band generator を用いたブレイドの標準型を構成するアルゴリズム

A-23

A polynomial-time algorithm for constructing band generator

田邊 利崇* 原 正雄† 山本 慎‡ 谷 聖一§
Toshitaka Tanabe Masao Hara Makoto Yamamoto Sei'ichi Tani

1 はじめに

K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J. Kang, C. Park [5] がブレイド群における共役問題の難しさに安全性の拠り所をお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．M.S. Paterson と A.A. Razborov [6] により，与えられたブレイドが最短表現かを判定する問題は co-$\mathcal{NP}$ 完全であることが示されている．一方，W.Thurston[3] は，多項式時間で構成可能な標準型を提案し，等価性判定問題が多項式時間で解けることを示した．E.S. Kang, K.H. Ko, S.J. Lee [4] は，紐の交差を複数まとめた生成元である band generator という概念と，この生成元を用いた表現に対する標準型を提案し，紐の本数が 4 本に限定された場合の共役問題が多項式時間で解けることを示した．さらに，J.S. Birman, K.H. Ko, S.J. Lee [1, 2] は，紐の本数が k 本に限定された場合に，W を任意のブレイドとし，$\delta^u A_1 A_2 \cdots A_p$ を W の標準型とするとき，この標準型を $\mathcal{O}(|W|^2 p)$ 時間で構成するアルゴリズムを示した．これに対して本研究では，$\mathcal{O}(|W|^2)$ 時間で W の標準型を構成するアルゴリズムを提案する．

2 ブレイド群に関する定義と性質

ブレイド (*braid*；組み紐) とは，2 つの平行な平面に接続した n 本の紐からなる集合のことである．左側の棒から右側の棒へ 1 本の紐をたどってゆくと，紐はいつでも右方向へ向かっている．2 つのブレイド V, W が **同値**とは，V の端点を固定し，左右の平面によって囲まれた空間から**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ときをいう．これを $V \equiv W$ と表すことにする．ここで，次のように積を定義する．任意のブレイド 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この演算に関してブレイドは群をなし，ブレイド群という．どの紐も 1 度も交差しないブレイド e はブレイド群の**単位元**となる．

σ_i を i 番目の紐と $i+1$ 番目の紐を 1 度だけ入れ替えたブレイドとする．ただし，交点の上下関係は負の傾きを持つ紐が上側にくるようにする．また，σ_i^{-1} は σ_i の紐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．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**という．

Artin の生成元は 1 つの紐の交差に対応しているが，E.S.Kang, K.H.Ko, S.J.Lee [4] により，複数の紐の交差を一まとめにした生成元 **band generator** が提案されている．

*東急バス株式会社
†東海大学理学部情報数理学科
‡中央大学理工学部数学科
§日本大学文理学部情報システム解析学科

$n \geq t > s \geq 1$ のとき，band generator a_{ts} を

$$a_{ts} = (\sigma_{t-1}\sigma_{t-2}\cdots\sigma_{s+1})\sigma_s(\sigma_{s+1}^{-1}\cdots\sigma_{t-2}^{-1}\sigma_{t-1}^{-1})$$

と定義する．これは，t 番目と s 番目の紐を他の紐の上で交差させたものであり（図 1），$\sigma_i = a_{(i+1)i}$ であることに注意．また，band generator の集合を BG_n と表す．

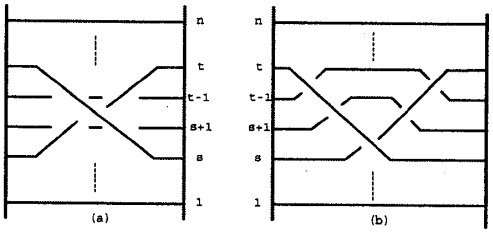

図 1: (a)：a_{ts} (b)：$(\sigma_{t-1}\cdots\sigma_{s+1})\sigma_s(\sigma_{s+1}^{-1}\cdots\sigma_{t-1}^{-1})$

BG_n の元とその逆元が生成するブレイドの群を BB_n と表す．また，正整数のベキ乗をもつ band generator のみで生成される BB_n の元を BB_n における**正ブレイド** といい，そのブレイド全体がなす半群を BB_n^+ と表す．

性質 1 ([1])
BG_n の各生成元 $\{a_{ts} \mid n \geq t > s \geq 1\}$ は，以下の性質を持つ．

1. $(t-r)(t-q)(s-r)(s-q) > 0$ のとき $a_{ts}a_{rq} \equiv a_{rq}a_{ts}$
2. $\forall t, s, r, (n \geq t > s > r \geq 1)$ のとき $a_{ts}a_{sr} \equiv a_{tr}a_{ts} \equiv a_{sr}a_{tr}$
3. $|t-s| > 1$ のとき $a_{t(t+1)}a_{s(s+1)} \equiv a_{s(s+1)}a_{t(t+1)}$
4. $|t-s| = 1$ のとき $a_{t(t+1)}a_{s(s+1)}a_{t(t+1)} \equiv a_{s(s+1)}a_{t(t+1)}a_{s(s+1)}$

任意の BB_n のブレイド W に対し，$\|W\|$ で W を構成している band generator の数を表すものとする．BB_n^+ の元 V, W が**正同値**とは，V に性質 1 の同値関係のみを有限回適用させることで W と一致させることができるときをいう．また，$a_{n(n-1)}a_{(n-1)(n-2)}\cdots a_{21}$ と正同値であるブレイドを **fundamental word** といい δ で表す．

定義 1
BB_n の元に対する半順序 $\leq$ を次のように定める．任意の $V, W \in BB_n$ に対して，BB_n^+ の元 P_1, P_2 が存在して，$W = P_1 V P_2$ となるとき $V \leq W$ とする．また，$r < s$ となる正整数 r, s に対して，BB_n^+ の集合 $[r, s]_n$ を $\{W \in BB_n^+ | \delta^r \leq W \leq \delta^s\}$ で定める．さらに，任意の $[0, 1]_n$ の元を ***canonical factor*** という．

定義 2
$X \in [0,1]_n$ とし，A を $A \geq e$ となる正ブレイドとする．このとき，$P \in BB_n^+$ に対して $P = XA$ となるとき，XA を P の分割という．また，P の分割 XA が ***left-weighted*** であるとは，任意の P の分割 $X'A'$ に対して，$X' \leq X$ となるときをいい，$X \neg A$ で表す．

定義 3
BB_n^+ の任意の元 a, b, c に対して，$ab = c$ のとき，a は c の ***head*** といい，b は c の ***tail*** という．また，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．

定理 2 ([1])
任意の $W \in BB_n$ に対して，$u \in \mathbb{Z}$ と 正ブレイド $A_1, \cdots, A_p \in [0,1]_n$ を用いた $W = \delta^u A_1 A_2 \cdots A_p$ という形式の表現で，$1 \leq i \leq p-1$ 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．

任意の表現 $W \in BB_n$ に対し，W が定理 2 の条件を満たす表現となっているとき **left-canonical form** という．

3 標準型構成アルゴリズム

補題 3
Find_max_head_[1_2] は，入力ブレイド $V \in [1,2]_k$ を V の *maximal head* とその *tail* に定数時間で分割する．

```
<procedure Find_max_head_[1_2]>
(入力) V ∈ [1,2]_k
(出力) V の maximal head とその tail の対 (H,T)

α ← {(V,λ)}
Repeat do
  β ← φ
  for each (H,T) ∈ α do
    H ← Enum_equiv(H)
    for each H' ∈ H do
      x ← H' の最右の band generator
      H'' ← H' から最右の x を取り除いた
            ブレイド
      β ← β ∪ {(H'', xT)}
    od
  od
  for each (H,T) ∈ β do
    if (H ∈ [0,1]_k)  return (H,T)
  od
  α ← β
od
```

定理 4
Find_max_head は，入力ブレイド $V \in BB_k^+$ を V の *maximal head* とその *tail* に線形時間で分割する．

```
<procedure Find_max_head>
(入力) V = x_1 x_2 ··· x_m ∈ BB_k^+
(出力) V の maximal head とその tail の対 (H,T)

H ← x_m,  T ← λ,  i ← 1
while (i < m) do
  H' ← x_{m-i} H
  if (H' ∉ [0,1]_k) do
    (H',T') ← H' の maximal head とその tail
    T ← T'T
  od
  H ← H',  i ← i+1
od
return (H,T)
```

系 5
Canonical_form は，入力ブレイド $V \in BB_k$ の *left-canonical form* を $\mathcal{O}(\|V\|^2)$ 時間で構成する．

```
<procedure Canonical_form>
(入力) V ∈ BB_k
(出力) δ^u A_1 A_2 ··· A_p(= V)   (u ∈ Z , ∀A_i ∈ [0,1]_k)

Stage 0: 同値類の表を作成
Stage 1: V = δ^u P となる u ∈ Z, P ∈ BB_k^+ を構成
Stage 2: T ← P,   i ← 0
         while (T ≠ λ) do
           i ← i+1
           (A_i, T) ← Find_max_head(T)
         od
         return δ^u A_1 A_2 ··· A_i
```

参考文献

[1] Joan S. Birman, Ki Hyoung Ko and Sang Jin Lee, *A new approach to the word and conjugacy problems in the braid groups*, Advances in Mathmatics, **139**, 322-353,1998.

[2] Joan S. Birman, Ki Hyoung Ko and Sang Jin Lee, *The infimum, supremum and geodesic length of a braid conjugacy class*, Advances in Mathmatics to appear.

[3] J. Cannon, D. Epstein, D. Holt, S. Levy, M. Paterson and W. Thurston, *Word Processing in Groups*, Jones & Ballet, 1992.

[4] Eun Sook Kang, Ki Hyoung Ko and Sang Jin Lee, *Band-generator presentation for the 4-braid group*, Topology and its applications **78**, 39-60,1997.

[5] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han,Ju-sung Kang and Choonsik Park, *New Public-key Cryptosystem Using Braid Groups*, Advances in Cryptography — CRYPTO 2000, Lecture Notes in Computer Science 1880, Springer-Verlag, 166-183, 2000.

[6] M.S. Paterson and A.A. Razborov, *The set of minimal braids is co-Np-complete*, J. Algorithm **12** 393-408, 1991.