ブレイド群における共役判定プログラムの試作

A software for conjugacy program of braids

谷　研究室　　笠谷　知生
Tomoki Kasaya

概要

2000 年に, ブレイド (組み紐) 群を利用した公開鍵暗号系が提案された。本研究ではブレイドで公開鍵暗号を考える上で基本となる標準形と共役なものを求めるプログラムを実装する。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ため、その有限集合 super summit set を求めるアルゴリズムを実装した。

1　はじめに

ネットワーク化が進んだ今日、情報の隠蔽を目的とした暗号技術は、数々のセキュリティ技術の中核を成すものの１つとして位置付けられている。暗号とは、当事者以外には意味がわからないように、鍵を使い決められた手順に従って変換した特殊な記号や文字、または方式のことをいう。

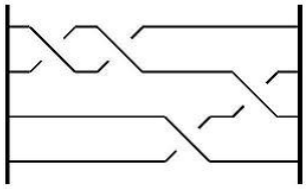
現在最も広く使われている公開鍵暗号系は、素因数分解の難しさを利用した RSA 暗号系である。この暗号系では、2 つの大きな素数の積を鍵としている。安全性を高めるためにより長い鍵を使うことが求められているが、携帯電話や IC カードのように限られた環境で大きな整数の演算を行うことは困難であり、RSA 暗号系はそのような環境に適していなそこで、楕円曲線暗号などの新しい公開鍵暗号系が研究されている。

本研究ではブレイド群を使った公開鍵暗号を考えるのに必要なプログラムの一部を実装し、２００５年に松葉氏によって行われた summit set の大きさを求める実験と比較検討した。２章ではブレイド群の基本的な定義の解説、３, ４, ５章ではその応用とブレイド群における困難な問題の紹介、６章ではアルゴリズムを紹介し、７, ８章では実験と今後の課題などを示した。

2　ブレイド群の定義

2.1　ブレイドとは

n - ブレイドとは平行な 2 つの面に接続している n 本の紐であり, 左の面から出ている紐をたどると常に右へ向かい必ず右の面につくものをいう。n - ブレイド群のことを B_n と表す。



４－ブレイドの例

2.2　単位元 e

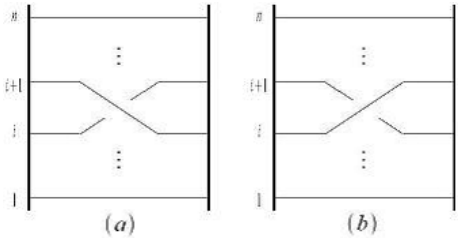
単位元 e とは，ブレイドのうち，紐が一度も交差しないもの。

2.3　Artin の生成元 σ

単位元 e において下から数えて i 番目と $i+1$ 番目の紐のみ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。これを σ_i を Artin の生成元と呼ぶ。

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。

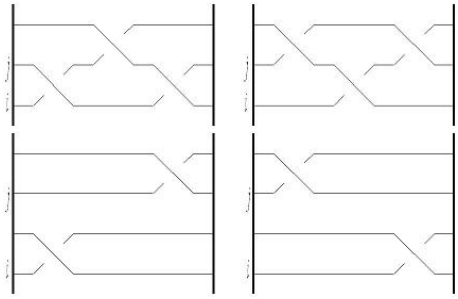


Artin の生成元 (a) σ　　(b) σ^{-1}

2.5　ブレイドの同値

2 つのブレイド V,W が同値とは、一方のブレイドを, 紐が面に接続している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もう一方のブレイドと同じものにできるとき,2 つのブレイドは同値であるという.

2.6 Artin の生成元における同値関係



1. $\sigma_i \sigma_j \sigma_i \equiv \sigma_j \sigma_i \sigma_j \qquad (|i-j|=1)$
2. $\sigma_i \sigma_j \equiv \sigma_j \sigma_i \qquad (|i-j|>1)$

2.7 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。

2.8 正ブレイド

σ_i^{-1} を含まないもの。正ブレイドの集合を B_n^+ と表す。

2.9 非冗長ブレイド

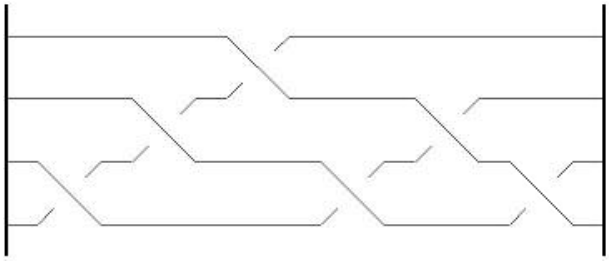
正ブレイドの中でそれぞれの紐が高々一回だけ交差するもの。非冗長ブレイドの集合を $\sum_n^{\sim}$ と表す。

2.10 基本ブレイド

非冗長ブレイドの中でそれぞれの紐がちょうど一回ずつ交差するもの。このブレイドを

$$\Delta = (\sigma_1 \sigma_2 ... \sigma_n)(\sigma_1 \sigma_2 ... \sigma_{n-1}) ... (\sigma_1 \sigma_2)\ \sigma_1$$

と表す。基本ブレイドから紐を一本以上取り除くと非冗長ブレイドになる。



基本ブレイドの例

3 canonical form

3.1 半順序≦

任意のブレイド V,W において $V \leqq W$ 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。

3.2 分割

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

3.3 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，$X \neg A$ と表す。

3.4 標準形表現

標準形表現とは，$V \in BBn^+$ に対して，$u \in$ と正ブレイド $A_1, A_2, \cdots A_p \in \sum_n$ 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、

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

となるものが唯一存在する。

3.5 head,tail

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

3.6 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。

3.7 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，それを繰り返し，出てきた tail を順に表していくもの。

4 ブレイド群における計算問題

ブレイド x と y が共役であるとは、$y = axa^{-1}$ となるブレイド a が存在するときを言う。

共役に関して、困難であると予想されている計算問題に以下のようなものがある。B_m を $m < n$ に対して $\sigma_1, ..., \sigma_{m-1}$ で表される B_n の部分群とする。

4.1 共役決定問題

入力： $(x, y) \in B_n \times B_n$

出力： x と y が共役であるか?

4.2 共役探索問題

入力： 互いに共役であるような $(x, y) \in B_n \times B_n$

出力： $y = axa^{-1}$ となるような $a \in B_m$

4.3 一般共役探索問題

入力： $b \in B_m, m \leq n$ に対して $y = bxb^{-1}$ となるような $(x, y) \in B_n \times B_n$

出力： $y = axa^{-1}$ となるような $a \in B_m$

4.4 共役分解問題

入力： $b \in B_m, m \leq n$ に対して $y = bxb^{-1}$ となるような $(x, y) \in B_n \times B_n$

出力： $y = a'xa''$ となるような $a', a'' \in B_m$

5 Summit set

5.1 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。

5.2 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。

5.3 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。

5.4 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。

5.5 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。

5.6 inf

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

$$inf(W) = p$$

5.7 inf

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

$$sup(W) = q$$

5.8 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、

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

を満たす集合は有限集合である。更に、

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

を満たすものを super summit set という。

6 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 ←紐の本数
  first_delta ←標準形の作成 (1) で作られた δ
  second_delta ←標準形の作成 (1) で作られた δ
  i ← 1
    while true
      first_delta ← second_delta(1)
      while i<=k-2 do
        cycling
        標準形の作成 (2)
        second_delta ←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 ←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 ←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 ← 1
    while true
      first_p+q ← second_p+q(1)
      while i<=k-2 do
        decycling
        標準形の作成 (2)
        second_p+q ←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
```

7 実験

7.1 実験内容

松葉氏により紐の本数を５本、語長が１～６０の時のブレイドをランダムに生成し、それに対する summit set の大きさを調べるという実験が行われている。私は語長が１～１０の時に限定しすべての組み合わせを列挙し、それに対する summit set の大きさを調べた。

7.2 実験結果

Max summit size		SUMMIT SET の元の canonical length										
		1	2	3	4	5	6	7	8	9	10	最大
語長	1～5	12	12	18	4							18
	6～10	10	60	104	156	96	120					156
	11～15	12	60	460	728	644	384	378	288	54		728
	16～20	8	120	344	1320	1160	1488	2056	2168	608	364	2168
	21～25	12	120	460	816	1960	2236	1580	1218	1356	1558	2236
	26～30	10	60	260	832	2760	3100	6494	4560	4926	2928	6494
	31～35	10	32	132	756	1848	3286	3682	4442	2034	3072	4442
	36～40			30	438	656	2812	3842	2956	3308	2324	3842
	41～45	8			146	214	2104	990	3644	5356	2208	5356
	46～50					34	44	1272	1832	976	3614	3614
	51～55						250	468	244	1522	678	1522
	56～60								1340	470	450	1340
最大		112	120	460	1320	2760	3286	6494	4560	5356	3614	6494

松葉氏データ

Max summit size		SUMMIT SET の元の canonical length										
		1	2	3	4	5	6	7	8	9	10	最大
語長	1	4										4
	2	6	4									6
	3	8	6	4								8
	4	8	6	6	4							8
	5	12	12	18	6	4						18
	6	10	24	18	24	6	4					24
	7	10	36	43	30	30	6	4				43
	8	6	46	60	63	42	34	6	4			63
	9	2	57	86	83	97	54	42	6	4		97
	10		47	92	81	107	120	66	48	6	4	120
最大		12	57	92	83	107	120	66	48	6	4	120

笠谷データ

7.3 考察

私のデータは全列挙しているはずなので語長が１～１０の時の松葉氏のデータと比べて同じかもしくは大きくならなければならないのに少なくなってしまっている部分がある。
どちらが間違っているのかはわからないが、確認、改善が必要である。

8 今後の課題

- 試作したプログラムの再確認をする
- 語長を増やした場合の全列挙をするとデータが膨大になってしまうので、summit set の大きさが大きくなるデータの取り方を考える

参考文献

[1] D.B.A.Epstein, James W. Cannon, Word Processing in Group,181-209, 1992

[2] 田邉利崇, band generator を用いたブレイドの標準形を構成する新しいアルゴリズムについて, 2003

[3] 松葉正志, ブレイド群における共役問題の計算量について, 2005