INSTITUTO DE COMPUTAÇÃO
UNIVERSIDADE ESTADUAL DE CAMPINAS

Sorting the Reverse Permutation by Prefix Transpositions

V. Fortuna *J. Meidanis*

Technical Report - IC-04-04 - Relatório Técnico

April - 2004 - Abril

Sorting the Reverse Permutation by Prefix Transpositions

Vinicius José Fortuna *   João Meidanis

Abstract

Dias and Meidanis [3] presented, without a proof, an algorithm to sort the reverse permutation $R_n = [n, n-1, \ldots, 1]$ by prefix transpositions. In this report we present a new algorithm based on the previous one and show a complete formal proof of its correctness. From this result we establish a new proved upper bound of $n - \lfloor n/4 \rfloor$ for the prefix transposition distance of R_n.

1 Introduction

Sequence comparison is one of the most studied problems in computer science. Usually we are interested in finding the minimum number of local operations, such as insertions, deletions and substitutions that transform a given sequence into another sequence. This is the edit distance problem, described in many Computational Biology textbooks [9]. Several studies, however, have shown that global operations such as reversals and transpositions (also called *rearrangement events*) are more appropriate when we wish to compare the genomes of two species [8].

A new research area called *Genome Rearrangement* appeared in the last years to deal with problems such as, for instance, to find the minimum number of rearrangement events needed to transform one genome into another. In the context of Genome Rearrangements, a genome is represented by an n-tuple of genes (or gene clusters). When there are no repeated genes, this n-tuple is a permutation.

The best studied rearrangement event is the reversal. A reversal inverts a block of any size in a genome. Caprara [2] proved that finding the minimum number of reversals needed to transform one genome into another is an NP-Hard problem. Hannenhalli and Pevzner [6] have studied the reversal distance problem when the orientation of genes is known. In this case they proved that there is a polynomial algorithm for the problem. Another interesting variation of this problem is the so-called *prefix reversal problem* or *pancake flipping problem* as it was originally called [4]. In this variation only reversals involving the first consecutive elements of a genome are permitted. Heydari and Sudborough [7] have proved that this problem is NP-Hard.

The rearrangement event called transposition has the property of exchanging two adjacent blocks of any size in a genome. The transposition distance problem, that is, the problem

*Work partially supported by FAPESP under grant 03/04578-5

of finding the minimum number of transpositions necessary to transform one genome into another, has been studied by Bafna and Pevzner [1], who presented some important results, including the best approximation algorithm for the problem at that time, which needs about $3n/4$ moves to sort any permutation, a lower bound of $\lfloor n/2 \rfloor$ for the transposition diameter for the symmetric group S_n, and an upper bound of $\lfloor n/2 \rfloor + 1$ for the transposition distance $d(R_n)$ of the reverse permutation R_n. Computational results proved that equality holds for $3 \leq n \leq 10$. They also conjectured that the transposition diameter for the symmetric group equals the transposition distance of the reverse permutation, which is in fact true for $n < 10$.

Later, Eriksson and coleagues [5] obtained an improved approximation algorithm that sorts any permutation with at most $\lfloor (2n-2)/3 \rfloor$ transpositions and proved that the exact value of the distance of the reverse permutation is indeed. $\lfloor n/2 \rfloor + 1$ for all $n > 0$. They also give a counterexample to the conjecture for the transposition diameter finding permutations of size 13 and 15 with transposition distance greater than for the reverse permutation. However they still believe that the conjecture is true for $n > 15$.

The transposition distance problem is still open: we do not know of any NP-Hardness proof, and there are no evidences that an exact polynomial algorithm exists.

In face of the difficulties of the transposition distance problem, Dias and Meidanis [3] introduced a new variation of problem: the prefix transposition problem, where the only allowed transpositions are those that involve the first element of the permutation. In their work they present an approximation algorithm with factor 2, adapted some results from the general transposition problem and gave an upper bound of $n - \lfloor n/4 \rfloor$ for the prefix transposition distance of the reverse permutation when $n \geq 4$, conjecturing that (1) this upper bound is actually the exact value of the prefix transposition distance of R_n; and (2) no other permutation has a larger distance than R_n. The first conjecture was proved true for $n \leq 16$ and the second for $n \leq 11$ by computational experiments. However, the upper bound for the prefix transposition distance was based on an algorithm whose correctness was not proved anywhere. In our work we present a new algorithm based on that one but with explicit formulas for the transpositions, which helped us to completely prove the correctness of the algorithm and finally establish this upper bound for sorting the reverse permutation by prefix transpositions.

2 Basic Definitions

Permutation A *permutation* of length n is any ordering of the elements from 1 to n. We can view a permutation as a bijection $\pi : 1, 2, \ldots, n \leftrightarrow 1, 2, \ldots, n$, in which $\pi(i) = j$ means that the element in position i is j. In other words, for all permutations π, $\pi = [\pi(1), \pi(2), \ldots, \pi(n)]$. Given a permutation π, we define its *inverse permutation* π^{-1} as being the inverse in the usual sense of inverse function. For example, given $\pi = [5, 1, 2, 4, 3]$, we have $\pi(1) = 5$, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(4) = 4$, $\pi(5) = 3$ and $\pi^{-1} = [2, 3, 5, 4, 1]$. We define the *identity permutation* ι of length n as a permutation such that $\iota(i) = i$, for all $i, 1 \leq i \leq n$. We define the *reverse permutation* R_n of length n as a permutation such that $R_n(i) = n - i + 1$, for all $i, 1 \leq i \leq n$.

Composition or application of permutations We can always change a permutation π into any another by changing the order of its elements. We achieve that by applying a permutation to π. To apply a permutation ϕ to a permutation π obtaining σ means to compose ϕ to the right of π, in the usual sense of functions, so that $\sigma = \pi \circ \phi$. In this case we can view ϕ as a *reordering* where $\phi(i) = j$ means that the element at position j moves to position i. Therefore, we can find ϕ by applying the desired reordering to the identity permutation. The resulting permutation is what we want. For example, let $\pi = [5, 1, 2, 4, 3]$ and suppose we want to invert the position of the first two elements and exchange them with the last two. Applying this operation to the identity yields $\phi = [4, 5, 3, 2, 1]$. Applying ϕ to π results in $\pi \circ \phi = [4, 3, 2, 1, 5]$, which has the desired effect.

Transposition A *transposition* is a reordering that removes a block of elements from the permutation and inserts it back in a new position. It can be seen as the exchange of two consecutive blocks of elements. We define $\tau(i, j, k)$, $1 \leq i \leq j \leq k \leq n+1$, as being the transposition that exchanges the block of elements in positions i to $j-1$ with the block of elements in positions j to $k-1$. If $i = j$ or $j = k$, one of the blocks is empty and the operation does not do anything. Analyzing the correspondence between the elements of the permutation before and after the transformation, it is not difficult to conclude that the transposition $\tau = \tau(i, j, k)$ can be characterized in the following way:

$$\tau(\ell) = \begin{cases} \ell & \text{if } 1 \leq \ell < i \\ \ell - i + j & \text{if } i \leq \ell < i + k - j \\ \ell - k + j & \text{if } i + k - j \leq \ell < k \\ \ell & \text{if } k \leq \ell < n \end{cases},$$

where n is the number of elements in τ.

As an example, let $\pi = [7, 4, 2, 8, 3, 1, 5, 6]$ and suppose we want to exchange the block of elements in positions 3 to 5 with the block of elements in positions 6 to 7. The desired transposition is $\tau = \tau(3, 6, 8) = [1, 2, 6, 7, 3, 4, 5, 8]$. So we have $\pi \circ \tau = [7, 4, 1, 5, 2, 8, 3, 6]$.

Notice that the inverse of a transposition is also a transposition. It is easy to see that $\tau(i, i+a, i+a+b)^{-1} = \tau(i, i+b, i+b+a)$ or, equivalently,$\tau(i, j, k)^{-1} = \tau(i, i+(k-j), k)$.

A *prefix transposition* is any transposition that moves the first element, that is, every transposition of the form $\tau(1, j, k)$.

Transposition Distance The *transposition distance* between two permutations π and σ is the minimum number of transpositions needed to change π into σ and is given by $d(\pi, \sigma)$. We define $d(\pi)$ as being the transposition distance between π and the identity permutation ι.

Prefix Transposition Distance The *prefix transposition distance* between two permutations π and σ is the minimum number of prefix transpositions needed to change π into σ and is given by $pd(\pi, \sigma)$. We define $pd(\pi)$ as being the prefix transposition distance between π and the identity permutation ι.

3 Algorithm to Sort R_n

Dias and Meidanis [3] present, without a proof, an algorithm to sort R_n. Based on that algorithm, we propose a new one, presented in Figure 1.

ALGORITHM SortRn
Input: $\pi = R_n$, with $n \geq 4$
Output: $\pi = \iota$

/ Phase 0: Reduces to n multiple of 4 */*
for($i \leftarrow 0$; $i < n \bmod 4$; $i++$)
    $\pi \leftarrow \pi \cdot \tau(1, 2, n + 1 - i)$
$n \leftarrow n - (n \bmod 4)$
/ At this point $\pi = R_n$, n multiple of 4 */*

/ Phase 1 */*
for($i \leftarrow 0$; $i < n/4 - 1$; $i++$)
    $\pi \leftarrow \pi \cdot \tau(1, 5, n - 2i)$
$\pi \leftarrow \pi \cdot \tau(1, 3, n/2 + 2)$
/ At this point $\pi = F_1$ */*

/ Phase 2 */*
for($i \leftarrow 0$; $i < n/4$; $i++$)
    $\pi \leftarrow \pi \cdot \tau(1, 3, n + 1 - 4i)$
/ At this point $\pi = F_2$ */*

/ Phase 3 */*
for($i \leftarrow 0$; $i < \lfloor n/8 \rfloor$; $i++$)
    $\pi \leftarrow \pi \cdot \tau(1, n - 4 - 4i, n - 4i)$
if($n \bmod 8 = 0$)
    $\pi \leftarrow \pi \cdot \tau(1, 3, n/2 + 2)$
else
    $\pi \leftarrow \pi \cdot \tau(1, n/2, n/2 + 2)$
/ At this point $\pi = F_3$ */*

/ Phase 4 */*
for($i \leftarrow 0$; $i < \lceil n/8 \rceil - 1$; $i--$)
    $\pi \leftarrow \pi \cdot \tau(1, 5, 4\lfloor n/8 \rfloor + 6 + 4i)$
/ At this point $\pi = \iota$ */*

return π

Figure 1: Algorithm to sort R_n

We will prove the correctness of this algorithm by splitting it into several phases and proving the transitions between them, working on the characterization of the permutation in each step of the process.

To characterize the permutations resulting from each intermediate phase of the algorithm, we will regard them as sequences and define a concatenation operator.

Definition The sequence $a \odot b$ will be the concatenation of the sequence a with the sequence b. We also define a generalized concatenation operator such that $\bigodot_{j=a}^{b} f(j)$ is the concatenation of the sequences $f(j)$ with j ranging from a to b. ∎

Example The following equalities illustrate the use of the operators:

$$[1,2,3] \odot [4,5,6] = [1,2,3,4,5,6]$$

$$\bigodot_{j=0}^{4} [1+3j, 2+3j] = [1,2,4,5,7,8,10,11,13,14] \quad \blacksquare$$

3.1 Phase 0

Phase 0 is responsible for reducing the problem of sorting R_n for any n to the problem of sorting R_n for n multiple of 4. What it does is nothing else than to place the n mod 4 extra elements, one at a time, at their final positions at the end of the permutation. This way they can be left out from this point on and thus we can consider n as being multiple of 4.

Example Phase 0 does, for $n = 6$, the following transformation:

$$[6,\ 5,\ 4,\ 3,\ 2,\ 1] \rightarrow [4,\ 3,\ 2,\ 1,\ 5,\ 6].$$

After this transformation, the problem reduces to sorting R_n for $n = 4$. ∎

3.2 Phase 1

To characterize *Phase 1* we will need to define a new family of permutations that will be called F_1.

Definition The permutation $F_1(n)$ is given by the following formula:

$$F_1(n) = [2] \odot \bigodot_{j=0}^{n/4-2} [n-4j,\ n-1-4j] \odot [4,\ 3] \odot \bigodot_{j=0}^{n/4-2} [6+4j,\ 5+4j] \odot [1]$$

When n is clear by the context, we will use just F_1. ∎

Example

$$F_1(12) = [2,\ 12,\ 11,\ 8,\ 7,\ 4,\ 3,\ 6,\ 5,\ 10,\ 9,\ 1] \quad \blacksquare$$

Lemma 1 Phase 1 *changes R_n, $n \geq 4$, into permutation $F_1(n)$.*

Proof Let π_i, $0 \le i \le n/4$, be the permutation obtained after i transpositions of *Phase 1*. Then we have the following recurrence:

$$\begin{array}{lcl} \pi_0 & = & R_n \\ \pi_i & = & \pi_{i-1} \cdot \tau(1,5,n-2i)\ ,\ \text{for } 1 \le i \le n/4-1 \\ \pi_{n/4} & = & \pi_{n/4-1} \cdot \tau(1,3,n/2+2) \end{array}$$

For $0 \le i \le n/4-1$ we have for permutation π_i the following formula:

$$\pi_i = \bigodot_{j=0}^{n-5-4i} [n-4i-j] \odot [4,\ 3,\ 2] \odot \bigodot_{j=0}^{i-1} [n-4j,\ n-1-4j] \odot \bigodot_{j=0}^{i-1} [n+2-4i+4j,\ n+1-4i+4j] \odot [1]$$

Or, equivalently:

$$\pi_i = \gamma_i \odot [4,\ 3,\ 2] \odot \alpha_i \odot \beta_i \odot [1],$$

where

$$\begin{array}{lcl} \gamma_i & = & \bigodot_{j=0}^{n-5-4i} [n-4i-j] \\ \alpha_i & = & \bigodot_{j=0}^{i-1} [n-4j,\ n-1-4j] \\ \beta_i & = & \bigodot_{j=0}^{i-1} [n+2-4i+4j,\ n+1-4i+4j]. \end{array}$$

The proof of this claim can be done by induction. For the base case $i = 0$ we have:

$$\begin{array}{lcl} \pi_0 & = & \bigodot_{j=0}^{n-5} [n-j] \odot [4,\ 3,\ 2] \odot \bigodot_{j=0}^{-1} [n-4j,\ n-1-4j] \odot \bigodot_{j=0}^{-1} [n+2+4j,\ n+1+4j] \odot [1] \\ & = & \bigodot_{j=0}^{n-5} [n-j] \odot [4,\ 3,\ 2] \odot [1] \\ & = & R_n \end{array}$$

Let us now prove that, for $1 \le i+1 \le n/4-1$, we have $\pi_i \cdot \tau(1,5,n-2i) = \pi_{i+1}$. Notice that what the i^{th} transposition of *Phase 1* does is to remove a prefix from γ_i and insert it back between α_i and β_i. This observation clarifies the following formulas relating the subsequences α, β and γ of π_i and π_{i+1}:

$$\begin{array}{lcl} \gamma_i & = & \bigodot_{j=0}^{n-5-4i} [n-4i-j] \\ & = & [n-4i,\ n-1-4i,\ n-2-4i,\ n-3-4i] \odot \\ & & \bigodot_{j=4}^{n-5-4i} [n-4i-j] \end{array}$$

$$
\begin{aligned}
&= [n-4i,\ n-1-4i,\ n-2-4i,\ n-3-4i] \odot \\
&\quad \bigodot_{j=0}^{n-5-4(i+1)} [n-4(i+1)-j,\ n-1-4(i+1)-j] \\
&= [n-4i,\ n-1-4i,\ n-2-4i,\ n-3-4i] \odot \gamma_{i+1}
\end{aligned}
$$

$$
\begin{aligned}
\alpha_{i+1} &= \bigodot_{j=0}^{i}[n-4j,\ n-1-4j] \\
&= \bigodot_{j=0}^{i-1}[n-4j,\ n-1-4j] \odot [n-4i,\ n-1-4i] \\
&= \alpha_i \odot [n-4i,\ n-1-4i]
\end{aligned}
$$

$$
\begin{aligned}
\beta_{i+1} &= \bigodot_{j=0}^{i}[n-2-4i+4j,\ n-1-4i+4j] \\
&= [n-2-4i,\ n-3-4i] \odot \bigodot_{j=1}^{i}[n-2-4i+4j,\ n-1-4i+4j] \\
&= [n-2-4i,\ n-3-4i] \odot \bigodot_{j=0}^{i-1}[n-2-4(i-1)+4j,\ n-3-4(i-1)+4j] \\
&= [n-2-4i,\ n-3-4i] \odot \beta_i
\end{aligned}
$$

It turns out that

$$
\begin{aligned}
\pi_i &= \gamma_i \odot [4,\ 3,\ 2] \odot \alpha_i \odot \beta_i \odot [1] \\
&= [n-4i,\ n-1-4i,\ n-2-4i,\ n-3-4i] \odot \gamma_{i+1} \odot [4,\ 3,\ 2] \odot \alpha_i \odot \beta_i \odot [1].
\end{aligned}
$$

Notice that transposition $\tau(1,5,n-2i)$ removes the 4-element prefix of π ant inserts it between α_i and β, since the size of $\beta_i \odot [1]$ is exactly $2i+1$. So we have

$$
\begin{aligned}
\pi_i \cdot \tau(1,5,n-2i) &= \gamma_{i+1} \odot [4,\ 3,\ 2] \odot \alpha_i \odot [n-4i,\ n-1-4i] \odot \\
&\quad [n-2-4i,\ n-3-4i] \odot \beta_i \odot [1] \\
&= \gamma_{i+1} \odot [4,\ 3,\ 2] \odot \alpha_{i+1} \odot \beta_{i+1} \odot [1] \\
&= \pi_{i+1},
\end{aligned}
$$

which proves that after $n/4-1$ transpositions of *Phase 1* we obtain the permutation

$$
\begin{aligned}
\pi_{n/4-1} &= \bigodot_{j=0}^{-1}[4-j] \odot [4,\ 3,\ 2] \odot \bigodot_{j=0}^{n/4-2} [n-4j,\ n-1-4j] \odot \bigodot_{j=0}^{n/4-2} [6+4j,\ 5+4j] \odot [1] \\
&= [4,\ 3,\ 2] \odot \bigodot_{j=0}^{n/4-2} [n-4j,\ n-1-4j] \odot \bigodot_{j=0}^{n/4-2} [6+4j,\ 5+4j] \odot [1].
\end{aligned}
$$

The last transposition of *Phase 1* is $\tau(1,3,n/2+2)$. So we have

$$\begin{aligned}\pi_{n/4} &= \pi_{n/4-1}\cdot\tau(1,3,n/2+2)\\ &= [2]\odot\bigodot_{j=0}^{n/4-2}[n-4j,\ n-1-4j]\odot[4,\ 3]\odot\bigodot_{j=0}^{n/4-2}[6+4j,\ 5+4j]\odot[1]\\ &= F_1(n),\end{aligned}$$

concluding our proof. ∎

3.3 Phase 2

To characterize *Phase 2* we will need to define a new family of permutations that will be called F_2.

Definition The permutation $F_2(n)$ is given by the following formula:

$$F_2(n) = [3]\odot\bigodot_{j=0}^{n/4-2}[6+4j,\ 7+4j,\ 4+4j,\ 5+4j]\odot[1,\ 2,\ n]$$

When n is clear by the context, we will use just F_2. ∎

Example

$$F_2(12) = [3,\ 6,\ 7,\ 4,\ 5,\ 10,\ 11,\ 8,\ 9,\ 1,\ 2,\ 12]$$ ∎

Lemma 2 Phase 2 *changes* $F_1(n)$*,* $n \geq 4$*, into permutation* $F_2(n)$*.*

Proof Let π_i, $0 \leq i \leq n/4$, be the permutation obtained after i transpositions of *Phase 2*. Then we have the following recurrence:

$$\begin{aligned}\pi_0 &= F_1(n)\\ \pi_{i+1} &= \pi_i\cdot\tau(1,3,n+1-4i)\ \text{, for } 0\leq i\leq n/4-1\end{aligned}$$

Then we have:

$$\begin{aligned}\pi_0 &= F_1(n)\\ &= [2]\odot\bigodot_{j=0}^{n/4-2}[n-4j,\ n-1-4j]\odot[4,\ 3]\odot\bigodot_{j=0}^{n/4-2}[6+4j,\ 5+4j]\odot[1]\\ &= [2,\ n]\odot[n-1]\odot\bigodot_{j=1}^{n/4-1}[n-4j,\ n-1-4j]\odot\bigodot_{j=0}^{n/4-2}[6+4j,\ 5+4j]\odot[1]\\ &= [2,\ n]\odot[n-1]\odot\bigodot_{j=0}^{n/4-2}[n-4-4j,\ n-5-4j]\odot\bigodot_{j=0}^{n/4-2}[6+4j,\ 5+4j]\odot[1]\end{aligned}$$

For $0 \leq i \leq n/4 - 1$, we have for permutation π_{i+1} the following formula:

$$\pi_{i+1} = [n-1-4i] \odot \alpha_{i+1} \odot \beta_{i+1} \odot \gamma_{i+1} \odot [1,\ 2,\ n],$$

where

$$\begin{aligned}
\alpha_{i+1} &= \bigodot_{j=0}^{n/4-2-i} [n-4-4i-4j,\ n-5-4i-4j] \\
\beta_{i+1} &= \bigodot_{j=0}^{n/4-2-i} [6+4j,\ 5+4j] \\
\gamma_{i+1} &= \bigodot_{j=0}^{i-1} [n+2-4i+4j,\ n+3-4i+4j,\ n-4i+4j,\ n+1-4i+4j].
\end{aligned}$$

The proof of this claim can be done by induction. For the base case $i = 0$ we have

$$\begin{aligned}
\pi_1 &= \pi_0 \cdot \tau(1, 3, n+1) \\
&= [n-1] \odot \bigodot_{j=0}^{n/4-2} [n-4-4j,\ n-5-4j] \odot \bigodot_{j=0}^{n/4-2} [6+4j,\ 5+4j] \odot [1] \odot [2,\ n] \\
&= [n+3-4\cdot 1] \odot \alpha_1 \odot \beta_1 \odot \gamma_1 \odot [1,\ 2,\ n],
\end{aligned}$$

where

$$\begin{aligned}
\alpha_1 &= \bigodot_{j=0}^{n/4-2} [n-4-4j,\ n-5-4j] \\
\beta_1 &= \bigodot_{j=0}^{n/4-2} [6+4j,\ 5+4j] \\
\gamma_1 &= \bigodot_{j=0}^{-1} [n+2+4j,\ n+3+4j,\ n+4j,\ n+1+4j] = [\ ].
\end{aligned}$$

Let us now prove that, for $1 \leq i \leq n/4 - 1$, we have $\pi_i \cdot \tau(1, 3, n+1-4i) = \pi_{i+1}$. It is important to check the following relationships among the subsequences of π_i and π_{i+1}:

$$\begin{aligned}
\alpha_i &= \bigodot_{j=0}^{n/4-2-(i-1)} [n-4i-4j,\ n-4i-4j-1] \\
&= [n-4i,\ n-1-4i] \odot \bigodot_{j=1}^{n/4-1-i} [n-4i-4j,\ n-1-4i-4j] \\
&= [n-4i,\ n-1-4i] \odot \bigodot_{j=0}^{n/4-2-i} [n-4(i+1)-4j,\ n-1-4(i+1)-4j] \\
&= [n-4i,\ n-1-4i] \odot \alpha_{i+1}
\end{aligned}$$

$$\begin{aligned}
\beta_i &= \bigodot_{j=0}^{n/4-1-i} [6+4j,\ 5+4j] \\
&= \bigodot_{j=0}^{n/4-1-(i+1)} [6+4j,\ 5+4j] \odot [n+2-4i,\ n+1-4i] \\
&= \beta_{i+1} \odot [n+2-4i,\ n+1-4i]
\end{aligned}$$

$$\begin{aligned}
\gamma_{i+1} &= \bigodot_{j=0}^{i-1} [n+2-4i+4j,\ n+3-4i+4j,\ n-4i+4j,\ n+1-4i+4j] \\
&= [n+2-4i,\ n+3-4i,\ n-4i,\ n+1-4i] \odot \\
&\quad \bigodot_{j=0}^{i-2} [n+6-4i+4j,\ n+7-4i+4j,\ n+4-4i+4j,\ n+5-4i+4j] \\
&= [n+2-4i,\ n+3-4i,\ n-4i,\ n+1-4i] \odot \gamma_i
\end{aligned}$$

It turns out that

$$\begin{aligned}
\pi_i &= [n+3-4i] \odot \alpha_i \odot \beta_i \odot \gamma_i \odot [1,\ 2,\ n] \\
&= [n+3-4i] \odot [n-4i,\ n+1-4i] \odot \alpha_{i+1} \odot \\
&\quad \beta_{i+1} \odot [n+2-4i,\ n+1-4i] \odot \gamma_i \odot [1,\ 2,\ n] \\
&= [n+3-4i,\ n-4i] \odot [n-1-4i] \odot \alpha_{i+1} \odot \\
&\quad \beta_{i+1} \odot [n+2-4i] \odot [n+1-4i] \odot \gamma_i \odot [1,\ 2,\ n].
\end{aligned}$$

Notice that transposition $\tau(1, 3, n+1-4i)$ removes prefix $[n+3-4i,\ n-4i]$ from π_i and inserts it between $[n+2-4i]$ and $[n+1-4i]$, as the size of the suffix $[n+1-4i] \odot \gamma_i \odot [1,\ 2,\ n]$ is exactly $1 + 4(i-1) + 3 = 4i$. Then we have

$$\begin{aligned}
\pi_{i+1} &= \pi_i \cdot \tau(1, 3, n+1-4i) \\
&= [n-4i-1] \odot \alpha_{i+1} \odot \beta_{i+1} \odot \\
&\quad [n-4i+2] \odot [n+3-4i,\ n-4i] \odot [n+1-4i] \odot \gamma_i \odot [1,\ 2,\ n] \\
&= [n-1-4i] \odot \alpha_{i+1} \odot \beta_{i+1} \odot \\
&\quad [n+2-4i,\ n+3-4i,\ n-4i,\ n+1-4i] \odot \gamma_i \odot [1,\ 2,\ n] \\
&= [n-1-4i] \odot \alpha_{i+1} \odot \beta_{i+1} \odot \gamma_{i+1} \odot [1,\ 2,\ n],
\end{aligned}$$

which proves that after all the $n/4$ transposition of *Phase 2* we obtain the permutation

$$\pi_{n/4} = [3] \odot \alpha_{n/4} \odot \beta_{n/4} \odot \gamma_{n/4} \odot [1,\ 2,\ n]$$

$$\begin{aligned}
\alpha_{n/4} &= \bigodot_{j=0}^{-1}[-4j,\ -1-4j] = [\ ] \\
\beta_{n/4} &= \bigodot_{j=0}^{-1}[6+4j,\ 5+4j] = [\ ] \\
\gamma_{n/4} &= \bigodot_{j=0}^{n/4-2}[6+4j,\ 7+4j,\ 4+4j,\ 5+4j].
\end{aligned}$$

That is,

$$\begin{aligned}
\pi_{n/4} &= [3] \odot \bigodot_{j=0}^{n/4-2}[6+4j,\ 7+4j,\ 4+4j,\ 5+4j] \odot [1,\ 2,\ n] \\
&= F_2(n),
\end{aligned}$$

concluding our proof. ■

3.4 Phase 3

To characterize *Phase 3* we will need to define a new family of permutations that will be called F_3.

Definition The permutation $F_3(n)$ is given by the following formula:

$$\begin{aligned}
F_3(n) &= \bigodot_{j=0}^{\lceil n/8\rceil-2}\bigodot_{k=0}^{3}[10-n \bmod 8+8j+k] \odot [1,\ 2,\ 3,\ 4,\ 5] \odot \\
&\quad \bigodot_{j=0}^{\lfloor n/8\rfloor-2}\bigodot_{k=0}^{3}[6+n \bmod 8+8j+k] \odot [n-2,\ n-1,\ n]
\end{aligned}$$

When n is clear by the context, we will use just F_3. ■

Example

$$F_3(16) = [10,\ 11,\ 12,\ 13,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 14,\ 15,\ 16]$$

$$F_3(20) = [6,\ 7,\ 8,\ 9,\ 14,\ 15,\ 16,\ 17,\ 1,\ 2,\ 3,\ 4,\ 5,\ 10,\ 11,\ 12,\ 13,\ 18,\ 19,\ 20]$$ ■

Lemma 3 Phase 3 *changes $F_2(n)$, $n \geq 8$, into permutation $F_3(n)$.*

Proof Let π_i, $0 \leq i \leq \lfloor n/8\rfloor + 1$, be the permutation obtained after i transpositions of *Phase 3*. Then we have the following recurrence:

$$\begin{aligned}
\pi_0 &= F_2(n) \\
\pi_{i+1} &= \pi_i \cdot \tau(1, n-4-4i, n-4i)\ \text{, for } 0 \leq i \leq \lfloor n/8\rfloor - 1 \\
\pi_{\lfloor n/8\rfloor+1} &= \begin{cases} \pi_{\lfloor n/8\rfloor} \cdot \tau(1, 3, n/2+2) & \text{, if } n \bmod 8 = 0 \\ \pi_{\lfloor n/8\rfloor} \cdot \tau(1, n/2, n/2+2) & \text{, if } n \bmod 8 \neq 0 \end{cases}
\end{aligned}$$

Then we have, for $n \geq 8$:

$$\begin{aligned}
\pi_0 &= F_2(n) \\
&= [3] \odot \bigodot_{j=0}^{n/4-2} [6+4j,\ 7+4j,\ 4+4j,\ 5+4j] \odot [1,\ 2,\ n] \\
&= [3] \odot \bigodot_{j=0}^{n/4-3} [6+4j,\ 7+4j,\ 4+4j,\ 5+4j] \odot [n-2,\ n-1,\ n-4,\ n-3,\ 1,\ 2,\ n].
\end{aligned}$$

For $0 \leq i \leq \lfloor n/8 \rfloor - 1$, we have for permutation π_{i+1} the following formula:

$$\pi_{i+1} = [n-4-8i,\ n-3-8i] \odot \alpha_{i+1} \odot [1,\ 2,\ 3] \odot \beta_{i+1} \odot \gamma_{i+1} \odot [n-2,\ n-1,\ n],$$

where

$$\begin{aligned}
\alpha_{i+1} &= \bigodot_{j=0}^{i-1} \bigodot_{k=0}^{3} [n+2-8i+8j+k] \\
\beta_{i+1} &= \bigodot_{j=0}^{n/4-3-2i} [6+4j,\ 7+4j,\ 4+4j,\ 5+4j] \\
\gamma_{i+1} &= \bigodot_{j=0}^{i-1} \bigodot_{k=0}^{3} [n-2-8i+8j+k].
\end{aligned}$$

We can prove this claim by induction. For the base case $i = 0$ we have

$$\begin{aligned}
\pi_1 &= \pi_0 \cdot \tau(1, n-4, n) \\
&= [n-4,\ n-3,\ 1,\ 2,\ 3] \odot \bigodot_{j=0}^{n/4-3} [6+4j,\ 7+4j,\ 4+4j,\ 5+4j] \odot [n-2,\ n-1,\ n] \\
&= [n+4-8,\ n+5-8] \odot \alpha_1 \odot [1,\ 2,\ 3] \odot \beta_1 \odot \gamma_1 \odot [n-2,\ n-1,\ n],
\end{aligned}$$

where

$$\begin{aligned}
\alpha_1 &= \bigodot_{j=0}^{-1} \bigodot_{k=0}^{3} [n+10-8+8j+k] = [\ ] \\
\beta_1 &= \bigodot_{j=0}^{n/4-3} [6+4j,\ 7+4j,\ 4+4j,\ 5+4j] \\
\gamma_1 &= \bigodot_{j=0}^{-1} \bigodot_{k=0}^{3} [n+6-8+8j+k] = [\ ].
\end{aligned}$$

Let us now prove that, for $1 \leq i \leq \lfloor n/8 \rfloor - 1$, we have $\pi_i \cdot \tau(1, n-4-4i, n-4i) = \pi_{i+1}$. It is important to check the following relationships among subsequences of π_i and π_{i+1}:

$$
\begin{aligned}
\alpha_{i+1} &= \bigodot_{j=0}^{i-1}\bigodot_{k=0}^{3}[n+2-8i+8j+k] \\
&= \bigodot_{k=0}^{3}[n+2-8i+k] \odot \bigodot_{j=0}^{i-2}\bigodot_{k=0}^{3}[n+2-8(i-1)+8j+k] \\
&= [n+2-8i,\ n+3-8i,\ n+4-8i,\ n+5-8i] \odot \alpha_i
\end{aligned}
$$

$$
\begin{aligned}
\beta_i &= \bigodot_{j=0}^{n/4-2i-1} [6+4j,\ 7+4j,\ 4+4j,\ 5+4j] \\
&= \bigodot_{j=0}^{n/4-2i-3} [6+4j,\ 7+4j,\ 4+4j,\ 5+4j] \odot \\
&\quad [n-2-8i,\ n-1-8i,\ n-4-8i,\ n-3-8i] \odot \\
&\quad [n+2-8i,\ n+3-8i,\ n-8i,\ n+1-8i] \\
&= \beta_{i+1} \odot [n-2-8i,\ n-1-8i] \odot \\
&\quad [n-4-8i,\ n-3-8i,\ n+2-8i,\ n+3-8i] \odot [n-8i,\ n+1-8i]
\end{aligned}
$$

$$
\begin{aligned}
\gamma_{i+1} &= \bigodot_{j=0}^{i-1}\bigodot_{k=0}^{3}[n-2-8i+8j+k] \\
&= \bigodot_{k=0}^{3}[n-2-8i+k] \odot \bigodot_{j=0}^{i-2}\bigodot_{k=0}^{3}[n-2-8(i-1)+8j+k] \\
&= [n-2-8i,\ n-1-8i,\ n-8i,\ n+1-8i] \odot \gamma_i
\end{aligned}
$$

It turns out that

$$
\begin{aligned}
\pi_i &= [n+4-8i,\ n+5-8i] \odot \alpha_i \odot [1,\ 2,\ 3] \odot \beta_i \odot \gamma_i \odot [n-2,\ n-1,\ n] \\
&= [n+4-8i,\ n+5-8i] \odot \alpha_i \odot [1,\ 2,\ 3] \odot \beta_{i+1} \odot \\
&\quad [n-2-8i,\ n-1-8i] \odot [n-4-8i,\ n-3-8i,\ n+2-8i,\ n+3-8i] \odot \\
&\quad [n-8i,\ n+1-8i] \odot \gamma_i \odot [n-2,\ n-1,\ n].
\end{aligned}
$$

Notice that transposition $\tau(1, n-4-4i, n-4i)$ removes block $[n-4-8i,\ n-3-8i,\ n+2-8i,\ n+3-8i]$ from π_i and inserts it at the beginning of the permutation, as the size of the suffix $[n-8i,\ n+1-8i] \odot \gamma_i \odot [n-2,\ n-1,\ n]$ is exactly $2+4(i-1)+3 = 4i+1$. Then we have

$$
\pi_{i+1} = \pi_i \cdot \tau(1, n-4-4i, n-4i)
$$

$$
\begin{aligned}
= \; & [n-4-8i,\; n-3-8i,\; n+2-8i,\; n+3-8i] \odot [n+4-8i,\; n+5-8i] \odot \\
& \alpha_i \odot [1,\; 2,\; 3] \odot \beta_{i+1} \odot \\
& [n-2-8i,\; n-1-8i] \odot [n-8i,\; n+1-8i] \odot \gamma_i \odot [n-2,\; n-1,\; n] \\
\\
= \; & [n-4-8i,\; n-3-8i] \odot [n+2-8i,\; n+3-8i,\; n+4-8i,\; n+5-8i] \odot \\
& \alpha_i \odot [1,\; 2,\; 3] \odot \beta_{i+1} \odot \\
& [n-2-8i,\; n-1-8i,\; n-8i,\; n+1-8i] \odot \gamma_i \odot [n-2,\; n-1,\; n] \\
\\
= \; & [n-4-8i,\; n-3-8i] \odot \alpha_{i+1} \odot [1,\; 2,\; 3] \odot \beta_{i+1} \odot \gamma_{i+1} \odot [n-2,\; n-1,\; n],
\end{aligned}
$$

which proves that after $\lfloor n/8 \rfloor$ transpositions of *Phase 3*, for $n \geq 8$, we obtain the permutation

$$
\begin{aligned}
\pi_{\lfloor n/8 \rfloor} \;=\; & [4+n \bmod 8,\; 5+n \bmod 8] \odot \alpha_{\lfloor n/8 \rfloor} \odot \\
& [1,\; 2,\; 3] \odot \beta_{\lfloor n/8 \rfloor} \odot \gamma_{\lfloor n/8 \rfloor} \odot [n-2,\; n-1,\; n],
\end{aligned}
$$

where

$$
\begin{aligned}
\alpha_{\lfloor n/8 \rfloor} &= \bigodot_{j=0}^{\lfloor n/8 \rfloor - 2} \bigodot_{k=0}^{3} [10 + n \bmod 8 + 8j + k] \\
\beta_{\lfloor n/8 \rfloor} &= \bigodot_{j=0}^{(n \bmod 8)/4-1} [6+4j,\; 7+4j,\; 4+4j,\; 5+4j] \\
\gamma_{\lfloor n/8 \rfloor} &= \bigodot_{j=0}^{\lfloor n/8 \rfloor - 2} \bigodot_{k=0}^{3} [6 + n \bmod 8 + 8j + k].
\end{aligned}
$$

Step $\lfloor n/8 \rfloor + 1$ depends on the value of $n \bmod 8$. We have two cases.

Case 1: $n \bmod 8 = 0$
In this case we have

$$
\pi_{\lfloor n/8 \rfloor} = [4,\; 5] \odot \alpha_{\lfloor n/8 \rfloor} \odot [1,\; 2,\; 3] \odot \beta_{\lfloor n/8 \rfloor} \odot \gamma_{\lfloor n/8 \rfloor} \odot [n-2,\; n-1,\; n],
$$

where

$$
\begin{aligned}
\alpha_{\lfloor n/8 \rfloor} &= \bigodot_{j=0}^{n/8-2} \bigodot_{k=0}^{3} [10 + 8j + k] \\
\beta_{\lfloor n/8 \rfloor} &= \bigodot_{j=0}^{-1} [6+4j,\; 7+4j,\; 4+4j,\; 5+4j] = [\;] \\
\gamma_{\lfloor n/8 \rfloor} &= \bigodot_{j=0}^{n/8-2} \bigodot_{k=0}^{3} [6 + 8j + k].
\end{aligned}
$$

Notice that transposition $\tau(1,3,n/2+2)$ removes block $[4,\ 5]$ from $\pi_{\lfloor n/8 \rfloor}$ and inserts it just after block [1, 2, 3], as the size of prefix $[4,\ 5] \odot \alpha_{\lfloor n/8 \rfloor} \odot [1,\ 2,\ 3]$ is exactly $2+4(n/8-1)+3 = n/2+1$. Then we have

$$\begin{aligned}
\pi_{\lfloor n/8 \rfloor + 1} &= \pi_{\lfloor n/8 \rfloor} \cdot \tau(1,3,n/2+2) \\
&= \alpha_{\lfloor n/8 \rfloor} \odot [1,\ 2,\ 3,\ 4,\ 5] \odot \gamma_{\lfloor n/8 \rfloor} \odot [n-2,\ n-1,\ n] \\
&= \bigodot_{j=0}^{\lceil n/8 \rceil - 2} \bigodot_{k=0}^{3} [10+8j+k] \odot [1,\ 2,\ 3,\ 4,\ 5] \odot \\
&\quad \bigodot_{j=0}^{\lfloor n/8 \rfloor - 2} \bigodot_{k=0}^{3} [6+8j+k] \odot [n-2,\ n-1,\ n] \\
&= F_3(n).
\end{aligned}$$

Case 2: $n \bmod 8 = 4$
In this case we have

$$\pi_{\lfloor n/8 \rfloor} = [8,\ 9] \odot \alpha_{\lfloor n/8 \rfloor} \odot [1,\ 2,\ 3] \odot \beta_{\lfloor n/8 \rfloor} \odot \gamma_{\lfloor n/8 \rfloor} \odot [n-2,\ n-1,\ n],$$

where

$$\begin{aligned}
\alpha_{\lfloor n/8 \rfloor} &= \bigodot_{j=0}^{(n-4)/8-2} \bigodot_{k=0}^{3} [14+8j+k] \\
\beta_{\lfloor n/8 \rfloor} &= \bigodot_{j=0}^{0} [6+4j,\ 7+4j,\ 4+4j,\ 5+4j] = [6,\ 7,\ 4,\ 5] \\
\gamma_{\lfloor n/8 \rfloor} &= \bigodot_{j=0}^{(n-4)/8-2} \bigodot_{k=0}^{3} [10+8j+k].
\end{aligned}$$

Notice that transposition $\tau(1,n/2,n/2+2)$ removes block $[6,\ 7]$ from $\pi_{\lfloor n/8 \rfloor}$ and inserts it at the beginning of the permutation, as the size of prefix $[8,\ 9] \odot \alpha_{\lfloor n/8 \rfloor} \odot [1,\ 2,\ 3]$ is exactly $2+4((n-4)/8-1)+3 = n/2-1$. Then we have

$$\begin{aligned}
\pi_{\lfloor n/8 \rfloor + 1} &= \pi_{\lfloor n/8 \rfloor} \cdot \tau(1,n/2,n/2+2) \\
&= [6,\ 7,\ 8,\ 9] \odot \alpha_{\lfloor n/8 \rfloor} \odot [1,\ 2,\ 3,\ 4,\ 5] \odot \gamma_{\lfloor n/8 \rfloor} \odot [n-2,\ n-1,\ n] \\
&= [6,\ 7,\ 8,\ 9] \odot \bigodot_{j=0}^{(n-4)/8-2} \bigodot_{k=0}^{3} [14+8j+k] \odot [1,\ 2,\ 3,\ 4,\ 5] \odot
\end{aligned}$$

$$\bigodot_{j=0}^{(n-4)/8-2} \bigodot_{k=0}^{3} [10+8j+k] \odot [n-2,\ n-1,\ n]$$

$$= \bigodot_{j=0}^{(n-4)/8-1} \bigodot_{k=0}^{3} [6+8j+k] \odot [1,\ 2,\ 3,\ 4,\ 5] \odot \bigodot_{j=0}^{(n-4)/8-2} \bigodot_{k=0}^{3} [10+8j+k] \odot [n-2,\ n-1,\ n]$$

$$= \bigodot_{j=0}^{\lceil n/8 \rceil -2} \bigodot_{k=0}^{3} [6+8j+k] \odot [1,\ 2,\ 3,\ 4,\ 5] \odot \bigodot_{j=0}^{\lfloor n/8 \rfloor -2} \bigodot_{k=0}^{3} [10+8j+k] \odot [n-2,\ n-1,\ n]$$

$$= F_3(n),$$

which concludes our proof. ∎

3.5 Phase 4

Lemma 4 Phase 4 *changes $F_3(n)$, $n \geq 8$, into the identity permutation ι.*

Proof We are now considering the case $n \geq 8$ only. Let π_i, $0 \leq i \leq (n + n \bmod 8)/8 - 1$, be the sequence obtained after i transpositions of *Phase 4*. Then we have the following recurrence:

$$\pi_{i+1} = \pi_i \cdot \tau(1, 5, 4\lfloor n/8 \rfloor + 6 + 4i).$$

We have for permutation π_i the following formula:

$$\pi_i = \bigodot_{j=0}^{\lceil n/8 \rceil -2-i} \bigodot_{k=0}^{3} [10 - n \bmod 8 + 8i + 8j + k] \odot \bigodot_{j=0}^{8-n \bmod 8+8i} [1+j] \odot \bigodot_{j=0}^{\lceil n/8 \rceil -2-i} \bigodot_{k=0}^{3} [14 - n \bmod 8 + 8i + 8j + k].$$

Notice that we have appended the element $n+1$ to the permutation to simplify its representation, what does not interfere with the result.

The proof of the formula above can be done by induction. For the base case $i = 0$ we have, for $n \bmod 8 = 0$,

$$\pi_0 = F_3(n)$$

$$= \bigodot_{j=0}^{n/8-2} \bigodot_{k=0}^{3} [10+8j+k] \odot [1,\ 2,\ 3,\ 4,\ 5] \odot$$

$$\bigodot_{j=0}^{n/8-2}\bigodot_{k=0}^{3}[6+8j+k]\odot[n-2,\ n-1,\ n].$$

Appending element $n+1$:

$$\begin{aligned}\pi_0 &= \bigodot_{j=0}^{n/8-2}\bigodot_{k=0}^{3}[10+8j+k]\odot[1,\ 2,\ 3,\ 4,\ 5]\odot\\ &\quad \bigodot_{j=0}^{n/8-2}\bigodot_{k=0}^{3}[6+8j+k]\odot[n-2,\ n-1,\ n,\ n+1]\\ &= \bigodot_{j=0}^{\lceil n/8\rceil-2}\bigodot_{k=0}^{3}[10-n \bmod 8+8j+k]\odot\bigodot_{j=0}^{8-n \bmod 8}[1+j]\odot\\ &\quad \bigodot_{j=0}^{\lceil n/8\rceil-2}\bigodot_{k=0}^{3}[14-n \bmod 8+8j+k].\end{aligned}$$

For $n \bmod 8 = 4$ we have

$$\begin{aligned}\pi_0 &= F_3(n)\\ &= \bigodot_{j=0}^{(n+4)/8-2}\bigodot_{k=0}^{3}[6+8j+k]\odot[1,\ 2,\ 3,\ 4,\ 5]\odot\\ &\quad \bigodot_{j=0}^{(n-4)/8-2}\bigodot_{k=0}^{3}[10+8j+k]\odot[n-2,\ n-1,\ n].\end{aligned}$$

Appending element $n+1$:

$$\begin{aligned}\pi_0 &= \bigodot_{j=0}^{(n+4)/8-2}\bigodot_{k=0}^{3}[6+8j+k]\odot[1,\ 2,\ 3,\ 4,\ 5]\odot\\ &\quad \bigodot_{j=0}^{(n-4)/8-2}\bigodot_{k=0}^{3}[10+8j+k]\odot[n-2,\ n-1,\ n,\ n+1]\\ &= \bigodot_{j=0}^{\lceil n/8\rceil-2}\bigodot_{k=0}^{3}[10-n \bmod 8+8j+k]\odot\bigodot_{j=0}^{8-n \bmod 8}[1+j]\odot\\ &\quad \bigodot_{j=0}^{\lceil n/8\rceil-2}\bigodot_{k=0}^{3}[14-n \bmod 8+8j+k].\end{aligned}$$

Let us now prove that, for $1 \le i+1 \le (n+n \bmod 8)/8-1$, we have $\pi_i \cdot \tau(1, 5, 4\lfloor n/8\rfloor+6+4i) = \pi_{i+1}$. Notice that the transposition removes prefix $\bigodot_{k=0}^{3}[10-n \bmod 8+8i+k]$ and inserts it just after block $\bigodot_{j=0}^{8-n \bmod 8+8i}[1+j]$, as the size of prefix $\bigodot_{j=0}^{\lceil n/8\rceil-2-i}\bigodot_{k=0}^{3}[10-n \bmod 8+$

$8i+8j+k] \odot \bigodot_{j=0}^{8-n \bmod 8+8i}[1+j]$ is exactly $4((n+n \bmod 8)/8-1-i)+9-n \bmod 8+8i = 4\lfloor n/8 \rfloor + 5 + 4i$. Then we have:

$$\begin{aligned}
\pi_{i+1} &= \pi_i \cdot \tau(1, 5, 4\lfloor n/8 \rfloor + 6 + 4i) \\
&= \bigodot_{j=0}^{\lceil n/8 \rceil - 3 - i} \bigodot_{k=0}^{3} [18 - n \bmod 8 + 8i + 8j + k] \odot \bigodot_{j=0}^{(8-n \bmod 8+8i)} [1+j] \odot \\
&\quad \bigodot_{k=0}^{3} [10 - n \bmod 8 + 8i + k] \odot \bigodot_{j=0}^{\lceil n/8 \rceil - 2 - i} \bigodot_{k=0}^{3} [14 - n \bmod 8 + 8i + 8j + k] \\
&= \bigodot_{j=0}^{\lceil n/8 \rceil - 3 - i} \bigodot_{k=0}^{3} [18 - n \bmod 8 + 8i + 8j + k] \odot \bigodot_{j=0}^{16-n \bmod 8+8i} [1+j] \odot \\
&\quad \bigodot_{j=0}^{\lceil n/8 \rceil - 3 - i} \bigodot_{k=0}^{3} [22 - n \bmod 8 + 8i + 8j + k] \\
&= \bigodot_{j=0}^{\lceil n/8 \rceil - 2 - (i+1)} \bigodot_{k=0}^{3} [10 - n \bmod 8 + 8(i+1) + 8j + k] \odot \bigodot_{j=0}^{8-n \bmod 8+8(i+1)} [1+j] \odot \\
&\quad \bigodot_{j=0}^{\lceil n/8 \rceil - 2 - (i+1)} \bigodot_{k=0}^{3} [14 - n \bmod 8 + 8(i+1) + 8j + k],
\end{aligned}$$

which proves that after the $\lceil n/8 - 1 \rceil$ transpositions of *Phase 4* we obtain the permutation

$$\begin{aligned}
\pi_{(n+n \bmod 8)/8-1} &= \bigodot_{j=0}^{-1} [n+2+8j,\ n+3+8j,\ n+4+8j,\ n+5+8j] \odot \bigodot_{j=0}^{n} [1+j] \odot \\
&\quad \bigodot_{j=0}^{-1} [n+6+8j,\ n+7+8j,\ n+8+8j,\ n+9+8j] \\
&= \iota,
\end{aligned}$$

concluding our proof. ∎

Theorem 1 *The algorithm presented in Figure 1 sorts R_n with $n - \lfloor n/4 \rfloor$ steps.*

Proof The theorem, for $n \geq 8$, is a direct consequence of the application of lemmas 2, 3, 4, 5 in sequence. For $n = 4$ it is enough to run the algorithm and verify that it sorts indeed. ∎

Corollary 1 $pd(R_n) \leq n - \lfloor n/4 \rfloor$

4 Conclusion and Future Work

We have concluded that the prefix transposition distance for the reverse permutation is at most $n - \lfloor n/4 \rfloor$. We conjecture that this value is not only an upper bound, but also the exactly distance. Computational results from Dias and Meidanis [3] shows that this is in fact true for n up to 16. A next step would be to find a lower bound that proves this claim, which would give a new lower bound for the prefix transposition diameter higher than the current $\lceil n/2 \rceil$ value.

Another conjecture is that the prefix transposition diameter for permutation of size n equals $pd(R_n)$. This would be a much better upper bound for the distance than the current $n-1$ value.

We have also seen that permutations F_1, F_2 and F_3 are special in the sense that they achieve the *breakpoint lower bound* that says $pd(\pi) \geq \lceil((\#breakpoints\ of\ \pi) - 1)/2\rceil$. The study of such permutations may give us a new insight about the problem.

References

[1] V. Bafna and P. A. Pevzner. Sorting by transpositions. In *Proceedings of the Sixth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 614–623, San Francisco, USA, January 1995.

[2] A. Caprara. Sorting by reversals is difficult. In *Proceedings of the First International Conference on Computational Molecular Biology - (RECOMB'97)*, pages 75–83, New York, USA, January 1997. ACM Press.

[3] Z. Dias and J. Meidanis. Sorting by prefix transpositions. In A. H. F. Laender and A. L. Oliveira, editors, *Proceedings of the String Processing and Information Retrieval (SPIRE'2002)*, number 2476 in Lecture Notes in Computer Science, pages 65–76, Lisboa, Portugal, September 2002. Springer-Verlag, Berlin.

[4] H. Dweighter. *American Mathematical Monthly*, volume 82, page 1010. The Mathematical Association of America, 1975.

[5] H. Eriksson, K. Eriksson, J. Karlander, L. Svensson, and J. Wästlund. Sorting a bridge hand. *Discrete Mathematics*, 241:289–300, 2001.

[6] S. Hannenhalli and P. A. Pevzner. Transforming cabbage into turnip (polynomial algorithm for sorting signed permutations by reversals). In *Proceedings of the Twenty-Seventh Annual ACM Symposium on the Theory of Computing*, pages 178–189, Las Vegas, USA, May 1995.

[7] M. H. Heydari and I. H. Sudborough. Sorting by prefix reversals is NP-complete. To be submitted.

[8] J. D. Palmer and L. A. Herbon. Plant mitochondrial dna evolves rapidly in structure, but slowly in sequence. *Journal of Molecular Evolution*, 27:87–97, 1988.

[9] J. C. Setubal and J. Meidanis. *Introduction to Computional Molecular Biology*. PWS Publishing Company, 1997.