A FAMILY OF PSEUDO-ANOSOV BRAIDS WITH LARGE
CONJUGACY INVARIANT SETS

BYUNG HEE AN AND KI HYOUNG KO

Abstract. We show that there is a family of pseudo-Anosov braids independently parameterized by the braid index and the (canonical) length whose smallest conjugacy invariant sets grow exponentially in the braid index and linearly in the length and conclude that the conjugacy problem remains exponential in the braid index under the current knowledge.

1. Introduction and Preliminaries

We use the following Artin’s presentation [1] of the group $B_n$ of $n$-braids:

$$B_n = \langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i \sigma_j = \sigma_j \sigma_i \text{ if } |i-j| > 1, \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j \text{ if } |i-j| = 1 \rangle,$$

An $n$-braid in the monoid $B_n^+$ of positive words is a permutation braid if a pair of $n$-strands crosses at most once. The set $S_n$ of permutation $n$-braids is in one-to-one correspondence with the permutation group of $n$ elements. For $\beta \in S_n$, the starting set $S(\beta)$ and the finishing set $F(\beta)$ is given by

$$S(\beta) = \{ i \mid \beta = \sigma_i \beta' \text{ for some } \beta' \in S_n \}, F(\beta) = \{ i \mid \beta = \beta' \sigma_i \text{ for some } \beta' \in S_n \}.$$

The half-twist braid $\Delta$ is the only braid in $S_n$ whose starting and finishing sets are the largest set $\{1, \ldots, n-1\}$. Every $n$-braid can be put into its left canonical form, that is,

$$\beta = \Delta^k \beta_1 \cdots \beta_\ell$$

where $\beta_i \in S_n$ and $F(\beta_i) \supset S(\beta_{i+1})$ for all $i = 1, \ldots, \ell - 1$. The integers $\ell, k,$ and $k + \ell$ are called the canonical length, the infimum, and the supremum of $\beta$, respectively. This decomposition introduced by Garside [7] immediately solves the word problem of $B_n$ and Garside showed that the summit set $SS(\beta)$, the set of all braids with the maximal infimum and conjugate to a $\beta \in B_n$, is finite to give a theoretical solution to the conjugacy problem.

Since then, several smaller sets that are invariant under conjugate have been proposed. Elrifai and Morton [5] studied super summit set $SSS(\beta)$, the set of all braids with the maximal infimum and the minimal supremum and conjugate to $\beta$, and proved that any braid can be pushed into its super summit set through iteration.
of two natural operations on a braid $\beta = \Delta^k \beta_1 \cdots \beta_\ell$ given by its canonical form. The cycling of $\beta$ is given by

$$c(\beta) = \Delta^k \beta_2 \cdots \beta_\ell \tau^k(\beta_1)$$

and the decycling of $\beta$ is given by

$$d(\beta) = \Delta^k \tau^k(\beta_\ell) \beta_1 \cdots \beta_{\ell-1}$$

where $\tau : B_n \to B_n$ be the involution defined by $\tau(\beta) = \Delta^{-1} \beta \Delta$. They also introduce a partial order $\prec$ among positive $n$-braids such that $\alpha \prec \beta$ if $\alpha$ is a prefix of $\beta$, that is, $\alpha \gamma = \beta$ for some $\gamma \in B^+_n$. In his thesis, Lee consider the reduced super summit set $RSSS(\beta)$ of all braids conjugate to $\beta$ and fixed by iterated cycling and decycling. On the other hand, Franco and González-Meneses [6] gave a practical algorithm to generate $SSS(\beta)$ by using the following lattice structure on $S_n$ with respect to the partial order $\prec$. Given $\gamma_1, \gamma_2 \in S_n$, the meet $\gamma_1 \wedge \gamma_2$ is the maximal common prefix of $\gamma_1$ and $\gamma_2$ and the join $\gamma_1 \vee \gamma_2$ is the minimal braid that has prefixes $\gamma_1$ and $\gamma_2$, and two operations can be extended over $B_n^+$. In fact, they showed that the meet operation $\wedge$ is closed among conjugators of $\beta$ that produce elements in $SSS(\beta)$ and so there are minimal conjugators moving around $SSS(\beta)$. Gebhardt [8] proposed the ultra summit set $USS(\beta)$ that collects all braids in $SSS(\beta)$ and fixed by iterated cycling and proved that the algorithm using minimal conjugators also works to generate $USS(\beta)$. Finally, Gebhardt and González-Meneses [9, 10] introduced a new conjugation operation called a cyclic sliding and considered the set $SC(\beta)$, called the sliding circuit, of orbits of $\beta$ under the operation. These finite conjugacy invariant sets of a given braid $\beta$ in general satisfy

$$SC(\beta) \subset RSSS(\beta) \subset USS(\beta) \subset SSS(\beta) \subset SS(\beta).$$

A braid $\beta = \Delta^k A_1 \cdots A_\ell$ given in canonical form is rigid if $\ell \geq 2$ and $F(A_1) \supset S(\tau^k(A_1))$. If a braid $\beta$ is conjugate to a rigid braid $\alpha$, then $\alpha \in RSSS(\beta)$ and moreover it was shown in [3, 9, 13] that $SC(\beta) = RSSS(\beta) = USS(\beta) = R(\beta)$ where $R(\beta)$ denotes the set of all rigid braids conjugate to $\beta$. When the canonical length $\ell$ is 1, cycling and decycling is meaningless. If we assume that the rigidity requires $F(A_1) \supset S(\tau^k(A_1))$ in this case, one can show that $SC(\beta) = SSS(\beta) = R(\beta)$. For a rigid braid $\beta$, $R(\beta)$ is the smallest among invariant conjugacy sets of $\beta$ under current knowledge and will be called the rigid conjugacy set of $\beta$.

As a self-homeomorphism on $n$-punctured 2-disk, an $n$-braid $\beta$ is of one of the following three dynamic types known as Nielsen-Thurston classification [19]: (1) $\beta$ is periodic if some power of $\beta$ is isotopic to some power of Dehn twist along the boundary of disk; (2) $\beta$ is reducible if there exists a family of pairwise disjoint essential non-peripheral simple closed curves in $D_n$, called reduction system, which is preserved by a $n$-braid isotopic to $\beta$; (3) $\beta$ is pseudo-Anosov is neither (1) nor (2).

The conjugacy problem for periodic braids is relatively easy [11, 4]. For reducible braids, once the reduction system is known, the conjugacy problem can be reduced into several pieces, which are for either periodic or pseudo-Anosov braids. It is reasonable to say that the conjugacy problem for pseudo-Anosov braids is essential.

If a reduction system consists of circles that intersect the axis containing all punctures exactly twice, then it is called a standard reduction system. Bernardete, Nitecki and GuitierrezIt [2] showed that cycling and decycling operations retain a
standard reduction system and so $RSSS(\beta)$ must contain a braid with a standard reduction system if $\beta$ is reducible. This also implies that if a braid has a standard reduction system then each factor of its canonical form retain a standard reduction system and so a standard reduction system can be detected in polynomial time [15].

For pseudo-Anosov braids, Masur and Minsky [16, 17] showed that there exists a constant $K$ which depends only on the braid index $n$ such that for any conjugate $\alpha, \beta \in B_n$, there exists a conjugator $\gamma$ satisfying $|\gamma| \leq K(|\alpha| + |\beta|)$. Even though their proof leaves no clue how to find such $\gamma$, the conjugacy problem for pseudo-Anosov braids seems to have a low complexity in length. On the other hand, Ko and Lee in [13] and Birman, Gebhardt and González-Meneses in [3] independently proved that a pseudo-Anosov braid becomes rigid up to taking power and cycling. We remark that the exponent of the power needed has an upper bound that is a polynomial only in the braid index but the number of cycling required is unknown even though it is relatively small on computer experiment. Consequently, the conjugacy problem for pseudo-Anosov braids boils down to that for rigid pseudo-Anosov braids. For rigid braids, the complexity of the current best solution ultimately relies on the size of the rigid conjugacy set of an input braid.

In this article, we show that there is a family of pseudo-Anosov braids independently parameterized by the braid index and the (canonical) length whose rigid conjugacy sets grow exponentially in the braid index and linearly in the length and conclude that the conjugacy problem remains exponential in the braid index under current knowledge. Our strategy is to construct a family of rigid $n$-braids of canonical length $k$ from the set of $k \times \lfloor \frac{n}{2} \rfloor$ binary matrices. Then we show that each member of the family carries no standard reduction system and the rigid conjugacy set of each member is a subset of the family and therefore each member is pseudo-Anosov. Finally we compute the size of the rigid conjugacy set of each member and conclude that the size of the rigid conjugacy set of a well chosen member is still exponential in $n$.

There have been some results relevant to our work. Prasolov [18] constructed a family of rigid pseudo-Anosov $n$-braids of canonical length $n$ whose rigid conjugacy sets grow exponentially in $n$. This family obviously has the limitation that the canonical length depends on the braid index. On the other hand, González-Meneses in [12] constructed a family of reducible $n$-braids of canonical length $k$ whose sliding circuits grow exponentially in both $n$ and $k$.

2. Braids corresponding to binary matrix

Let $\{0, 1\}^p$ be the set of binary $p$-tuples and $\mathbf{a} \in \{0, 1\}^p$. Using the four building blocks $\alpha_I, \alpha_0, \alpha_1$ and $\alpha_T$ depicted in Figure 1, we construct a braid $\alpha(\mathbf{a})$ for a given $\mathbf{a} = (a_1, \ldots, a_p) \in \{0, 1\}^p$ by gluing adjacent blocks together by identifying circled crossings in the row $\alpha_I, \alpha_{a_1}, \ldots, \alpha_{a_p}, \alpha_T$ of building blocks. Then $\alpha(\mathbf{a})$ is a positive $(2p + 2)$-braid of $4p + 1$ crossings in which every pair of strands crosses each other at most once. This can be seen, for example, by the fact that every strand can be drawn by a straight line. Thus $\alpha(\mathbf{a})$ is a permutation braid and we obtain a function $\alpha : \{0, 1\}^p \to S_{2p+2}$. Figure 2 shows the braid $\alpha(0, 1, 1, 0, 0, 1)$.

For any permutation braid $\beta$, we consider the induced permutation $\pi(\beta)$ defined by $\pi(\beta)(i) = j$ when $i$-th strand in $\beta$ ends at $j$-th position. Unless confusion arises, we simply use the notation $\beta$ for $\pi(\beta)$ so that $\beta(i) = j$ whenever $\pi(\beta)(i) = j$. 
For $a \in \{0, 1\}^p$, the set of transposing indices $T(a)$ of $a$ consists of all $1 \leq i \leq 2p+2$ such that $|a(i) − i| = 1$. For example, $T(0, 1, 1, 0, 0, 1) = \{3, 4, 6, 9, 11, 12\}$ and the thicker strands in Figure 2 correspond to transposing indices. For each $i \in T(a)$, the $i$-th strand has no circled crossing in the braid $a$. For instance, in Figure 2, the $1$-th strand has no circled crossing in the braid $a$ and the thicker strands in Figure 2 correspond to transposing indices. For each $i \in T(a)$, $i$-th strand cross the strand that ends at the $i$-th puncture in $a$. For any $i \in T(a)$, $i$-th strand corresponds to the transposing indices $T(a)$ and renumbering indices as $\{1, 2, 4, \cdots, 2p, 2p+1\}$ in order. For example, in Figure 2, $\vartheta(a) = (2, 8, 10, 13, 12, 6, 4, 1)$ written as a cycle.

The following Lemma states basic properties of $\alpha(a)$ that can be easily derived from the picture of $\alpha(a)$ using building blocks.

**Lemma 2.1.** For $a \in \{0, 1\}^p$ with $p \geq 2$, let $\vartheta = \vartheta(a)$. Then the following holds.

1. For any $i$, the $i$-th strand cross the strand that ends at the $i$-th puncture in $\alpha(a)$. 
2. If $a_i = 0$ and $\vartheta(2i) = 2j$, then $j$ is the smallest index $j$ such that $i < j$ and $a_j = 0$. 
3. The permutation $\vartheta$ is always a cycle of length $(p + 2)$.

For positive integers $k$ and $p$, let $M_{k,p}(\{0, 1\})$ denote the set of all $k \times p$ matrices over $\{0, 1\}$. For $A \in M_{k,p}(\{0, 1\})$, let $A_i$ and $A^j$ denote the $i$-th row vector and the $j$-th column vector of $A$, respectively. And let $0$ and $1$ denote the column vectors that consist of all $0$'s and all $1$'s, respectively. We extend the function $\alpha$ over $M_{k,p}(\{0, 1\})$ via braid multiplication, that is, 
\[
\alpha(A) = \alpha(A_1) \cdots \alpha(A_k).
\]

For $(A, b) \in M_{k,p}(\{0, 1\}) \times \{0, \cdots, p\}$, $\alpha(A, b)$ denotes the unique positive $(2p + 3)$-braid obtained from $\alpha(A)$ by adding a straight vertical strand between the $(2b + 1)$-st puncture and $(2b + 2)$-nd puncture of $\alpha(A)$. We may recover $\alpha(A)$ by removing $(2b + 2)$-nd strand from $\alpha(A, b)$.

For $n \geq 6$, define
\[
M_{k,n} = \begin{cases} 
\{A \in M_{k,p}(\{0, 1\)}|A^1 = 0, A^p = 1\}, & n = 2p + 2 \\
\{(A, b) \in M_{k,p}(\{0, 1\}) \times \{0, \cdots, p\}|A^1 = 0, A^p = 1\}, & n = 2p + 3.
\end{cases}
\]

We now have a function $\alpha : M_{k,n} \rightarrow B_n$ defined by $\alpha(A)$ if $n$ is even and $\alpha(A, b)$ if $n$ is odd. We sometimes use the notations $[A^1 \cdots A^p]$ and $[A^1 \cdots A^b|A^{b+1} \cdots A^p]$ to denote $\alpha(A)$ and $\alpha(A, b)$, respectively.

**Lemma 2.2.** For $n \geq 6$, the function $\alpha : M_{k,n} \rightarrow B_n$ has the following properties:

1. $\alpha(A) = \alpha(A_1) \cdots \alpha(A_k)$ and $\alpha(A, b) = \alpha(A_1, b) \cdots \alpha(A_k, b)$ are left weighted as written and rigid, hence $\alpha$ is injective;
2. There is no standard reduction system for $\alpha(A)$ or $\alpha(A, b)$.

**Proof.** Let $p = \lfloor \frac{n-2}{2} \rfloor$.

1. We already observed that $\alpha$ is injective on $M_{1,n}$. The starting set $S(\alpha(a)) = \{2, 4, \cdots, 2p\}$ and the finishing set $F(\alpha(a)) = \{1, 2, 4, \cdots, 2p, 2p+1\}$, and so $\alpha(A) = \alpha(A_1) \cdots \alpha(A_k)$ is rigid and this is the left weighted form as written for any $A \in M_{k,n}$ and so $\alpha$ is injective on $M_{k,n}$.

Now suppose $n$ is odd. As before, the transposing indices and the vertical strand of $\alpha(a, b)$ completely determine $(a, b) \in M_{1,n}$. And the starting and finishing sets
of $\alpha(a, b)$ are obtained from those of $\alpha(a)$ by shifting indices $\geq 2b + 2$ by 1. Hence $\alpha(A)$ is rigid and left weighted as written and so $\alpha$ is injective on $M_{k,n}$.

(2) By considering punctures contained inside, a standard circle $C$ in a disk with $n$ punctures can be expressed as a subset $\{i, i+1, \ldots, j\}$ of consecutive integers in $\{1, 2, \ldots, n\}$ such that $1 \leq |C| \leq n-2$ where $|C|$ denotes the diameter of $C$ defined by $|C| = j - i$. As a self-homeomorphism of a disk with $n$ punctures, $n$-braids are to act from the right to maintain the consistency between composition and multiplication. If $C$ is a standard reduction circle for a $n$-braid $\beta$ with the left weighted form $\beta = \beta_1 \cdots \beta_k$, then $\beta_1 \cdots \beta_i(C)$ is also standard for each $1 \leq i \leq k$ (for example, see [2, 15]). In particular, $\beta_1(C)$ is standard and $|\beta_1(C)| = |C|$.

Let $n = 2p + 2$. Suppose $\alpha(A)$ has a standard circle $C = \{i, i+1, \ldots, j\}$ for $A \in M_{k,n}$. By (1), the left weighted form $\alpha(A) = \beta_1 \cdots \beta_k$ is given by $\beta_i = \alpha(A_i)$. We show that it is impossible to have $|\beta_1(C)| = |C|$ and so $\alpha(A)$ has no standard reduction system. If $1 < i$, then either $\beta_1(i) < i$ or $\beta_1(i+1) \leq i$. Similarly, if $j < 2p + 2$, then either $\beta_1(j) > j$ or $\beta_1(j-1) \geq j$. Unless both equalities hold, $|\beta_1(C)| > j - i = |C|$. Thus $\beta_1(i+1) = i$ and $\beta_1(j-1) = j$. Hence both $i+1$ and $j-1$ are transposing indices and they correspond to 0 and 1 in the sequence $A_1$. Let $j'$ be the non-transposing index corresponding to the last 0 before the 1 corresponding to the $(j-1)$-st strand. Then $i \leq j' < j-1$ and the $j'$-th strand
crosses the \((j - 1)\)-st strand and \(\beta_i(j') > j\). In fact, \(\beta_j(j') \geq j + 2\) for \(j < 2p + 1\) and \(\beta_j(j') = j + 1\) for \(j = 2p + 1\). Hence \(|b_j(C)| \geq \beta_j(j') - i > j - i = |C|\).

Consider now the case \(i = 1\). Then \(3 \leq j < 2p + 2\). Since \(A^1 = 0\), \(\beta_j(3) = 2\). As above, there exists \(j'\) such that \(\beta_j(j') \geq j + 2\) unless \(j = 2p + 1\). This implies that \(\beta_j(C) \geq (j + 2) - 2 \geq j - 1 = |C|\) unless \(j = 2p + 1\). The remaining possibility is that \(C = \{1, \ldots, 2p + 1\}\) and \(\beta_j(2p + 2) = 1\). However this is also impossible because \(A^0 = 1\) and \(\beta_j(2p + 2) = 2p \geq 1\). The case \(j = 2p + 2\) is symmetric to the case \(i = 1\).

Let \(n\) be odd. Suppose \(\alpha(A, b)\) has a standard circle \(C = \{i, i + 1, \ldots, j\}\) for \(A \in \mathcal{M}_{k,n}\). By forgetting the \((2b + 2)\)-nd strand, consider \(C - \{2b + 2\}\). If \(|C - \{2b + 2\}| > 0\), then it is a standard reduction circle for \(\alpha(A)\) and so this is impossible. If \(|C - \{2b + 2\}| = 0\), then \(C\) is either \(\{2b + 1, 2b + 2\}\) or \(\{2b + 2, 2b + 3\}\). But these two cases are impossible by an easy observation on diameters.

By cycling rows, we define the cycling operation \(\mathcal{M}_{k,n} \to \mathcal{M}_{k,n}\) similar to the cycling operation \(c : \mathcal{B}_n \to \mathcal{B}_n\) of braids groups. That is, \(c(A)\) is obtained from \(A\) by moving the first row of \(A\) to the bottom so that \(\alpha(c(A)) = \alpha(A_2) \cdots \alpha(A_k) \alpha(A_1)\) and \(c(A, b) = (c(A), b)\). Note that \(cA = Ac\) by Lemma \([2.2](1)\). Hence the order of \(A\) or \(A, b\) under cycling is well defined and denoted by \(|c(A)|\) or \(|c(A, b)|\).

Let \(\tau : \mathcal{B}_n \to \mathcal{B}_n\) be the involution sending \(\sigma_i\) to \(\sigma_{n-i}\). Then for any \(\beta \in \mathcal{B}_n\), \(\tau(\beta) = \Delta^{-1}\beta\Delta\) where \(\Delta\) is the permutation braid corresponding to the half-twist.

For any column vector \(a\) over \(\{0, 1\}\), let \(\bar{a}\) denote the column vector obtained by taking Boolean negation for each entry of \(a\). Given a left-weighted form \(\alpha = \bar{a}\) or an \(\alpha\)-conjugator for \(A\), we call \(\alpha\) a nontrivial or \(\alpha\)-conjugator for \(A\). The invariant set \(I(\beta)\) is generated by iterated conjugations by minimal \(\alpha\)-conjugators. Given a left-weighted form \(x = \Delta^k x_1 \cdots x_t \in I(\beta)\) and a minimal \(\alpha\)-conjugator \(\rho\) of \(x\), there are two possibilities that \(\rho < \alpha(x)\) or \(\rho < \alpha(x)^{-1}\Delta\) and we call \(\rho\) a cut-head or an add-tail conjugator of \(x\), respectively. If \(x\) is rigid, the two kinds of minimal \(\alpha\)-conjugators are mutually exclusive.

For \(x, y \in R(\beta)\) and a minimal \(\alpha\)-conjugator \(\rho\), we use \(x \xrightarrow{\rho} y\) if \(\rho^{-1}xp = y\). Then \(R(\beta)\) can be regarded as a directed graph. And we use \(x \xrightarrow{\rho} y\) if there is a directed path from \(x\) to \(y\) in \(R(\beta)\).

3. Cut-head Conjugators for \(\alpha(A)\)

For \(A \in \mathcal{M}_{k,n}\), we will show that there is only one cut-head \(\alpha\)-conjugator for \(\alpha(A)\).

**Lemma 3.1.** Let \(a = (0, a_2, \cdots, a_{p-1}, 1) \in \{0, 1\}^p\) for \(p \geq 2\) and \(\varphi = \varphi(a)^{-1}\). Suppose \(\beta \prec \alpha(a)\) and \(\beta^{-1}\alpha(a)\gamma\) is a permutation braid for some permutation \((2p + 2)\)-braid \(\gamma\).

(i) If \(\sigma_2j \prec \gamma\) for \(1 \leq j \leq p\), then \(\sigma_{2j}\sigma_\varphi(2j) \prec \beta\);
(ii) If \(\sigma_1 \prec \gamma\), then \(\sigma_{2}\sigma_\varphi(1) \prec \beta\);
(iii) If \(\sigma_{2p+1} \prec \gamma\), then \(\sigma_{2p}\sigma_\varphi(2p+1) \prec \beta\).
Proof. Consider two strands that end at $2j$-th and $(2j + 1)$-st punctures. One of them corresponds to a transposing index, and the other corresponds to $\varphi(2j)$. If $\sigma_{2j} \prec \gamma$, then $2j \notin F(\beta^{-1}\alpha(a))$ since $\beta^{-1}\alpha(a)\gamma$ is a permutation braid. Thus any crossing formed by a strand $s$ and one of the above two strands must be cancelled out by $\beta^{-1}$ if the strand $s$ crosses only one of the two. In particular, $\sigma_{2j}$ and $\sigma_{\varphi(2j)}$ are such crossings for $2 \leq j \leq p - 1$. Figure 3 shows $\alpha(a)\sigma_{2j}$ and the shaded region represents $\beta < \alpha(a)$ and two crossings surrounded by dotted circles are $\sigma_{2j}$ and $\sigma_{\varphi(2j)}$. For $j = 1$, $\varphi(2) = 1$ and it is easy to see that $\sigma_{2}\sigma_{1} \prec \beta$ to have $2 \notin F(\beta^{-1}\alpha(a))$. Similarly we have $\sigma_{2p}\sigma_{2p+1} \prec \beta$ if $2p \notin F(\beta^{-1}\alpha(a))$. Thus we establishes (i). The cases (ii) and (iii) are similar to the case (i) with $2 \leq j \leq p - 1$. □

![Figure 3](image_url)

**Figure 3.** An intuitive figure for the proof of Lemma 3.1

**Lemma 3.2.** For $A \in \mathcal{M}_{k,n}$, there is only one cut-head minimal $R$-conjugator $\alpha(A_1)$ of $\alpha(A)$.

**Proof.** Let $\rho$ be an arbitrary cut-head SSS-conjugator for $\alpha(A)$. Suppose $n = 2p + 2$. Since $S(\alpha(A_1)) = \{2, 4, \ldots, 2p\}$ and $\rho$ is nontrivial, $2j \in S(\rho)$ for some $1 \leq j \leq p$. Also there exists $\rho_i$'s that make

$$
\rho^{-1}\alpha(A)\rho = (\rho^{-1}\alpha(A_1)\rho_1) \cdots (\rho_{k-1}^{-1}\alpha(A_k)\rho)
$$

left-weighted as written. Each block in this decomposition satisfies the hypothesis of Lemma 3.1. Since $\rho$ feeds back at the end and $\varphi$ is a cycle on the set $\{1, 2, \ldots, 2p, 2p + 1\}$ by Lemma 2.1, iterated application of Lemma 3.1 shows

$$(\sigma_{2}\sigma_{1})\sigma_{4} \cdots \sigma_{2p-2}(\sigma_{2p}\sigma_{2p+1})$$

is a prefix of $\rho$ and $\rho_i$ for all $i$. We note that $\sigma_{2}\sigma_{1}$, $\sigma_{4}$, $\ldots$, $\sigma_{2p-2}$, $\sigma_{2p}\sigma_{2p+1}$ are mutually commutative and so they are not interfered each other. In particular, $(\sigma_{2}\sigma_{1})\sigma_{4} \cdots \sigma_{2p-2}(\sigma_{2p}\sigma_{2p+1}) \prec \rho_1$ implies $F(\rho^{-1}\alpha(A_1)) \cap \{1, 2, \ldots, 2p, 2p + 1\} = \emptyset$. Since $F(\rho^{-1}\alpha(A_1)) \subset \{1, 2, \ldots, 2p, 2p + 1\}$, we must have $F(\rho^{-1}\alpha(A_1)) = \emptyset$, that is, $\rho = \alpha(A_1)$. Since $\alpha(A_1)$ is clearly an $R$-conjugator of $\alpha(A)$, it is a unique cut-head $R$-conjugator of $\alpha(A)$.

Now suppose $n = 2p + 3$. Let $(A, b) \in \mathcal{M}_{k,n}$, $\rho$ be an arbitrary cut-head SSS-conjugator for $\alpha(A, b)$, and $\rho'$ be obtained from $\rho$ by removing $(2b + 2)$-nd strand.
Since the starting and finishing sets of $\alpha(A_i, b)$ are obtained from those of $\alpha(A_i)$ by shifting indices $\geq 2b+2$ by 1 for all $i$, $\rho'$ is a cut-head SSS-conjugator of $\alpha(A)$. Thus $\rho' = \alpha(A_1)$ and so $\rho = \alpha(A_1, b)$. Then $\alpha(A_1, b)$ is clearly an $R$-conjugator of $\alpha(A, b)$ and so it is a unique cut-head $R$-conjugator of $\alpha(A, b)$. □

4. Add-tail conjugators for $\alpha(A)$

Suppose $n$ is even. For $A \in \mathcal{M}_{k,n}$, let $\rho$ be an arbitrary add-tail minimal $R$-conjugator for $\alpha(A)$. Then $F(\alpha(A_0)) = \{1, 2, 4, \ldots, 2p, 2p+1\}$ and so $S(\rho) \subseteq \{3, 5, \ldots, 2p-1\}$. Hence we only need to consider add-tail conjugator starting with $\sigma_{2i+1}$ for $1 \leq i \leq p-1$.

**Lemma 4.1.** Let $a \in \{0,1\}^p$ for $p \geq 2$, and $\vartheta = \vartheta(a)$. Suppose $\alpha(a)\gamma$ is a permutation braid for some permutation $(2p+2)$-braid $\gamma$ and $\sigma_{2i+1} \prec \alpha(a)\gamma$ for $1 \leq i \leq p-1$.

(i) If $a_i = 0$ and $a_{i+1} = 1$, then $\sigma_{2i+1}\sigma_{2i+2}\sigma_{2i+1} \prec \gamma$;

(ii) If $a_{i+1} = 0$, then $\sigma_{2i+1}(\sigma_{2i+3}\sigma_{2i+4} \cdots \sigma_{\vartheta(2i+2)}) \prec \gamma$;

(iii) If $a_{i+1} = 0$ and $\sigma_{2i+3}\sigma_{2i+4} \cdots \sigma_{2j-1} \prec \alpha(a)\gamma$ for the smallest $j > i+1$ such that $a_j = 0$, then $\sigma_{2j+1} \prec \gamma$;

(iv) If $a_i = 1$, then $\sigma_{2i+1}(\sigma_{2i-1}\sigma_{2i-2} \cdots \sigma_{\vartheta(2i)}) \prec \gamma$;

(v) If $a_i = 1$ and $\sigma_{2i-1}\sigma_{2i-2} \cdots \sigma_{2j+1} \prec \alpha(a)\gamma$ for the largest $j < i$ such that $a_j = 1$, then $\sigma_{2j+1} \prec \gamma$.

**Proof.** (i) This follows from Figure 4(a). The crossing $a = \sigma_{2i+1}^{-1}$ in the picture must be canceled by multiplying $\gamma$ and so $\gamma$ has the crossing $A$. Since strands of $\alpha(a)\gamma$ can cross each other at most once, crossings $b$ and $c$ force crossings $B$ and $C$, respectively.

Recall the permutation $\vartheta = \vartheta(a)$ of non-transposing indices of $a$. If $a_{i+1} = 0$, $\vartheta(2i+2) = 2j$ for the smallest $j > i+1$ such that $a_j = 0$ if such $j$ exists or $\vartheta(2i+2) = 2p+1$ otherwise by Lemma 2.1.

(ii) In Figure 4(b), the shaded band represents a bundle of strands. The crossing $a = \sigma_{2i+1}^{-1}$ must be canceled by multiplying $\gamma$ and so $\gamma$ has the crossing $A$. Since $\alpha(a)\gamma$ is a permutation braid, the crossings $b$, $c$, $d$, and $e$ in $\alpha(a)$ force the corresponding crossings $B$, $C$, $D$, and $E$ in $\gamma$, respectively. In particular, $ECB \prec \gamma$ where $C = \sigma_{2i+1}\sigma_{\vartheta(2i+2)-1}$, $B = \sigma_{\vartheta(2i+2)}$, and $E = \sigma_{2i+1}$.

(iii) In Figure 4(c), the crossings $(\sigma_{2i+3}\sigma_{2i+4} \cdots \sigma_{2j})^{-1}$ must be canceled by $\gamma$. In particular, $\gamma$ must have the crossing $A$ canceling $a$. Since the crossing $b$ forces the crossing $B$ and $\vartheta(2i+2) = 2j$, $\sigma_{2j+1} \prec \gamma$ and so $\sigma_{2j+1} \prec \gamma$.

(iv) and (v) are equivalent to (ii) and (iii) via the involution $\tau$. □

In addition we need to consider the following possibilities for odd braids.

**Lemma 4.2.** Let $a, \vartheta$ be as before and $1 \leq b \leq p-1$ be an integer. Suppose $\alpha(a, b)\gamma$ is a permutation braid for some permutation $(2p+3)$-braid $\gamma$ and $\sigma_{2b+c} \prec \alpha(a, b)\gamma$ for some $1 \leq c \leq 2$.

(i) If $c = 1$ and $a_b = 0$, then $\sigma_{2b+1}\sigma_{2b} \prec \gamma$;

(ii) If $c = 1$ and $a_b = 1$, then $\sigma_{2b+1}(\sigma_{2b-1} \cdots \sigma_{\vartheta(2i)}) \prec \gamma$;

(iii) If $c = 2$ and $a_{b+1} = 0$, then $\sigma_{2b+2}(\sigma_{2b+4} \cdots \sigma_{\vartheta(2i+2)}) \prec \gamma$.

(iv) If $c = 2$ and $a_{b+1} = 1$, then $\sigma_{2b+2}\sigma_{2b+3} \prec \gamma$. □
Proof. By using Figure 5 and the argument similar to the proof of the previous lemma, (i) and (ii) follow. The assertions (iii) and (iv) also follow using the involution $\tau$. □

Lemmas 4.1 and 4.2 apply to each row of $A \in M_{k,n}$ and every contribution forced by the lemma must accumulate on an add-tail SSS-conjugator $\rho$ of $\alpha(A)$ to avoid an increase of the canonical length of $\rho^{-1}\alpha(A)\rho$. We in general expect to have a long add-tail SSS-conjugator for $\alpha(A)$ and the randomness among rows $A$ defeats our purpose since longer add-tail minimal $R$-conjugators of $\alpha(A)$ generate a smaller rigid conjugacy set $R(\alpha(A))$. In order to make our discussion the simplest
possible, we consider the following subset $\mathcal{M}_{k,n}^0$ of $\mathcal{M}_{k,n}$ that still allows enough add-tail conjugators to serve our purpose. For $n \geq 10$ and $k \geq 2$, we define

$$\mathcal{M}_{k,n}^0 = \{ A \mid A^i = 0 \text{ or } 1 \text{ for } 2 \leq i \leq p - 3, \text{ and } |c(A)| = k \} \quad \text{for } n = 2p + 2$$

and

$$\mathcal{M}_{k,n}^0 = \{(A,p - 2) \mid A \in \mathcal{M}_{k,n-1}^0\} \quad \text{for } n = 2p + 3.$$ 

Since the location of the vertical strand is fixed at $p - 2$ for an odd $n$, we simply denote an element of $\mathcal{M}_{k,n}^0$ by a matrix $A \in \mathcal{M}_{k,p}^0(\{0,1\})$ if no ambiguity occurs.

Notice that a $k \times p$ binary matrix $A$ in $\mathcal{M}_{k,n}^0$ has constant columns except the $(p - 2)$-nd and the $(p - 1)$-st columns. We assume $n \geq 10$ and $k \geq 2$ whenever we consider $\mathcal{M}_{k,n}^0$ since the notation makes no sense otherwise.

**Lemma 4.3.** Let $A \in \mathcal{M}_{k,n}^0$ and $p = \lfloor \frac{n-2}{2} \rfloor$. If there is $2 \leq j \leq p - 3$ such that $A^j = 1$, then every add-tail minimal $R$-conjugator for $\alpha(A)$ is either of the form $\rho_{2i+1} = \sigma_{2i+1} \sigma_{2i} \sigma_{2i+2} \sigma_{2i+1}$ for $2 \leq i \leq p - 4$ or of the form $\rho_3 = \sigma_3 \sigma_2 \sigma_4 \sigma_3 \sigma_1$. Moreover, $\rho_{2i+1}$ arises exactly when $A^i = 0$ and $A^{i+1} = 1$.

**Proof.** First consider even braids, that is, $n = 2p + 2$. If $A^i = 0$ and $A^{i+1} = 1$ for $2 \leq i \leq p - 4$, then $\rho_{2i+1}$ is clearly an add-tail minimal $R$-conjugator in the view of Lemma 4.1(i) and in fact

$$[\cdots 01 \cdots] \xrightarrow{\rho_{2i+1}} [\cdots 10 \cdots].$$

If $A^1 = 0$ and $A^2 = 1$, then $\rho_3$ is also an add-tail minimal $R$-conjugator in the view of Lemma 4.1(i) except the fact that the extra $\sigma_1$ is needed to make the result rigid and in fact

$$[01 \cdots] \xrightarrow{\rho_3} [00 \cdots].$$
On the other hand, let $\rho$ be an arbitrary add-tail minimal $R$-conjugator. Since $F(\alpha(A)) = \{1, 2, 4, \ldots, 2p, 2p + 1\}$, we may assume that $\sigma_{2i+1} \prec \rho$ some $1 \leq i \leq p - 1$. It is suffice to show that this is impossible if $A^i \neq 0$ or $A^{i+1} \neq 1$.

Suppose $A^i = 0$ and $A^{i+1} \neq 1$. Then Lemma 4.1(ii) and (iii) are applicable and $2j + 1 \in S(\rho)$ for the smallest $j > i + 1$ such that $A^j \neq 1$. If $A^j = 0$ and $A^{j+1} \neq 1$, we go back and repeat the argument by replacing $i$ by $j$. Since $A^{p-2} \neq 1$, this repetition eventually yields the cases considered next. If $A^j = 0$ and $A^{j+1} = 1$, an add-tail minimal $R$-conjugator $\rho_{2j+1}$ starting with $2j + 1$ exists and it does not start with $\sigma_{2i+1}$ and this contradicts the minimality of $\rho$. If $A^j \neq 0$, then $j = p - 2$ and this is the case we consider next since $A^{p-2} \neq 0$.

Suppose $A^i \neq 0$. Then Lemma 4.1(iv) and (v) are applicable and so $2(j-1) + 1 \in S(\rho)$ for the largest $j < i$ such that $A^j = 1$. If $A^{j-1} \neq 0$, we go back and repeat the argument by replacing $i$ by $j - 1$. Since $A^1 = 0$, this repetition eventually yields the case considered next. If $A^{j-1} = 0$, an add-tail minimal $R$-conjugator $\rho_{2j-1}$ starting with $2j - 1$ exists and it does not start with $\sigma_{2i+1}$ and this contradicts the minimality of $\rho$.

Now consider odd braids, that is, $n = 2p + 3$. When $A^i = 0$ and $A^{i+1} = 1$ for $i = 1, \ldots, p - 4$, the existence of the add-tail minimal $R$-conjugators $\rho_{2i+1}$ is identical to the case of even braids. Let $\rho$ be an add-tail minimal $R$-conjugator for $\alpha(A)$. Then $S(\rho) \subset \{3, 5, \ldots, 2p - 3, 2p - 2, 2p\}$ since

$$F(\alpha(A)) = \{1, 2, 4, \ldots, 2p - 4, 2p - 1, 2p + 1, 2p + 2\}. $$

Let $\rho'$ be a braid obtained by removing the $(2p - 2)$-nd strand from $\rho$. Then $\rho'$ is an add-tail SSS-conjugator for $\alpha(A) \in B_{n-1}$.

If $\sigma_{2i+1} \prec \rho$ for some $1 \leq i \leq p - 3$ such that $A^i \neq 0$ or $A^{i+1} \neq 1$ or $\sigma_{2p} \rho$, then $\sigma_{2i+1} \prec \rho$ for some $1 \leq i \leq p - 1$ such that $A^i \neq 0$ or $A^{i+1} \neq 1$. By the above argument for even braids, $2j + 1 \in S(\rho')$ for some $1 \leq j \leq p - 4$ such that $A^j = 0$ and $A^{j+1} = 1$. By inserting the vertical strand back to $\rho'$, we have $2j + 1 \in S(\rho)$ for some $1 \leq j \leq p - 4$ such that $A^j = 0$ and $A^{j+1} = 1$. Since the minimal $R$-conjugator $\rho_{2j+1}$ exits and does not start with $\sigma_{2i+1}$, $\rho$ cannot be minimal.

Finally if $2p - 3$ or $2p - 2$ are in $S(\rho)$, then by Lemma 4.2 $\sigma_{2i+1} \prec \rho$ for some $1 \leq i \leq p - 3$ or $\sigma_{2p} \prec \rho$ since both $A^{p-2}$ and $A^{p-1}$ are neither $0$ nor $1$. We have already shown that $\sigma_{2j+1} \prec \rho$ for some $1 \leq j \leq p - 4$ such that $A^j = 0$ and $A^{j+1} = 1$ under this situation. Since $\rho_{2j+1}$ starts with neither $\sigma_{2p-3}$ nor $\sigma_{2p-2}$, $\rho$ cannot be minimal.

Lemma 4.3 completely determined all add-tail minimal $R$-conjugators of $\alpha(A)$ for $A \in M_{k,n}^0$ except the case when $A^1 = A^2 = \cdots = A^{p-3} = 0$. In fact we will show that such a braid has a unique add-tail minimal $R$-conjugator. However it seems difficult to find the minimal $R$-conjugator via a direct computation since it is quite long.

As we observed in the proof of Lemma 4.3, the conjugation by a minimal $R$-conjugator $\rho_{2i+1}$ for $2 \leq i \leq p - 4$ exchanges the $i$-th column of 0's and the $(i+1)$-st column of 1's in $A \in M_{k,n}^0$ and the conjugation by $\rho_3$ turns the 2nd column of 1's into the column of 0's. Thus we have the following diagrams:

$$\begin{align*}
\cdots \cdot 01 \cdots & \xrightarrow{\rho_{2i+1}} \cdots \cdot 10 \cdots, \\
\cdots \cdot 01 \cdots & \xrightarrow{\rho_3} \cdots \cdot 00 \cdots
\end{align*}$$
We call these conjugations switching. It is clear that for \( i = 1, p - 2, p - 1, p \), the \( i \)-th column and the vertical strand of an odd braid remains unchanged by switchings and so switchings are operations within \( M^0_{k,n} \).

For \( A \in M^0_{k,n} \), we may regard the rigid conjugacy set \( R(\alpha(A)) \) as a directed graph with each edge labeled by a minimal \( R \)-conjugator. Let \( \Gamma(A) \) be the directed graph generated by switchings and their inverses starting from \( \alpha(A) \). Then \( \Gamma(A) \) forms a connected subgraph of \( R(\alpha(A)) \). Let

\[
\hat{A} = (01 \cdots 1 A^{p-2} A^{p-1} 1) \quad \text{and} \quad \hat{A} = (00 \cdots 0 A^{p-2} A^{p-1} 1).
\]

Given any \( A \in M^0_{k,n} \), it is clear that we can convert \( \hat{A} \) into \( A \) and \( A \) into \( \hat{A} \) via series of switchings. Thus the directed graph \( \Gamma(A) \) forms a lattice and \( \alpha(\hat{A}) \) and \( \alpha(A) \) are the unique initial element and the unique terminal element, respectively.

If there are two directed paths from \( \beta_0 \) to \( \beta_1 \) in \( \Gamma(A) \), that is, \( \gamma^{-1} \beta_0 \gamma = \beta_1 = \gamma'^{-1} \beta_0 \gamma' \) for some \( \gamma, \gamma' \) that are products of add-tail minimal \( R \)-conjugators, then the region between the two directed paths is completely filled by squares of the following type:

\[
\begin{array}{c}
\vdots
\end{array}
\begin{array}{c}
\vdots
\end{array}
\begin{array}{c}
\vdots
\end{array}
\]

where \( |j - j'| \geq 2 \) by the requirement on \( \beta_0 \) for \( \rho_{2j+1} \) and \( \rho_{2j'+1} \) to exist as described in Lemma 4.3. Since \( \rho_{2j+1} \rho_{2j'+1} = \rho_{2j'+1} \rho_{2j+1} \), we have \( \gamma = \gamma' \). Let \( \rho_A \) denote the unique braid that is a product of add-tail minimal \( R \)-conjugators such that \( \rho^{-1}_A \alpha(A) \rho_A = \alpha(A) \).

**Example 4.4.** Let \( \alpha(A) = \left[ \begin{array}{cccccc}
0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1
\end{array} \right] \in B_{17} \). Two columns that are not supposed to be constant are indicated by slanted entries.

Then \( \alpha(\hat{A}) = \left[ \begin{array}{cccccc}
0 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 1
\end{array} \right] \) and \( \alpha(\hat{A}) = \left[ \begin{array}{cccccc}
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0
\end{array} \right] \). And the following diagram shows \( \alpha(\hat{A}), \alpha(A) \) and \( \alpha(\hat{A}) \) in the direct graph \( \Gamma(A) \).

\[
\begin{array}{ccc}
\alpha(\hat{A}) = \left[ \begin{array}{cccccc}
0 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 1
\end{array} \right] & \xrightarrow{\rho_A} & \left[ \begin{array}{cccccc}
0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 1
\end{array} \right] \\
\alpha(A) = \left[ \begin{array}{cccccc}
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0
\end{array} \right] & \xrightarrow{\rho_{17}} & \left[ \begin{array}{cccccc}
0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1
\end{array} \right] & \xrightarrow{\rho_5} & \left[ \begin{array}{cccccc}
0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1
\end{array} \right] = \alpha(A)
\end{array}
\]

And we have

\[
\rho_A = \rho_3 \rho_5
\]

\[
= (\sigma_3 \sigma_2 \sigma_4 \sigma_2 \sigma_1) (\sigma_5 \sigma_4 \sigma_6 \sigma_3)
\]

\[
= (\sigma_3 \cdots \sigma_6) (\sigma_2 \cdots \sigma_5) \sigma_1
\]

and similarly,

\[
\rho_{\hat{A}} = (\rho_3 \rho_5 \rho_7) (\rho_{3} \rho_5 \rho_3)
\]

\[
= (\sigma_3 \cdots \sigma_8) (\sigma_2 \cdots \sigma_7) (\sigma_3 \cdots \sigma_6) (\sigma_1 \cdots \sigma_3) (\sigma_3 \sigma_4)(\sigma_1 \sigma_2 \sigma_3) \sigma_1
\]

\[
= (\sigma_3 \sigma_5 \sigma_7)(\sigma_4 \cdots \sigma_8)(\sigma_2 \cdots \sigma_7)(\sigma_4 \sigma_5 \sigma_6)(\sigma_1 \cdots \sigma_5) \sigma_4 (\sigma_1 \sigma_2 \sigma_3) \sigma_1.
\]
In general, for any \( n \geq 10 \) and \( A \in \mathcal{M}_{k,n}^0 \), we have
\[
\rho_A = (p_3 p_5 \cdots p_{2p-7})(p_3 p_5 \cdots p_{2p-9}) \cdots (p_3 p_5) p_3
\]
\[
= \sigma_1^{-1} \left( \prod_{i=4}^{p-1} (\sigma_3 \cdots \sigma_{2(p-i)+2})(\sigma_1 \cdots \sigma_{2(p-i)+1}) \right) \sigma_1
\]
\[
= (\sigma_3 \sigma_5 \cdots \sigma_{2p-7}) \sigma_1^{-1} \left( \prod_{i=4}^{p-1} (\sigma_4 \cdots \sigma_{2(p-i)+2})(\sigma_1 \cdots \sigma_{2(p-i)+1}) \right) \sigma_1.
\]
where \( p = \lfloor \frac{n-2}{2} \rfloor \). Therefore \( S(\rho_A) = \{3, 5, \ldots, 2p-7\} \) and \( \rho_A \) is the same for any terminal element in \( \mathcal{M}_{k,n}^0 \).

In the proof of the following lemma, we need to consider \( \tau(\mathcal{M}_{k,n}^0) \). To avoid any unnecessary complication, we need \( \mathcal{M}_{k,n}^0 \cap \tau(\mathcal{M}_{k,n}^0) = \emptyset \) and this is guaranteed by assuming \( n \geq 14 \) from now on.

**Lemma 4.5.** Let \( A \) be an element of \( \mathcal{M}_{k,n}^0 \) such that \( A = \hat{A} \). Then there exists a unique add-tail minimal \( R \)-conjugator
\[
\rho = \alpha(A_k)^{-1} \rho_\hat{A}^{-1} \Delta
\]
where \( A_k \) is the last row of \( A \).

**Proof.** Suppose \( n \) is even. By hypothesis, \( A = \hat{A} = (0 \cdots 0 A^{p-2} A^{p-1} 1) \) for some \( A^{p-2}, A^{p-1} \neq 0, 1 \). Then \( \hat{A} = (01 \cdots 1 A^{p-2} A^{p-1} 1) \). Let \( \rho \) be an add-tail minimal \( R \)-conjugator for \( \alpha(\hat{A}) \). Then \( 2i+1 \in S(\rho) \) for some \( 1 \leq i \leq p-1 \). By a repeated application of Lemma 4.4(iii), we eventually find \( \sigma_2 \rho \prec \sigma \) whatever \( i \) is.

Let \( \gamma \) be a minimal element among all add-tail \( R \)-conjugators for \( \alpha(\hat{A}) \) starting with \( \sigma_2 \). Since no add-tail minimal \( R \)-conjugators for braids in \( \Gamma(A) \) except \( \hat{A} \) start with \( \sigma_2 \) by Lemma 4.3, the conjugation of \( \alpha(\hat{A}) \) by some prefix of \( \gamma \) must first reach \( \hat{A} \) and therefore \( \rho_\hat{A} \prec \gamma \). Let \( \gamma = \rho_\hat{A} \gamma' \). Then \( \gamma' \) is an add-tail \( R \)-conjugator for \( \alpha(A) \). Since \( \sigma_{2p-1} \) and \( \rho_\hat{A} \) commute by (\#), \( 2p-1 \in S(\gamma') \) and so \( \rho \prec \gamma' \) by the minimality of \( \rho \).

On the other hand, since \( \rho_A \rho_\hat{A} \) is an add-tail \( R \)-conjugator for \( \alpha(\hat{A}) \) starting with \( \sigma_2 \), \( \gamma \prec \rho_A \rho_\hat{A} \) by the minimality of \( \gamma \) and so \( \gamma' \prec \rho \). Therefore \( \gamma' = \rho \) and \( \gamma = \rho_A \rho_\hat{A} \).

But any \( SSS \)-conjugator for \( \alpha(\hat{A}) \) starting with \( \sigma_2p \), \( \gamma \prec \rho_A \rho_\hat{A} \) as a prefix by Lemma 4.1 and so \( S(\rho_A \rho_\hat{A}) = \{3, 5, \ldots, 2p-1\} \) because \( S(\rho_A) = \{3, 5, \ldots, 2p-7\} \) as we discussed just before this lemma. Since \( \rho_A \rho_\hat{A} \) is an add-tail \( SSS \)-conjugator, \( \rho_A \rho_\hat{A} \prec \alpha(\hat{A}) \rho_A \rho_\hat{A} \). Since \( S(\alpha(\hat{A})) = \{2, 4, \ldots, 2p\} \), we have \( \{2, 3, \ldots, 2p\} \subseteq S(\alpha(\hat{A})) \) and so
\[
\Delta \prec \sigma_1 \sigma_{2p+1} \alpha(\hat{A}) \rho_A \rho_\hat{A}.
\]

Then by considering the right-weighted form for \( \sigma_1 \sigma_{2p+1} \alpha(\hat{A}) \rho_A \rho_\hat{A} \), there exists \( \beta \prec \sigma_1 \sigma_{2p+1} \) such that \( \alpha(A_k) \rho_A \rho_\hat{A} \beta = \Delta \), that is, \( \rho = \rho_A^{-1} \alpha(A_k) \Delta \beta^{-1} \).

Since \( \rho_A^{-1} \alpha(A_k) \rho_A = \alpha(A_k) \), \( \rho_A^{-1} \alpha(A_k) \rho_A = \alpha(A_k) \). Thus \( \rho = \rho_A^{-1} \alpha(A_k) \Delta \beta^{-1} = \alpha(A_k)^{-1} \rho_A^{-1} \Delta \beta^{-1} \) and so
\[
\rho^{-1} \alpha(A) \rho = \beta \Delta^{-1} \rho_A \alpha(A_k) \alpha(A) \alpha(A_k)^{-1} \rho_A^{-1} \Delta \beta^{-1} = \beta \alpha(\tau c^{-1}(\hat{A})) \beta^{-1},
\]
since \( \alpha(A_k) \alpha(A) \alpha(A_k)^{-1} \) is again a terminal element and is sent to its initial element via the conjugation by \( \rho_A^{-1} \). If we consider the involuted versions of Lemma 4.1
and for , an initial element cannot have an -conjugator starting with or . Thus and so we have as desired and .

Suppose is odd. Assume . Let be an add-tail minimal -conjugator for , and let be the braid obtained by removing the -th strand from . Then 's is not trivial. Indeed, if were trivial then consists of either or . But Lemma forces to contain for some permutation braid . Clearly this equation we have . Thus is a contradiction. Thus is an add-tail -conjugator for .

Let be the -braid obtained from by inserting a vertical strand between the -rd and -nd punctures. Note that and has the identical braid word. Clearly is an add-tail -conjugator and contains as a prefix where is understood to be the half twist of the braid index being considered. By the minimality of ,

for some permutation braid . By removing the -nd strand in both sides of this equation, we have where is the braid obtained from . Thus and so .

Let . Since the -nd strand is vertical in , we have . Since , we have . Here are either or 1, and becomes trivial when the -th strand is removed.

Now we have

Let be the reversed word of the part inside the braces in the right hand side. Then is obviously in its super summit set. If was nontrivial, the braid obtained by removing the -th strand is also nontrivial by the same reason why was nontrivial in the above. But this contradicts the assumption of . Thus and . This implies , otherwise cannot be an -conjugator. Consequently, we have and the notations for the vertical strand can be suppressed to obtain the desired add-tail minimal -conjugator. □

We call this type of conjugation initializing because it convert a terminal element from or to an initial element in or , respectively.

5. MAIN THEOREM

We summarize our results in the following theorem.

**Theorem 5.1.** For , the rigid conjugacy set is contained in .

**Proof.** By , the conjugation of by a cut-head minimal -conjugator is cycling. By Lemma and Lemma , the conjugation by an add-tail minimal -conjugator is either switching or initializing. Thus is closed under all of these operations and so includes the rigid conjugacy set . □
Figure 6 displays $R(\alpha(A))$ for $A \in \mathcal{M}_{k,n}^0 \cup \tau(\mathcal{M}_{k,n}^0)$ as a directed graph. The ordinary arrows and the dashed arrows indicates cycling and initializing, respectively. All switching occurs inside lattices indicated by shaded rhombi.

Finally we give the main theorem.

**Theorem 5.2.** For $n \geq 14$, let $A \in \mathcal{M}_{k,n}^0$ be given arbitrarily. Then the rigid conjugacy set $R(\alpha(A))$ of $\alpha(A)$ is made of pseudo-Anosov braids and its size is given by

$$|R(\alpha(A))| = k \cdot 2^{p-3} \geq \frac{1}{23} k \sqrt{2} n$$

where $p = \lfloor \frac{n-2}{2} \rfloor$.

**Proof.** Since $R(\alpha(A)) \subset \alpha(\mathcal{M}_{k,n}^0 \cup \tau(\mathcal{M}_{k,n}^0)) \subset \alpha(\mathcal{M}_{k,n})$ and none of braids in $\alpha(\mathcal{M}_{k,n})$ has a standard reduction system by Lemma 2.2(2), all of braids in $R(\alpha(A))$ is pseudo-Anosov according to [2].

To compute the size of the rigid conjugacy set $R(\alpha(A))$, it is enough to consider the contributions of cycling, switching, and initializing. By the definition of $\mathcal{M}_{k,n}^0$, it is easy to see that cyclings contribute the factor $k$.

Switching operates on constant columns from the 2nd to $(p-3)$rd for $\alpha(\mathcal{M}_{k,n}^0)$ and from 4th to $(p-1)$st for $\alpha(\tau(\mathcal{M}_{k,n}^0))$ and can generate any sequence of 0’s and 1’s. Since the length of sequences is $p-4$, switchings contribute the factor $2^{p-4}$.

Since $n \geq 14$, $\mathcal{M}_{k,n}^0 \cap \tau(\mathcal{M}_{k,n}^0) = \emptyset$ and so an initialization contributes the factor 2. By multiplying all these factors, we have the desired formula for $|R(\alpha(A))|$. □

**References**

[1] E. Artin, *Theorie der Zopfe*, Hamburg Abh. 4 (1925), 47–72.

[2] D. Bernardete, Z. Nitecki, M. Gutiérrez, *Braids and the Nielsen-Thurston classification*, J. Knot Theory Ramifications 4 (1995), no. 4, 549–618.

[3] J. S. Birman, V. Gebhardt, J. González-Meneses, *Conjugacy in Garside Groups I: Cyclings, Powers, and Rigidity*, Groups Geom. Dyn. 1 (2007), no. 3, 221–279.

[4] J. S. Birman, V. Gebhardt, J. González-Meneses, *Conjugacy in Garside Groups III: Periodic braids*, J. Algebra 316 (2007), no. 2, 746–776.
[5] E. A. Elrifai, H. R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford Ser. (2) **45** (1994), no. 180, 479–497.
[6] N. Franco, J. González-Meneses, *Conjugacy problem for braid groups and Garside groups*, J. Algebra **266** (2003), no. 1, 112–132.
[7] F. A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford Ser. (2) **20** (1969) 235–254.
[8] V. Gebhardt, *A new approach to the conjugacy problem in Garside groups*, J. Algebra **292** (2005), 282–302.
[9] V. Gebhardt, J. González-Meneses, *The cyclic sliding operation in Garside groups*, Math. Z. **265** (2010), no. 1, 85–114.
[10] V. Gebhardt, J. González-Meneses, *Solving the conjugacy problem in Garside groups by cyclic sliding*, J. Symbolic Comput. **45** (2010), no. 6, 629–656.
[11] J. González-Meneses, *The nth root of a braid is unique up to conjugacy*, Algebr. Geom. Topol. **3** (2003), 1103–1118.
[12] J. González-Meneses, *On reduction curves and Garside properties of braids*, Topology of algebraic varieties and singularities, 227–244, Contemp. Math., 538, Amer. Math. Soc., Providence, RI, 2011.
[13] K. H. Ko, J. W. Lee, *A fast algorithm for the conjugacy problem on generic braids*, On the proceedings of Knot theory for Scientific Objects, 201–212, March, 2006, Osaka, Japan.
[14] S. J. Lee, *Algorithmic solutions to decision problems in the braid groups*, Ph. D. Thesis in KAIST (2000).
[15] E. Lee, S. Lee, *A Garside-theoretic approach to the reducibility problem in braid groups*, J. Algebra **320** (2008), no. 2, 783–820.
[16] H. A. Masur, Y. N. Minsky, *Geometry of the complex of curves I : Hyperbolicity*, Invent. Math. **138** (1999), no. 1, 103–149.
[17] H. A. Masur, Y. N. Minsky, *Geometry of the complex of curves II : Hierarchical structure*, Geom. Funct. Anal. **10** (2000), no. 4, 902–974.
[18] M. Prasolov, *Small braids having a big ultra summit set*, Mat. Zametki **89** (2011), no. 4, 577–588; translation in Math. Notes **89** (2011), no. 3-4, 545–55.
[19] W. P. Thurston, *On the topology and geometry of diffeomorphisms of surfaces*, Bull. Amer. Math. Soc. **19** (1988), 109–140.