



ブレイド群における 共役判定プログラムの試作 A program for conjugacy problem of braids

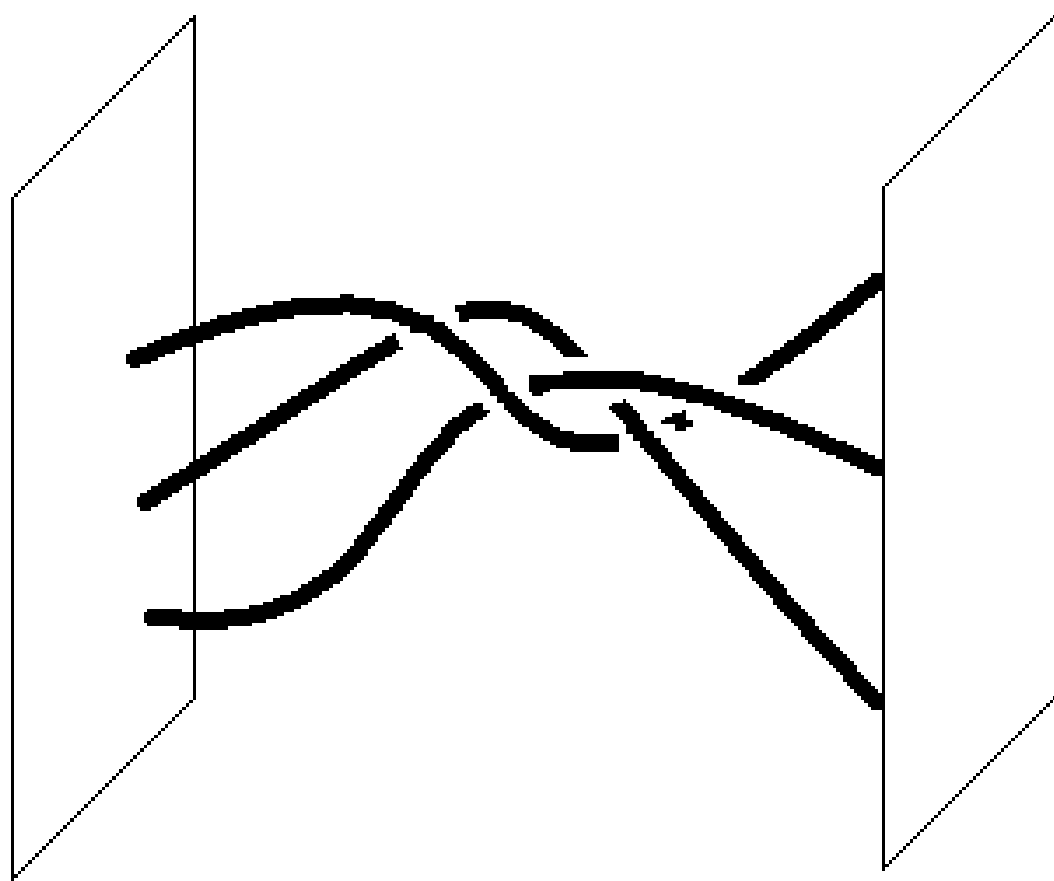
谷聖一研究室
三角哲也



目次

- ブレイドについて
- 基礎的な定義1
- 研究目的
- 基礎的な定義2
- 標準形
- Summit Set
- 実験
- 今後の課題

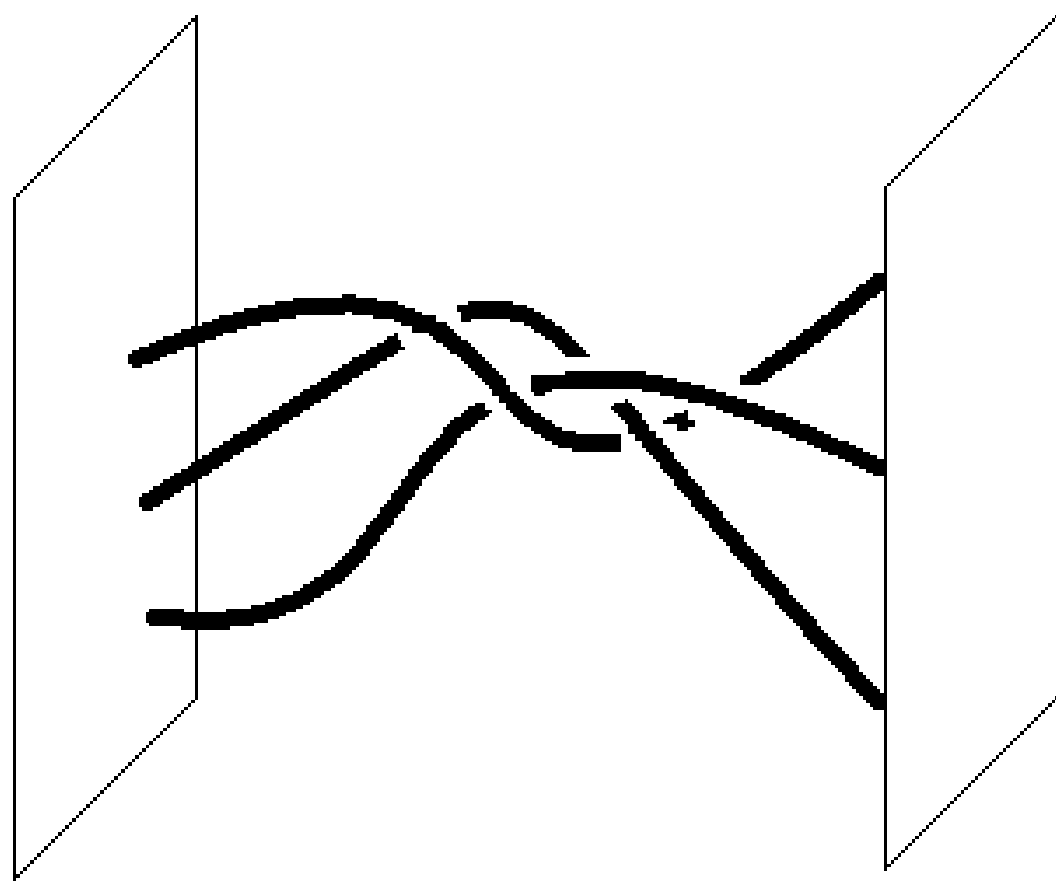
ブレイド(組み紐)について



- 2つの平行な平面に接続する紐からなる集合
- 右から1つの紐をたどると必ず左につく



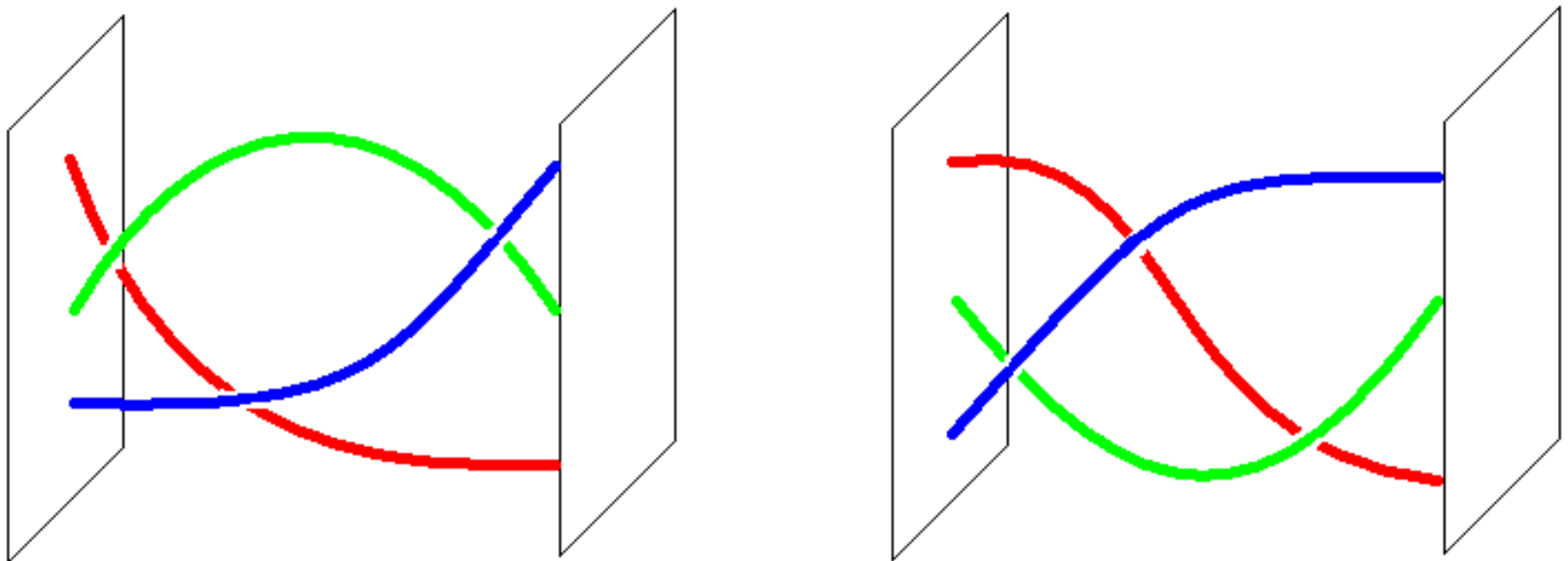
ブレイドについて



- 紐を切ることとは出来ない
- 両端を固定したまま紐を自由に移動できる



ブレイドの同値

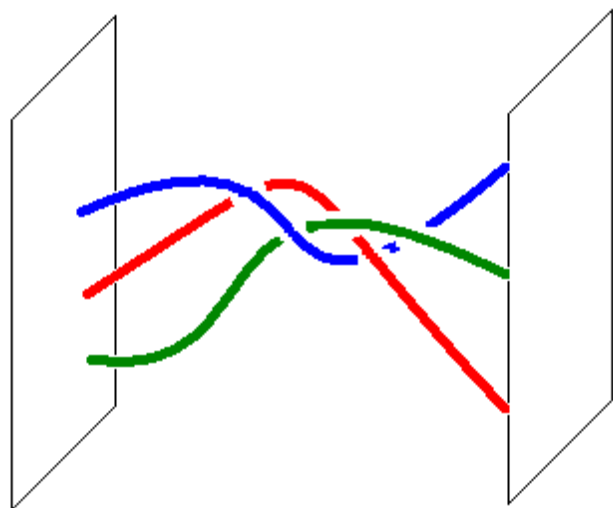


紐の両端を固定したまま, 紐を伸び縮みできる

交差する位置について
別の表現に変形できるとき
同値なブレイドと見なす

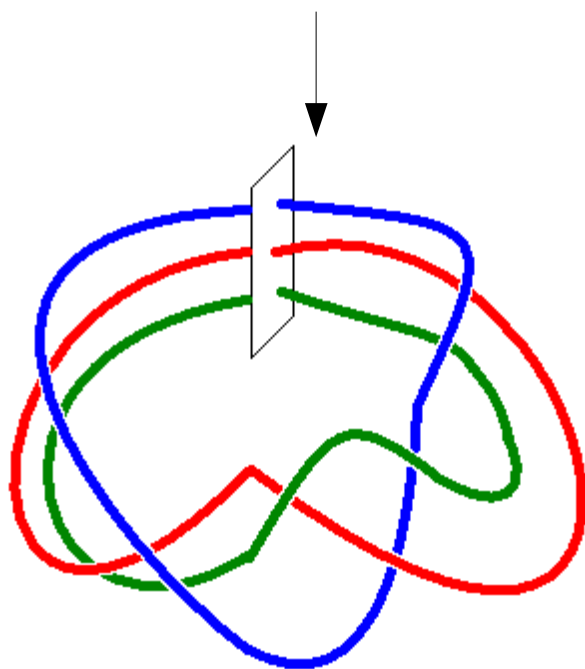


ブレイドについて



○平面の紐の出ていない
面同士を重ねて

“**閉じた組み紐**” を作れる
(結び目, 絡み目との関連)



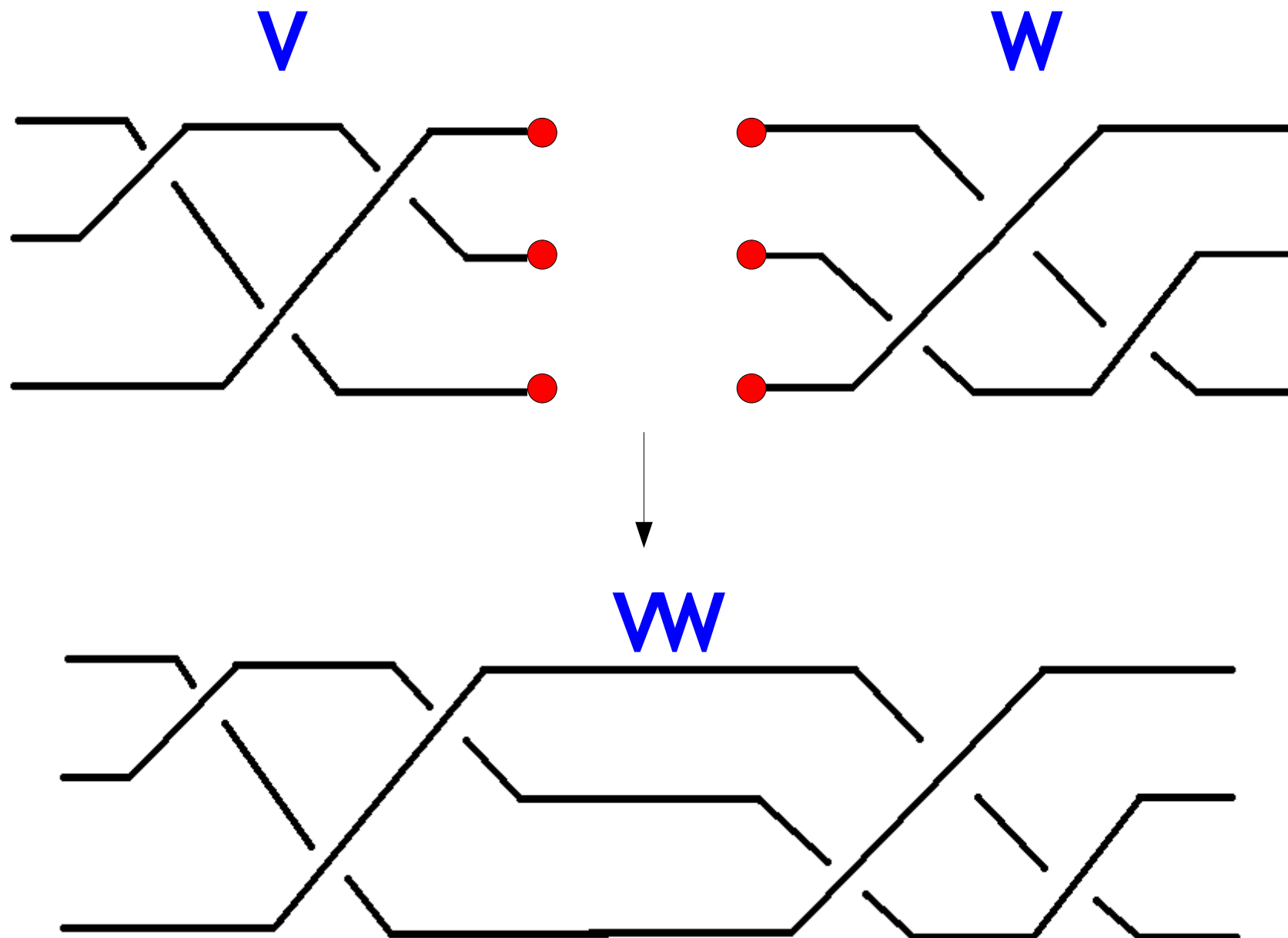
○特定の条件を利用した
公開鍵暗号が提案されている



目次

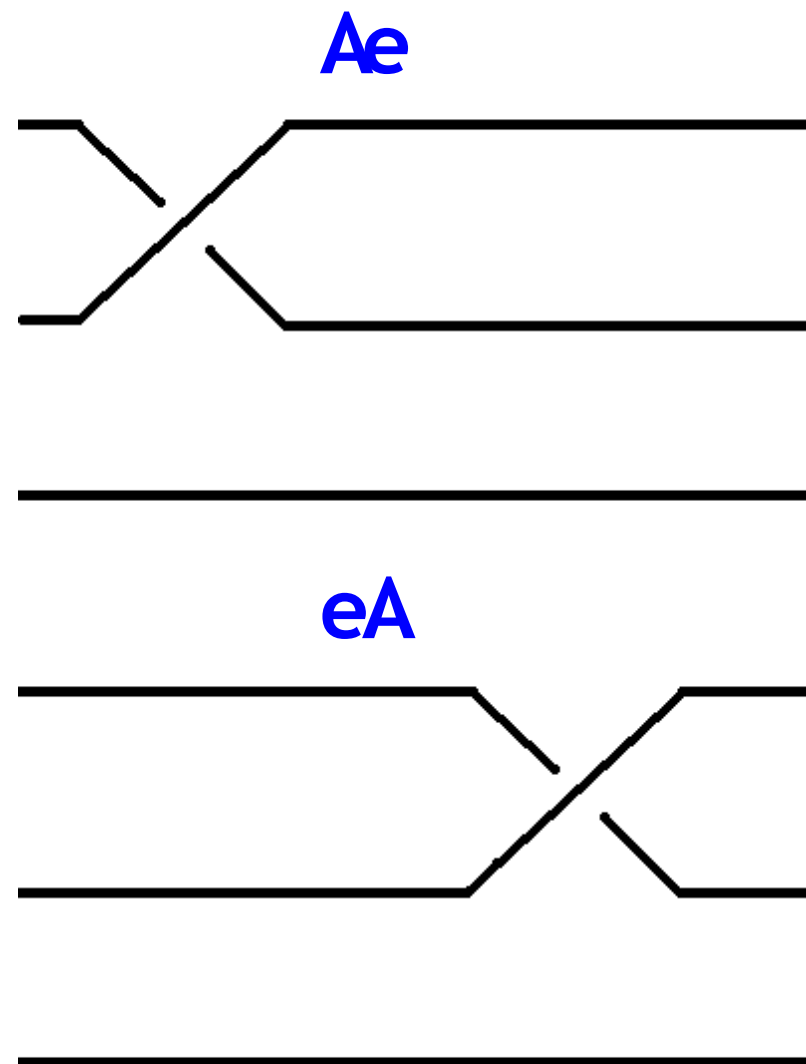
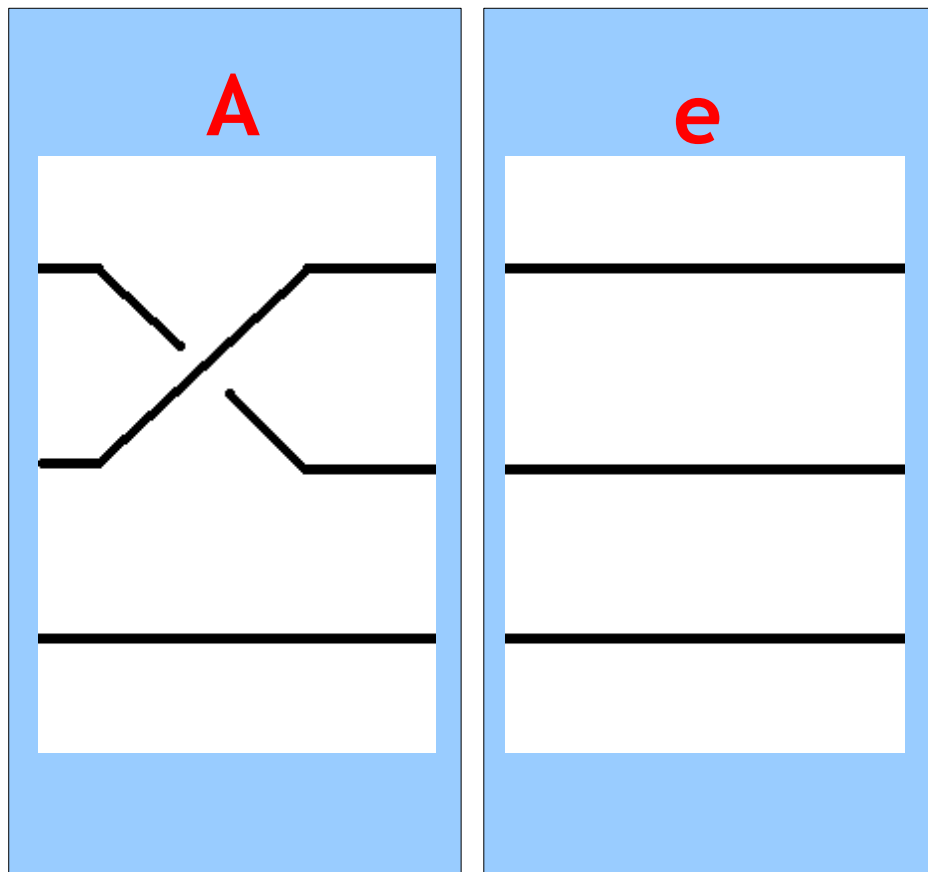
- ブレイドについて
- **基礎的な定義1**
- 研究目的
- 基礎的な定義2
- 標準形
- Summit Set
- 実験
- 今後の課題

積の定義



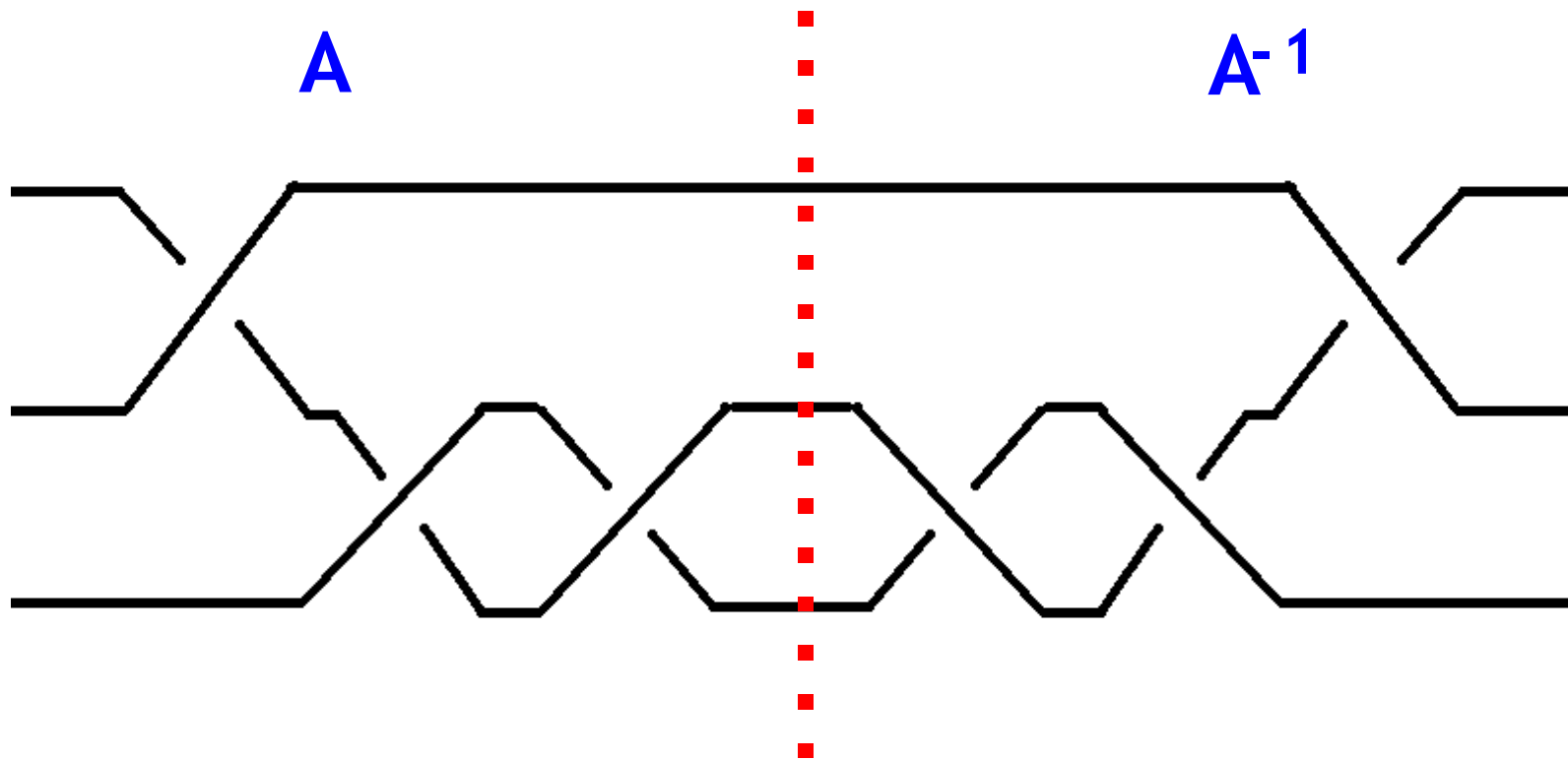
単位元の定義

どの紐も交差しないブレイドを e とする
この e が単位元になる



逆元の定義

$AA^{-1} = A^{-1}A = e$ となる A^{-1} がある
この A^{-1} が A の逆元になる





目次

- ブレイドについて
- 基礎的な定義1
- **研究目的**
- 基礎的な定義2
- 標準形
- Summit Set
- 実験
- 今後の課題



研究目的

2000年に K.H.Ko, S.J.Lee らによって
ブレイド群を利用した公開鍵暗号が提案される

公開鍵暗号

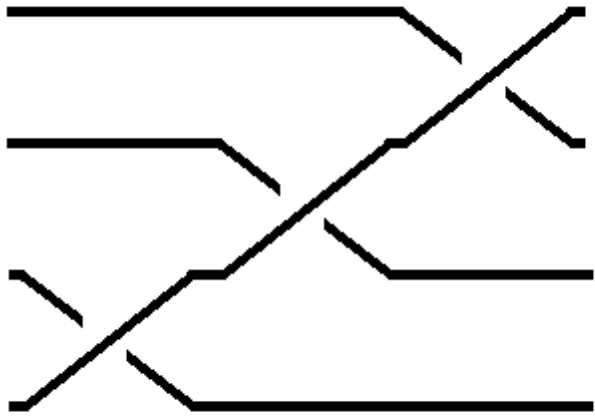
暗号化は容易だが、復号化が困難
2つのブレイドが共役かどうかを判定する問題

本当に難しいかどうかは証明されていない
素因数分解の難しさ

ブレイド群

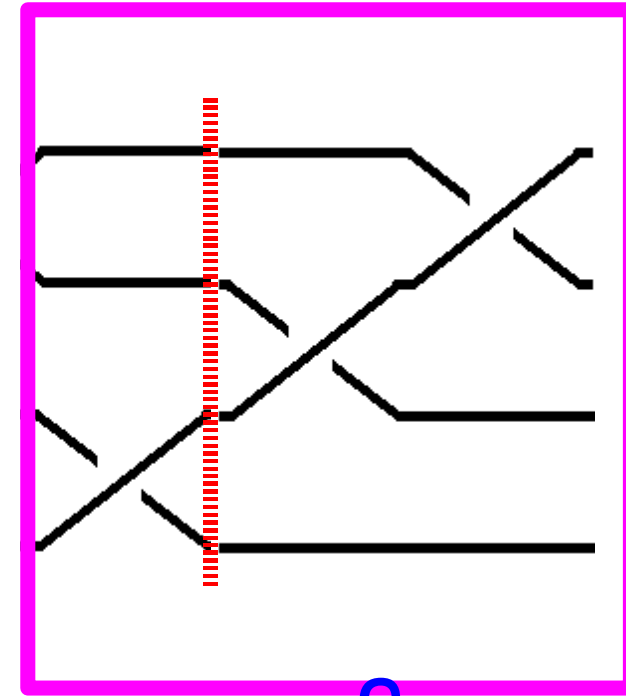
共役 ($W = C^{-1}VC$)

研究目的



W

a^{-1}



V

a

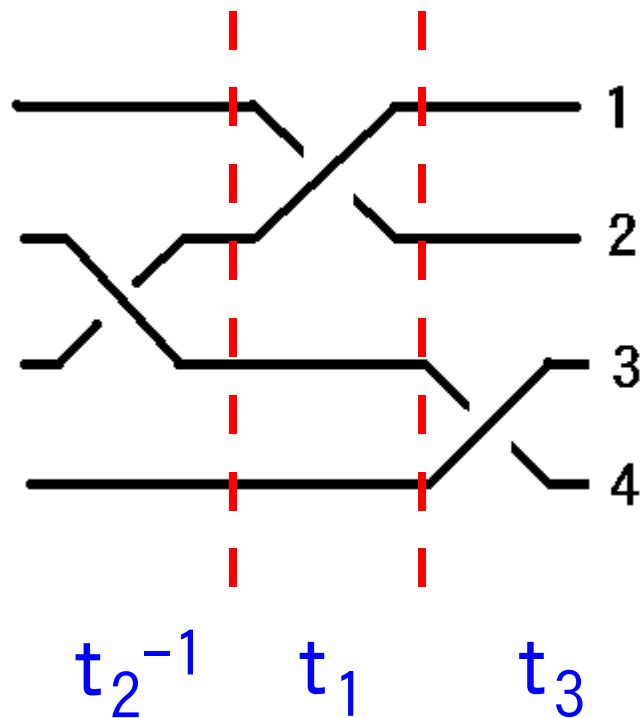
$\Rightarrow$ は a を見つけるのが難しいと思われる
 $(\exists a \in B_n)$



目次

- ブレイドについて
- 基礎的な定義1
- 研究目的
- **基礎的な定義2**
- 標準形
- Summit Set
- 実験
- 今後の課題

生成元



- ・ 紐は上から1段目, 2段目, ... と数える

- ・ i 段目と $i+1$ 段目で交わっていれば、

i 段目の紐が手前のとき t_i

i 段目の紐が奥のとき t_i^{-1}

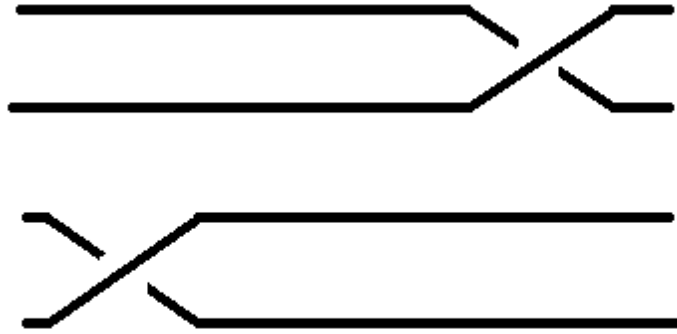
と表す

- ・ ブレイドは生成元とその逆元の積で表現される

→ 文字列として処理可能

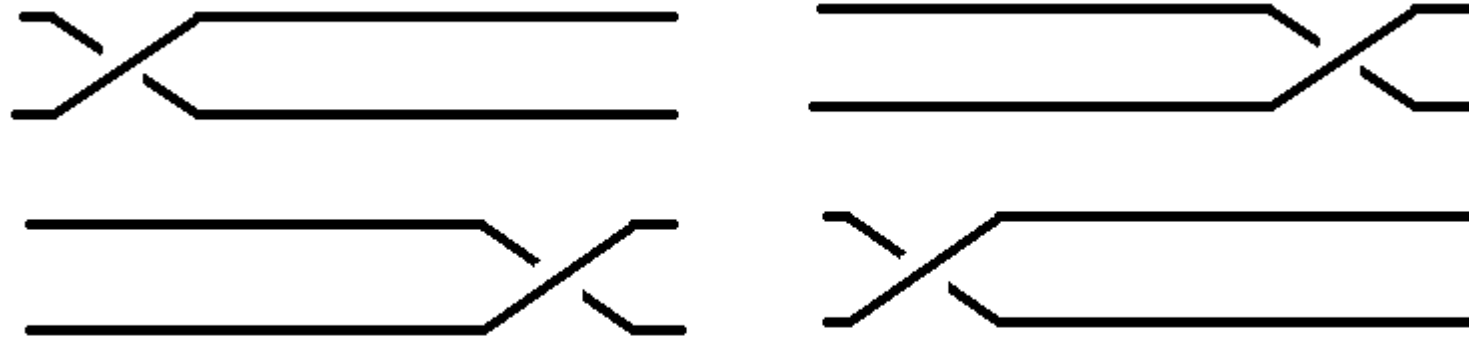


ブレイドの同値（生成元）



と図が交わった部分で端移動出来るため、

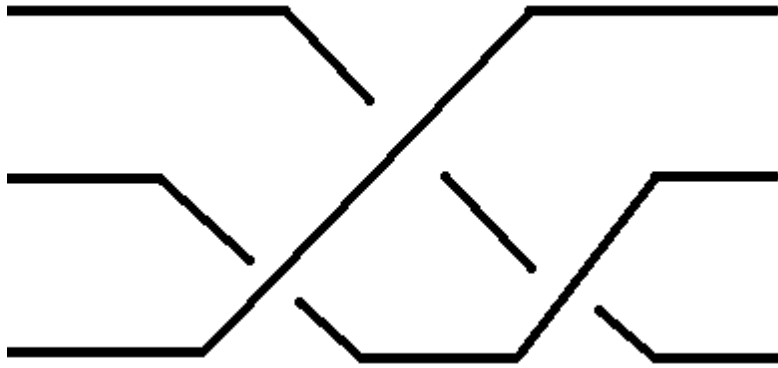
ブレイドの同値 (生成元)



$$t_i t_j = t_j t_i \quad \text{if } |i-j| > 1. \quad (\text{式1})$$

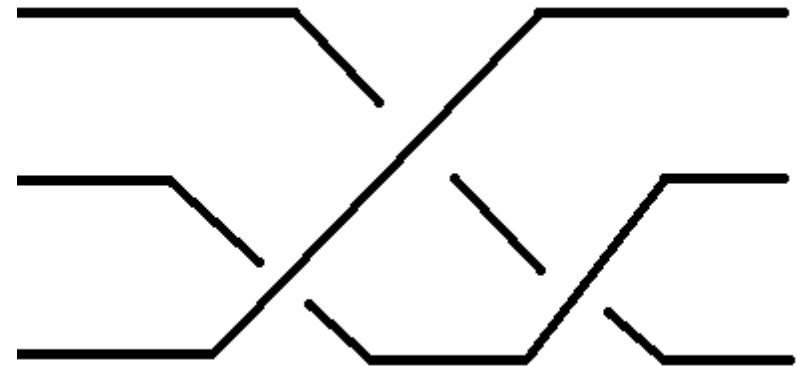
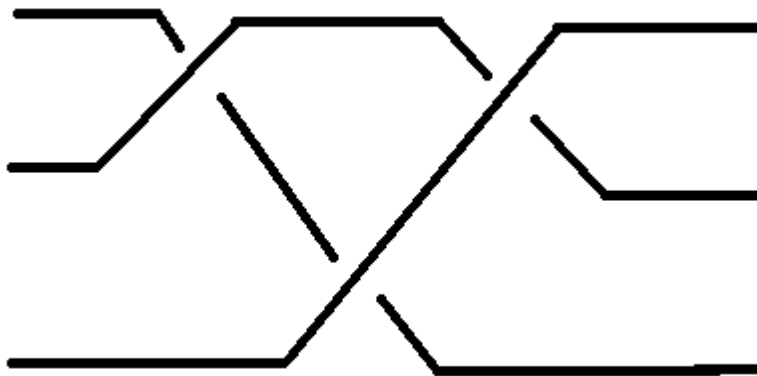
上の式が成り立つ

ブレイドの同値 (生成元)



図を移動出たのブレイドは

ブレイドの同値 (生成元)



$$t_i t_{i+1} t_i = t_{i+1} t_i t_{i+1} \quad (\text{式2})$$

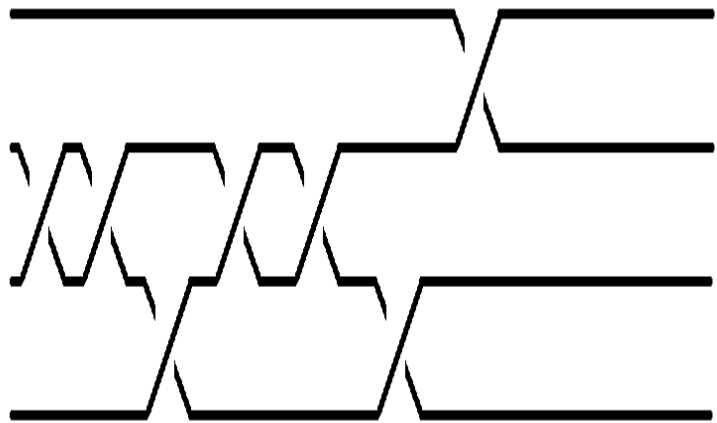
上の式が成り立つ

ブレイドの同値 (生成元)

$$t_i t_j = t_j t_i$$

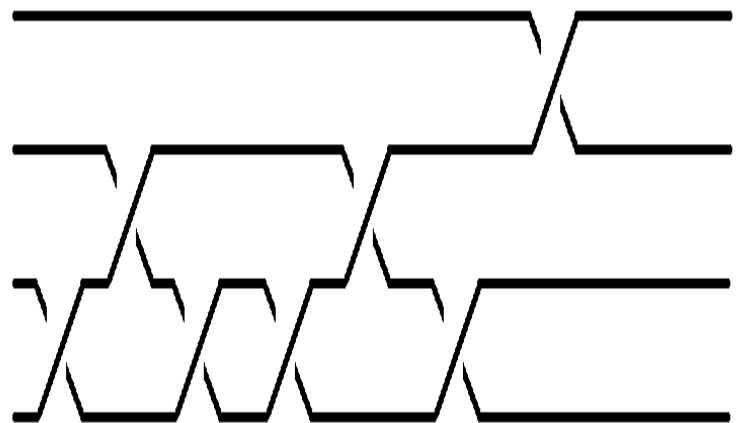
$$\text{if } |i-j| > 1. \quad (\text{式1})$$

$$t_i t_{i+1} t_i = t_{i+1} t_i t_{i+1} \quad (\text{式2})$$



A

有限回



B



目次

- ブレイドについて
- 基礎的な定義1
- 研究目的
- 基礎的な定義2
- **標準形**
- Summit Set
- 実験
- 今後の課題

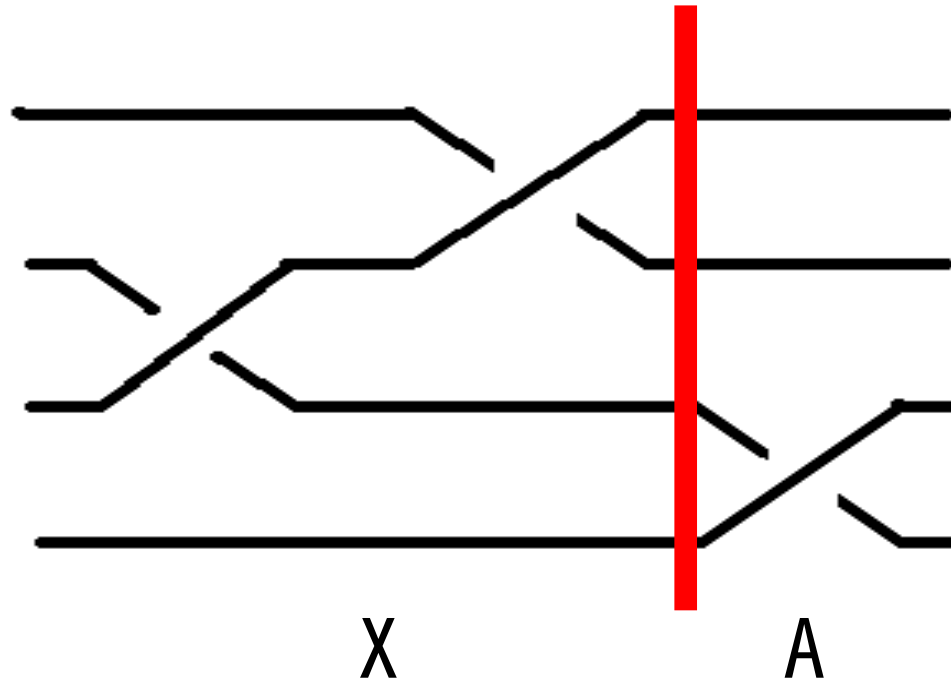
分割

<非冗長ブレイド>

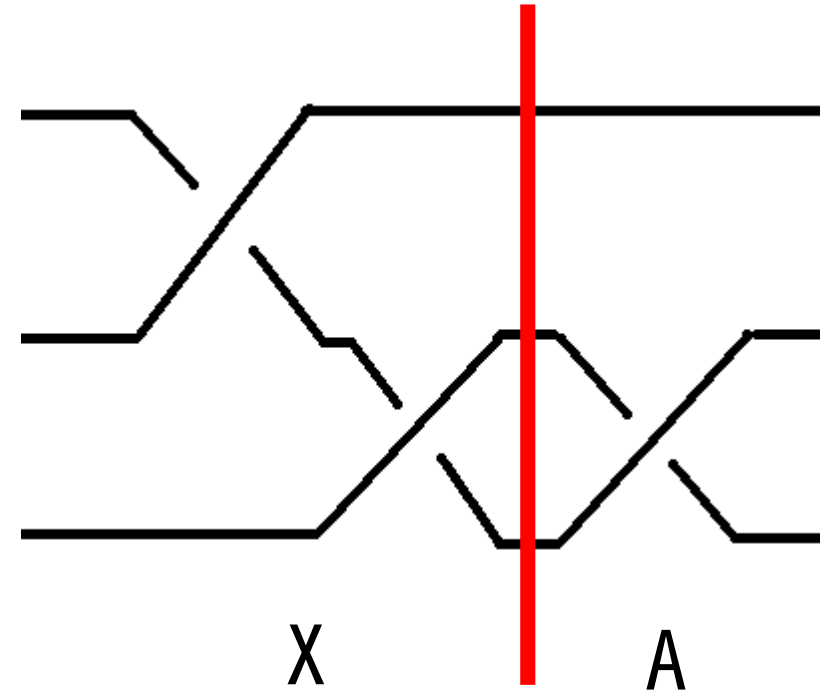
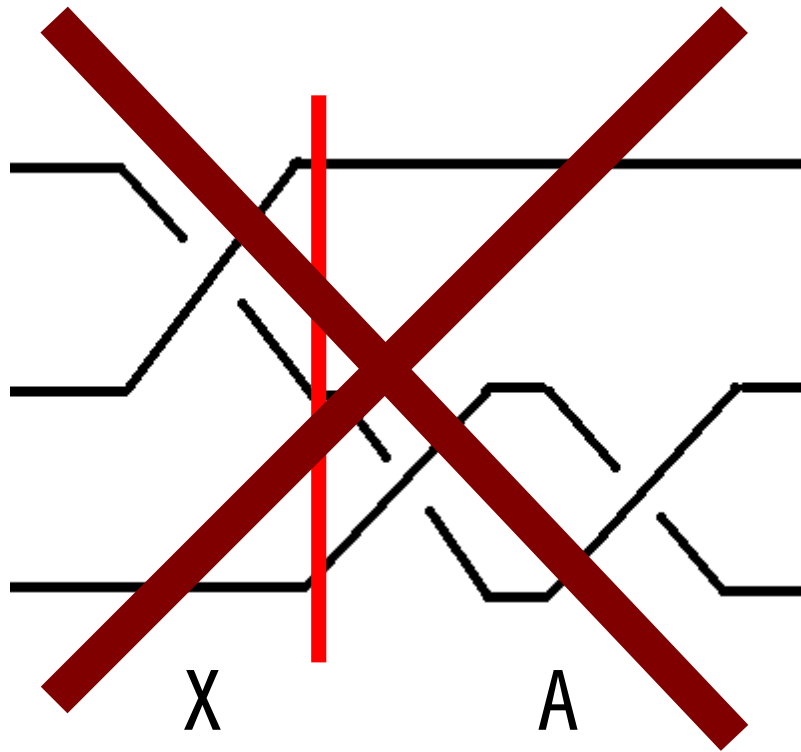
B_n^+ の中で
どの紐のペア
も高々1回だけ
交差するもの

$X \in D_n$, $A \in B_n^+$ で
 $P = XA$ となるとき、
 XA を P の分割という

<正ブレイド>
 t_i^{-1} を含まない
ブレイド



Left-weighted



P の分割 XA が Left-weighted であるとは,
 $P \in B_n^+$ の 任意の分割 $X'A'$ に対して,
 $X' \leq X$ となるとき
をいい, $X \lhd A$ と表す。

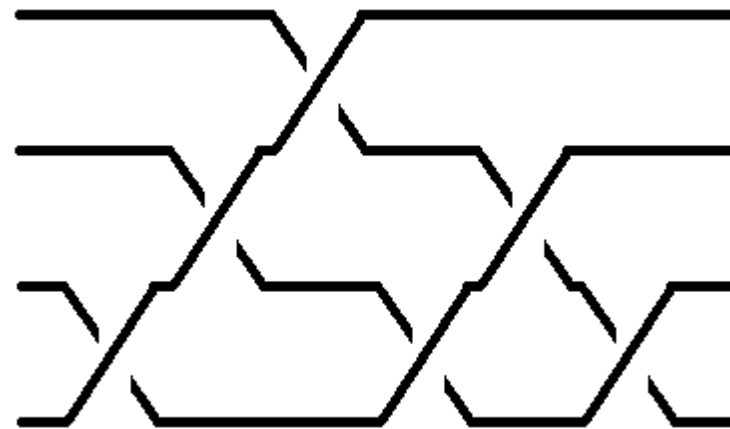


基本ブレイド

どの二本の紐もちょうど1回だけ交差するブレイド

- 紐が4本 のとき

$$\begin{aligned}\Omega &= t_3 t_2 t_3 t_1 t_2 t_3 \\ &= t_3 t_2 t_1 t_3 t_2 t_3 \\ &= \dots\end{aligned}$$



Ω の例

標準形

$W \in B_n$, $p \in \mathbb{Z}$, $A_1 A_2 \dots A_q \in D_n$ として,
次のような表現になっているものを標準形と呼ぶ

$$W = \Omega^p A_1 A_2 \dots A_q$$

(ただし、 $1 < i < q-1$ について $A_i \neg A_{i+1}$)

⇒ 様々な表現のあるブレイドを
一意に表現可能

- 標準形を作る効率的なアルゴリズムが発見されている
- 標準形が最短とは限らない



目次

- ブレイドについて
- 基礎的な定義1
- 研究目的
- 基礎的な定義2
- 標準形
- **Summit Set**
- 実験
- 今後の課題

summit set

$C(V)$ 無限集合

$C^{\text{sum}}(V)$ 有限集合

$\inf(W)$ が最大

かつ

$\sup(W)$ が最小

V と W が共役

$$W = C^{-1}VC \quad (\exists C \in B_n)$$

V と共役なブレイドの集合: $C(V)$

V の summit set

$$(W \text{ の標準形}) \quad W = \Omega^p A_1 \dots A_q$$

$$\inf(W) = p, \quad \sup(W) = p+q$$

$$C^{\text{sum}}(V) :=$$

$$W \in C(V):$$

$$\inf(W) = \max \{ \inf(W') : W' \in C(V) \}$$

かつ

$$\sup(W) = \min \{ \sup(W') : W' \in C(V) \}$$



cycl ing, decycl ing

$$\tau(W) = \Omega^{-1}W\Omega, \quad \tau^{-1}(W) = \Omega W\Omega^{-1} \quad \text{とする}$$

V の標準形が $V = \Omega^p W_1 W_2 \cdots W_q$ のとき、

cycl ing

$$\text{cyc}(V) = \Omega^p \bigcirc W_2 \cdot \cdot \cdot W_q \tau^{-p}(W_1)$$

decycl ing

$$\text{decyc}(V) = \Omega^p \tau^p(W_q) W_1 \cdot \cdot \cdot W_{q-1} \bigcirc$$

cycl ing を繰り返すことで $\inf(V)$ が増加

decycl ing を繰り返すことで $\sup(V)$ が減少

$\Rightarrow V$ の summit set の元の一つが求まる

Summit Set の元を 1 つ求める

(INPUT) $W \in B_n$

(OUTPUT) W の summit set の元の一つ

```
1:  i ← 1
2:  while i ≤ |Ω| - 1 do
3:    W ← cyc(W).
4:    i ← i + 1.
5:  od
6:  i ← 1
7:  while i ≤ |Ω| - 1 do
8:    W ← decyc(W).
9:    i ← i + 1.
10: od
11: return W
```

(2005, 松葉 正志)



Summit Set

V_1 と V_2 は共役である $\Leftrightarrow C^{\text{sum}}(V_1) = C^{\text{sum}}(V_2)$

V_1 と V_1 は共役ではない $\Leftrightarrow C^{\text{sum}}(V_1) \cap C^{\text{sum}}(V_2) = \emptyset$

Summit set の二つの元の共役判定

(INPUT) $V' \in C^{\text{sum}}(V)$, $W' \in C^{\text{sum}}(W)$
(OUTPUT ACCEPT もしくは REJECT

```
1: if  $\inf(V') \neq \inf(W')$  or  $\sup(V') \neq \sup(W')$ 
2: then return REJECT.
3: repeat
4:   guess  $C \in D_n$ .
5:   if  $C^{-1} V' C \in C^{\text{sum}}(V)$ .
6:   then  $V' \leftarrow$  標準形の  $C^{-1} V' C$ .
7:   else return REJECT.
8:   until  $V' \equiv W'$ 
9: return ACCEPT.
```

(2005, 松葉 正志)



目次

- ブレイドについて
- 基礎的な定義1
- 研究目的
- 基礎的な定義2
- 標準形
- Summit Set
- **実験**
- 今後の課題



実験

2004 年、松葉氏により

紐の本数:5 本, ブレイドの長さ:1~ 60

ランダムにブレイドを入力し、

その summit set の大きさを調べる実験が行われている。

それに対し、

紐の本数:5本, ブレイドの長さ:1~10

ブレイドを全列挙して入力し、

その summit set の大きさを調べる実験を行った。

結果

		SUMMIT SET の元の canonical length										
Max summit size		1	2	3	4	5	6	7	8	9	10	最大
	1～5	12	12	18	4							18
	6～10	10	60	104	156	96	120					156

(2004 松葉正志)

		SUMMIT SET の元の canonical length										
Max summit size		1	2	3	4	5	6	7	8	9	10	最大
語長	1	2	0	0	0	0	0	0	0	0	0	2
	2	6	2	0	0	0	0	0	0	0	0	6
	3	10	3	2	0	0	0	0	0	0	0	10
	4	10	11	3	2	0	0	0	0	0	0	11
	5	12	16	10	3	2	0	0	0	0	0	16
	6	8	17	15	10	3	2	0	0	0	0	17
	7	8	25	16	15	10	3	2	0	0	0	25
	8	6	34	33	16	15	10	3	2	0	0	34
	9	4	39	40	33	16	15	10	3	2	0	40
	10	0	30	49	40	33	16	15	10	3	2	49
最大		12	39	49	40	33	16	15	10	3	2	49



実験結果と考察

- ・ 全列挙しているので、語長が1～10 のときの松葉氏のデータの値と同じかより大きくなるはず
- ・ 値が小さくなってしまう部分がある
- ・ 松葉氏のプログラムと比較検討する必要がある。



目次

- ブレイドについて
- 基礎的な定義1
- 研究目的
- 基礎的な定義2
- 標準形
- Summit Set
- 実験
- **今後の課題**



今後の課題

●summit set が大きくなるようなデータの取り方を考える

理由: 語長を増やした場合で全列挙しようとする
とデータが膨大になる



終わり

ご清聴有り難うございました