で表すことにする．

定理 4.13 $P \geq e$ とする．このとき P に対し，次を満たすような分解 $P = A_1A_2\cdots A_k$ がただ 1 つ存在する．

$$A_i \in [0,1] \quad (i = 1,2,\ldots,k) \tag{4.16}$$

$$A_k \neq e \tag{4.17}$$

$$S(A_{j+1}) \subset F(A_j) \quad (j = 1,2,\ldots,k-1) \tag{4.18}$$

この分解を **left-canonical form** (以下では l.c.f. とかく) という．

証明 $P = A_1P_1$ $(A_1 \in [0,1])$ を命題 4.3 で得られた P の l.w.f. とする．このとき $S(P_1) \subset F(A_1)$ である．また $P_1 = A_2P_2$ $(A_2 \in [0,1])$ を P_1 に命題 4.3 を適用して得られる P_1 の l.w.f. とする．このとき $S(P_2) \subset F(A_2)$ である．さらに分解を続けると P の $[0,1]$ の元による分解 $P = A_1A_2\cdots A_k$ $(A_k \neq e)$ が得られる．このとき $P_{j-1} = A_jP_j$ は P_{j-1} の l.w.f. であるから $S(P_j) \subset F(A_j)$ がわかる．一方 $P_j = A_{j+1}P_{j+1}$ は P_j の l.w.f. であるから，系 4.12 より $S(A_{j+1}) = S(P_j)$ である．よって $S(A_{j+1}) \subset F(A_j)$ を得る． □

命題 4.14 P の l.c.f. を $P = A_1A_2\cdots A_k$ とする．このとき $\inf P$ に対して次が成り立つ．

$$\inf P \;=\; \max\{i : A_i = \Delta\} \tag{4.19}$$

命題 4.14 の証明を与える前に，まず P の l.c.f. $P = A_1A_2\cdots A_k$ に対して次の 2 つが成り立つことに注意する．

注意 4.15 $P \geq \Delta \Leftrightarrow A_1 = \Delta$ が成り立つ．

実際これは，次のようにして証明できる．
[⇒] $P \geq \Delta$ とする．このとき命題3.7より，ある $Q \geq e$ が存在して $P = \Delta Q$ とかける．いま $F(\Delta) = \{1,2,\ldots,n-1\}$ (4.9)であるから，$S(Q) \subset F(\Delta)$ は明らか．よって $P = \Delta Q$ はl.w.f.である．したがって，系4.12より $S(P) = S(\Delta) = \{1,2,\ldots,n-1\}$ がわかる．一方，$P = A_1(A_2\cdots A_k)$ は命題 4.3 で得られた P の l.w.f. であるから，系 4.12 より $S(A_1) = S(P)$ が成り立つ．ゆえに $S(A_1) = \{1,2,\ldots,n-1\}$ がわかる．よって補題 4.11 より $A_1 = \Delta$ を得る．
[⇐] $A_1 = \Delta$ とすると $P = \Delta A_2A_3\cdots A_k$ とかける．よって $P \geq \Delta$ を得る．

注意 4.16 任意の $j < i$ に対して，$A_i = \Delta \Rightarrow A_j = \Delta$ が成り立つ．

実際 $j = i-1$，すなわち $P = A_1A_2\cdots A_jA_i\cdots A_k$ とする．このとき，定理 4.13 より $S(A_i) \subset F(A_j)$ がわかる．一方 $A_i = \Delta$ であるから，(4.10) より $S(A_i) = \{1, 2, \ldots, n-1\}$ を得る．よって $F(A_j) = S(A_i) = \{1, 2, \ldots, n-1\}$ がわかるから，補題 4.11 より $A_j = A_{i-1} = \Delta$ を得る．次に $A_{i-1} = \Delta$ を用いて同様に議論すると $A_{i-2} = \Delta$ が示される．これを繰り返して，任意の $j < i$ に対して $A_j = \Delta$ を得る．

命題 4.14 の証明 $[\leq]$ $r = \inf P$ とする．(3.13) より $\Delta^r \leq P$ であるから，ある $Q \geq e$ が存在して $P = \Delta^r Q$ とかける．よって $P \geq \Delta$ となり，注意 4.15 より $A_1 = \Delta$ がわかる．ゆえに P の l.w.f. は $P = \Delta P_1$ とかける．いま $P = \Delta^r Q$ であるから $P_1 = \Delta^{r-1}Q$，すなわち $P_1 \geq \Delta$ を得る．また $P_1 = A_2(A_3\cdots A_k)$ は命題 4.3 で得られた P_1 の l.w.f. になっている．ゆえに注意 4.15 より $A_2 = \Delta$ がわかる．これを繰り返して $A_1 = A_2 = \cdots = A_r = \Delta$ を得る．よって $r \leq \max\{i : A_i = \Delta\}$ がわかる．
$[\geq]$ $s = \max\{i : A_i = \Delta\}$ とする．このとき，注意 4.16 より $A_1 = A_2 = \cdots = A_s = \Delta$ がわかる．よって $P = \Delta^s A_{s+1}\cdots A_k$ を得る．いま $A_{s+1}\cdots A_k \geq e$ であるから，$s \leq \max\{r : \Delta^r \leq P\} = \inf P$ を得る． □

定理 4.18 で P の l.c.f. から $\sup P$ の値も簡単に求められることを示す．そのためにまず次のことを示す．

命題 4.17 $P \geq e$ とする．$P = A_1P_1$ $(A \in [0,1])$ を命題 4.3 で得られた P の l.w.f. とする．このとき次が成り立つ．

$$B \geq e,\ BP \geq \Delta \ \Rightarrow\ BA_1 \geq \Delta \tag{4.20}$$

証明 $\mathrm{wt}(B)$ に関する帰納法で示す．
(1) $\mathrm{wt}(B) = 0$ とする．このとき

$$B = e,\ P \geq \Delta \ \Rightarrow\ A_1 \geq \Delta \tag{4.21}$$

が成り立つことを示す．$P \geq \Delta$ とすると，注意 4.15 より $A_1 = \Delta$ を得る．よって (4.21) は成り立つ．
(2) $\mathrm{wt}(B) > 0$ とする．$\mathrm{wt}(B) < k$ となる B に対して (4.20) が成り立つと仮定する．いま $\mathrm{wt}(B) = k$ とする．このとき，$i \in F(B)$ がとれて $B = B'\sigma_i$ $(B' \geq e)$ とかける．また $P' = \sigma_i P$ とおき，$P' = A_1'P_1'$ $(A_1' \in [0,1])$ を P' の l.w.f. とする．このとき $BP = B'\sigma_i P = B'P' = B'A_1'P_1'$ が成り立つ．
いま $BP \geq \Delta$ とする．このとき $\mathrm{wt}(B') = k-1$ であるから，帰納法の仮定より $B = B',\ P = P'$ とみなすと

$$B'A_1' \ \geq\ \Delta \tag{4.22}$$

が成り立つ．また $i \in S(P')$ であるから，系 4.12 より $i \in S(A_1')$ がわかる．よって，ある $A_1'' \in [0,1]$ が存在して $A_1' = \sigma_i A_1''$ とかける．このとき $\sigma_i P = P' = A_1' P_1' = \sigma_i A_1'' P_1'$ であるから，$P = A_1'' P_1'$ を得る．これに命題 4.3 を適用すると，ある $Q \geq e$ が存在して $A_1 = A_1'' Q$ とかける．また $BA_1'' = B'\sigma_i A_1'' = B' A_1'$ であるから，(4.22) より $BA_1'' \geq \Delta$ がわかる．一方，$BA_1 = BA_1'' Q$ であるから，$BA_1 \geq \Delta$ が成り立つ． □

定理 4.18 $P \geq e$ とする．また P の l.c.f. を $P = A_1 A_2 \cdots A_k$ とする．このとき $\sup P$ に対して次が成り立つ．

$$\sup P = k \tag{4.23}$$

証明 $s = \sup P$ とおく．
$[s \leq k]$ $P = A_1 A_2 \cdots A_k$ は P の l.c.f. であるから，$A_i \in [0,1]$ $(i = 1, 2, \ldots, k)$ である．このとき命題 3.8 より $P \in [0, k]$，よって $P \leq \Delta^k$ がわかる．ゆえに $s \leq k$ を得る．
$[s \geq k]$ k に関する帰納法でを示す．
(1) $s = 0$ のとき:

> $P \leq \Delta^0 = e$ と $P \geq e$ より $P = e$ となり，これは P の l.c.f. である．よって $k = 0$，ゆえに $s = k$ が成り立つ．

(2) $s \geq 1$ のとき:

> $P \leq \Delta^s$ であるから，命題 3.6 より，ある $B \geq e$ が存在して $BP = \Delta^s$ とかける．ここで命題 4.17 を適用すると $BA_1 \geq \Delta$ がわかるから，命題 3.7 より，ある $B_1 \geq e$ が存在して $BA_1 = \Delta B_1$ とかける．このとき $P_1 = A_2 \cdots A_k$ とおくと，$(\Delta^s =)\ BP = BA_1 P_1 = \Delta B_1 P_1$ となる．よって $B_1 P_1 = \Delta^{s-1}$，ゆえに $P_1 \leq \Delta^{s-1}$ となり $\sup P_1 \leq s - 1$ を得る．一方，$P_1 = A_2 \cdots A_k$ は P_1 の l.c.f. であるから，帰納法の仮定より $\sup P_1 \geq k - 1$ が成り立つ．よって $s - 1 \geq k - 1$，すなわち $k \leq s$ を得る．

以上より，定理 4.18 が成り立つことがわかる． □

一般に $P \geq \Delta^r$ のとき，$P' = \Delta^{-r} P \geq e$ とおくと

$$\sup P = r + \sup P' \tag{4.24}$$

が成り立つ．実際，$s = \sup P$ とおくと $P \leq \Delta^s$ がわかる．またある $P' \geq e$ が存在して $P = \Delta^r P'$ とかけるから，$\Delta^r P' \leq \Delta^s$ がわかる．このとき，ある $Q \geq e$ が存在して $\Delta^s = \Delta^r P' Q$ とかけるから，$\Delta^{s-r} = P'Q$ が成り立つ．よって $P' \leq \Delta^{s-r}$，すなわち $\sup P' \leq s - r$ がわかる．ゆえに $\sup P' + r \leq \sup P$ を得る．$\sup P \leq r + \sup P'$ も同様にして示せる．

また同様の議論により

$$\inf P = r + \inf P' \tag{4.25}$$

が成り立つことも示せる．

注意 4.19 $P \geq e$ とする．また $\mathrm{rev}(P)$ の l.c.f. を $\mathrm{rev}(P) = A'_1 A'_2 \cdots A'_k$ とする．このとき $A_i = \mathrm{rev}(A'_{k-i+1})$ $(i = 1, 2, \ldots, k)$ とすると $P = A_1 A_2 \cdots A_k$ が成り立つ．またこのとき

$$A_i \in [0, 1] \quad (i = 1, 2, \ldots, k) \tag{4.26}$$

$$A_k \neq e \tag{4.27}$$

$$S(A_{j+1}) \supset F(A_j) \quad (j = 1, 2, \ldots, k-1) \tag{4.28}$$

が成り立つ．Braid の l.c.f. は一意的だから (定理 4.13)，このような分解も一意的であることがわかる．この分解を P の **right-canonical form** (以下では r.c.f. とかく) という．

5 The word algorithm

ここでは次の問題について考える.

問題 (**word problem**):
$\{\sigma_i\}$ の 2 つの words P, Q が与えられたとき，これらが B_n の同じ元を表しているかどうか判定せよ.

5.1 Algorithm

この問題は 4.2 節で紹介した l.c.f. を用いることにより，次のように解決することができる.

いま P と Q の l.c.f. がそれぞれ次のように求まったとする.

$$P = \Delta^r A_1 A_2 \cdots A_m \tag{5.1}$$
$$Q = \Delta^s C_1 C_2 \cdots C_n \tag{5.2}$$

このとき，もし P と Q が B_n の同じ元を表しているならば，l.c.f. の一意性 (定理 4.13) より,

> $r = s,\ m = n$ で A_i と C_i $(i = 1, 2, \ldots, m)$ は同じ置換を導く positive permutation braid である

ことがわかる．逆にこの条件を満たすならば，補題 4.6 より P と Q は同じ B_n の元を表していることがわかる．よって，以下ではこの r と $A_1, A_2, \ldots, A_m$ の求め方について述べる.

Algorithm P を $\{\sigma_i\}$ の word で与えられた B_n の元とする.

Step 1: ある $r \in \mathbb{Z}$ と $P' \geq e$ で $P = \Delta^r P'$ となるものを求める.

このような r と P' を見つけるために，P の中に含まれる σ_i^{-1} を消すことを考える．いま (4.10) より，任意の i $(= 1, 2, \ldots, n-1)$ に対して $i \in F(\Delta)$ がわかる．よって，ある $\sigma_i^* \in [0, 1]$ が存在して $\Delta = \sigma_i^* \sigma_i$ とかけるから，$\sigma_i^{-1} = \Delta^{-1} \sigma_i^*$ を得る．これを P の中に含まれる各 σ_i^{-1} に代入してやる．このようにして word の中に現れた Δ^{-1} を (3.8) を用いて左に集めてやれば，求める $P = \Delta^r P'$ が得られる.

例 $\sigma_2^{-1} \in B_3$ とする．このとき $\Delta = \sigma_1\sigma_2\sigma_1$ $(= \sigma_2\sigma_1\sigma_2)$ であるから，$\Delta^{-1} = \sigma_2^{-1}\sigma_1^{-1}\sigma_2^{-1}$ を得る．よって $\sigma_2^{-1} = \Delta^{-1}\sigma_2\sigma_1$ がわかる．これを利用すると，$\sigma_1\sigma_2^{-1}$

は次のようにして Δ のベキと positive braid の積に表すことができる．

$$\sigma_1\sigma_2^{-1} = \sigma_1\Delta^{-1}\sigma_2\sigma_1 = \Delta^{-1}\sigma_2^2\sigma_1$$

次に Step 1 で求めた P' を $P' = B_1B_2\cdots B_k$ $(B_i \in [0,1])$ と表してやる．実際のところ，各 σ_i は $[0,1]$ の元であるから，P' の中の σ_i を左から順に $B_1, B_2, \ldots$ と定めてやればこのような分解が存在することがわかる．ただし word を左から順に読んでいき，$[0,1]$ の元であるような一番長い subword をとって，それを B_1 としてやれば，より効率的に表すことができる．

Step 2: 命題 4.7 を用いて，P' の各 B_i $(i = 1, 2, \ldots, k)$ に対して $S(B_i)$ と $F(B_i)$ を求める．そして各 i $(= 1, 2, \ldots, k-1)$ に対して，$S(B_{i+1}) \subset F(B_i)$ かどうか調べる．

もしすべての i に対して $S(B_{i+1}) \subset F(B_i)$ が成り立つなら，定理 4.13 より $P' = B_1B_2\cdots B_k$ は P' の l.c.f. である．

いまある i に対して $S(B_{i+1}) \not\subset F(B_i)$ とする．ここで i はこのような条件を満たすものの中で最小とする．このとき，ある $j \in S(B_{i+1})$ で $j \notin F(B_i)$ となるものが存在する．ここで $C_i = B_i\sigma_j$, $C_{i+1} = \sigma_j^{-1}B_{i+1}$ とおくと $C_i, C_{i+1} \in [0,1]$ となり，$P' = B_1\cdots B_{i-1}C_iC_{i+1}B_{i+2}\cdots B_k$ とかける．このとき $C_{i+1} = e$，または $C_i = \Delta$ となる可能性がある．そこで e が現れたときにはそれを取り除き，Δ が現れたときには (3.7) を用いて Δ^r に組み込んでやる．こうして得られた新しい P' の分解に対して，Step 2 の先頭に戻って同様の考察を繰り返す．

注意 5.1 上の操作は有限回で停止する．

実際これは，次のようにして証明できる．B_i を C_i に置き換えたとき，その前後の weight の列

$$\begin{aligned} B &= (\mathrm{wt}(B_1), \ldots, \mathrm{wt}(B_k)) \\ B' &= (\mathrm{wt}(B_1), \ldots, \mathrm{wt}(C_i), \mathrm{wt}(C_{i+1}), \ldots, \mathrm{wt}(B_k)) \end{aligned}$$

を辞書式順序* で比較すると，必ず B' の方が大きくなっている．また total weight $\mathrm{wt}(B)$ $(= \mathrm{wt}(B_1) + \cdots + \mathrm{wt}(B_k))$ は変化していない．固定された total weight をもつ列は有限個しかないから，この操作も有限回で停止する．以上により，P の l.c.f. を求める algorithm が得られる．

---

*$A = (a_1, a_2, \ldots, a_k)$, $B = (b_1, b_2, \ldots, b_k)$ とする． このとき 2 つの列 A, B に対して，ある $i \geq 0$ で

$$a_j = b_j \ (\forall j > i) \quad \text{かつ} \quad a_i > b_i$$

となるものが存在するとき，A は B より大きいと定める．この順序を**辞書式順序**といい，$A > B$ で表す．

5.2 Implementation

5.1 節の algorithm をコンピュータ等で実行するにあたり，与えられた permutation braid B_i に対して $S(B_i)$ と $F(B_i)$ を求める部分が問題となる．ここでは [8] で導入された **fractorical coodinate method** を用いて $S(B_i)$ と $F(B_i)$ を求める方法について紹介する．

まず S_n から $\{1, 2, \ldots, n!\}$ への対応 ξ を次のように定める．

$$\xi : t \in S_n \ \mapsto \ \xi(t) = 1 + g_1 1! + g_2 2! + \cdots + g_{n-1}(n-1)! \tag{5.3}$$

ただし g_i $(i = 1, 2, \ldots, n-1)$ は置換 t を導く permutation braid A_t のひも $i+1$ がひも $1, 2, \ldots, i$ の union とつくる交点の個数を表す．

例 S_3 の各元を ξ で写したときの値を求める．
$t_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ に対して，A_{t_1} は図 5.1 のとおりである．これより

$$\xi(t_1) = 1 + 0 \cdot 1! + 0 \cdot 2! = 1$$

がわかる．

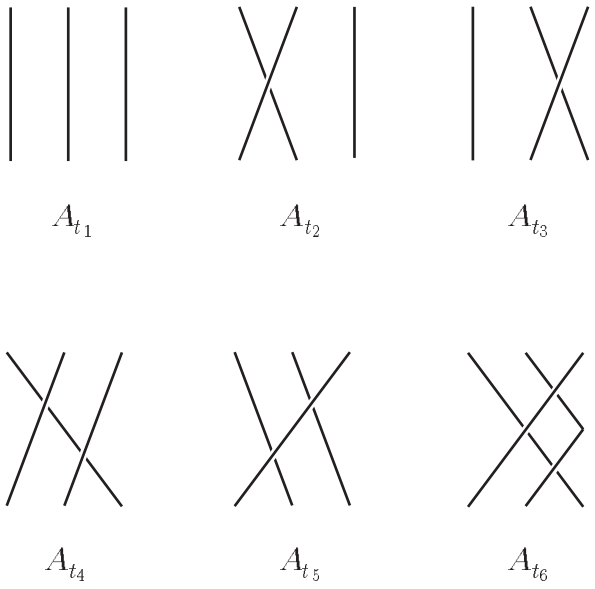


図 5.1: A_t

以下同様にして次の結果を得る．

$$t_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{のとき} \qquad \xi(t_2) = 1 + 1 \cdot 1! + 0 \cdot 2! = 2$$

$$t_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \text{のとき} \qquad \xi(t_3) = 1 + 0 \cdot 1! + 1 \cdot 2! = 3$$

$$t_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \text{のとき} \qquad \xi(t_4) = 1 + 1 \cdot 1! + 1 \cdot 2! = 4$$

$$t_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{のとき} \qquad \xi(t_5) = 1 + 0 \cdot 1! + 2 \cdot 2! = 5$$

$$t_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{のとき} \qquad \xi(t_6) = 1 + 1 \cdot 1! + 2 \cdot 2! = 6$$

実は任意の n に対して $\xi : S_n \to \{1, 2, \ldots, n-1\}$ が一対一対応になっていることが知られている．さらに π_i で互換 $(i, i+1) \in S_n$ を表すことにすると，$t \in S_n$ に対して次が成り立つことが知られている．

$$\sigma_i A_t \in S_n^+ \ \Leftrightarrow \ \xi(\pi_i t) > \xi(t) \tag{5.4}$$

このことを用いて，与えられた permutation braid の starting set を次のような方法で求めることができる．

各 i $(= 1, 2, \ldots, n!)$ に対して，fractrical coodinate method で i に対応する S_n の元を t_i で表すことにする．まず (i, j) 成分が $\xi(\pi_j t_i)$ となる縦 $n!$，横 $n-1$ の表をつくる．この表を用いれば与えられた t が (5.4) の右の条件を満たすかどうか，すなわち $\sigma_i A_\pi$ が S_n^+ の元であるかどうかを高速に判定できる．命題 4.8 より $i \in S(A_\pi)$ となる必要十分条件は $\sigma_i A_\pi \notin S_n^+$ となることであるから，結局 $S(A_\pi)$ を高速に求めることができる．また reverse を利用することで $F(A_\pi)$ も高速に求めることができる．

5.3 Geometric example

次に幾何的な例を示しておく．Positive braid が幾何的に与えられたとき，視覚的に変形し，その l.c.f. を簡単に求めることができる．ここではその方法について紹介する．

例えば $P = \sigma_1\sigma_3\sigma_2^2\sigma_3\sigma_1\sigma_3\sigma_2\sigma_3\sigma_2$ が与えられたとき，この braid は図 5.2(左端) のように描かれる．まずこの braid を permutation braid の積に分解する．これは次のようにして成される．

まず必要ならば，braid を少しだけ動かして交点はすべて異なる高さにあるようにしておく．そしてその交点に対し，高さに従って上から順番を付けてやる．このとき隣り合った交点の間の高さを決めてその高さの水平線を引いておく．次に一番上の水平線から順に取り除いてやり，braid の上面と水平線に挟まれた領域を広げていくことを考える．このとき領域内のある 2 本のひもが，すでに 1 回交差していて，さらに 2 回目に交差しようとする直前の水平線で braid を区切ってやる．さらにいま入れた区切りより下にある残りの braid についても同様に見ていき，braid に区切りを入れてやる．こうして P は permutation braid $B_1 = \sigma_1\sigma_3\sigma_2$, $B_2 = \sigma_2\sigma_3\sigma_1$, $B_3 = \sigma_3\sigma_2\sigma_3$, $B_4 = \sigma_2$ の積に分解できる (図 5.2 左端).

次にこの permutation braid の連続した組 $(B_i\ B_{i+1})$ に注目する．B_{i+1} の中の隣り合った点から出発する ひもがつくる交点で，その 2 本のひもが B_i の中で交差していないようなものがあればその交点を B_i の中まで持ち上げてやる．この操作を上のように変形できる交点が見つからなくなるまで続ける．こうして最終的に得られる分解 $P = (\sigma_1\sigma_3\sigma_2\sigma_1)(\sigma_2\sigma_1\sigma_3\sigma_2)(\sigma_2)(\sigma_2)$ は P の l.c.f. になっている (図 5.2 右端).

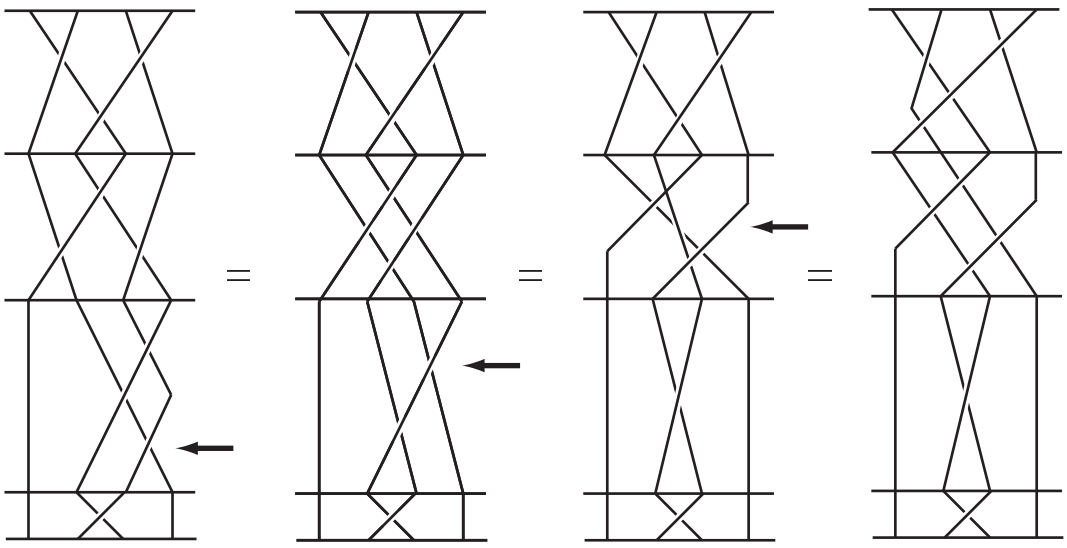


図 5.2: P の変形

注意 5.2 ここで原論文 [5] では上の下線部の文章が含まれていなかった．この条件がない場合，上の例では図 5.3 に示すようにもう 1 度交点を持ち上げることができる．しかし，このとき一番上の braid に σ_3^{-1} ができ，これは permutation braid ではない．

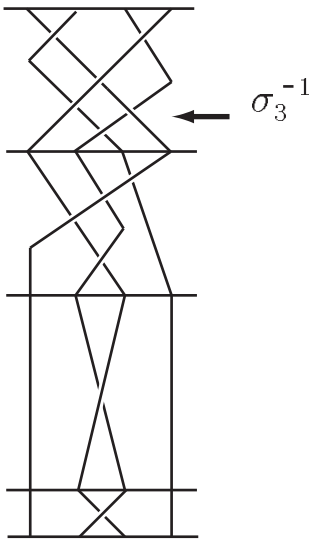


図 5.3: この持ち上げ方は不適

6 The conjugacy algorithm

ここでは次の問題について考える.

問題 (**conjugacy problem**):
$\{\sigma_i\}$ の 2 つの words P, Q が与えられたとき，これらが B_n の conjugate な元を表しているか，すなわち次を満たすかどうか判定せよ.

$$\text{ある } A \in B_n \text{ で } Q = A^{-1}PA \text{ となるものが存在する.}$$

6.1 Preliminaries

まずこの問題を考えるにあたり，$A \geq e$ として考えればよいことを注意しておく.

注意 6.1 P と Q は conjugate とする．このとき，ある $A \geq e$ で $Q = A^{-1}PA$ となるものが存在する.

実際これは，次のようにして証明できる．P, Q は conjugate であるから， $Q = B^{-1}PB$ となるような B が存在する．いま十分大きな整数 $j \geq 0$ をとってやれば $\Delta^{2j}B \geq e$ となる (5.1 節 Step 1 の議論を参照)．この $\Delta^{2j}B$ を A とおくと

$$A^{-1}PA = (\Delta^{2j}B)^{-1}P(\Delta^{2j}B) = B^{-1}\Delta^{-2j}P\Delta^{2j}B = B^{-1}PB = Q$$

を得る.

定理 6.2 P, Q $(\geq \Delta^r)$ は conjugate とする．このとき注意 6.1 より，ある $A \geq e$ で $A^{-1}PA = Q$ となるものが存在する．このとき，$A = A_1A_2 \cdots A_k$ を A の l.c.f. とすると $A_1^{-1}PA_1 \geq \Delta^r$ が成り立つ.

証明 定理 6.2 が $r = 0$ (または $r = 1$) のときに成り立っているとする．いま一般の r に対して $P, Q \geq \Delta^r$ とする．このとき次の 2 つの場合に分けて考える.
(1) $r = 2j$ $(j \in \mathbb{Z})$ のとき:

> $P' = \Delta^{-2j}P$ とすると $P' \geq e$，同様に $Q' = \Delta^{-2j}Q$ とすると $Q' \geq e$ である．また $Q = A^{-1}PA$ であるから，両辺に Δ^{-2j} を掛けてやると $Q' = \Delta^{-2j}Q = \Delta^{-2j}A^{-1}PA = A^{-1}\Delta^{-2j}PA = A^{-1}P'A$ を得る．ここで定理 6.2 が $r = 0$ のときに成り立っているので，$A_1^{-1}P'A_1 \geq e$ を得る．よって $A_1^{-1}\Delta^{-2j}PA_1 \geq e$ となる．これと (3.5) より $A_1^{-1}PA_1 \geq \Delta^{2j} = \Delta^r$ を得る．よって $r = 2j$ のときに定理 6.2 は成り立つ.

(2) $r = 2j + 1$ のとき:

> 上と同様の議論により (定理 6.2 が $r = 1$ のときに成り立つことを用いて) $r = 2j + 1$ のときも定理 6.2 が成り立つことがわかる.

以上のことより $r=0$ (または $r=1$) のときに定理 6.2 を示せばよい.

Case 1: $r=0$ のとき

A_1 は positive permutation braid だから，ΔA_1^{-1} は positive braid である．よってこの positive braid を A_1^* で表す．このとき

$$\begin{aligned} A_1^*PA &= A_1^*AQ \quad (PA=AQ) \\ &= A_1^*A_1A'Q \quad (A=A_1A',\ A'=A_2\cdots A_k) \\ &= \Delta A'Q \quad (A_1^*=\Delta A_1^{-1}) \end{aligned}$$

となる．いま $Q\geq\Delta^r=\Delta^0=e$ であるから $A'Q\geq e$ となる．これと上の式より $A_1^*PA\geq\Delta$ を得る．ここで $B=A_1^*P,\ P=A$ において命題 4.17 を適用すると，$A_1^*PA_1\geq\Delta$ となることがわかる．よって $\Delta^{-1}A_1^*PA_1\geq e$ を得る．このとき $A_1^{-1}=\Delta^{-1}A_1^*$ より $A_1^{-1}PA_1\geq e$ がわかる．よって $r=0$ のとき定理 6.2 は成り立つ.

Case 2: $r=1$ のとき

$P'=P\Delta^{-1},\ Q'=Q\Delta^{-1}$ とする．また τ に対して

$$\begin{aligned} \tau(A) &= \Delta A\Delta^{-1} \quad ((3.6)\text{ より}) \\ &= \Delta A_1A'\Delta^{-1} \quad (A=A_1A',\ A'=A_2\cdots A_k) \\ &= \Delta A_1\Delta^{-1}\Delta A'\Delta^{-1} \\ &= \tau(A_1)\tau(A') \end{aligned}$$

が成り立つ．これは $\tau(A)$ の l.c.f. である．いま Case 1 と同様に，$\Delta A_1^{-1}=A_1^*\in[0,1],\ A_1^*PA=\Delta A'Q$ が成り立っている．このとき

$$\begin{aligned} A_1^*P'\tau(A)\Delta &= A_1^*P\Delta^{-1}\tau(A)\Delta \quad (P'=P\Delta^{-1}) \\ &= A_1^*PA \quad ((3.6)\text{ より}) \\ &= \Delta A'Q \quad (\text{上の式より}) \\ &= \Delta A'Q'\Delta \quad (Q'=Q\Delta^{-1}) \end{aligned}$$

であるから，$A_1^*P'\tau(A)=\Delta A'Q'$ がわかる．いま $Q\geq\Delta^r=\Delta$ であるから $Q'=Q\Delta^{-1}\geq\Delta\Delta^{-1}=e$ となる．よって $A'Q'\geq e$ となる．これと上の式 $A_1^*P'\tau(A)=\Delta A'Q'$ より $A_1^*P'\tau(A)\geq\Delta$ を得る．ここで命題 4.17 を適用すると $A_1^*P'\tau(A_1)\geq\Delta$ となることがわかる．一方,

$$\begin{aligned} \tau(A_1^{-1}PA_1) &= \tau(A_1^{-1})\tau(P)\tau(A_1) \\ &= \Delta A_1^{-1}\Delta^{-1}\Delta P\Delta^{-1}\tau(A_1) \\ &= \Delta A_1^{-1}P\Delta^{-1}\tau(A_1) \\ &= \Delta A_1^{-1}P'\tau(A_1) \\ &= A_1^*P'\tau(A_1) \end{aligned}$$

であるから，$\tau(A_1^{-1}PA_1) \geq \Delta$ となる．よって $\Delta^{-1}A_1^{-1}PA_1\Delta \geq \Delta$，すなわち $A_1^{-1}PA_1 \geq \Delta$ となることがわかる．よって $r = 1$ のときも定理 6.2 は成り立つ． □

系 6.3 P, Q $(\in [r, s])$ は conjugate とする．このとき注意 6.1 より，ある $A \geq e$ で $A^{-1}PA = Q$ となるものが存在する．このとき $A = A_1A_2 \cdots A_k$ をこの A の l.c.f. とし，$P_0 = P,\ P_i = A_i^{-1}P_{i-1}A_i$ $(i = 1, 2, \ldots, k)$ とおくと $P_i \in [r, s]$ が成り立つ．

ここで $P_k = Q$ となっていることに注意する．

証明 l に関する帰納法で $P_l \in [r, s]$ $(l = 1, 2, \ldots, k)$ を証明する．
(1) $l = 1$ のとする．このとき $P_1 \in [r, s]$ を示す．いま定理 6.2 より $P_1 \geq \Delta^r$ がわかっている．よって $P_1 \leq \Delta^s$ を示す．$P, Q \leq \Delta^s$ より $P^{-1}, Q^{-1} \geq \Delta^{-s}$ がわかる．よって $A^{-1}PA = Q$ より $A^{-1}P^{-1}A = Q^{-1}$ $(\geq \Delta^{-s})$ がわかる．さらに定理 6.2 を適用すると $A_1^{-1}P^{-1}A_1 \geq \Delta^{-s}$ を得る．一方，$P_1 = A_1^{-1}PA_1$ の逆元をとると $P_1^{-1} = A_1^{-1}P^{-1}A_1$ となる．よって $P_1^{-1} \geq \Delta^{-s}$ であるから，(3.10) より $P_1 \leq \Delta^s$ を得る．
(2) l まで成り立つと仮定する．このとき $P_{l+1} = A_{l+1}^{-1}P_lA_{l+1} \in [r, s]$ を示す．いま $A^{(l+1)} = A_{l+1}A_{l+2} \cdots A_k$ とおくと，これは $A^{(l+1)}$ の l.c.f. である．このとき

$$
\begin{aligned}
&A^{(l+1)^{-1}}P_lA^{(l+1)} \\
&= (A_{l+1}A_{l+2} \cdots A_k)^{-1}(A_l^{-1}A_{l-1}^{-1} \cdots A_1^{-1}PA_1 \cdots A_{l-1}A_l)(A_{l+1}A_{l+2} \cdots A_k) \\
&= Q
\end{aligned}
$$

とかける．ここで帰納法の仮定より $P_l \leq \Delta^s$ がわかる．また $Q \leq \Delta^s$ であるから，$P_l^{-1}, Q^{-1} \geq \Delta^{-s}$ がわかる．よって $A^{(l+1)^{-1}}P_lA^{(l+1)} = Q$ より $A^{(l+1)^{-1}}P_l^{-1}A^{(l+1)} = Q^{-1}$ となるから，$A^{(l+1)^{-1}}P_l^{-1}A^{(l+1)} \geq \Delta^{-s}$ がわかる．さらに定理 6.2 を適用すると $A_{l+1}^{-1}P_l^{-1}A_{l+1} \geq \Delta^{-s}$ を得る．一方，$P_{l+1}^{-1} = A_{l+1}^{-1}P_l^{-1}A_{l+1}$ であるから $P_{l+1}^{-1} \geq \Delta^{-s}$，すなわち $P_{l+1} \leq \Delta^s$ を得る． □

6.2 Cycling and algorithm

Conjugacy problem を解くには，次に定める super summit set と呼ばれる braid の集合に含まれる元をすべてリストアップすればよい．

定義 P と conjugate な braid 全体の集合を考える．この集合の元 P' で，infP' がこの集合の中で最大かつ supP' がこの集合の中で最小となるようなもの全体の集合を P の **super summit set** (以下では s.s.s. とかく) という．

このとき，conjugasy problem は次のようにして解決できる．

Algorithm P, Q が $[r, s]$ の元であるとする．

Step 1: P の s.s.s. を求める．

P の s.s.s. を見つけるために，P から出発して $[0, 1]$ に含まれる元で conjugate をとり，出てきた元のそれぞれに対して inf と sup を求めるという操作を繰り返し行う．この操作の途中で，inf が大きくなったり sup が小さくなったりした場合には，その元は s.s.s. の候補から取り除くことにする．こうして得られる元が P の s.s.s. の候補になる．このような操作は必ず有限回で終了することが証明できる (以下で示す)．その結果として P の s.s.s. が求まる．

Step 2: Q の s.s.s. の元を 1 つ求め，それが P の s.s.s. に属するどうか調べる．

以上により，P と Q が conjugate かどうか判定できる．以下では上の algorithm を具体的に実行する方法について述べる．

P の conjugacy class における inf の最大値を P の **summit power** という．まずこの summit power を求める方法から述べる．いま $P = \Delta^r P_1 P_2 \cdots P_k$ $(P_1 \neq \Delta)$ を P の l.c.f. とする．

定義 B_n の元 $c(P)$ を次のように定める．

$$c(P) = \Delta^r P_2 \cdots P_k \tau^r(P_1) \tag{6.1}$$

このとき $c(P)$ は P を **cycling して得られる** という．

注意 6.4 $c(P)$ は P の conjugate になっている．

注意 6.5 $P_2\cdots P_k\tau^r(P_1)$ が $c(P)$ の l.c.f. かどうかはわからない．しかし次のことがわかる．

$$\inf P \underset{①}{\leq} \inf c(P) \underset{②}{\leq} \inf P + 1 \tag{6.2}$$

$$\sup P - 1 \underset{③}{\leq} \sup c(P) \underset{④}{\leq} \sup P \tag{6.3}$$

実際これは，次のようにして証明できる．① は (6.1) より，④ は (6.1) に 5.1 節の algorithm (Step 2) を適用すれば成り立つことがわかる．また $c(P) \in [r', s']$ とする．このとき $P = A^{-1}c(P)A$ $(A \in [0,1])$ とすると，命題 3.8 より $P \in [r'-1, s'+1]$ を得る．これより次がわかるから，②と③も成り立つことがわかる．

$$\inf P \geq r' - 1 \geq \inf c(P) - 1 \tag{6.4}$$

$$\sup P \leq s' + 1 \leq \sup c(P) + 1 \tag{6.5}$$

次の補題は P の summit power を求める高速な algorithm を与える．

補題 6.6 いま P に conjugate な元 Q で $\inf Q > \inf P$ となるものが存在したとする．このとき，P から出発して cycling を何回か繰り返して得られる元 $c^j(P)$ で $\inf c^j(P) > \inf P$ となるものが存在する．

証明 $P = \Delta^r P'$ とする．ただし $r = \inf P$, $P' = P_1P_2\cdots P_k$ $(P_i \in [0,1])$ は P' の l.c.f. とする．このとき注意 6.1 より，ある $A \geq e$ で $Q = APA^{-1}$ となるものが存在する．補題 6.6 はこのような A の $\mathrm{wt}(A)$ に関する帰納法で証明する．

いま $\inf Q > \inf P$ より $Q = \Delta^r Q'$ $(Q' \geq \Delta)$ とかける．よって

$$\Delta^r Q' = Q = APA^{-1} = A\Delta^r P' A^{-1} \tag{6.6}$$

すなわち $\Delta^r Q'A = A\Delta^r P'$ を得る．ここで右辺 $= \Delta^r\tau^r(A)P'$ となるから $\Delta^r Q'A = \Delta^r\tau^r(A)P'$，すなわち $Q'A = \tau^r(A)P'$ を得る．このとき $Q' \geq \Delta$, $A \geq e$ から $\tau^r(A)P' \geq \Delta$ がわかる．ここで命題 4.17 を適用すると $\tau^r(A)P_1 \geq \Delta$ がわかる．いま両辺に τ^r を掛けてやると $A\tau^r(P_1) \geq \Delta$ を得る．したがって，ある $A' \geq e$ が存在して

$$A\tau^r(P_1) = A'\Delta \tag{6.7}$$

とかける．一方 $\tau^r(P_1) \leq \Delta$ であるから，ある $A'' \geq e$ が存在して $\Delta = A''\tau^r(P_1)$ とかける．よって $A\tau^r(P_1) = A'\Delta = A'A''\tau^r(P_1)$，すなわち $A = A'A''$ を得る．このとき

$$\mathrm{wt}(A') = \mathrm{wt}(A) - \mathrm{wt}(A'') < \mathrm{wt}(A) \tag{6.8}$$

である．いま

$$\begin{aligned} \tau^r(P_1)c(P) &= \tau^r(P_1)\Delta^r P_2\cdots P_k\tau^r(P_1) \quad (c(P)\text{ の定義}) \\ &= \Delta^r P_1P_2\cdots P_k\tau^r(P_1) \\ &= P\tau^r(P_1) \end{aligned}$$

がわかる．よって

$$\begin{aligned} QA\tau^r(P_1) &= AP\tau^r(P_1) \quad (Q = APA^{-1}) \\ &= A\tau^r(P_1)c(P) \end{aligned}$$

であるから，これと (6.7) より $QA'\Delta = A'\Delta c(P)$ を得る．この両辺の Δ を前に出してやると $\Delta\tau(Q)\tau(A') = \Delta\tau(A')c(P)$，したがって $\tau(Q)\tau(A') = \tau(A')c(P)$，すなわち $\tau(Q) = \tau(A')c(P)\tau(A')^{-1}$ となる．ゆえに $\tau(Q)$ は $\tau(A')$ による $c(P)$ の conjugate になっている．このとき (6.8) より帰納法が使えて，$c(P)$ のある cycling $c^k(c(P)) = c^{k+1}(P)$ に対して

$$\inf c^{k+1}(P) > \inf c(P) = \inf(P) \tag{6.9}$$

$$\inf c^{k+1}(P) = \inf c(P) > \inf(P) \tag{6.10}$$

のいずれかが成り立つ．よって補題 6.6 が示せた． □

系 6.7 任意の conjugacy class において，inf の最大値と sup の最小値は同じ元で実現できる．

系 6.7 より，s.s.s. は conjugacy class の部分集合で，その canonical length が最小となるものを集めてできる集合であることがわかる．

証明 P は sup の最小値を実現しているとする．また Q は P の conjugate で inf の最大値を実現しているとする．このとき $\inf P < \inf Q$ ならば P のある cycling $c^j(P)$ は次を満たす．

$$\inf c^j(P) > \inf P \quad (\text{補題 } 6.6) \tag{6.11}$$

$$\sup c^j(P) \leq \sup P \quad (\text{注意 } 6.5) \tag{6.12}$$

ここで P は sup の最小値を満たしているから，(6.12) で等号が成り立つ．これを繰り返すと，ある $c^n(P)$ で inf の最大値が実現できる．この $c^n(P)$ は inf の最大値と sup の最小値を実現している． □

以上により，P の summit power を次のようにして求めることができる．P の cycling をすでに現れた元が再び現れるまで繰り返し行う．こうして得られた元の中に inf の最大値を実現する元がある．

$$P \to c(P) \to c^2(P) \to \cdots \to c^j(P) = c^n(P)\ (0 \leq n < j)$$

これら $P, c(P), \ldots, c^{j-1}(P)$ の inf の最大値が P の summit power になっている．

注意 6.8 $c(P)$ の cycling は $c(P)$ の表示から直ちに求まるわけではない．

例 $P = \sigma_1\sigma_2^2\sigma_3\sigma_1\sigma_2^2$ とする．P の l.c.f. は $P = (\sigma_1\sigma_2)(\sigma_2\sigma_3\sigma_1\sigma_2)(\sigma_2)$ である (図 6.1)．このとき命題 4.14 より $\inf P = 0$，定理 4.18 より $\sup P = 3$ である．

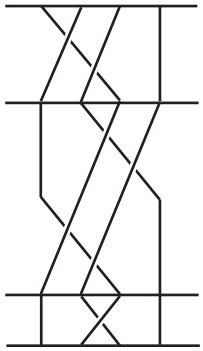


図 6.1: P の l.c.f.

次に P を cycling して図 6.2 のように変形してやると，

$$\begin{aligned} c(P) &= (\sigma_2\sigma_3\sigma_1\sigma_2)(\sigma_2)(\sigma_1\sigma_2) \\ &= (\sigma_2\sigma_3\sigma_2\sigma_1\sigma_2)(\sigma_2\sigma_1) \end{aligned}$$

となり，これは $c(P)$ の l.c.f. である．このとき $\inf c(P) = 0$，$\sup c(P) = 2$ である．

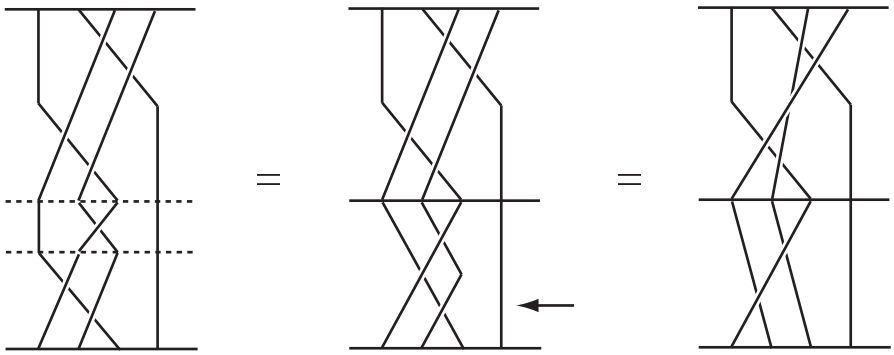


図 6.2: $c(P)$ の変形

さらに cycling して図 6.3 のように変形してやると，

$$\begin{aligned} c^2(P) &= (\sigma_2\sigma_1)(\sigma_2\sigma_3\sigma_2\sigma_1\sigma_2) \\ &= \Delta\sigma_2 \end{aligned}$$

となり，これは $c^2(P)$ の l.c.f. である．このとき $\inf c^2(P) = 1$，$\sup c^2(P) = 2$ である．

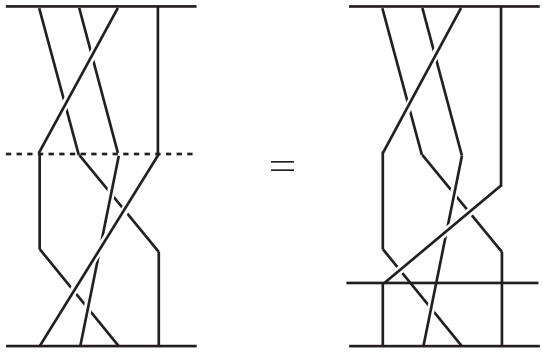


図 6.3: $c^2(P)$ の変形

さらに cycling してやると $c^3(P) = \Delta\sigma_2 = c^2(P)$ となるので，P の cycling は $c^2(P)$ で終わる．よって $\inf P$ の最大値は 1 である．

$\sup P$ に関しては次のように考えればよい．注意 3.13 より，$\sup P = -\inf P^{-1}$ がわかる．よって P^{-1} を cycling することで inf の最大値と sup の最小値を求めることができる．P^{-1} の cycling を考えるために，P の **reverse cycling** を次のように定める．いま $P = \Delta^r P_1 P_2 \cdots P_k$ $(P_1 \neq \Delta)$ を P の l.c.f. とする．

定義 B_n の元 $r(P)$ を次のように定める．

$$r(P) = \Delta^r \tau^r(P_k) P_1 \cdots P_{k-1} \tag{6.13}$$

このとき $r(P)$ は P **を reverse cycling して得られる** という．

命題 6.9 $(r(P))^{-1} = \tau(c(P^{-1}))$ が成り立つ．

証明 $P = \Delta^r P_1 P_2 \cdots P_k$ より，

$$\begin{aligned}
P^{-1} &= P_k^{-1} \cdots P_1^{-1} \Delta^{-r} && (6.14)\\
&= \Delta^{-r} \tau^r(P_k^{-1}) \cdots \tau^r(P_1^{-1}) && (6.15)\\
&= \Delta^{-r-1} \tau^{r+1}(P_k^{-1}) \cdots \tau^{r+1}(P_2^{-1})(\tau^{r+1}(P_1^{-1})\Delta) && (6.16)\\
&\vdots && (6.17)\\
&= \Delta^{-r-k}(\tau^{r+k}(P_k^{-1})\Delta) \cdots (\tau^{r+1}(P_1^{-1})\Delta) && (6.18)
\end{aligned}$$

ここで $P_i' = \tau^{r+i}(P_i^{-1})\Delta$ $(i = 1, 2, \ldots, k)$ とおくと，

$$P^{-1} = \Delta^{-r-k} P_k' \cdots P_1' \tag{6.19}$$

とかける．また，上の式変形において

$$\begin{aligned}
(6.15) &= \Delta^{-r-1} \tau^{r+1}(P_k^{-1}) \cdots \tau^{r+1}(P_2^{-1})(\Delta\tau^r(P_1^{-1})) && (6.20)\\
&\vdots && (6.21)\\
&= \Delta^{-r-k}(\Delta\tau^{r+k-1}(P_k^{-1})) \cdots (\Delta\tau^r(P_1^{-1})) && (6.22)
\end{aligned}$$

とする．ここで $P'_i = \Delta\tau^{r+i-1}(P_i^{-1})$ $(i = 1, 2, \ldots, k)$ となることに注意すると

$$P^{-1} = \Delta^{-r-k} P'_k \cdots P'_1 \tag{6.23}$$

とかけることがわかる．次にこれが P^{-1} の l.c.f. であることを示す．

一般に，ある $A, B \geq e$ に対して $AB = \Delta$ が成り立つとすると，注意 4.4 と注意 4.5 より

$$\begin{aligned} F(A) \cup S(B) &= \{1, 2, \ldots, n-1\} & (6.24) \\ F(A) \cap S(B) &= \phi & (6.25) \end{aligned}$$

がわかる．ここで

$$\begin{aligned} P'_i &= \tau^{r+i}(P_i^{-1})\Delta \\ &= (\tau^{r+i}(P_i))^{-1}\Delta \end{aligned}$$

より $\tau^{r+i}(P_i)P'_i = \Delta$ を得る．この両辺に τ^{r+i} を掛けてやると $P_i\tau^{r+i}(P'_i) = \Delta$ となるから，$A = P_i,\ B = \tau^{r+i}(P'_i)$ とみなすと (6.24)，(6.25) より

$$\begin{aligned} F(P_i) \cup S(\tau^{r+i}(P'_i)) &= \{1, 2, \ldots, n-1\} & (6.26) \\ F(P_i) \cap S(\tau^{r+i}(P'_i)) &= \phi & (6.27) \end{aligned}$$

を得る．よって次のことがわかる．

$$F(P_i) = \{1, 2, \ldots, n-1\} \setminus S(\tau^{r+i}(P'_i)) \tag{6.28}$$

また同様に，

$$\begin{aligned} P'_i &= \Delta\tau^{r+i-1}(P_i^{-1}) \\ &= \Delta(\tau^{r+i-1}(P_i))^{-1} \end{aligned}$$

より $P'_i\tau^{r+i-1}(P_i) = \Delta$ を得る．この両辺に τ^{r+i-1} を掛けてやると $\tau^{r+i-1}(P'_i)P_i = \Delta$ となるから，$A = \tau^{r+i}(P'_{i+1}),\ B = P_{i+1}$ とみなすと

$$\begin{aligned} F(\tau^{r+i}(P'_{i+1})) \cup S(P_{i+1}) &= \{1, 2, \ldots, n-1\} & (6.29) \\ F(\tau^{r+i}(P'_{i+1})) \cap S(P_{i+1}) &= \phi & (6.30) \end{aligned}$$

を得る．よって次のことがわかる．

$$S(P_{i+1}) = \{1, 2, \ldots, n-1\} \setminus F(\tau^{r+i}(P'_{i+1})) \tag{6.31}$$

いま $P = \Delta^r P_1 P_2 \cdots P_k$ は l.c.f. だから $S(P_{i+1}) \subset F(P_i)$ である．よって (6.28) と (6.31) より $S(\tau^{r+i}(P'_i)) \subset F(\tau^{r+i}(P'_{i+1}))$，すなわち $S(P'_i) \subset F(P'_{i+1})$ を得る．

次に P^{-1} を cycling してやると，

$$c(P^{-1}) = \Delta^{-r-k} P'_{k-1} \cdots P'_1 \tau^{r+k}(P'_k) \tag{6.32}$$

を得る．これを用いて $r(P)\tau(c(P^{-1})) = e$ となることが次のように示せるから，命題 6.9 が成り立つことがわかる．

$$\begin{aligned}
& r(P)\tau(c(P^{-1})) && (6.33)\\
&= (\Delta^r \tau^r(P_k) P_1 \cdots P_{k-1})(\tau(\Delta^{-r-k} P'_{k-1} \cdots P'_1 \tau^{r+k}(P'_k))) && (6.34)\\
&= (\Delta^r \tau^r(P_k) P_1 \cdots P_{k-1})(\Delta^{-r-k} \tau(P'_{k-1}) \cdots \tau(P'_1) \tau^{r+k+1}(P'_k)) && (6.35)
\end{aligned}$$

となる．ここで，

$$\begin{aligned}
P_{k-1}\Delta^{-r-k}\tau(P'_{k-1}) &= P_{k-1}\tau^{-r-k+1}(P'_{k-1})\Delta^{-r-k} \\
&= P_{k-1}\tau^{r+k-1}(P'_{k-1})\Delta^{-r-k} \\
&= \Delta^{-r-k+1}
\end{aligned}$$

となるから，(6.35) は中心から順に Δ に置き換えられ，次の結果を得る．

$$\begin{aligned}
(6.35) &= \Delta^r \tau^r(P_k)\Delta^{-r-1}\tau^{r+k+1}(P'_k) \\
&= \Delta^{-1}\tau^{-1}(P_k)\tau^{r+k+1}(P'_k) \\
&= \Delta^{-1}\tau(P_k)\tau^{r+k+1}(P'_k) \\
&= \Delta^{-1}\tau(P_k\tau^{r+k}(P'_k)) \\
&= \Delta^{-1}\tau(\Delta) \\
&= \Delta^{-1}\Delta \\
&= e
\end{aligned}$$

よって命題 6.9 が示せた． □

いま命題 6.9 と注意 3.13 を用いて $\sup P$ を次のように求める．

$$\begin{aligned}
\sup r(P) &= -\inf(r(P))^{-1} \\
&= -\inf\tau(c(P^{-1})) \quad (\text{命題 6.9}) \\
&= -\inf c(P^{-1})
\end{aligned}$$

であるから，

$$\sup r^j(P) = -\inf c^j(P^{-1}) \tag{6.36}$$

がわかる．したがって，次に示す $P^{-1}, c(P^{-1}), \ldots, c^{j-1}(P^{-1})$ の inf の最大値が sup の最小値を実現している．

$$P^{-1} \ \to \ c(P^{-1}) \ \to \ c^2(P^{-1}) \ \to \ \cdots \ \to \ c^j(P^{-1}) = c^n(P^{-1}) \ (0 \le n < j)$$

実際に，P, Q に対してこの algorithm を適用することを考える．もし P の s.s.s. が完全に分かっているならば，Q に cycling と reverse cycling を適用して P の s.s.s. の元が現れるかどうか調べればよい．しかし，一般に cycling だけでは完全な s.s.s. を生成することはできない．

例えば $P = \sigma_1$ のとき σ_i $(i = 2, 3, \ldots, n-1)$ は σ_1 と conjugate である (図 6.4, 6.5) が，これらは σ_1 の cycling では求めることができない．なぜなら σ_1 の cycling で得られる word は σ_1 ただ 1 つだからである．

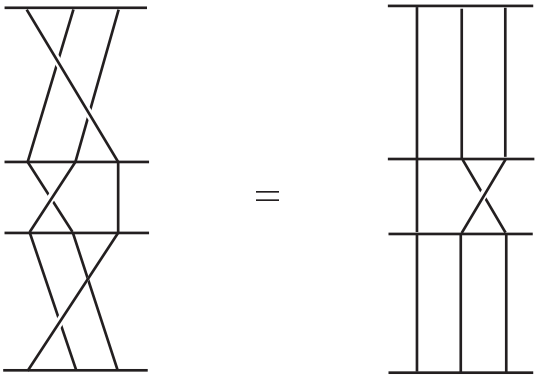


図 6.4: σ_2

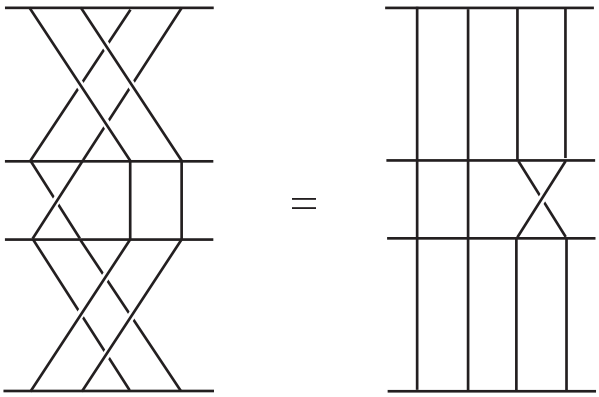


図 6.5: σ_3

しかし 5.2 節の表と併せて，考察を s.s.s. だけに制限することで，Garside の algorithm よりずっと実用的な algorithm を得ることができる．

付録A Concluding remark

ここでは注意 3.10 で紹介した命題の証明を与える.

命題 $[r_1, r_2][s_1, s_2] = [r_1 + r_2, s_1 + s_2]$ が成り立つ.

証明 $[\subset]$ 命題 3.8 ですでに示した.
$[\supset]$ $P \in [r_1 + r_2, s_1 + s_2]$ とする. このとき $P = \Delta^{r_1+r_2} A_1 A_2 \cdots A_k,\ \Delta^{-r_1-r_2} P = A_1 A_2 \cdots A_k$ を $\Delta^{-r_1-r_2} P$ の l.c.f. とすると, (4.24) より $r_1 + r_2 + k = \sup P \leq s_1 + s_2$ がわかる. ここで $t_1 = s_1 - r_1,\ t_2 = s_2 - r_2$ とおくと, $k \leq t_1 + t_2$ となる.
(1) $k \leq t_1$ のとき

$P' = \Delta^{r_1} A_1 A_2 \cdots A_k,\ P'' = \Delta^{r_2}$ とすると,

$$\begin{aligned} P' &\in [r_1, r_1 + k] \subset [r_1, r_1 + t_1] = [r_1, s_1] \\ P'' &\in [r_2, s_2] \end{aligned}$$

となる. また $P = P'P''$ が成り立っている.

(2) $k > t_1$ のとき

$P' = \Delta^{r_1} A_1 A_2 \cdots A_{t_1},\ P'' = \Delta^{r_2} A_{t_1+1} A_{t_1+2} \cdots A_k$ とすると,

$$\begin{aligned} P' &\in [r_1, r_1 + t_1] = [r_1, s_1] \\ P'' &\in [r_2, r_2 + k - t_1] \subset [r_2, r_2 + t_2] = [r_2, s_2] \end{aligned}$$

となる. また $P = P'P''$ が成り立っている.

以上により, $P \in [r_1 + s_1][r_2 + s_2]$ が示せた. □

参考文献

[1] E. Artin, 'Theorie der Zöpfe', *Abh. math. Semin. Hamburg Univ.* 4 (1926), 47-72.

[2] E. Artin, 'Theory of braids', *Ann. Math.* 48 (1947), 101-126.

[3] J. S. Birman, 'Braids, links and mapping-class groups', *Annals of Maths. Studies* 82 (1974), Princeton University Press.

[4] J. S. Birman, K. H. Ko and S. J. Lee, 'A new approach to the word and conjugacy problems in the braid groups', *Advances in Math* 139 (1998), 322-353

[5] E. A. Elrifai and H. R. Morton, 'Algorithms for positive braids', *Quart. J. Math. Oxford* (2), 45 (1994), 479-497.

[6] F. A. Garside, 'The braid group and other groups', *Quart. J. Math. Oxford* (2), 78 (1969), 235-254.

[7] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang and C. Park, 'New Public-Key Cryptosystem Using Braid groups', *CRYPT* 2000, 166-183, *Lecture Notes in Comput. Sci.*, 1880, *Springer*, *Berlin*, 2000.

[8] H. R. Morton and H. B. Short, 'Calculating the 2-variable polynomials of knots', *Journal of Algorithms* 11 (1990), 117-131.

[9] W. Thurston, 'Finite state algorithms for the braid group', Chapter 9 of '*Word processing in groups*', D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Patterson and W. P. Thurston. Jones and Bartlett, Boston and London 1992.