

ブレイド群における super summit を求めるアルゴリズムの実装

GUI Tools for Braid Groups

<http://www.tani.cs.chs.nihon-u.ac.jp/g-2004/ebi/>

谷 研究室 蝦名 綾子
Ayako EBINA

概要

任意のブレイド V において、 V と共役なものの集合は無限集合である。その有限集合 super summit set $C^{sum}(V)$ を 1 つ求めるアルゴリズムを実装した。また、ブレイドの研究をしている人達への支援ツールとして、ブレイドの基本的な操作や演算の GUI ツールを作成した。

1 はじめに

K.h.Ko,S.J.Lee,Cheon,J.W.Han,J.Kang,C.Park がブレイド群における共役問題の難しさに安全のより所を置いた公開鍵暗号系を提案するなど、ブレイド群に関する計算問題の計算量解析は、応用も含めて活発に研究されている。共役問題は難しく、公開鍵暗号系への利用が提案されている。これが難しいと証明できれば、高い安全性を保証している公開鍵暗号系の基礎理論を開発したことと等しく、逆に、簡単だと証明できれば、共役の暗号系を破れることになる。あるブレイドに対して共役なブレイドの集合は無限集合になるが、その有限部分集合で super summit set と呼ばれるものが知られている。この super summit set の元を 1 つ発見する高速なアルゴリズムが知られており、そのアルゴリズムを実装した。また、その可視化も行った。

2 章ではブレイドに関する諸定義を、3 章では今回実装したアルゴリズムを紹介する。4 章では実装したプログラムの構造を示す。

2 ブレイドの定義

2.1 ブレイドとは

ブレイドとは、2 つの平行な平面に接した n 本の紐からなる集合のことである。左側の平面から右側の平面へ 1 本の紐をたどっていくと、紐はいつでも右方向へ向かっている。

2.2 単位元 e

単位元 e とは、ブレイドのうち、紐が一度も交差しなものの。

2.3 σ

e において下から数えて i 番目と $i+1$ 番目の紐が交差しているブレイドで、負の傾きを持つ紐が上側にきて

いるものを σ_{i+1} と表現する。

2.4 逆元

σ_i^{-1} は、 σ_i の上下関係を逆にしたブレイドであり、 σ_i の逆元となっている。

2.5 Artin の生成元

これらはブレイド群の生成元となっており、 σ_i を Artin の生成元と呼ぶ。

2.6 band generator

Artin の生成元に対し、複数の交差をひとまとめにした生成元を band generator と呼ぶ。下から数えて i 番目の紐と j 番目の紐が交差しているとき、 a_{ij} と表現する。

2.7 正ブレイド

正ブレイドとは、 a_{ij} において、 $i > j$ が成り立つものの。単位元も正ブレイドの一つ。また、これらで作られた集合を BBn^+ と定義する。

2.8 同値

2 つのブレイド V, W が同値とは、 V の端点を固定し、紐を出さずに上下関係を維持したまま動かし、 W に一致させることができることをいう。

2.8.1 Artin の生成元における同値関係

$$\sigma_{i+1} \sigma_i \sigma_{i+1} \equiv \sigma_i \sigma_{i+1} \sigma_i$$

2.8.2 Artin の生成元における同値関係

$$\sigma_i \sigma_j \equiv \sigma_j \sigma_i$$

2.8.3 band generator における同値関係

$n \geq t > s > r \geq 1$ のとき

$$\sigma_{ts} \sigma_{rq} \equiv \sigma_{rq} \sigma_{ts}$$

2.8.4 band generator における同値関係

$(t-r)(t-q)(s-r)(s-q) > 0$ のとき

$$\sigma_{ts} \sigma_{sr} \equiv \sigma_{tr} \sigma_{ts} \equiv \sigma_{sr} \sigma_{tr}$$

2.9 正同値

以上 4 つの関係を有限回適用することによって得られるブレイドを正同値という。

2.10 積

2 つのブレイド V, W の積 VW とは, V の右端と W の左端を繋げたブレイドのことをいう。

2.11 共役

2 つのブレイド V, W が共役とは, 以下の条件が成り立つ α が存在するときをいう。

$$V = \alpha W \alpha^{-1}$$

このとき, α は一意ではない。

2.12 fundamental word δ

fundamental word δ とは, 紐の本数 $n(n > 0)$ のとき, $a_{n-1}a_{n-2}\cdots a_1$ と同値なもの。表現の仕方は一意ではない。

2.13 半順序

任意のブレイド V, W において $V \leq W$ とは, V の両端に正ブレイドをつけて W になるときをいう。

2.14 $[r, s]n$

以下の条件を満たすブレイド W の集合

$$\{W \in BBn^+ \mid \delta^r W \delta^s\}$$

2.15 分割

$X \in [0, 1]n$, A が正ブレイドで, $P = XA$ となるとき, XA を P の分割という。

2.16 Left-weighted

P の分割 XA が Left-weighted であるとは, 任意の正ブレイド P の分割 $X'A'$ に対して, $X' \leq X$ となるときをいい, $X \dashv A$ と表す。

2.17 標準形表現

標準形表現とは, $V \in BBn^+$ に対して, $u \in [0, 1]n$ と正ブレイド $A_1, A_2, \dots, A_p \in [0, 1]n$ を用いた

$$V = \delta^u A_1 A_2 \cdots A_p$$

という表現をするもので, $1 \leq i \leq p-1$ となる各 i に対し、

$$A_i \dashv A_{i+1}$$

となるものが唯一存在する。

2.18 head, tail

$a, b, c \in BBn^+$ において $ab = c$ のとき, a は b の head といい, b は c の tail という。

2.19 maximal head

P の head H が maximal head であるとは, H と H を取り除いた P の tail が Left-weighted となるときをいう。

2.20 標準形の作り方

任意のブレイド V から標準形を作るには, maximal head と tail に分け, 更に tail を maximal head と tail に分け, それを繰り返す, 出てきた tail を順に表していくもの。

2.21 τ 2.21.1 τ

任意のブレイド V に τ を施すとは, V に対して, $\delta^{-1}V\delta$ という積を作ること。

2.21.2 τ^{-1}

任意のブレイド V に τ^{-1} を施すとは, V に対して, $\delta V \delta^{-1}$ という積を作ること。

2.21.3 τ の性質

τ もしくは τ^{-1} を施す前のブレイドと施した後のブレイドは共役である。

2.22 cycling

2.22.1 cycling

cycling とは, ブレイド V の標準形表現が

$$V = \delta^p W_1 W_2 \cdots W_q$$

のとき,

$$V = \delta^p W_2 \cdots W_q \tau^{-p}(W_1)$$

とするもので, これを $cyc(V)$ と表す。

2.22.2 decycling

decycling とは, ブレイド V の標準形表現が

$$V = \delta^p W_1 W_2 \cdots W_q$$

のとき,

$$V = \delta^p \tau^p(W_q) W_1 \cdots W_{q-1}$$

とするもので, これを $decyc(V)$ と表す。

2.23 inf

標準形表現 $W = \delta^p W_1 W_2 \cdots W_q$ において

$$\inf(W) = p$$

2.24 inf

標準形表現 $W = \delta^p W_1 W_2 \cdots W_q$ において

$$\sup(W) = q$$

2.25 super summit set

任意のブレイド V において、 V と共役なものの集合のうち、

$$C^{\geq u}(V) = \left\{ \begin{array}{l} W \quad B = n|V \text{ と } W \text{ は共役かつ} \\ W = \delta^v W_1 W_2 \cdots W_p (\text{ただし } v \geq u) \end{array} \right\}$$

を満たす集合は有限集合である。更に、

$$C^{sum}(V) := \left\{ S \quad C(V) : \begin{array}{l} \inf(S) = \max\{\inf(S') : S' \in C(V)\} \\ \sup(S) = \min\{\sup(S') : S' \in C(V)\} \end{array} \right\}$$

を満たすものを super summit set という。

3 super summit set の元を 1 つ求めるアルゴリズム

標準形の作成 (1)

$k \leftarrow$ 紐の本数

first_delta $\leftarrow$ 標準形の作成 (1) で作られた δ

second_delta $\leftarrow$ 標準形の作成 (1) で作られた δ

$i \leftarrow 1$

while true

first_delta $\leftarrow$ second_delta(1)

while $i \leq k-2$ do

cycling

標準形の作成 (2)

second_delta $\leftarrow$ 標準形の作成 (2) で作られた δ

od

if(first_delta=second_delta(1))

break

od

od

first_p+q $\leftarrow$ この直前の while ループ内での

標準形の作成での標準形表現の p+q

second_p+q $\leftarrow$ この直前の while ループ内での

標準形の作成での標準形表現の p+q

$i \leftarrow 1$

while true

first_p+q $\leftarrow$ second_p+q(1)

while $i \leq k-2$ do

decycling

標準形の作成 (2)

second_p+q $\leftarrow$ 標準形の作成 (2) での標準形表現の p+q

od

if(first_p+q=second_p+q(1))

break

od

od

4 アルゴリズムの実装

4.1 環境

・ Java

4.2 band generator で super summit を求めるアルゴリズムを実装するに当たり、作成したクラス

4.2.1 BGLine

ブレイドの基本情報を band generator で入力するメソッドを持ち、それら (以下のもの) をオブジェクトとして記憶

・入力ブレイドの紐の本数 [band_value]

・band generator[bgn]

・band generator の合計 (交点) の数 [length]

・ δ (後に標準形作成 (*) で使用。初期値は 0)[delta]

band generator は int 型の配列として記憶している。

例えば、 a_{21} は整数の 21 という形で記憶する。

・入力したものを表示

・それらを BGList(*) に渡す

4.2.2 Pro_tau

・int 型整数を 1 つ受け取り、 τ もしくは τ^{-1} を施す

・BGLine を受け取り、line(一次元配列) 全体に τ もしくは τ^{-1} を施す

・BGList を受け取り、任意の位置に τ もしくは τ^{-1} を施す (#)

このうち、(#) は今回のプログラムで使用していない。

4.2.3 Cyc

・BGList(*) を受け取り、cycling もしくは decycling を施し BGLine に答えを格納

4.2.4 注釈

(*) の BGList は、2003 年、富士作成のものを使用している。

4.3 Artin の生成元を同値を保ったまま表示 を変えるアルゴリズム、また、標準形を 求めるアルゴリズムの実装に当たり作成 したクラス

4.3.1 Artindouch

一次元配列と紐の本数を入力し、好きな位置に同値元
を保持したまま生成元の表示を変えるルールを施す。

4.3.2 ARLine

ブレイドの基本情報を Artin で入力するメソッドを持
ち、それら (以下のもの) をオブジェクトとして記憶

- ・入力ブレイドの紐の本数 [string_num]
- ・生成元 [aln]
- ・Artin 生成元の合計 (交点) の数 [length]

Artin の生成元は int 型の配列として記憶している。

例えば、 σ_2 は整数の 2 という形で記憶する。

- ・入力したものを表示

4.3.3 Per

入力された Artin の生成元を置換ブレイドで記憶。置
換ブレイドを Artin の生成元に変換。・入力ブレイドの
紐の本数 [string_num]

- ・生成元 [per]
- ・Artin 生成元の合計 (交点) の数 [length]

4.3.4 Maxhead

・置換ブレイド表現を 2 つ受け取り、head と tail を
返す。

(2004, 松葉) を使用。

4.3.5 Hantei

- ・置換ブレイド表現を受け取り、Artin の生成元を返す。

4.3.6 Artinloop

Artin の生成元で標準形を返すアルゴリズムの実装。
ARLine で受け取り、ARLine で返す。

5 今後の課題

- ・band generator で super summit set を全部求める。
- ・Artin の生成元で同様のことを行う