CIRCULAR SORTING

RON M. ADIN, NOGA ALON, AND YUVAL ROICHMAN

Abstract. We determine the maximal number of steps required to sort n labeled points on a circle by adjacent swaps. Lower bounds for sorting by all swaps, not necessarily adjacent, are given as well.

Contents

1. Introduction

In this paper we determine the maximal number of steps required to sort n labeled points on a circle by adjacent swaps. This problem was explored, for example, in the context of micro-rearrangements of gene order in viruses; see, e.g., [4]. The analogous problem for labeled points on a line is classical. In fact, permutation sorting by adjacent transpositions may be traced back to early works in combinatorial group theory. Since Cayley graphs are vertex transitive, the (worst case) sorting time of a permutation by a set of involutions (generating the symmetric group) is equal to the diameter of the corresponding Cayley graph; equivalently, to the maximal length of an element in the prescribed generating set. Of special interest is sorting by adjacent transpositions, where the diameter is the maximal Coxeter length of an element. For any finite reflection group, the maximal Coxeter length is equal to the number of all reflections [8, §1.7]. In the symmetric group S_n, this is the number of all transpositions, namely $\binom{n}{2}$. For sorting permutations by other sets of involutions see, e.g., [5], [6] and follow-ups.

Date: February 11, 2025.

A *cyclic permutation* of order n, also called circular permutation, is an equivalence class of arrangements of the numbers $1,\ldots,n$ on a circle, where all cyclic shifts of an arrangement are considered equivalent [1]. Permutations are linearly ordered sets, while cyclic permutations are "cyclically ordered" sets. An axiomatic approach to cyclic orders was developed by Huntington [9], and extended to partial cyclic orders by Megiddo [10]. This concept was extensively studied and used since then. A different type of cyclic order, called toric order, was introduced by Develin, Macauley and Reiner [3]. Total cyclic orders, as well as total toric orders, on the set $[n]$ correspond to the $(n-1)!$ cyclic permutations.

Let π be a cyclic permutation of order n, represented by a labeling of the vertices of a cycle of length n by the elements of $[n]=\{1,2,\ldots,n\}$ in a bijective way. An *adjacent swap* is any labeling obtained from π by swapping the labels of two adjacent vertices along the cycle. How many adjacent swaps are needed in order to convert π into the trivial cyclic permutation $u=(1,2,\ldots,n)$? Equivalently, what is the diameter of the graph on all cyclic permutations represented as above, in which two cyclic permutations are adjacent if and only if one can be obtained from the other by a single adjacent swap? This graph is vertex transitive, and hence its diameter is indeed the maximum, over all cyclic permutations π, of the minimum number of adjacent swaps required to transform π into u. Let $f(n)$ denote this diameter. We prove the following.

Theorem 1.1. *For any $n\geq 1$,*

$$f(n)=\left\lfloor\frac{(n-1)^2}{4}\right\rfloor. \tag{1}$$

The rest of the paper is organized as follows. In Subsection 2.1 we prove that the RHS of Equation (1) is an upper bound for the sorting time of a cyclic permutation by adjacent swaps. In Subsection 2.2 we prove that this upper bound is tight, completing the proof of Theorem 1.1. Finally, in Section 3 we obtain bounds for the sorting time of cyclic permutations by all possible swaps, not necessarily adjacent.

2. Sorting by adjacent swaps

In this section, all swaps mentioned are adjacent swaps.

2.1. **Upper bound.** In this subsection we prove the following.

Theorem 2.1. *For any $n\geq 1$,*

$$f(n)\leq\left\lfloor\frac{(n-1)^2}{4}\right\rfloor.$$

Proof. We distinguish four cases, according to the remainder of n upon division by 4.

(a) Assume first that n is divisible by 4: $n=4m$. Let π be a cyclic permutation, and consider its representation as a labeled cycle C. Call a label small if it lies in $\{1,2,\ldots,2m\}$ and large if it lies in $\{2m+1,2m+2,\ldots,4m\}$. We claim that there is a partition of C into

two arcs, A_1 and A_2, each being a path of $2m$ consecutive vertices along C, so that each A_i contains exactly m small labels and m large labels. Indeed, starting with any arc A of $2m$ vertices, when we shift it by one step the number of small labels can change by at most 1. If A contains at most m small labels then its complement contains at least m small labels, and thus the assertion of the claim follows by the discrete intermediate value theorem.

Fix two disjoint arcs, A_1 and A_2, each containing exactly m small and m large labels. Think about these two arcs as the left and right halves of the cycle C, and subdivide each of them into a top quarter and a bottom quarter. We now consider two possible sequences of swaps. The first shifts all the m small labels of A_1 to its top quarter and all m small labels of A_2 to its top quarter, while the second shifts all the small labels of A_1 to its bottom quarter and all those of A_2 to its bottom quarter. Let the vertices of A_1 be $v_1, v_2, \ldots, v_{2m}$, in order, from top to bottom. Let the small labels in A_1 be $s_1, s_2, \ldots, s_m$, also ordered from top to bottom. Then, in the first process, s_1 has to move to the vertex v_1, and in the second process it has to move to vertex v_{m+1}. Similarly, s_2 has to reach vertex v_2 in the first process and vertex v_{m+2} in the second, and in general s_i has to reach vertex v_i in the first process and vertex v_{i+m} in the second. It is easy to check that the current location of each label s_i is between these two destinations it has to reach (since there are $i-1$ small labels in A_1 before it and $m-i$ after it). Therefore, the sum of the two distances from the location of s_i to its two destinations in the two possible processes above is m. The total number of swaps required to shift all small labels in A_1 to its top part is exactly the sum of distances of these labels from their destinations in the first process, and the analogous statement holds for the number of swaps required to shift them to the bottom part. The same reasoning applies, of course, to the arc A_2 as well. Let f_1 denote the total number of swaps required for the first process (shifting all small labels in A_1 to its top part and all those in A_2 to its top part), and let f_2 denote the total number of swaps required for the second process. By the discussion above it follows that

$$f_1 + f_2 = m \cdot m + m \cdot m = 2m^2,$$

since the total number of swaps in both processes in which any fixed small label moves is exactly m.

Let S_1 denote the set of m small labels in A_1, let L_1 denote the set of m large labels in A_1, and define S_2, L_2 analogously for the arc A_2. In order to complete the sorting after the first process, it suffices to sort the labels in $S_1 \cup S_2$ that lie in the top half of the circle, and sort the labels $L_1 \cup L_2$ in the bottom half. The number of swaps required to do so is the number of inversions in $S_1 \cup S_2$ in the order they ended at the top, plus the number of inversions in $L_1 \cup L_2$ in the order they ended in the bottom. Denote this number by g_1. Similarly, in order to complete the sorting after the second process it suffices to sort the labels in $S_1 \cup S_2$ that ended in the bottom and the labels in $L_1 \cup L_2$

that ended in the top. Let this sum be g_2. The crucial observation now is that each pair of labels $s_1 \in S_1$ and $s_2 \in S_2$ form an inversion at the end of the first process if and only if they do not form an inversion in the second. Therefore, the sum $g_1 + g_2$ satisfies

$$g_1 + g_2 \leq 2 \cdot 4\binom{m}{2} + m \cdot m + m \cdot m = 6m^2 - 4m.$$

Indeed, the total number of inversions between pairs of labels in S_1, in S_2, in L_1 and in L_2, which are counted twice in g_1+g_2, is at most $2\cdot 4\binom{m}{2}$. The total number of inversions between pairs of labels with one in S_1 and one in S_2 contributes to the sum $g_1 + g_2$ only $m \cdot m$, since each such pair forms an inversion only once, and the same applies for pairs with one label in L_1 and one in L_2.

Summing the equality (for $f_1 + f_2$) and inequality (for $g_1 + g_2$) above, we get

$$f_1 + f_2 + g_1 + g_2 \leq 8m^2 - 4m.$$

Therefore either $f_1 + g_1$ or $f_2 + g_2$ is at most

$$4m^2 - 2m = \frac{n^2 - 2n}{4} = \left\lfloor \frac{(n-1)^2}{4} \right\rfloor.$$

As we can complete the sorting with $f_1 + g_1$ swaps, and also with $f_2 + g_2$ swaps, this completes the proof for n divisible by 4.

(b) Assume now that $n = 4m + 2$. Following the previous proof, with the necessary adaptations, call a label small if it lies in $\{1, 2, \ldots, 2m + 1\}$ and large if it lies in $\{2m + 2, 2m + 3, \ldots, 4m + 2\}$. By the same argument as before, there is an arc A_1 of $2m + 1$ consecutive points with exactly m small (and $m + 1$ large) labels. Its complement A_2 is also an arc of length $2m + 1$, with $m + 1$ small (and m large) labels. View A_1 (A_2) as the left (respectively, right) half of the whole cycle. Consider two possible sequences of swaps: one shifting all the small labels of A_1 to its top, and all the small labels of A_2 to its top; and the other shifting all small labels of each arc to its bottom. The i-th small label in A_1 ($1 \leq i \leq m$, counting from top to bottom) will move to either the i-th or the $(m + 1 + i)$-th position in A_1 (again, counting from top to bottom). Its current position is somewhere between i and $m + 1 + i$, and therefore the sum of its distances from the two possible endpoints is $m + 1$. A similar argument for A_2, with $1 \leq i \leq m + 1$ and positions i and $i + m$, yields sum of distances m. If f_1 (f_2) is the total number of swaps required for the first (respectively, second) process, then

$$f_1 + f_2 = m \cdot (m + 1) + (m + 1) \cdot m = 2m(m + 1).$$

Let S_1 denote the set of m small labels in A_1, let L_1 denote the set of $m+1$ large labels in A_1, and define analogously S_2 and L_2 (of sizes $m+1$ and m, respectively) for the arc A_2. Denote by g_1 (g_2) the number of swaps require to sort $S_1 \cup S_2$ as well as $L_1 \cup L_2$ in the first (respectively, second) process. The crucial observation is that each pair of labels $s_1 \in S_1$ and $s_2 \in S_2$ form an inversion at the end of the first process if and only if

they do not form an inversion in the second; and a similar claim for $\ell_1 \in L_1$ and $\ell_2 \in L_2$. Therefore

$$g_1 + g_2 \leq 2 \cdot \left(2\binom{m}{2} + 2\binom{m+1}{2} \right) + 2m(m+1) = 6m^2 + 2m.$$

Summing the equality (for $f_1 + f_2$) and inequality (for $g_1 + g_2$) above, we get

$$f_1 + f_2 + g_1 + g_2 \leq 8m^2 + 4m.$$

Therefore either $f_1 + g_1$ or $f_2 + g_2$ is at most

$$4m^2 + 2m = \frac{(n-2)^2 + 2(n-2)}{4} = \frac{n^2 - 2n}{4} = \left\lfloor \frac{(n-1)^2}{4} \right\rfloor.$$

This completes the proof for $n = 4m + 2$.

(c) Next assume that $n = 4m + 1$. Call a label small if it lies in $\{1, 2, \ldots, 2m\}$ and large if it lies in $\{2m + 1, 2m + 2, \ldots, 4m + 1\}$. Then there is an arc A_1, consisting of $2m$ consecutive points, with exactly m small (and m large) labels. Its complement A_2 is an arc of length $2m + 1$, with m small (and $m + 1$ large) labels. Then, using notations as before,

$$f_1 + f_2 = m \cdot m + m \cdot (m+1) = 2m^2 + m$$

and

$$g_1 + g_2 \leq 2 \cdot \left(3\binom{m}{2} + \binom{m+1}{2} \right) + m^2 + m(m+1) = 6m^2 - m.$$

Therefore either $f_1 + g_1$ or $f_2 + g_2$ is at most

$$4m^2 = \frac{(n-1)^2}{4}.$$

This completes the proof for $n = 4m + 1$.

(d) Finally, assume that $n = 4m+3$. Call a label small if it lies in $\{1, 2, \ldots, 2m+2\}$ and large if it lies in $\{2m + 3, 2m + 4, \ldots, 4m + 3\}$. By a slightly modified argument (considering only arcs that do not contain a specific point with a large label), there is an arc A_1, consisting of $2m + 1$ consecutive points, with exactly $m + 1$ small (and m large) labels. Its complement A_2 is an arc of length $2m+2$, with $m+1$ small (and $m+1$ large) labels. Then, using notations as before,

$$f_1 + f_2 = (m+1) \cdot m + (m+1) \cdot (m+1) = 2m^2 + 3m + 1$$

and

$$g_1 + g_2 \leq 2 \cdot \left(3\binom{m+1}{2} + \binom{m}{2} \right) + (m+1)^2 + m(m+1) = 6m^2 + 5m + 1.$$

Therefore either $f_1 + g_1$ or $f_2 + g_2$ is at most

$$4m^2 + 4m + 1 = (2m+1)^2 = \frac{(n-1)^2}{4}.$$

This completes the proof for $n = 4m + 1$.

Having dealt with all four cases, we have now completed the proof of Theorem 2.1. □

2.2. **Lower bound.** Recall that any swap mentioned in this section is an adjacent swap.

In this subsection we prove

Theorem 2.2. *For any $n \geq 1$,*

$$f(n) \geq \left\lfloor \frac{(n-1)^2}{4} \right\rfloor .$$

Proof. By induction on n, carried out separately for odd and even values of n.

Assume first that n is odd. We shall prove that any circular sorting of the cyclic permutation $(n, n-1, \ldots, 1)$ to the trivial cyclic permutation $u = (1, 2, \ldots, n)$ requires at least $(n-1)^2/4$ swaps. This implies the claimed lower bound on the diameter $f(n)$.

The claim clearly holds for $n = 1$. For the induction step, assume that $n > 1$ is odd, and that the claim holds for $n-2$. Consider an arbitrary circular sorting of $(n, n-1, \ldots, 1)$ to u. This can be viewed as a (non-circular) sorting to the identity permutation, using affine swaps from the set $\{(1,2), (2,3), \ldots, (n-1,n), (n,1)\}$, of a suitable cyclic shift of the permutation w, which is defined by $w(i) := n + 1 - i$ $(1 \leq i \leq n)$. Such a cyclic shift is a permutation $w_{n,k} : [n] \to [n]$ of the form

$$w_{n,k}(i) \equiv k - i \pmod{n} \qquad (\forall i),$$

for some fixed integer k. Observe that, for odd n and any k, $w_{n,k}$ is an involution with one fixed point.

Let d denote circular distance on the set of n points on the circle, namely

$$d(i,j) := \min\{|i-j|, n - |i-j|\} \qquad (\forall i, j \in [n]).$$

For any $i \in [n]$, define the *gap* of i to be the distance $d(i, w_{n,k}(i))$. The gap of the unique fixed point is 0. The other gap values are the integers $1 \leq d \leq (n-1)/2$, each attained by exactly two points forming a 2-cycle of $w_{n,k}$. Let i and $j = w_{n,k}(i)$ be the two points having maximal gap $d = (n-1)/2$. Denote $A := \{i, j\}$ and $B := [n] \setminus A$; clearly, A and B are invariant under $w_{n,k}$. The restriction of $w_{n,k}$ to B can be viewed, after a suitable relabeling of the points, as the permutation $w_{n-2,\ell}$ for some ℓ.

Consider now a sequence of swaps that sorts $w_{n,k}$ to the identity permutation. Distinguish two kinds of swaps: those involving only elements of B, and those that involve at least one element of A. The latter swaps do not change the relative order of the elements of B, and therefore the former swaps yield a sorting of $w_{n-2,\ell}$ to the identity permutation. By the induction hypothesis, this requires at least $(n-3)^2/4$ swaps. Each of the remaining swaps involves at least one element of A, and it is clear that this part of the sorting, eventually interchanging i and j which are at circular distance $(n-1)/2$, requires at least $2 \cdot (n-1)/2 - 1 = n - 2$ swaps. Altogether, the sequence contains at least

$$\frac{(n-3)^2}{4} + (n-2) = \frac{(n-1)^2}{4}$$

swaps, as claimed. This proves the claim for any odd n.

Assume now that n is even. Again, we can view a circular sorting of the cyclic permutation $(n, n-1, \ldots, 1)$ to the cyclic permutation u as a sorting to the identity permutation, using affine swaps, of a permutation $w_{n,k} : [n] \to [n]$ of the form

$$w_{n,k}(i) \equiv k - i \pmod{n} \qquad (\forall i),$$

for some fixed k. This is again an involution, but now (for n even) there are two options for its number of fixed points: $w_{n,k}$ has two fixed points if k is even, and none if k is odd. We shall prove that the number of swaps needed to sort $w_{n,k}$ to the identity permutation is at least $N_{n,k}$, where

$$N_{n,k} = \begin{cases} (n^2 - 2n)/4, & \text{if } k - n/2 \text{ is odd;} \\ (n^2 - 2n + 4)/4, & \text{if } k - n/2 \text{ is even.} \end{cases}$$

Note that these numbers are $\lfloor (n-1)^2/4 \rfloor$ and $\lfloor (n-1)^2/4 \rfloor + 1$, respectively, so that our claim implies the required lower bound on the diameter $f(n)$.

The proof will proceed by induction on (even values of) n. The claim clearly holds for $n = 2$: $w_{2,k}$ is the identity permutation for even k (with $N_{2,k} = 0$), and the non-identity element of S_2 for odd k (with $N_{2,k} = 1$).

For the induction step, assume that $n > 2$ is even, and that the claim holds for $n - 2$. We consider four cases, depending on the parity of k and of $n/2$.

(a) Assume that both k and $n/2$ are even. The involution $w_{n,k}$ has two fixed points, and all its gaps are even. The minimal gap 0 and maximal gap $n/2$ are each attained by two points, while each intermediate value $2 \leq 2d \leq (n-4)/2$ is attained by four points. Let i and $j = w_{n,k}(i)$ be the two points with maximal (even) gap $n/2$; denote $A := \{i, j\}$ and $B := [n] \setminus A$. Clearly, A and B are invariant under $w_{n,k}$. The restriction of $w_{n,k}$ to B can be viewed, after a suitable relabeling of the points, as the permutation $w_{n-2,\ell}$ for some even ℓ. Noting that $(n-2)/2$ is odd, we thus get at least

$$N_{n-2,\ell} + (2 \cdot n/2 - 1) = \frac{(n-2)^2 - 2(n-2)}{4} + (n-1) = \frac{n^2 - 2n + 4}{4} = N_{n,k}$$

swaps.

(b) Assume that k is even but $n/2$ is odd. The involution $w_{n,k}$ has two fixed points, and all its gaps are even. The minimal gap 0 is attained by two points, while each other gap $2 \leq 2d \leq (n-2)/2$ is attained by four points. Let i and $j = w_{n,k}(i)$ be two of the points with maximal (even) gap $(n-2)/2$; denote $A := \{i, j\}$ and $B := [n] \setminus A$. Clearly, A and B are invariant under $w_{n,k}$. The restriction of $w_{n,k}$ to B can be viewed, after a suitable relabeling of the points, as the permutation $w_{n-2,\ell}$ for some even ℓ. Noting that $(n-2)/2$ is even, we thus get at least

$$N_{n-2,\ell} + (2 \cdot (n-2)/2 - 1) = \frac{(n-2)^2 - 2(n-2) + 4}{4} + (n-3) = \frac{n^2 - 2n}{4} = N_{n,k}$$

swaps.

(c) Assume that k is odd and $n/2$ is even. The involution $w_{n,k}$ has no fixed points, and all its gaps are odd. Each odd number $1 \le 2d-1 \le (n-2)/2$ is attained as a gap by four points. Let i and $j = w_{n,k}(i)$ be two of the points with maximal (odd) gap $(n-2)/2$; denote $A := \{i,j\}$ and $B := [n] \setminus A$. Clearly, A and B are invariant under $w_{n,k}$. The restriction of $w_{n,k}$ to B can be viewed, after a suitable relabeling of the points, as the permutation $w_{n-2,\ell}$ for some odd ℓ. Noting that $(n-2)/2$ is odd, we thus get at least

$$N_{n-2,\ell} + (2 \cdot (n-2)/2 - 1) = \frac{(n-2)^2 - 2(n-2) + 4}{4} + (n-3) = \frac{n^2 - 2n}{4} = N_{n,k}$$

swaps.

(d) Assume that both k and $n/2$ are odd. The involution $w_{n,k}$ has no fixed points, and all its gaps are odd. The maximal gap $n/2$ is attained by two points, while each other odd value $1 \le 2d-1 \le (n-4)/2$ is attained by four points. Let i and $j = w_{n,k}(i)$ be the two points with maximal (odd) gap $n/2$; denote $A := \{i,j\}$ and $B := [n] \setminus A$. Clearly, A and B are invariant under $w_{n,k}$. The restriction of $w_{n,k}$ to B can be viewed, after a suitable relabeling of the points, as the permutation $w_{n-2,\ell}$ for some odd ℓ. Noting that $(n-2)/2$ is even, we thus get at least

$$N_{n-2,\ell} + (2 \cdot n/2 - 1) = \frac{(n-2)^2 - 2(n-2)}{4} + (n-1) = \frac{n^2 - 2n + 4}{4} = N_{n,k}$$

swaps.

This proves our claim for any even n, and completes the proof of Theorem 2.2. □

3. Sorting by all swaps

The circular sorting question can be asked when a swap of any two (not necessarily adjacent) elements is allowed. In this case $n-2$ swaps always suffice (Observation 3.1). For $n = p^k$, where p is an odd prime, at least $n - 1 - \log_p n$ swaps are required (Proposition 3.2). It follows that for every prime n, the bound $n-2$ is tight (Corollary 3.3). For general n we get a lower bound of $n - O(\log n)$ (Theorem 3.10).

3.1. **Upper bound.** Let $c := (1, 2, \ldots, n)$ be an n-cycle in S_n, and let $C_n = \langle c \rangle$ be the cyclic subgroup of S_n generated by c. A cyclic permutation, namely an equivalence class $[\pi]$ where $\pi \in S_n$, may be identified with a coset πC_n.

Denote by $t([\pi])$ the sorting time of a cyclic permutation $[\pi]$ to the trivial cyclic permutation $[c]$, where a permissible step is a multiplication (on the left, or equivalently on the right) by any transposition, and let

$$t(n) := \max_{\pi \in S_n} t([\pi]).$$

Consider the graph on all cyclic permutations in which two cyclic permutations are adjacent if and only if one can be obtained from the other by a single a swap of any two letters. Since this graph is vertex transitive, its diameter is equal to $t(n)$.

For a permutation $\pi \in S_n$, let $\mathrm{cyc}(\pi)$ be the number of cycles in π. Observe that, for any $\pi \in S_n$, the sorting time of $[\pi]$

$$t([\pi]) = \min_{\sigma \in \pi C_n} (n - \mathrm{cyc}(\sigma)).$$

Hence

$$t(n) = \max_{\pi \in S_n} \min_{\sigma \in \pi C_n} (n - \mathrm{cyc}(\sigma)).$$

Observation 3.1. *For every $n \geq 2$,*

$$t(n) \leq n - 2.$$

Proof. Every permutation has a cyclic shift with a fixed point, thus with at least 2 cycles. □

Computer experimentation show that, for $n \leq 11$, this upper bound is attained only for prime values of n. In the following section we prove a general lower bound for prime powers, implying that the upper bound is indeed tight for every prime n.

3.2. **Primes and prime powers.**

Proposition 3.2. *If $n = p^k$, where p is an odd prime and $k \geq 1$, then*

$$t(n) \geq n - k - 1 = n - \log_p n - 1.$$

Proof. For $a \in \mathbb{Z}_n$ define a map $\pi_{n,a} : \mathbb{Z}_n \to \mathbb{Z}_n$ by

$$\pi_{n,a}(i) \equiv a \cdot i \pmod{n} \qquad (\forall\, i \in \mathbb{Z}_n).$$

Let $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$ be the group of units of the ring $\mathbb{Z}_n$. If $a \in \mathbb{Z}_n^\times$ then $\pi_{n,a}$ is a bijection; identifying $[n]$ with $\mathbb{Z}_n$, we can write $\pi_{n,a} \in S_n$. Moreover, if $\sigma \in \pi_{n,a} C_n$ then, for a suitable $j \in \mathbb{Z}_n$,

$$\sigma(i) \equiv a \cdot (i + j) \pmod{n} \qquad (\forall\, i \in \mathbb{Z}_n).$$

We want each σ to have a fixed point. Thus we want to have, for every $j \in \mathbb{Z}_n$, a solution i to the congruence

$$i \equiv a \cdot (i + j) \pmod{n},$$

namely to

$$(1 - a) \cdot i \equiv a \cdot j \pmod{n}.$$

This has a solution for every $j \in \mathbb{Z}_n$ (in particular, for $j = a^{-1}$) if and only if $a - 1 \in \mathbb{Z}_n^\times$. Assuming, indeed, that $a, a - 1 \in \mathbb{Z}_n^\times$, let

$$i_\sigma \equiv (1 - a)^{-1} \cdot a \cdot j \pmod{n}$$

be the (unique) fixed point of σ. Then

$$\sigma(i) - i_\sigma = \sigma(i) - \sigma(i_\sigma) = a \cdot (i + j) - a \cdot (i_\sigma + j) = a \cdot (i - i_\sigma) \qquad (\forall\, i \in \mathbb{Z}_n).$$

Thus σ is conjugate (in S_n) to $\pi_{n,a}$, by the permutation corresponding to a cyclic shift by i_σ, and therefore σ and $\pi_{n,a}$ have the same number of cycles:

$$\mathrm{cyc}(\sigma) = \mathrm{cyc}(\pi_{n,a}) \qquad (\forall \sigma \in \pi_{n,a}\mathbb{Z}_n).$$

Now let p be an odd prime and k a positive integer. The following facts regarding generators of the cyclic group $\mathbb{Z}_{p^k}^\times$ are part of the remarks following [2, Lemma 1.4.5]. Let $1 < g_0 < p$ be a generator of the cyclic group $\mathbb{Z}_p^\times$, and define

$$g := \begin{cases} g_0, & \text{if } g_0^{p-1} \not\equiv 1 \pmod{p^2}; \\ g_0 + p, & \text{otherwise.} \end{cases}$$

Then g is a generator of $\mathbb{Z}_{p^k}^\times$, simultaneously for all $k \geq 1$. The additive group $\mathbb{Z}_{p^k}$ is a disjoint union of its subsets $C_0, \ldots, C_k$, where $C_i = p^i \mathbb{Z}_{p^{k-i}}^\times$ $(0 \leq i \leq k-1)$ and $C_k = \{0\}$. For the above choice of a generator g, each of these sets forms a single cycle of $\pi_{p^k,g}$, thus $\mathrm{cyc}(\pi_{p^k,g}) = k+1$. Note also that $\gcd(g-1, p) = 1$, thus $g - 1 \in \mathbb{Z}_{p^k}^\times$ for any $k \geq 1$. It follows that

$$\mathrm{cyc}(\sigma) = \mathrm{cyc}(\pi_{p^k,g}) = k+1 \qquad (\forall \sigma \in \pi_{p^k,g}\mathbb{Z}_{p^k})$$

and therefore

$$t(p^k) = \max_{\pi \in S_{p^k}} \min_{\sigma \in \pi\mathbb{Z}_{p^k}} (p^k - \mathrm{cyc}(\sigma)) \geq \min_{\sigma \in \pi_{p^k,g}\mathbb{Z}_{p^k}} (p^k - \mathrm{cyc}(\sigma)) = p^k - (k+1). \qquad \square$$

Corollary 3.3. *If n is prime then*

$$t(n) = n - 2.$$

Proof. This clearly holds for $n = 2$. By Observation 3.1 and Proposition 3.2, it also holds if n is an odd prime. $\square$

Conjecture 3.4. *$t(n) = n - 2$ if and only if n is prime.*

Lemma 3.5. *Assume that $n > 2$ and that $\pi \in S_n$ satisfies*

$$\max_{\sigma \in \pi C_n} \mathrm{cyc}(\sigma) = 2.$$

Then each $\sigma \in \pi C_n$ has cycle structure $(n-1, 1)$.

Proof. Clearly, each $j \in [n]$ is a fixed point of a unique cyclic shift $\sigma \in \pi C_n$. This defines a mapping $f : [n] \to \pi C_n$. If $\mathrm{cyc}(\sigma) = 2$ then σ cannot have more than one fixed point (since $n > 2$). It follows that f is injective, thus bijective, and each $\sigma \in \pi C_n$ has a unique fixed point. Its other cycle is, of course, of length $n - 1$. $\square$

Conjecture 3.6. *If $n > 2$ and $\pi \in S_n$ satisfies*

$$\max_{\sigma \in \pi C_n} \mathrm{cyc}(\sigma) = 2,$$

then n is prime and

$$\pi(i) \equiv a \cdot i \pmod{n} \qquad (\forall i)$$

for some $a \in \mathbb{Z}_n^\times$.

Conjecture 3.6 implies Conjecture 3.4. Both have been verified for $n \leq 11$.

By similar arguments one can prove the following statements.

Proposition 3.7. *If $n = 2p^k$, where p is an odd prime and $k \geq 1$, then*

$$t(n) \geq n - 2k - 2.$$

Proof. Let g be a simultaneous generator for $\mathbb{Z}_{p^t}^\times$ for all $t \geq 1$, as in the proof of Proposition 3.2, and fix an integer $k \geq 1$. Then either g or $g + p^k$ (whichever is odd) is a generator of $\mathbb{Z}_{2p^k}^\times$ [2, p. 26]. It follows that there exists a simultaneous odd generator g for all $\mathbb{Z}_{2p^j}^\times$, $1 \leq j \leq k$. Using the notation $\pi_{n,a}$ from the proof of Proposition 3.2, it is easy to see that $\mathrm{cyc}(\pi_{2p^k,g}) = 2k + 2$, with cycles corresponding to the subsets $C_i^{\mathrm{odd}} = p^i \mathbb{Z}_{2p^{k-i}}^\times$ and $C_i^{\mathrm{even}} = 2p^i \mathbb{Z}_{2p^{k-i}}^\times$, $0 \leq i \leq k$.

Consider now the shifts of $\pi_{2p^k,g}$, of the form $\sigma_j := \pi_{2p^k,g} c^j$ where $c = (1, 2, \ldots, 2p^k)$. We would like to have a fixed point for σ_j for each value of j, since then σ_j is conjugate to $\sigma_0 = \pi_{2p^k,g}$; but this is impossible, since one of the two consecutive integers $g - 1$ and g must be even. We therefore only claim that σ_j has a fixed point for *even* values of j.

Indeed, a fixed point i for σ_j (j even) must satisfy

$$(1 - g) \cdot i \equiv g \cdot j \pmod{2p^k},$$

or equivalently, since both j and $g - 1$ are even,

$$\frac{1 - g}{2} \cdot i \equiv g \cdot \frac{j}{2} \pmod{p^k},$$

This has a solution for each even j if and only if $(g-1)/2$ is invertible in $\mathbb{Z}_{p^k}$, which is indeed the case (since otherwise $g \equiv 1 \pmod{p}$, contradicting the fact that g generates $\mathbb{Z}_p^\times$). Thus indeed σ_j has a fixed point, and is thus conjugate to σ_0, implying that

$$\mathrm{cyc}(\pi_{2p^k,g} c^j) = \mathrm{cyc}(\pi_{2p^k,g}) = 2k + 2 \qquad (\forall \text{ even } j).$$

Now consider odd values of j. Since

$$\sigma_j(i) \equiv g \cdot (i + j) \pmod{2p^k},$$

and g is odd, the number $\sigma_j(i)$ is odd if and only if i is even. It follows that each cycle of σ_j alternates between even and odd numbers, and therefore has even length. It follows that each cycle of σ_j splits into two cycles of σ_j^2, thus

$$\mathrm{cyc}(\sigma_j^2) = 2 \cdot \mathrm{cyc}(\sigma_j) \qquad (\forall \text{ odd } j).$$

On the other hand, we claim that, for any value of j, σ_j^2 has a fixed point and is thus conjugate to σ_0^2. Indeed,

$$\sigma_0^2(i) \equiv g^2 \cdot i \pmod{2p^k} \qquad (\forall i)$$

while

$$\sigma_j^2(i) \equiv g^2 \cdot i + (g^2 + g) \cdot j \pmod{2p^k} \qquad (\forall i).$$

In order to have $\sigma_j^2(i) = i$ we need

$$(1-g^2)\cdot i \equiv (g^2+g)\cdot j \pmod{2p^k}$$

or, equivalently,

$$\frac{1+g}{2}\cdot(1-g)\cdot i \equiv \frac{1+g}{2}\cdot g\cdot j \pmod{p^k}.$$

To this end, it is sufficient (though not necessary!) to have

$$(1-g)\cdot i \equiv g\cdot j \pmod{p^k}.$$

As noted above, this equation has a solution i for each value of j, since $g-1 \in \mathbb{Z}_{p^k}^\times$. The (now established) existence of a fixed point i_0 for σ_j^2 implies that

$$\sigma_j^2(i) - i_0 \equiv \sigma_j^2(i) - \sigma_j^2(i_0) \equiv g^2\cdot(i-i_0) \equiv \sigma_0^2(i-i_0) \pmod{2p^k},$$

so that $\sigma_j^2 = c^{i_0}\sigma_0^2 c^{-i_0}$ is conjugate to σ_0^2 in S_{2p^k}. We therefore have

$$\mathrm{cyc}(\sigma_j^2) = \mathrm{cyc}(\sigma_0^2) \qquad (\forall j).$$

Finally, the above description of the cycles of $\sigma_0 = \pi_{2p^k,g}$ shows that all its cycle lengths are divisible by $p-1$, hence even, except for the two fixed points. It follows that

$$\mathrm{cyc}(\sigma_0^2) = 2\cdot\mathrm{cyc}(\sigma_0) - 2.$$

Putting it all together, we have

$$\mathrm{cyc}(\sigma_j) = \mathrm{cyc}(\sigma_0) - 1 \qquad (\forall \text{ odd } j),$$

namely

$$\mathrm{cyc}(\pi_{2p^k,g}c^j) = \mathrm{cyc}(\pi_{2p^k,g}) - 1 = 2k+1 \qquad (\forall \text{ odd } j).$$

Thus

$$\begin{aligned} t(2p^k) &= \max_{\pi\in S_{2p^k}} \min_{\sigma\in\pi\mathbb{Z}_{2p^k}} (2p^k - \mathrm{cyc}(\sigma)) \geq \min_{\sigma\in\pi_{2p^k,g}\mathbb{Z}_{2p^k}} (2p^k - \mathrm{cyc}(\sigma)) \\ &= \min(2p^k-(2k+2), 2p^k-(2k+1)) = 2p^k-(2k+2). \end{aligned}$$

□

Proposition 3.8. *If $n = 2^k$ and $k \geq 2$ then*

$$t(n) \geq n - 2k + 1.$$

Proof. First, for $k=2$ the lower bound holds, since $t(4) = 1 = 4 - 2\cdot 2 + 1$.

Assume that $k \geq 3$. It was shown by Gauss [7, Art. 90–91] that, in this case, $\mathbb{Z}_{2^k}^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$, where 3 is a generator of the factor $\mathbb{Z}_{2^{k-2}}$ and -1 is a generator of the factor $\mathbb{Z}_2$; see also [11, Ch. 6, §6].

Note that 3 also generates the cyclic group $\mathbb{Z}_4^\times$. Using the notation $\pi_{n,a}$ from the proof of Proposition 3.2, one concludes that the cycles of $\pi_{2^k,3}$ are the subsets $C_i^\varepsilon := \{\varepsilon\cdot 2^i 3^j : 0 \leq j < 2^{k-2-i}\}$ $(0 \leq i \leq k-3, \varepsilon \in \{1,-1\})$, $C_{k-2} = \{2^{k-2}, -2^{k-2}\}$, $C_{k-1} = \{2^{k-1}\}$ and $C_k = \{0\}$. Hence $\mathrm{cyc}(\pi_{2^k,3}) = 2k-1$.

Regarding the shifts, by arguments as above, for every even j, $\pi_{2^k,3}c^j$ and $\pi_{2^k,3}$ are conjugate, hence have the same number of cycles. Finally, we claim that for every odd j, $\pi_{2^k,3}c^j$ has two cycles. Indeed, for $d \geq 1$ and any m we have

$$(\pi_{2^k,3}c^j)^d(m) \equiv m \cdot 3^d + 3j \cdot \sum_{i=0}^{d-1} 3^i \equiv m \pmod{2^k}$$

if and only if

$$(2m + 3j) \cdot \frac{3^d - 1}{2} \equiv 0 \pmod{2^k},$$

which holds (for an odd j) if and only if

$$3^d - 1 \equiv 0 \pmod{2^{k+1}}.$$

Recalling that the order of 3 in $\mathbb{Z}^\times_{2^{k+1}}$ is 2^{k-1}, this holds if and only if 2^{k-1} divides d, so that indeed $\pi_{2^k,3}c^j$ for odd j has two cycles of length 2^{k-1} each. Overall, for $k \geq 3$,

$$\begin{aligned} t(2^k) &= \max_{\pi \in S_{2^k}} \min_{\sigma \in \pi\mathbb{Z}_{2^k}} (2^k - \mathrm{cyc}(\sigma)) \geq \min_{\sigma \in \pi_{2^k,3}\mathbb{Z}_{2^k}} (2^k - \mathrm{cyc}(\sigma)) \\ &= \min(2^k - (2k-1), 2^k - 2) = 2^k - (2k-1). \end{aligned}$$

□

Question 3.9. *Is the function $t(n)$ monotone?*

If the function $t(n)$ is monotone, one can apply the above bounds to other integers. Note, however, that adding a fixed point to $\pi \in S_n$ may decrease the value of t. For example, $t([\pi_{11,3}]) = 9$, while defining $\sigma \in S_{12}$ by $\sigma(i) = \pi_{11,3}(i)$ for $i \leq 11$ and $\sigma(12) = 12$ yields $t([\sigma]) = 8$.

3.3. **General lower bound.** In this section we prove a general lower bound, which is independent of the prime decomposition of n.

Theorem 3.10. *For any $n > 1$*

$$t(n) \geq n - \lceil e \cdot (\ln n + 1) \rceil.$$

Note that for large $n = 2^k$ this bound is stronger than the one in Proposition 3.8.

First we show that the probability that a random permutation has a large number of cycles is small. The following result is surely known in a very precise form; for completeness we include a self contained elementary proof.

Proposition 3.11. *For any $k \geq 0$, the probability that a random permutation in S_n has exactly $k+1$ cycles is at most*

$$\frac{(\ln(n-1) + 1)^k}{n \cdot k!}.$$

Proof. We count the number of permutations with $k+1$ cycles as follows. Write each cycle of the permutation with the smallest element of the cycle first, and arrange the cycles in increasing order of their first elements. The first cycle starts with the element 1. We can select the next element of the cycle arbitrarily, then the next one, and so on. If the length of this cycle is n_1 then this gives $(n-1)(n-2)\cdots(n-n_1+1)$ possibilities. The second cycle must start with the smallest number that was not chosen yet. Proceed in the same manner to choose the other cycle elements. If its length is n_2 then this gives $(n-n_1-1)(n-n_1-2)\cdots(n-n_1-n_2+1)$ possibilities. Proceeding in this way, we see that the number of permutations with $k+1$ cycles of lengths $n_1,\ldots,n_{k+1}$ (arranged according to the above convention) is

$$\frac{n!}{n(n-n_1)(n-n_1-n_2)\cdots(n-n_1-n_2\ldots-n_k)}.$$

Summing over all possibilities of cycle lengths gives

$$\frac{n!}{n}\cdot\sum\frac{1}{m_1m_2\cdots m_k},$$

where the summation is over all k-tuples $(m_1,m_2,\ldots,m_k)$ of integers satisfying $n>m_1>m_2>\cdots>m_k>0$.

Consider now the expression

$$\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n-1}\right)^k.$$

In this expression, every product as above appears $k!$ times (and there are also additional products with non-distinct factors). Therefore, the total number of permutations with $k+1$ cycles is at most

$$\frac{n!}{n\cdot k!}\cdot\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n-1}\right)^k,$$

implying the desired result by the standard bound on the harmonic series. □

Proof of Theorem 3.10. For simplicity, replace the upper bound in Proposition 3.11 by the slightly larger bound

$$p_k := \frac{(\ln n+1)^k}{n\cdot k!}.$$

Recalling that $k!>(k/e)^k\cdot\sqrt{2\pi k}$ for every $k\geq 1$, Proposition 3.11 implies that the probability of having k_0+1 cycles, for $k_0:=\lceil e(\ln n+1)\rceil$, is at most

$$p_{k_0}<\frac{1}{n\cdot\sqrt{2\pi k_0}}\cdot\left(\frac{e(\ln n+1)}{k_0}\right)^{k_0}\leq\frac{1}{n\cdot\sqrt{2\pi k_0}}.$$

Now note that, by definition, for $k\geq k_0$

$$p_{k+1}=p_k\cdot\frac{\ln n+1}{k+1}\leq p_k\cdot\frac{\ln n+1}{e(\ln n+1)}=p_k\cdot\frac{1}{e}.$$

It follows that the probability of a random permutation in S_n to have more than k_0 cycles is at most

$$\sum_{k=k_0}^{n-1} p_k < p_{k_0} \cdot \sum_{m=0}^{\infty} e^{-m} < \frac{1}{n} \cdot \frac{1}{(1-e^{-1}) \cdot \sqrt{2\pi k_0}} < \frac{1}{n}\,.$$

Therefore, for a random permutation π, $\mathrm{cyc}(\pi c^j) \leq k_0$ for every j with high probability, and hence there exists such a permutation π. □

Acknowledgment Noga Alon is supported in part by NSF grant DMS-2154082.

References

[1] R. A. Brualdi, Introductory Combinatorics (5th ed.), Prentice-Hall, 2010.
[2] H. Cohen, A Course in Computational Algebraic Number Theory, Springer, Berlin, 1993.
[3] M. Develin, M. Macauley and V. Reiner, *Toric partial orders*, Trans. Amer. Math. Soc. **368** (2016), 2263–2287.
[4] X. Feng, B. Chitturi and H. Sudborough, *Sorting circular permutations by bounded transpositions*, in: Advances in Computational Biology, Springer, New York, 2010, pp. 725–736.
[5] W. H. Gates and C. H. Papadimitriou, *Bounds for sorting by prefix reversal*, Discrete Math. **27** (1979), 47–57.
[6] E. Győri and G. Turán, *Stack of pancakes*, Studia Sci. Math. Hungar. **13** (1978), 133–137.
[7] C. F. Gauss, Disquisitiones Arithmeticae, Translated and with a preface by A. A. Clarke, Revised by W. C. Waterhouse, C. Greither and A. W. Grootendorst with a preface by W. C. Waterhouse, Springer, New York, 1986.
[8] J. E. Humphreys, Reflection groups and Coxeter groups. Cambridge Stud. Adv. Math. **29**, Cambridge University Press, Cambridge, 1990.
[9] E. V. Huntington, *Sets of completely independent postulates for cyclic order*, Proc. National Acad. Sci. USA **10** (1924), 74–78,
[10] N. Megiddo, *Partial and complete cyclic orders*, Bull. Amer. Math. Soc. **82** (1976), 274-–276.
[11] I. M. Vinogradov, *Elements of Number Theory*, English translation by S. Kravetz, Dover Publications, 1954.

Department of Mathematics, Bar-Ilan University, Ramat-Gan 52900, Israel
Email address: radin@math.biu.ac.il

Department of Mathematics, Princeton University, Princeton, NJ 08544, USA
Email address: nalon@math.princeton.edu

Department of Mathematics, Bar-Ilan University, Ramat-Gan 52900, Israel
Email address: yuvalr@math.biu.ac.il