Factoring a Permutation on a Broom

Theresa P. Vaughan
Department of Mathematics
University of North Carolina at Greensboro
Greensboro, NC 27412

May 19, 1997

Abstract

A tree T consisting of a line with edges $\{(1,2),(2,3),\cdots,(n-1,n)\}$ and with edges $\{(1,a_1),(1,a_2),\cdots,(1,a_k)\}$ (a star) attached on the left, is called a broom. The edges of the tree T are called T-transpositions. We give an algorithm to factor any permutation σ of $\{a_1,a_2,\cdots,a_k,1,2,\cdots,n\}$ as a product of T-transpositions, and prove that the factorization produced by the algorithm has minimal length.

1 Introduction

Let $T=\{t_1,t_2,\cdots,t_m\}$ be a set of distinct transpositions in the symmetric group S_n. Cayley [1] proved that T is a minimal generating set for S_n if and only if $m=n-1$ and the t_i form the edges of a tree with n vertices. If $\sigma\in S_n$, and if σ is written as a product of members of T, then this product is called a $T-factorization$ of σ, and the minimum length of such a product is called the $T-rank$ of σ; a T- factorization of σ whose length is the T-rank of σ, is called a minimal T-factorization. If T is a line (two vertices of degree 1 and n-2 vertices of degree 2) or a star (one vertex of degree n-1 and n-1 vertices of degree 1), then algorithms are known which produce minimal T-factorizations, and the computation of T-rank is almost trivial in the case of a star (see, e.g. [6]), and straightforward in the case of a line (see [2]).

For general trees T, comparatively little is known about T-rank or minimal T-factorizations. Some upper and lower bounds for T-rank are given in [3], and a general factoring algorithm is given in [5], which —although it does not always produce minimal factorizations—is easily implemented on a computer, is quite fast, and usually comes fairly close (indeed, for the line and the star, it is minimal).

In this paper we describe an algorithm which gives minimal T-factorizations when T is a broom (a line with a star attached at one end). Easy examples show

JCMCC **30** (1999), pp. 129-148

that the general algorithm of [5] is not always minimal. However, by studying these factorizations and attempting to reduce them, it became apparent that we must make greater use of the geometric structure of the broom, in order to avoid the excesses of the general algorithm.

We begin by describing the algorithm, and then observe that a T-factorization produced by the algorithm has certain properties. Next, taking these properties one by one, we show that any T- factorization can be rewritten, rearranged, and generally transformed, in such a way that the result of the rearrangement is a T-factorization of no greater length, and having the property in question. Then, having arrived at a T-factorization having all of a crucial set of properties, we show that it can always be rewritten so that it agrees with the minimal T-factorization produced by the algorithm in at least one transposition on the far right side; then by induction it follows that every T-factorization can be rearranged, without increasing its length, to agree with the minimal T- factorization produced by the algorithm. The details of the argument depend heavily on the nature of the minimal algorithms for the line and the star, and we discuss these, and a few other things, in Section 2. In Section 3 we describe the algorithm, and list the pertinent properties of a T-factorization produced by the algorithm. In Section 4, we describe nine transformations used to get a factorization in a useful form, which is then used in Sections 5 and 6 to derive the final result. In Section 7 we discuss the T-rank.

2 Preliminaries

In this section we give some preliminary definitions, and notation to be used throughout the paper, and state briefly some well-known properties of factorizations of permutations on the line and the star.

Definition 2.1 *Let T be a finite tree, with vertex set $V(T) = \{1, 2, \cdots, m\}$ and edge set $E(T) = \{[a_1, b_1], \cdots, [a_{m-1}, b_{m-1}]\}$. The transpositions (a_i, b_i) are the T- transpositions, and we may also refer to them (an abuse of language) as "edges of T".*

Definition 2.2 *If σ is any permutation in S_m, and if $\sigma = t_k \cdots t_1$ where each t_i is a T-transposition, then $t_k \cdots t_1$ is a T-factorization of σ, of length k. If $\sigma = t_k \cdots t_1$ is a T-factorization of minimal length, then the factorization is said to be minimal, and the integer k is the T-rank of σ. If $\sigma = t_k \cdots t_1$ is any T- factorization, then $E(t_k \cdots t_1)$ is the set of those edges of T, $\{t_1, t_2, \cdots, t_k\}$, which appear in the factorization.*

Definition 2.3 *A line is a tree T with vertex set $V(T) = \{1, 2, \cdots, n\}$ and edge set $E(T) = \{[1, 2], [2, 3], \cdots, [n-1, n]\}$. A star is a tree T with $V(T) = \{1, a_1, a_2, \cdots, a_k\}$ and $E(T) = \{[1, a_1], [1, a_2], \cdots, [1, a_k]\}$; the vertex 1 is the center of the star. A broom is a tree T with $V(T) = \{a_1, a_2, \cdots, a_k, 1, 2, \cdots, n\}$*

and $E(T) = \{[1,a_1],[1,a_2],\cdots,[1,a_k],[1,2],[2,3],\cdots,[n-1,n]\}$. *For a broom* T, *we refer to the subgraph with vertices* $\{1,2,\cdots,n\}$ *as the line* L, *and the subgraph with edges* $[1,a_1],[1,a_2],\cdots,[1,a_k]$ *as the star* S, *and we define a partial order* $<$ *on* T *such that if* $x,y \in L$, *then* $x < y$ *means that* x *is smaller than* y, *and if* $x \in L$, *then* $a_i < x$ *for all* $i = 1,2,\cdots,k$.

For a permutation on a tree T which is either a line or a star, there are known algorithms to produce minimal factorizations, and also methods to compute the T-rank. We summarize these briefly here. For details, see Knuth [2] for the line, and Portier and Vaughan [6] for the star.

If σ is a permutation on a line $L = \{1,2,\cdots,n\}$, then an inversion pair of σ is a pair $\{i,j\}$ such that $i < j$ and $\sigma(i) > \sigma(j)$. The L-rank of σ is the number of inversion pairs of σ. An adjacent inversion pair of σ is an inversion pair of the form $\{i,i+1\}$; if σ is not the identity then there must be at least one adjacent inversion pair $\{i,i+1\}$. If σ has L-rank $m \geq 1$, and if $\{i,i+1\}$ is an inversion pair, then $\sigma = \sigma_1(i,i+1)$, where σ_1 has L-rank $m-1$, and $\{i,i+1\}$ is not an inversion pair of σ_1. A convenient factoring algorithm for the line is the "fix left- hand vertex" algorithm. Suppose the L-rank of σ is m, and $\sigma(i) = i$ for $i = 1,2,\cdots,j-1$, and $\sigma(j) \neq j$. Then $\sigma(k) = j$ for some $k > j$, $m \geq k-j$, and we can write $\sigma = \tau(j,j+1)(j+1,j+2).....(k-1,k)$. Then $\tau(i) = i$ for $i = 1,2,\cdots,j$, and the L-rank of τ is $m-(k-j)$.

If σ is a permutation on a star S with edges $[1,a_1],[1,a_2],\cdots,[1,a_k]$, let $C_1,\cdots,C_r$ be the disjoint cycles of σ, and put $\delta(\sigma) = 0$ if $\sigma(1) = 1$, and $\delta(\sigma) = 2$ if $\sigma(1) \neq 1$. Let $M(\sigma)$ be the number of members x of $V(S)$ such that $\sigma(x) \neq x$. Then the S-rank of σ is $M(\sigma)+r-\delta(\sigma)$. If C is a cycle on the star S, and $C(1) \neq 1$, say $C = (1,a_1,a_2,\cdots,a_j)$, then C can be factored minimally in only one way, as $C = (1,a_j)(1,a_{j-1})\cdots(1,a_2)(1,a_1)$.

If C is a cycle on the star S, and $C(1) = 1$, say $C = (a_1,a_2,\cdots,a_j)$, then C can be factored minimally in precisely j ways, as

$$(1,a_i)(1,a_{i-1})\cdots(1,a_2)(1,a_1)(1,a_j)(1,a_{j-1})\cdots(1,a_{i+1})(1,a_i)$$

If σ is a product of disjoint cycles $C_1\cdots C_r$, then a product (i.e., concatenation) of minimal factorizations of the cycles C_i, is a minimal factorization of σ.

In this paper, we shall be considering only trees T which are brooms (and of course their associated line and star trees), and we will not use the prefix T, but refer only to "rank", "factorization", and so on.

3 The Algorithm

Throughout this section, T is a broom with vertices $\{1,2,\cdots,n,a_1,\cdots,a_k\}$ where $L = \{1,2,\cdots,n\}$ forms a line, and $S = \{1,a_1,\cdots,a_k\}$ forms a star. Put $A = \{a_1,\cdots,a_k\}$.

Definition 3.1 *Let σ be a fixed permutation on T and suppose that $\sigma = C_1....C_j$ as a product of disjoint cycles. If C_i is a permutation of $\{a_1, \cdots, a_k\}$ we say that C_i is an A-cycle of σ; if C_i is a permutation of L, we say that C_i is an L-cycle of σ and if C_i is neither an A-cycle nor an L-cycle, then C_i is a mixed cycle of σ. Put $C(j,k) = (k, k+1)(k+1, k+2).....(j-2, j-1)(j-1, j)$ for $k, j \in L$ and $k < j$, and if $k = j$ we agree that $C(j,k)$ is the identity (no edges).*

Step 0. This step may be described as: take out all the disjoint A-cycles of σ, factor them minimally, and write them on the far left of the (eventual) minimal factorization: that is, we write $\sigma = X\sigma_1$ where X is the product of all the disjoint A-cycles of σ. Since X is a permutation on the star S, its minimal factorization is easily given, and the algorithm proper is applied only to σ_1, that is, to a permutation without A- cycles. Replace σ by σ_1 and go to Step 1.

Step 1. (Now σ has no A-cycles.) If σ has mixed cycles, then go to Step 2. If σ has no mixed cycles, then σ is a permutation of L, and then factor σ using any minimal algorithm for the line L. End.

Step 2. (σ has no A-cycles.) If σ has no A- cycles, and σ has mixed cycles, then proceed as follows. Choose the smallest x in L such that $\sigma(x) < \sigma(a_i)$ for some $a_i \in A$. Suppose that $\max\{\sigma(a_i)\} = k = \sigma(b)$ where $b \in A$. Then $k \in L$ (since σ does have mixed cycles), and one of the mixed cycles C of σ contains a segment of the following form: $C = (\cdots, m, b_1, b_2, \cdots, b_{r-1}, b, k, \cdots)$; $m, k \in L$ and $b_i, b \in A$ (i.e. $\sigma(m) = b_1$, $\sigma(b_1) = b_2, \cdots, \sigma(b_{r-1}) = b$, $\sigma(b) = k, \cdots$). Then put

$$\sigma = \sigma_1(1,b)(1,b_{r-1})(1,b_{r-2})\cdots(1,b_2)(1,b_1)C(x,1)$$

Replace σ by σ_1 and go to Step 0.

The factorization of σ produced by this algorithm has the following form:

$$(*) \quad \sigma = XZ\alpha_m C(x_m,1)\alpha_{m-1}C(x_{m-1},1)\cdots\alpha_1 C(x_1,1)\alpha_0 C(x_0,1)$$

Theorem 3.2 *The form (*) produced by this algorithm has all of the following properties:*

(P1) X is the product of all the disjoint A-cycles of σ (written minimally)

(P2) Z is a permutation of L (written minimally)

(P3) For $i = 0, 1, \cdots, m$, α_i is a cycle on the star S (written minimally) which satisfies $\alpha_i(1) \neq 1$.

(P4) If $a \in A$ and $X(a) \neq a$, then $(1, a)$ does not appear in α_i for all i.

(P5) If $\alpha_i = (1, b_r).....(1, b_2)(1, b_1)$ where $r \geq 2$, then for $j = 2, \cdots, r$, $(1, b_j)$ does not appear in any α_t with $t > i$.

(P6) $1 \leq x_0 < x_1 < x_2 < \cdots < x_m$

(P7) If $1 \leq j < k \leq m+1$, then $Z(j) < Z(k)$, i.e. Z has no inversions between 1 and $m+1$.

Proof: P1, P2, P3, and P4 are obvious from the statement of the algorithm. To see that P5 is true, suppose that Step 2 gives

$$\sigma = \sigma_1(1,b)(1,b_{r-1})(1,b_{r-2})\cdots(1,b_2)(1,b_1)C(x,1).$$

Since $\sigma(b_1) = b_2$, $\sigma(b_2) = b_3, \cdots, \sigma(b_{r-1}) = b$, then evidently $b_2, b_3, \cdots, b_{r-1}, b$ are all fixed by σ_1, and the edges $(1,b_2), \cdots, (1,b)$ will never appear in the steps of the algorithm for σ_1. For P6 and P7, suppose that σ has no disjoint A-cycles, and that Step 2 is applicable twice; say

$$\sigma = \sigma_1(1,b)(1,b_{r-1})(1,b_{r-2})\ldots\ldots(1,b_2)(1,b_1)C(x_0,1),$$

$$\sigma_1 = \sigma_2(1,c)(1,c_{s-1})(1,c_{s-2})\ldots\ldots(1,c_2)(1,c_1)C(x_1,1);$$

i.e. $\sigma = \sigma_2\alpha_1 C(x_1,1)\alpha_0 C(x_0,1)$. By Step 2, we had $\max\{\sigma(a_i)\} = k \in L$, say, and x_0 was the smallest integer in $\{1,2,\cdots,n\}$ such that $\sigma(x_0) < k$. Now $\sigma_1(b_1) = \sigma(x_0)$, $\sigma_1(1) = \sigma(b) = k$, $\sigma_1(b_2) = b_2, \cdots, \sigma_1(b) = b$. For all other $a_i \in A$, $\sigma_1(a_i) = \sigma(a_i)$, and x_1 is least in $\{1,2,\cdots,n\}$ such that $\sigma_1(x_1)$ is less than $\max\{\sigma_1(a_i)\}$. Since $\sigma_1(1) = k$, then $x_1 \geq 2$.

Suppose first that $\max\{\sigma_1(a_i)\} = \sigma_1(b_1) = \sigma(x_0)$. If $x_1 \leq x_0$, then $\sigma_1(x_1) = \sigma(x_1 - 1)$, and so $\sigma(x_1 - 1) < \sigma(x_0) < k$. But since $x_1 - 1 < x_0$, this contradicts the choice of x_0 at the first application of Step 2. Now suppose that $\max\{\sigma_1(a_i)\} = \sigma_1(c) \neq \sigma(x_0)$. Then $\sigma_1(c) = \sigma(c)$, and we have $\sigma(x_1 - 1) < \sigma(c) < k$ (by the choice of k in the first application of Step 2), and again $x_1 - 1 < x_0$ contradicts the choice of x_0. Then $x_1 > x_0$. If Step 2 is applicable a third time, we get $x_2 > x_1$, and so on, and so by induction P6 holds. If $\max\{\sigma_1(a_i)\} = \sigma_1(b_1) = \sigma(x_0)$, then $\sigma_2(2) = k$ and $\sigma_2(1) = \sigma(x_0)$, and so $\sigma_2(1) < \sigma_2(2)$. If $\max\{\sigma_1(a_i)\} = \sigma_1(c) \neq \sigma(x_0)$, then $\sigma_2(2) = k$ and $\sigma_2(1) = \sigma(c)$, and again $\sigma_2(1) < \sigma_2(2)$. If Step 2 is applicable a third time, then we will have $\sigma_3(1) < \sigma_3(2)$, and since $\sigma_3(2) = \sigma_2(1)$ and $\sigma_3(3) = \sigma_2(2)$, we have $\sigma_3(1) < \sigma_3(2) < \sigma_3(3)$, and so on. Then by induction P7 is satisfied.

The idea behind this algorithm is based on the geometry of the tree T. Picture T laid out with the star S on the far left, and the line L extending to the right, and labelled with two sets of labels $\{a_1, \cdots, a_k, 1, 2, \cdots, n\}$: black labels are fixed, and red labels can move, but only by interchanging two red labels across an edge of T. We want a sequence of moves whose final result has red label x sitting at black label $\sigma(x)$, for all vertices x of T. Suppose e.g. that $\sigma(1) = 3$, and for $i = 1,2,3$, $\sigma(a_i) > 3$. If red label 1 remains on L throughout our sequence of moves, then red label 1 will have to trade places (i.e., cross) with all three of the red labels a_1, a_2, a_3; each of these moves contributes a transposition to the factorization of σ we end up with. But if red label 1 is moved to sit at one of the vertices of S, and while it sits there, the red labels a_1, a_2, a_3 are moved out to L, then red label 1 might avoid crossing with at least two of a_1, a_2, a_3—thus possibly we might have a shorter factorization. Furthermore, if we move out the a_1, a_2, a_3 so that the one with largest image moves out first, we might also avoid extra crossings (i.e., extra transpositions).

4 The Basic Transformations

In order to show that the algorithm of Section 3 actually produces a minimal factorization of σ, we will eventually show that if we begin with any factorization, say $\sigma = t_m \cdots t_1$, it can be rearranged, rewritten, and generally transformed into another factorization $\sigma = s_k \cdots s_1$ such that s_1 is actually the rightmost transposition appearing in the factorization produced by the algorithm. Then the desired result follows by induction. In this section, we describe nine transformations which are used to change any factorization of σ into a more manageable form (factorization), which of course is still equal to the original σ.

If $\sigma = t_m \cdots t_1$ is a factorization, then each t_i is either an edge of the line L, or an edge of the star S. So we can write

$$(F0) \quad \sigma = t_m \cdots t_1 = XZ\alpha_r\tau_r\alpha_{r-1}\tau_{r-1}\cdots\alpha_1\tau_1\alpha_0\tau_0$$

where the t_i belonging to α_i or to X are edges of the star $S = \{1, a_1, ..., a_k\}$, and the t_i belonging to τ_i or to Z are edges of the line $L = \{1, 2, ..., n\}$; e.g. if $t_1, t_2, \cdots, t_i \in E(S)$, and $t_{i+1} \in E(L)$, then τ_0 has length 0 (no edges), and $\alpha_0 = t_i \cdots t_1$ has length i (i edges). Evidently X, Z, and τ_0 might have length 0 (no edges), but if σ is not the identity, there must be some portions of F0 with positive length (having edges).

Definition 4.1 *Let $\sigma = t_m \cdots t_1$. The total number of edges t_i in $\{t_1, \cdots, t_m\}$ belonging to the star S, is called the A-length of the factorization and the total number of edges belonging to the line L is called the L-length. In (F0), the α_i are called the A-factors, and the τ_i are the L-factors. The total length of the segment $\alpha_r\tau_r\alpha_{r-1}\tau_{r-1}\cdots\alpha_1\tau_1\alpha_0\tau_0$ is called the ALF-length (for A,L-Factor length). The number of A-factors is called the height of the factorization.*

We will define nine transformations, which may be applied to a factorization of σ in form F0, producing another factorization of σ. We give no explicit proofs of the equality of the factorizations; in each case this is either very obvious, or can be seen by straightforward computation.

The first three transformations affect only the L-factors. None of them change the A-length, and only T1 changes (reduces) the L- length.

(T1) If Z or any τ_i is not minimal, replace it by a minimal factorization

(T2) If $0 \leq i \leq r$ and $\tau_i(1) = 1$, replace $\alpha_i\tau_i$ by $\tau_i\alpha_i$

(T3) If $\tau_i(1) \neq 1$, and $\tau_i(k_i) = 1$, write $\tau_i = \tau_i^* C(k_i, 1)$ minimally, and replace $\alpha_i\tau_i$ by $\tau_i^*\alpha_i C(k_i, 1)$.

In T2, we use the fact that if $\tau_i(1) = 1$, then it commutes with α_i, and in T3, we are calling on an aspect of minimal factorizations on the line L, i.e.

if $\tau_i(1) \neq 1$, and $\tau_i(k_i) = 1$, and we write $\tau_i = \tau_i^* C(k_i, 1)$ minimally, then $\tau_i^*(1) = 1$, and so τ_i^* commutes with α_i.

We will say that a transformation is "possible" for the factorization $t_m \cdots t_1$, to mean that it actually produces a different rewriting of $t_m \cdots t_1$; in the case of T1, that would be a shorter rewriting, and for T2, a mere "rearrangement". For instance if Z and all the τ_i are already minimally written, then we would say that T1 is "not possible".

Lemma 4.2 *Let $\sigma = t_m \cdots t_1 = XZ\alpha_r\tau_r\alpha_{r-1}\tau_{r-1}\cdots\alpha_1\tau_1\alpha_0\tau_0$ be given. Then by a finite sequence of tranformations T1, T2, T3, we can rewrite $t_m \cdots t_1$ as*

$$(F1) \qquad \sigma = XZ\beta_s C(k_s, 1)\beta_{s-1}C(k_{s-1}, 1)\cdots\beta_1 C(k_1, 1)\beta_0 C(k_0, 1)$$

where $s \leq r$, the length of (F1) is $\leq m$, and none of the transformations T1, T2, T3 are possible. The ALF-length of F1 is no more than the ALF-length of F0.

Proof: First, apply T1 to Z and to all the τ_i. Then, apply T2 consecutively, from right to left. Repeat this process, until no T1 or T2 is possible. Since T1 reduces total length, and T2 reduces the number of L-factors, then after finitely many repetitions, no more T1 or T2 are possible, and we have s L-factors with $s \leq r$, the total length is $\leq m$, and the ALF-length has not been increased. At this stage, no L-factor fixes 1, with the possible exception of the rightmost L-factor τ_0, which may be the identity. Now apply T3 consecutively from right to left; each L-factor is replaced by a factor of the form $C(k, 1)$, and the number of L-factors is unchanged (at each application of T3, we "push left" a permutation of L which fixes 1). Continue the whole process as long as possible; there can be only finitely many repetitions. The length and the ALF-length do not increase.

The second set of transformations primarily affect the α_i. The basic idea here is this: for any permutation of the star S, a minimal factorization can be given as the product of minimal factorizations of its disjoint cycles. If a cycle C on S fixes the center 1, then this cycle commutes with all the τ_i and with Z, and also commutes with any α_i which fixes all the elements moved by C. On the other hand, if any α_i moves an element which is also moved by C, then $\alpha_i C$ and $C\alpha_i$ are not minimal. So, in the factorization of σ, such a cycle C can be either moved all the way to the left (next to X) by commuting, or else it can be moved either to the left or the right by commuting until it is sitting next to some α_i such that $\alpha_i C$ (respectively, $C\alpha_i$) is not minimal.

(T4) For X or any α_i, replace it by a minimal factorization in the form of a product of disjoint cycles.

(T5) (Move cycle to X (far left)) If $0 \leq i \leq r$, and if $\alpha_i = C_1 \cdots C_t$ as a product

of disjoint cycles, and $C_1(1) = 1$, and if for all $k \neq i$ we have $E(\alpha_k) \cap E(C_1) = \emptyset$, then replace X by a minimal factorization of XC_1, and α_i by $C_2 \cdots C_t$.

(T6) (Move cycle left) If $0 \leq i \leq r-1$, and if $\alpha_i = C_1 \cdots C_t$ as a product of disjoint cycles, and $C_1(1) = 1$, and $i < j$, and if for all $i < k < j$, we have $E(\alpha_k) \cap E(C_1) = \emptyset$, while $E(\alpha_j) \cap E(C_1) \neq \emptyset$ then replace α_j by the minimal factorization of $\alpha_j C_1$ and α_i by $C_2 \cdots C_t$.

(T7) (Move cycle right) If $1 \leq i \leq r$, and if $\alpha_i = C_1 \cdots C_t$ (respectively, $X = C_1 \cdots C_t$) as a product of disjoint cycles, $C_1(1) = 1$, and $j < i$, and if for all $j < k < i$ (respectively, all $j < k \leq m$) we have $E(\alpha_k) \cap E(C_1) = \emptyset$ while $E(\alpha_j) \cap E(C_1) \neq \emptyset$, then replace α_j by the minimal factorization of $C_1 \alpha_j$ and α_i (respectively, X) by $C_2 \cdots C_t$.

It should be noted that if $\alpha_i(1) \neq 1$ for all $i = 0, 1, 2, \cdots, m$, then none of the transformations T4-T7 will change the number of A-factors, and the L-factors will remain unchanged.

Lemma 4.3 *Let $\sigma = t_m \cdots t_1 = XZ\alpha_r\tau_r\alpha_{r-1}\tau_{r-1}\cdots\alpha_1\tau_1\alpha_0\tau_0$ be given. Then by a finite sequence of tranformations T1—T7, we can rewrite $t_m \cdots t_1$ as*

$$(F2) \qquad \sigma = X_1 Z_1 \beta_s C(k_s, 1)\beta_{s-1} C(k_{s-1}, 1) \cdots \beta_1 C(k_1, 1)\beta_0 C(k_0, 1)$$

where $s \leq r$, the length of F2 is $\leq m$, the ALF-length of F2 is no more than the ALF length of F0, and none of the transformations T1–T7 are possible. Furthermore, X_1 is a product of disjoint A-cycles of σ, and the factorization F2 satisfies the properties P2, P3, P4.

Proof: We may begin with a factorization in the form F1. Since T4, T6 and T7 all reduce length, these are possible only finitely many times in any sequence. Since T5 either reduces length or ALF-length, then T5 is possible only finitely many times. After carrying out T4— T7 as far as possible, some of T1—T3 may become possible; but if this should happen then either the height has been reduced, or the total length, or the ALF-length, has been reduced. So eventually we must arrive at a form in which all of T1—T7 are not possible. Since T6 and T7 are not possible, then $E(X_1) \cap E(\beta_i) = \emptyset$ for all i, and so P4 holds, and X_1 is a product of disjoint A-cycles of σ. Since T5, T6, T7 are not possible, then every α_i satisfies P3. Since T1 is not possible, P2 holds.

Finally, transformation T8 permits the rearrangement of the $C(k_i, 1)$ needed for property P6, and transformation T9 is used for property P5. We shall see that, once we have these, we can deduce P1 and P7.

T8: Let $\sigma = XZ\alpha_r C(k_r, 1)\alpha_{r-1} C(k_{r-1}, 1) \cdots \alpha_1 C(k_1, 1)\alpha_0 C(k_0, 1)$. Suppose for some i, $0 \leq i \leq r-1$, $1 < k_{i+1} \leq k_i$, and that $\alpha_i = (1, b_1)(1, b_2) \cdots (1, b_s)$,

$b_j \in A$. Replace $C(k_{i+1},1)\alpha_i C(k_i,1)$ by $(1,b_s)C(k_i,1)\alpha_i C(k_{i+1}-1,1)$.

T9: Suppose $\sigma = XZ\alpha_r\tau_r\alpha_{r-1}\tau_{r-1}\cdots\alpha_1\tau_1\alpha_0\tau_0$. Suppose $0 \le i \le r-1$ and $\alpha_i = (1,b_1)(1,b_2)\cdots(1,b_s)$, with $b_j \in A$ and all distinct, and $s > 1$. Suppose for some $1 \le t \le s-1$, $(1,b_t) \in E(\alpha_u)$ for some $u > i$. Suppose that u is the least integer such that $u > i$ and $E(\alpha_u) \cap \{(1,b_t)\cdots(1,b_m)\} \neq \emptyset$.

Replace α_u by the minimal factorization of $\alpha_u(1,b_t)(1,b_{t+1})....(1,b_s)(1,b_t)$ and replace α_i by $(1,b_1)(1,b_2)\cdots(1,b_t)$.

Lemma 4.4 *Let* $\sigma = XZ\alpha_r C(k_r,1)\alpha_{r-1}C(k_{r-1},1)\cdots\alpha_1 C(k_1,1)\alpha_0 C(k_0,1) = t_m\cdots t_1$ *be factored in form F2, where T1—T7 are not possible. Then by a finite sequence of transformations T1—T8,* σ *can be factored in the form*

$$(F3) \quad \sigma = X_1 Z_1 \beta_s C(x_s,1)\beta_{s-1}C(x_{s-1},1)\cdots\beta_1 C(x_1,1)\beta_0 C(x_0,1)$$

where $s \le r$, *the length is* $\le m$, *the ALF-length is not increased, and none of T1-T8 are possible. This factorization satisfies properties P2, P3, P4, and P6.*

Proof: Suppose a T8 is possible; for some i, $0 \le i \le m-1$, we have $1 < k_{i+1} \le k_i$, and $\alpha_i = (1,b_1)\cdots(1,b_t), b_j \in A$ and the b_j are all distinct. So, we replace $C(k_{i+1},1)\alpha_i C(k_i,1)$ by $(1,b_t)C(k_i,1)\alpha_i C(k_{i+1}-1,1)$.

In the result, the sequence of integers $(k_0,\cdots,k_r)$ is modified in only two places; k_{i+1} is replaced by k_i, and k_i by $k_{i+1}-1$. Note that the maximal value of the k_i is not increased. The (new) i-th A-factor is $\alpha_{i+1}(1,b_t)$, and it may happen that one of T4—T7 is now possible. Each of these reduces ALF-length, and so there can be only finitely many T8 transformations which are followed by any of T4—T7. If $k_{i+1} = 2$, then C(1,1) is the identity (no edges), and in this case we "lose" an L-factor; the height has been reduced, and again some of T4—T7 may become possible (with a consequent reduction of ALF-length). Clearly there can be only finitely many T8-transformations which reduce height. The T8 transformations which do not reduce height, and are not followed by any of T4—T7, have the effect (more or less) of "rearranging adjacent members of the sequence $(k_0,...,k_r)$ by size", and since none of T1—T8 can increase the maximal value of the k_i, again there can be only finitely many of these.

Thus, we may continue to apply T1-T8 until none remain possible, and the result follows.

Lemma 4.5 *Let* $\sigma = XZ\alpha_r C(k_r,1)\alpha_{r-1}C(k_{r-1},1)\cdots\alpha_1 C(k_1,1)\alpha_0 C(k_0,1) = t_m\cdots t_1$ *be factored in form F3, where T1—T8 are not possible. Then by a finite sequence of transformations T1—T9,* σ *can be factored in the form*

$$(F4) \quad \sigma = X_1 Z_1 \beta_s C(x_s,1)\beta_{s-1}C(x_{s-1},1)\cdots\beta_1 C(x_1,1)\beta_0 C(x_0,1)$$

where $s \le r$, *the length is* $\le m$, *the ALF-length is not increased, and none of T1—T9 are possible. This factorization satisfies properties P2, P3, P4, P5 and P6.*

Proof: Suppose $\alpha_0 = (1,b_1)\cdots(1,b_v)$, $b_j \in A$ and the b_j are all distinct. and $u > 1$. Suppose a T9 is possible at α_0, and t is least with $1 \le t \le v-1$ and $(1,b_t) \in E(\alpha_u)$ for some $u > 0$. Suppose that u is the least integer such that $u > 0$ and $E(\alpha_u) \cap \{(1,b_t),\cdots(1,b_m)\} \neq \emptyset$.

Replace α_u by the minimal factorization of $\alpha_u(1,b_t)(1,b_{t+1})....(1,b_s)(1,b_t)$ and call it δ_u, and replace α_i by $(1,b_1)(1,b_2)\cdots(1,b_t)$. The result has the same length as the original. One (or more) of T4—T7 may now be possible (at δ_u); if so, they will reduce the ALF-length, and if not, then we have a factorization with the same sequence of L-factors, new A-factors ($\beta_0 = (1,b_1)\cdots(1,b_t)$, and δ_u) in the 0-th and u-th places, and where β_0 satisfies property P5. Continuing this process from right to left, only finitely many T9's are possible.

This form F4 has several nice properties that make it very suitable for further modification in the direction of the final form of the algorithm of Section 2. We first show that the form allows a partial prediction of the values $\sigma(a)$ for $a \in A$, and use this to show that a factorization in form F4 has all of the properties P1—P6.

Lemma 4.6 *Suppose* $\sigma = XZ\alpha_r C(k_r,1)\alpha_{r-1}C(k_{r-1},1)\cdots\alpha_1 C(k_1,1)\alpha_0 C(k_0,1)$ *is factored in form F4. If* $a \in A$, *and if* $(1,a) \notin E(X)$ *and if* i *is the least integer such that* $(1,a) \in E(\alpha_i)$, *and if* $\alpha_i = (1,b_1)\cdots(1,b_t)$, *then:*

(i) if $a = b_1$, *then* $\sigma(a) = Z(r+1-i) \in L$

(ii) if $t > 1$ *and if* $1 < j \le t$ *and* $a = b_j$, *then* $\sigma(a) = b_{j-1} \in A$

Proof: For $0 \le s \le r$, write $\delta_s = \alpha_s C(x_s,1).....\alpha_0 C(x_0,1)$. Then for all $y > x_s$, $\delta_s(y) = y$. If $s < r$ and $1 \le y < x_s$, and if $\delta_s(z) = y$, then, since $x_{s+1} > x_s$, we have $\delta_{s+1}(z) = y+1$. It follows that $\delta_r(z) = y + r - s > 1$, i.e. $\delta_r(z) \in L$, and then $\sigma(z) = Z(z)$ is also in L. Now if the first appearance of $(1,a)$ immediately precedes a $C(x_{i+1},1)$, then we will have $\delta_i(a) = 1$, and then $\sigma(a) = 1 + r - i$. If the first appearance of $(1,a)$ immediately precedes some $(1,b)$ in α_i (where $b \in A$), then by P5, $(1,b)$ does not appear in any α_j (or in X) for any $j > i$, that is $\sigma(a) = b$.

Theorem 4.7 *Suppose that* σ *is factored in form F4. Then the factorization satisfies all of properties P1—P6.*

Proof: In view of Lemma 4.5, we need only show P1, i.e. that X is the product of all the disjoint A-cycles of σ.

We have $\sigma = XZ\alpha_r C(k_r,1)\alpha_{r-1}C(k_{r-1},1)\cdots\alpha_1 C(k_1,1)\alpha_0 C(k_0,1)$ and by P6, $x_r > x_{r-1} > \cdots > x_1 > x_0 \ge 1$. Suppose that $\alpha_0 = (1,b_1)\cdots(1,b_t)$. Then $\sigma(b_1) = Z(r+1) \in L$, and so b_1 belongs to a mixed cycle of σ. If $t > 1$, then we have $\sigma(b_t) = b_{t-1},\cdots,\sigma(b_2) = b_1$ by P5, and so all of $b_t,\cdots,b_1$ belong to some mixed cycle of σ. Thus α_0 is disjoint from any of the A-cycles of σ. Then the A-cycles of σ are the same as the A-cycles of

$$\sigma_1 = XZ\alpha_r C(k_r,1)\alpha_{r-1}C(k_{r-1},1)\cdots\alpha_1 C(k_1,1)$$

and the result follows by induction.

Corollary 4.8 *If σ has no mixed cycles, then given any factorization of σ, transformations T1—T9 can be applied to produce a factorization of σ in the form XZ, where X is a product of disjoint A-cycles, and Z is a permutation of L. In particular, if σ has no mixed cycles, and we write $\sigma = XZ$ where X is the product of the disjoint A-cycles of σ, and Z is the product of the disjoint L-cycles of σ, then the rank of σ is the sum of the S-rank of X and the L-rank of Z.*

Proof: The first statement follows from the proof of Theorem 4.7. Suppose we have any minimal factorization of σ. Then the transformations T1—T9 produce a factorization in the form XZ of no greater length, which must then itself be minimal, and the result follows.

5 Blocks and Z-ordering

Definition 5.1 *Suppose that σ has a mixed cycle. Then there exist $x, y \in L$, and $b_1, \cdots, b_t$ in A such that $\sigma(x) = b_t, \sigma(b_t) = b_{t-1}, \cdots, \sigma(b_2) = b_1$, and $\sigma(b_1) = y$. Then the sequence $[b_t, b_{t-1}, \cdots, b_1]$ is a block of σ. We will also refer to the product $(1, b_1)(1, b_2)....(1, b_t)$ as a block of σ.*

In this section, we show that a factorization in form F4, can be further modified to a factorization which is not only in form F4, but also has property P7, and its right-most A-factor is a complete block of σ.

In the factorization produced by the algorithm of Section 2, the right-most A-factor is a particular block of σ. In this section, we first show that we can always transform any factorization in form F4, into another, also in form F4, but with its right-most A-factor being some block of σ, using the transformation T10 described below. (If we call T9 a "right-to-left" operation, then T10 is its "left-to-right" sibling.) Then we show that such a factorization can always be rearranged to satisfy P7 also.

T10: Suppose for some i, $1 \leq i \leq r$, $\alpha_i = (1, b_1)(1, b_2).....(1, b_m)$, with $b_j \in A$, and all distinct, and $m > 1$. Suppose for some $1 \leq t \leq m-1$, $(1, b_t) \in E(\alpha_u)$ for some $u < i$. Suppose that u is the greatest integer such that $u < i$ and $E(\alpha_u) \cap \{(1, b_1).....(1, b_t)\} \neq \emptyset$.

Replace α_i by $(1, b_t)(1, b_{t+1}) \cdots (1, b_m)$ and replace α_u by the minimal factorization of $(1, b_t)(1, b_1)(1, b_2).....(1, b_t)\alpha_u$.

Lemma 5.2 *Suppose that σ is factored in form F4,*

$$\sigma = t_m \cdots t_1 = XZ\alpha_r C(k_r, 1)\alpha_{r-1} C(k_{r-1}, 1) \cdots \alpha_1 C(k_1, 1)\alpha_0 C(k_0, 1).$$

Then by a finite sequence of transformations T1—T10, σ can be factored in the form

$$(F5) \quad \sigma = X_1 Z_1 \beta_s C(x_s, 1)\beta_{s-1} C(x_{s-1}, 1) \cdots \beta_1 C(x_1, 1)\beta_0 C(x_0, 1)$$

where $s \leq r$, the length is $\leq m$, the ALF-length is not increased, and none of T1—T9 are possible, and β_0 is a block of σ. This factorization satisfies properties P1—P6.

Proof: Suppose that $\alpha_0 = (1, b_1) \cdots (1, b_t)$. Then $\sigma(b_1) = Z(r+1) \in L$ and so b_1 belongs to some block of σ. If this block has length t then we are done (by P5, we have $\sigma(b_t) = b_{t-1}, \cdots, \sigma(b_2) = b_1$), so we suppose that α_0 is part of a block of length $n > t$, $[b_n, \cdots, b_t, \cdots, b_1]$. Then $b_n, \cdots, b_{t+1}$ must all appear in various α_u with $u > 0$, and since $\sigma(b_{t+1}) = b_t$, we must also have b_t appearing in some α_u. Let u be the least integer such that $(1, b_{t+1}) \in E(\alpha_u)$, say $\alpha_u = (1, c_1) \cdots (1, c_v)$.

By Lemma 4.6, $c_1 \neq b_{t+1}$. By P5, none of the c_i can be equal to any of $b_1, \cdots, b_{t-1}$. Since $\sigma(b_{t+1}) = b_t$, then by Lemma 4.6, if $c_i = b_{t+1}$, then $c_{i-1} = b_t$, i.e. $i > 1$ and so $v > 1$. So α_u has the form

$$\alpha_u = (1, c_1) \cdots (1, c_j)(1, b_t)(1, b_{t+1}) \cdots (1, b_{t+k})\ (1, c_{j+k+2}) \cdots (1, c_v)$$

for some integers j,k with $k \geq 1$. Put $\delta = (1, b_t) \cdots (1, b_{t+k})$, and define γ by $\alpha_u = (1, c_1) \cdots (1, c_j)\delta\gamma$.

Now let w be the least integer which is less than u and such that $(1, b_t) \in E(\alpha_w)$. We claim that if $w \neq 0$, then $(1, b_t)$ must appear on the far right of α_w, i.e. $\alpha_w = (1, d_1).....(1, d_j)(1, b_t)$ for some (distinct) $d_i \in A$. To see this, put $\mu_1 = \alpha_w C(k_w, 1) \cdots \alpha_0 C(k_0, 1)$ and $\mu_2 = XZ\alpha_r C(k_r, 1) \cdots \alpha_{w+1} C(k_{w+1})$, and note that (since $w < u$) $\mu_1(b_{t+1}) = b_{t+1}$. Suppose that $w > 0$ and $\alpha_w = (1, d_1).....(1, d_j)$ with $j > 1$. If $b_t = d_k$ with $k < j$, then for some x we have $\mu_1(x) = b_t = d_k$ and by P5, $\mu_2(d_k) = d_k$ so that $\sigma(x) = \mu_2(\mu_1(x)) = d_k = b_t$. But then, $x = b_{t+1}$, contradicting the fact that $\mu_1(b_{t+1}) = b_{t+1}$.

We will apply T10 to the following segment of the original factorization:

$$\delta\gamma C(k_u, 1)\alpha_{u-1} \cdots C(k_{w+1}, 1)\alpha_w$$

replacing δ by $\beta = (1, b_{t+k})$, and α_w by $\beta_w = (1, b_{t+k})\delta\alpha_w$, factored minimally. Note that if $j \geq 1$, then none of the $(1, d_i)$ appear in α_u (by P5), and for $i = 1, 2, \cdots, t-1$, none of $(1, b_i)$ appear in either α_u or α_w (by P5). Then since $(1, b_{t+k})\delta$ is an A-cycle, fixing 1, and disjoint from $(1, d_1).....(1, d_j)$, we have:

$$\begin{aligned}
&\beta_w = (1, b_{t+k})\delta\alpha_w \\
&= (1, b_{t+k})(1, b_t)(1, b_{t+1})(1, b_{t+2}) \cdots (1, b_{t+k})\alpha_w \\
&= (1, b_t)(1, b_{t+1}) \cdots (1, b_{t+k})(1, b_t)(1, d_1) \cdots (1, d_j)(1, b_t) \\
&= (1, d_1)....(1, d_j)(1, b_t)(1, b_{t+1}) \cdots (1, b_{t+k})(1, b_t)(1, b_t)
\end{aligned}$$

$$= (1, d_1)....(1, d_j)(1, b_t)(1, b_{t+1})....(1, b_{t+k})$$

and this last factorization is minimal. Now in the original F4 factorization of σ, we replace α_u by $(1, c_1)....(1, c_j)\beta\gamma$, and α_w by β_w. The result has the same length as the original, and the same L-factors, and still has all the properties of an F4 factorization; and now the first (rightmost) appearance of b_{t+1} is in the w-th A-factor, where $w < u$. If $w \neq 0$, then we can repeat the process above on the new factorization; each time, the first appearance of b_{t+1} is further to the right. Thus we may assume without loss of generality, that $w = 0$. If $w = 0$, then the new β_0 is $(1, b_1).....(1, b_{t+k})$, which is longer than $\alpha_0 = (1, b_1).....(1, b_t)$ by at least one transposition (since $k \geq 1$), and β_0 is still an initial segment of the same block of σ. If the new β_0 is not a complete block of σ, then the whole process above can be repeated. At each repetition, the "new" β_0 acquires at least one more transposition, and each "new factorization" has the same length as the original, and all the properties of F4; since the blocks of σ have finite length, then in finitely many repetitions we arrive at a factorization which is an F4, and in which the rightmost A-factor is a complete block of σ.

Corollary 5.3 *Let*

$$\sigma = XZ\alpha_r C(k_r, 1)\alpha_{r-1}C(k_{r-1}, 1)\cdots\alpha_1 C(k_1, 1)\alpha_0 C(k_0, 1) = t_m \cdots t_1$$

be factored in form F4. Then by a finite sequence of transformations T1-T10, σ can be factored in the form

$$(F6) \quad \sigma = X_1 Z_1 \beta_s C(x_s, 1)\beta_{s-1}C(x_{s-1}, 1)\cdots\beta_1 C(x_1, 1)\beta_0 C(x_0, 1)$$

where $s \leq r$, the length is $\leq m$, the ALF-length is not increased, and none of T1-T8 are possible, and β_i is a complete block of

$$\sigma_i = X_1 Z_1 \beta_s C(x_s, 1)\beta_{s-1}C(x_{s-1}, 1)\cdots\beta_i C(x_i, 1).$$

The factorization (F6) satisfies properties P1- P6, and is also an F4- factorization.

Proof: This is an easy consequence of the lemma above.

We will show next, that an F6-factorization can be rewritten into another F6-factorization with property P7. The basic idea is to show that we can successively "remove" adjacent inversions of Z in $\{1, 2, \cdots, r+1\}$; if Z has no adjacent inversions in $\{1, 2, \cdots, r+1\}$, then it has no inversions at all in $\{1, 2, \cdots, r+1\}$. We use the well-known property of permutations on the line: if $(i-1, i)$ is an inversion of Z, then there is a minimal factorization of Z which has the form $Z^*(i-1, i)$.

Definition 5.4 *Let $\sigma = XZ\alpha_r C(k_r, 1)\alpha_{r-1}C(k_{r-1}, 1)\cdots\alpha_1 C(k_1, 1)\alpha_0 C(k_0, 1)$ be in form F6. If this factorization has the property that Z has no inversions in $\{1, 2, \cdots, r+1\}$, we say that the factorization is Z-ordered.*

Recall that $C(k+j,j) = (j,j+1)(j,j+2).....(k+j-1,k+j)$ for positive integers j,k .

Lemma 5.5 *Suppose that α is a permutation of the star S. If $2 < j \leq k$, then $(j-1,j)\alpha C(k,1) = \alpha C(k,1)(j-2,j-1)$.*

Proof: It is straightforward to compute that the given expressions are equal.

Theorem 5.6 *Suppose that σ is factored in the form F6,*

$$(*) \quad \sigma = XZ\alpha_r C(k_r,1)\alpha_{r-1}C(k_{r-1},1)\cdots\alpha_1 C(k_1,1)\alpha_0 C(k_0,1) = t_m\cdots t_1$$

Then this can be rearranged to give a factorization of σ in the form

$$(F7) \quad \sigma = X_1 Z_1 \beta_s C(x_s,1)\beta_{s-1}C(x_{s-1},1)\cdots\beta_1 C(x_1,1)\beta_0 C(x_0,1)$$

which has length $\leq m$, $s \leq r$, has all the properties of form F6, $x_s \leq k_r$, and Z_1 has no inversions in $\{1,2,\cdots,s+1\}$.

Proof: In view of Corollary 5.3, it is sufficient to show that we can transform the factorization into a factorization of form F5 which either has one less inversion in $\{1,2,\cdots,r+1\}$, or else has smaller length or height. We carry out the argument for the case when $(r,r+1)$ is an inversion of Z (the argument is essentially the same for any inversion $(i+1,i)$ with $i \leq r$). So, we can write $Z = Z^*(r,r+1)$. Note that, since $k_r > k_{r-1} > .... > k_0 \geq 1$, we have $k_i \geq i+1$ for $i = 0,1,\cdots,r$. Then by successive applications of Lemma 5.5, we can "move" $(r,r+1)$ to the right, to get

$$\sigma = XZ^*\alpha_r C(k_r,1)\alpha_{r-1}C(k_{r-1},1)\cdots C(k_2,1)(1,2)\alpha_1 C(k_1,1)\alpha_0 C(k_0,1)$$

We now consider the rightmost segment, $\delta = (1,2)\alpha_1 C(k_1,1)\alpha_0 C(k_0,1)$, by cases, according to the structure of α_0 and α_1.

Case 1. $\alpha_0 = (1,b_1)....(1,b_t)(1,a)$, and $\alpha_1 = (1,a)$. Then we have:

$$\begin{aligned}
&\delta = (1,2)(1,a)(1,2)(1,b_1)....(1,b_t)(1,a)C(k_1,2)C(k_0,1)\\
&= (1,b_1)....(1,b_t)(1,2)(1,a)(1,2)(1,a)C(k_1,2)C(k_0,1)\\
&= (1,b_1)....(1,b_t)(1a)(1,2)C(k_1,2)C(k_0,1)\\
&= \alpha_0 C(k_1,1)C(k_0,1) = \alpha_0 C(k_0+1,2)C(k_1,1) = C(k_0+1,2)\alpha_0 C(k_1,1).
\end{aligned}$$

At the penultimate equality, we used Lemma 5.5 (since $k_0 < k_1$); the last equality follows since α_0 and $C(k_0+2,1)$ are disjoint. Now, applying Lemma 5.5 successively, we can "move" the factor $C(k_0+1,2)$ to the left, getting

$$\sigma = XZ^*C(x_0+r,r+1)\alpha_r C(k_r,1)\alpha_{r-1}C(k_{r-1},1)\cdots\alpha_2 C(k_2,1)\alpha_0 C(k_1,1).$$

The length has been reduced by 2, and the height by 1, and since the original α_0 was a block of σ, this factorization is of form F5.

Case 2. $\alpha_0 = (1,b_1)\cdots(1,b_u)(1,a)$ and $\alpha_1 = (1,c_1)\cdots(1,c_t)(1,a), t \geq 1$. Then all the b_i and c_i (and a) are distinct, and we have

$$\begin{aligned}
&\delta = (1,2)\alpha_1(1,2)\alpha_0 C(k_1,2)C(k_0,1)\\
&= (1,b_1)\cdots(1,b_u)(1,2)\alpha_1(1,2)(1,a)C(k_1,2)C(k_0,1)\\
&= (1,b_1)\cdots(1,b_u)(1,2)(1,c_1)\cdots(1,c_t)(1,a)(1,2)(1,a)C(k_1,2)C(k_0,1)\\
&= (1,b_1)\cdots(1,b_u)(1,a)(1,2)(1,c_1)\cdots(1,c_t)(1,a)(1,a)C(k_1,2)C(k_0,1)\\
&= (1,b_1)\cdots(1,b_u)(1,a)(1,2)(1,c_1)\cdots(1,c_t)C(k_1,2)C(k_0,1)\\
&= (1,b_1)\cdots(1,b_u)(1,a)C(k_1,1)(1,c_1)\cdots(1,c_t)C(k_0,1)\\
&= \alpha_0 C(k_1,1)(1,c_1)\cdots(1,c_t)C(k_0,1)
\end{aligned}$$

Then the "new" factorization of σ has the same L-factors (and the same height), the length has been reduced by 2, and the 0-th and 1-st A-factors only have been changed. We need only to show that in fact $[c_1,\cdots,c_t]$ is a block of σ. From the original factorization (*) of σ, we have $\sigma(k_0) = c_t, \sigma(c_t) = c_{t-1},\cdots,\sigma(c_1) = r$, and since $k_0, r \in L$, then indeed $[c_1,...,c_t]$ is a block of σ. Then this factorization is in form F5.

Case 3. Recall that $\sigma_i = XZ\alpha_r\cdots C(x_i,1)$ and $\delta_i = \alpha_i\cdots C(x_0,1)$. We suppose for this case that $\alpha_0 = (1,b_1)\cdots(1,b_u)$ and $\alpha_1 = (1,c_1)....(1,c_t), b_u \neq c_t$. Then all the b_i and c_i are distinct, so that $(1,2)\alpha_1(1,2)$ commutes with α_0, and we get

$$\begin{aligned}
&\delta = (12)\alpha_1(12)\alpha_0 C(k_1,2)C(k_0,1) = \alpha_0(12)\alpha_1(12)C(k_1,2)C(k_0,1)\\
&= \alpha_0(12)(1,c_1)\cdots(1,c_t)(1,2)C(k_1,2)C(k_0,1)\\
&= \alpha_0(1,c_t)(1,2)(1,c_1)\cdots(1,c_{t-1})(1,c_t)C(k_1,2)C(k_0,1)\\
&= \alpha_0(1,c_t)C(k_1,1)\alpha_1 C(k_0,1)
\end{aligned}$$

Here, we have from (*), that α_0 is a block of σ, and α_1 is a complete block of σ_1. We need to show that α_1 is also a block of σ, i.e. that for some $x, y \in L$ we have $\sigma(x) = c_t, \sigma(c_t) = c_{t-1},\cdots,\sigma(c_2) = c_1, \sigma(c_1) = y$. From the original factorization (*), and the fact that c_t is not equal to any b_i, we know that $\sigma(c_t) = c_{t-1},\cdots,\sigma(c_2) = c_1, \sigma(c_1) = r$, and it only remains to show that $\sigma(x) = c_t$ for some $x \in L$. So, suppose that $\sigma(x) = c_t$ and note that $x \neq c_i$ for any $i = 1,2,\cdots,t$. Since $\sigma(x) = \sigma_1(\delta_0(x))$, and α_1 is a block of σ_1, then $\delta_0(x) \in L$. If $x \neq c_i$ but $x \in A$, then we would have $\delta_0(x) = x \notin L$, a contradiction. Thus $x \in L$, and α_1 is a block of σ. Now the new factorization has the form F5.

Corollary 5.7 *Every factorization of σ can be rearranged to a factorization which has the form F6, and which satisfies all of properties P1-P7.*

6 Minimality of the Factorization

In this section, let σ be fixed, and suppose the factorization produced by the algorithm is:

$$(*) \qquad \sigma = XZ\alpha_m C(x_m, 1)\alpha_{m-1} C(x_{m-1}, 1) \cdots \alpha_1 C(x_1, 1)\alpha_0 C(x_0, 1).$$

If we also have a factorization of σ in the form F6, which is Z- ordered, say

$$(**) \qquad \sigma = X_1 Z_1 \beta_r C(k_r, 1)\beta_{r-1} C(k_{r-1}, 1) \cdots \beta_1 C(k_1, 1)\beta_0 C(k_0, 1),$$

then the sequence $k_0, k_1, \cdots, k_r$ may be different from the sequence $x_0, \cdots, x_m$, and the sequence $\alpha_0, ..., \alpha_m$ may differ from the sequence $\beta_0, ..., \beta_r$. We will show that the factorization (**) can be modified (without increasing length) to "agree with (*) on the far right". Then, by induction, it will follow that (**) can actually be transformed (without increasing length) into (*). But we could assume that (**) is minimal, since every factorization can be transformed into a form F6 which is Z-ordered; then (*) must also be a minimal factorization. We first give some of the properties of (**).

Lemma 6.1 *Suppose that σ has at least one mixed cycle, and is factored in form F6 and is Z-ordered;*

$$\sigma = X_1 Z_1 \beta_r C(k_r, 1)\beta_{r-1} C(k_{r-1}, 1) \cdots \beta_1 C(k_1, 1)\beta_0 C(k_0, 1).$$

This factorization has the following properties:

(a) $X_1 = X$

(b) If $x \in L$ *and* $\sigma(x) \in A$, *then* $x = k_i$ *for some* i

(c) $k_r = \max\{\sigma^{-1}(a_i) | a_i \in A\}$

(d) If $a \in A$ *and* $\sigma(a) \in L$, *and if the rightmost appearance of* $(1, a)$ *is in* β_i, *then either* $\beta_i = (1, a)$ *or* β_i *has the form* $(1, a)(1, d_1) \cdots (1, d_j)$, *and* $\sigma(a) = Z_1(r + 1 - i)$

(e) $\beta_0 = \alpha_0$

(f) $\sigma(k_0) < \max\{\sigma(a_i) | a_i \in A\}$

(g) $x_0 \leq k_0$.

Proof: Statement (a) follows from Theorem 4.7. For (b), recall that

$$\delta_i = \beta_i C(k_i, 1)\beta_{i-1} C(k_{i-1}, 1) \cdots \beta_1 C(k_1, 1)\beta_0 C(k_0, 1)$$

If $x \in L$ and $\sigma(x) \in A$, then $\sigma(x) = \delta_r(x)$. Suppose that $x \neq k_i$ for any i. If $x > k_r$, then $\delta_r(x) = x$, and if $k_i < x < k_{i+1}$, then $\delta_r(x) = k_i + (r - i + 1) \in L$; either way, $\sigma(x) = Z_1(\delta_r(x)) \in L$, and (b) follows.

For (c), we have $\beta_r = (1, b_1) \cdots (1, b_t)$, and $\delta_r(k_r) = b_t = \sigma(k_r)$. Since $k_r > \cdots > k_0 \geq 1$, it follows from (b) that (c) holds.

For (d), suppose $a \in A$ and $\sigma(a) \in L$, and the rightmost appearance of $(1, a)$ is in β_i. Then $\delta_{i-1}(a) = a$. Suppose that $\beta_i = (1, b_1) \cdots (1, b_t)$. If $t = 1$, then (d) holds; if $t > 1$ and $a = b_j, j > 1$, then $\delta_i(a) = \delta_i(b_j) = b_{j-1} = \delta_r(a) = \sigma(a)$, contradicting $\sigma(a) \in L$. So it must be that $a = b_1$. Then $\delta_i(a) = 1$, and so $\delta_r(a) = r - i + 1$ and $\sigma(a) = Z_1(r - i + 1)$. This proves (d).

For (e), suppose that $\beta_0 = (1, c_1) \cdots (1, c_j)$. Then $\delta_r(c_1) = r + 1$. For all $a \in A$ such that $\sigma(a) \in L$, $\delta_r(a) = r - i + 1$ for some i (from (d)), and if $a \neq c_1$, then $i \geq 1$. Thus for all a with $a \neq c_1$ and $\sigma(a) \in L$, $\delta_r(a) < \delta_r(c_1) = r + 1$. Since the factorization is Z-ordered, Z_1 has no inversions in $\{1, 2 \cdots, r + 1\}$, so if $i \geq 1$, then $Z_1(r + i - 1) < Z_1(r + 1)$, i.e. $\sigma(a) < \sigma(c_1)$. Since β_0 is a block of σ, then it is actually the first block chosen by the algorithm, i.e. $\beta_0 = \alpha_0$.

For (f), suppose that $\beta_0 = (1, c_1) \cdots (1, c_j)$. Then $\delta_0(k_0) = c_j \in A$, and it follows (as in (d)) that $\delta_r(k_0) = x \leq r$ (recall that $x \leq r$ means that either $x \in A$ or $1 \leq x \leq r$). Then since the factorization is Z-ordered, $\sigma(k_0) = Z_1(x) \leq Z_1(r) < Z_1(r + 1) = \sigma(c_1)$, and this proves (f).

Now (g) follows trivially from (f), since x_0 was chosen to be the least member of L with $\sigma(x_0) < \max\{\sigma(a_i)\}$.

Remark. If $k_0 = x_0$, then we already have the desired "agreement" on the right. The next order of business is the case $x_0 < k_0$; we will show that we can modify the factorization so that the rightmost L-factor is $C(x_0, 1)$.

Theorem 6.2 *Suppose that σ is factored in form F6 and is Z-ordered;*

$$\sigma = X_1 Z_1 \beta_r C(k_r, 1)\beta_{r-1} C(k_{r-1}, 1) \cdots \beta_1 C(k_1, 1)\beta_0 C(k_0, 1).$$

Suppose that $x_0 < k_0$, and $\alpha_0 = (1, c_1) \cdots (1, c_t)$. Then without increasing length, this factorization can be transformed into

$$\sigma = X_1 Z_2 \beta_r C(k_r, 1)\beta_{r-1} C(k_{r-1}, 1) \cdots \beta_1 C(k_1, 1)(1, c_1) C(k_0, 1)\beta_0 C(x_0, 1).$$

Proof. Since $x_0 < k_0$, then $k_0 \geq 2$, and for all $y, 1 \leq y < k_0$, we have $\delta_r(y) = r + 1 + y$, and in particular $\delta_r(x_0) = r + 1 + x_0$. By choice, x_0 is least in L such that $\sigma(x_0) < \max\{\sigma(a_i)\} = \sigma(c_1)$, and so if $1 \leq y < x_0$, then $\sigma(y) > \sigma(c_1) > \sigma(x_0)$. Thus $(r + 1 + x_0, r + x_0)$ is an inversion of Z_1, and we can write $Z_1 = Z_1^*(r + 1 + x_0, r + x_0)$; if $x_0 > 1$, then $(r + x_0, r + x_0 - 1)$ is an

inversion of Z_1^*, and we can write $Z_1^* = Z_1^{**}(r+x_0, r+x_0-1)$, and so on. That is, we can write $Z_1 = Z_2C(r+1+x_0, r+1)$.

Now we use the elementary fact that, for any permutation τ and any transposition (a,b), we have $\tau(a,b) = (\tau(a), \tau(b))\tau$. Applying this (successively) to the transpositions of $C(r+1+x_0, r+1)$ in the factorization $C(r+1+x_0, r+1)\delta_r$, we get

$$C(r+1+x_0, r+1)\delta_r = \delta_r(x_0, x_0-1)(x_0, x_0-2)\cdots(x_0,1)(x_0,c_1)$$
$$= \delta_r(1,c_1)(1,2)(2,3).....(x_0-1, x_0)$$
$$= \delta_r(1,c_1)C(x_0,1)$$

Now we have

$$\sigma = X_1Z_2\beta_rC(k_r,1)\beta_{r-1}C(k_{r-1},1)\cdots\beta_1C(k_1,1)\beta_0C(k_0,1)(1,c_1)C(x_0,1)$$

and clearly the length remains the same. Rewrite the right-hand segment as

$$\beta_0C(k_0,1)(1,c_1)C(x_0,1) = (1,c_1)\cdots(1,c_t)(1,2)(1,c_1)C(k_0,2)C(x_0,1)$$

$$= (1,c_t)(1,2)(1,c_1)\cdots(1,c_t)C(k_0,2)C(x_0,1)$$
$$= (1,c_t)C(k_0,1)\beta_0C(x_0,1),$$

and now we have rewritten the original factorization of σ in the form

$$\sigma = X_1Z_2\beta_rC(k_r,1)\beta_{r-1}C(k_{r-1},1)\cdots\beta_1C(k_1,1)(1,c_1)C(k_0,1)\beta_0C(x_0,1).$$

and the length has not been increased.

Theorem 6.3 *The algorithm of Section 2 produces a minimal T-factorization.*

Proof: If σ has no mixed cycles, the result is stated in Corollary 4.8. If σ has mixed cycles, then every minimal factorization of σ will have height at least 1, and as we have just seen, such a factorization can be transformed (without increasing length) into another factorization whose right-most segment is the first "step" of the algorithm. The result follows by induction.

7 The rank of a permutation on a broom

For a broom T, we have not been able to find an exact formula or counting method, to determine the rank of a permutation, other than actually carrying out the algorithm. In order to discuss this problem we first need a definition. This definition applies to any tree T.

Definition 7.1 *Let σ be factored as $\sigma = t_m \cdots t_1$, and let x be a vertex of T. For $i = 1, 2, \cdots m$, define $\sigma_i = t_i \cdots t_1$ and $x_i = \sigma_i(x)$. Put $x_0 = x$. Then the ordered sequence $R(x) = (x_0, x_1, x_2, \cdots, x_m)$ is called the trajectory of x determined by the factorization $t_m \cdots t_1$. If $x_i \neq x_{i+1}$, then $[x_i, x_{i+1}]$ is an edge of T, and the number of edges of T in the trajectory of x, is called the length of the trajectory, and denoted by $|R(x)|$. The smallest possible value for $|R(x)|$, over all possible factorizations of σ, is denoted by $M(x, \sigma)$, or just $M(x)$ if σ is understood. The sum over all x of $M(x, \sigma)$ is denoted by $M(\sigma)$.*

The path of x, denoted by $P(x)$, is the (unique) path in T from x to $\sigma(x)$, and $|P(x)|$ is the number of edges in this path.

The next definition is stated only for a broom; however, the notion of path-containment can be generalized to any tree.

Definition 7.2 *The path-containment numbers $I(x)$ are defined as follows.*

If $x \leq \sigma(x)$, then $I(x) = |\{y : y < x \text{ and } \sigma(y) > \sigma(x)\}|$ and if $\sigma(x) < x$, then $I(x) = |\{y : y > x \text{ and } \sigma(y) < \sigma(x)\}|$.

Since $x_i = t_i(x_{i-1})$, then clearly for every $i = 0, 1, \cdots, m-1$, precisely two of the trajectories will have their i-th and $(i-1)$-st entries unequal, and so the sum of the lengths of all the trajectories is just $2m$, i.e. twice the length of the factorization $t_m \cdots t_1$, and obviously $M(\sigma)/2$ is a lower bound for the rank of σ.

If the tree T is a line (a very restricted geometry), then in any minimal factorization, the length $|R(x)|$ of the trajectory of x must be exactly the number of inversion pairs of the form $\{x, y\}$, and it can be shown (see [4]) that this number is just $|P(x)| + 2I(x) = M(x, \sigma)$. Furthermore, for any $x \in T$, in any factorization (minimal or not), $|R(x)|$ is always at least as large as $|P(x)|+2I(x)$. We may say that for a line, a factorization is minimal if and only if all the trajectories have minimal length, and in particular, $M(\sigma)/2$ is the rank.

If the tree T is a star, however, this last statement is not generally true. For instance, if σ is a product of two disjoint cycles both fixing the center vertex, a minimal trajectory for the center has length 2 and the minimal trajectory for a non-fixed point has length 2. A minimal factorization for this σ can always be arranged so that any given trajectory has length 2 more than the minimum, and the rest have minimal length. There is an overall "excess" of 2, which could appear in any of the trajectories; this is very different from the situation for a line. In general, if any σ has no more than one disjoint cycle fixing the center, then the rank of σ is just $M(\sigma)$; if there are $j \geq 2$ cycles fixing the center, then the rank is $M(\sigma)/2 + j - 1$.

For a permutation σ on a broom T, we always have $\text{rank}(\sigma) = M(\sigma)/2 + E$, where E is the "excess". In the factorization given by the algorithm of Section 2, the length of each trajectory is either minimal, or exceeds the minimum by 2, and E is the number of trajectories for this factorization, which are not of minimal length. If there are j disjoint A-cycles, this contributes $j-1$ to E, and

(in the factorization of the algorithm), the only other trajectories which may fail to have minimal length are those $R(x)$ with $x \in L$ and $\sigma(x) \in A$. Thus, E can never exceed $|A|$, and if σ has j disjoint A-cycles, E cannot be less than $j-1$. Within these bounds, however, if σ has more than one block, it appears that all possibilities can occur. In fact, even if two permutations σ and τ have the same A-cycles, and the same blocks, $E(\sigma)$ and $E(\tau)$ may differ by any amount allowable within the given bounds. In practice, in order to compute $E(\sigma)$, we need almost all the information used to find the factorization of the algorithm.

References

[1] Arthur Cayley, *The collected mathematical papers of Arthur Cayley, Cambridge University Press 1889-97* , New York, Johnson Reprint Corp., 1963.

[2] D. E. Knuth, *The Art of Computer Programming, Vol. 3, Sorting and Searching* , Addison-Wesley (1973).

[3] T. P. Vaughan, *Bounds for the Rank of a Permutation on a Tree* , Journal of Combinatorial Mathematics and Combinatorial Computing **10** (1991) 65-81.

[4] T. P. Vaughan, *A Permutation Associated with $GF(2^n)$* , Journal of Combinatorial Mathematics and Combinatorial Computing **21** (1996) .

[5] F. J. Portier and T. P. Vaughan, *An Algorithm for the Factorization of Permutations on a Tree* , Journal of Combinatorial Mathematics and Combinatorial Computing **18** (1995) 11-31.

[6] F. J. Portier and T. P. Vaughan, *Whitney Numbers of the Second Kind for the Star Poset* , European Journal of Combinatorics **11** (1990) 277-288.