

# On the Subgroup Distance Problem in Cyclic Permutation Groups

Andreas Rosowski  
rosowski@eti.uni-siegen.de

University of Siegen, Germany

## Abstract

We show that the SUBGROUP DISTANCE PROBLEM regarding the Hamming distance, the Cayley distance, the  $l_\infty$  distance, the  $l_p$  distance (for all  $p \geq 1$ ), the Lee distance, Kendall's tau distance and Ulam's distance is NP-complete when the input group is cyclic. When we restrict the  $l_\infty$  distance to fixed values we show that it is NP-complete to decide whether there are numbers  $z_1, z_2 \in \mathbb{N}$  such that  $l_\infty(\beta, \alpha_1^{z_1} \alpha_2^{z_2}) \leq 1$  for permutation  $\alpha_1, \alpha_2, \beta \in S_n$  where  $\alpha_1$  and  $\alpha_2$  commute. However on the positive side we can show that it can be decided in NL whether there is a number  $z \in \mathbb{N}$  such that  $l_\infty(\beta, \alpha^z) \leq 1$  for permutations  $\alpha, \beta \in S_n$ . For the former we provide a tool, namely for all numbers  $t_1, t_2, t \in \mathbb{N}$  where  $t$  is required to be odd,  $0 \leq t_1 < t_2 < t$  and  $t_1 \not\equiv t_2 \pmod q$  for all primes  $q \mid t$  we give a constructive proof for the existence of permutations  $\alpha, \beta \in S_t$  with  $l_\infty(\beta, \alpha^{t_1}) \leq 1$  and  $l_\infty(\beta, \alpha^{t_2}) \leq 1$ .

## 1 Introduction

Bijjective functions on a set  $\Omega$  are called permutations. The set of all permutations on  $\Omega$  forms a group  $\text{Sym}(\Omega)$ , the so called symmetric group on  $\Omega$ . The group operator is the composition of functions. Subgroups of  $\text{Sym}(\Omega)$  are also called permutation groups. We only consider finite permutation groups. With  $S_n$  we denote the symmetric group where  $\Omega = \{1, \dots, n\}$ . The order of a subgroup of  $S_n$ , i.e. the number of elements of this group, can be exponentially large in  $n$ . For instance  $S_n$  contains  $n!$  permutations. Therefore permutation groups are usually given by a set of generators. And in fact for  $n > 3$  every subgroup of  $S_n$  can be generated by a generating set of size at most  $\frac{n}{2}$  [14] and thereby provides a much more succinct representation. In such a setting where the group elements are no longer given explicitly it is a priori not clear how efficient subgroup membership checking can be done. However it was shown that subgroup membership checking can be done in polynomial time when the permutation group is given by a set of generators [11, 20]. Later it was shown that it can even be done in NC by [3]. There are many more algorithmic problems that can be solved in polynomial time when the permutation group is given by a set of generators [19, Chapter 3].

Even in the case that a given permutation is not a member of a group  $G$  one might still ask how close this permutation is to  $G$ . This leads us to the following problem that we study:

**Problem 1** (SUBGROUP DISTANCE PROBLEM).

*Input:*  $\gamma_1, \dots, \gamma_m, \gamma \in S_n, k \in \mathbb{N}$ .

*Question:* Is there an element  $\delta \in \langle \gamma_1, \dots, \gamma_m \rangle$  such that  $d(\gamma, \delta) \leq k$ ?

Here  $d$  is a metric on  $S_n$ . Note that the unary encoded number  $n$  is part of the input. For evaluation  $\pi(i)$  of a permutation  $\pi \in S_n$  at position  $i \in \{1, \dots, n\}$  we use the notation  $i^\pi$ . We investigate the SUBGROUP DISTANCE PROBLEM with respect to the following metrics:

- The Hamming distance of two permutations  $\tau, \pi \in S_n$  is defined as

$$H(\tau, \pi) = |\{i \mid i^\tau \neq i^\pi\}|.$$

- The Cayley distance of two permutations  $\tau, \pi \in S_n$  is defined as

$$C(\tau, \pi) = \text{minimum number of transpositions taking } \tau \text{ to } \pi.$$

By [9] this can be expressed as

$$C(\tau, \pi) = n - \text{number of cycles in } \tau\pi^{-1}$$

where fixed-points also count as cycles. We will always use the second expression.

- The  $l_\infty$  distance of two permutations  $\tau, \pi \in S_n$  is defined as

$$l_\infty(\tau, \pi) = \max_{1 \leq i \leq n} |i^\tau - i^\pi|.$$

- The  $l_p$  distance of two permutations  $\tau, \pi \in S_n$  is defined as

$$l_p(\tau, \pi) = \sqrt[p]{\sum_{i=1}^n |i^\tau - i^\pi|^p}.$$

- The Lee distance of two permutations  $\tau, \pi \in S_n$  is defined as

$$L(\tau, \pi) = \sum_{i=1}^n \min(|i^\tau - i^\pi|, n - |i^\tau - i^\pi|).$$

- Kendall's tau distance of two permutations  $\tau, \pi \in S_n$  is defined as

$$K(\tau, \pi) = \text{the minimum number of pairwise adjacent transpositions to obtain } \pi \text{ from } \tau.$$

By [6] this can also be expressed as

$$K(\tau, \pi) = |\{(i, j) \mid 1 \leq i, j \leq n, i^\tau < j^\tau, i^\pi > j^\pi\}|.$$

We will always use the second expression.

- Ulam's distance of two permutations  $\tau, \pi \in S_n$  is defined as

$$U(\tau, \pi) = n - \text{the length of the longest increasing subsequence in } (1^{\tau\pi^{-1}}, \dots, n^{\tau\pi^{-1}}).$$

The paper [8] is a good survey about metrics and their applications, see also [9, Chapter 6] for more information about these metrics.

Our main result is that the SUBGROUP DISTANCE PROBLEM regarding all these metrics is NP-complete when the input permutation group is cyclic. Our motivating results for this are from [4] where it was shown that the SUBGROUP DISTANCE PROBLEM regarding all metrics mentioned above is NP-complete when the input group is abelian of exponent 2 and from [15] where it was shown that the SUBGROUP DISTANCE PROBLEM has applications in cryptography. Moreover we investigate the SUBGROUP DISTANCE PROBLEM regarding the  $l_\infty$  distance in the case when  $k$  from Problem 1 is a fixed constant. For  $k = 1$  we show that the SUBGROUP DISTANCE PROBLEM is NP-complete when the input group is abelian and given by at least two generators and can be solved in non-deterministic logspace (NL for short) when the input group is given by a single generator.

We also would like to mention that the SUBGROUP DISTANCE PROBLEM regarding the Cayley distance was already shown to be NP-complete when the input group is abelian of exponent 2 by [17]. When considering the SUBGROUP DISTANCE PROBLEM in the case  $k = 0$  this problem simply becomes a subgroup membership problem for permutation groups which can be solved in polynomial time by the Schreier-Sims algorithm [11, 20] and was later shown to be solvable in NC [3].

## 1.1 Related Work

In [4] also the maximum subgroup distance problem was studied where for given permutations  $\pi_1, \dots, \pi_m, \tau \in S_n$  and  $k \in \mathbb{N}$  it is asked whether there is an element  $\pi \in \langle \pi_1, \dots, \pi_m \rangle$  such that  $d(\tau, \pi) \geq k$ ? This problem has also been shown to be NP-complete when the input group is abelian of exponent 2 regarding all metrics mentioned in the introduction except for the  $l_\infty$  metric. In this case the problem can be solved in polynomial time.

In [6] the weight problem and variants were studied. The weight of a permutation  $\pi \in S_n$  with respect to some metric  $d$  is defined as  $w_d(\pi) = d(\pi, \text{id})$  and the question is whether for given permutations  $\pi_1, \dots, \pi_m \in S_n$  and  $k \in \mathbb{N}$  there is  $\pi \in \langle \pi_1, \dots, \pi_m \rangle$  such that  $w_d(\pi) = k$ ? In the maximum weight problem it is instead asked whether there is  $\pi \in \langle \pi_1, \dots, \pi_m \rangle$  such that  $w_d(\pi) \geq k$ ? The minimum weight problem asks whether there is  $\pi \in \langle \pi_1, \dots, \pi_m \rangle \setminus \{\text{id}\}$  such that  $w_d(\pi) \leq k$ ? These problems regarding several metrics were shown to be NP-complete except for the maximum weight problem regarding the  $l_\infty$  metric which has been shown to be solvable in polynomial time. Note that the NP-completeness of the weight problem regarding the Hamming metric was already shown in [5].

In [2] the computational complexity of the minimum weight problem and the subgroup distance problem was studied in a deterministic setting regarding exact and approximation versions.

In [1] the parameterized complexity of the maximum weight problem regarding the Hamming metric was studied.

## 2 Preliminaries

We will occasionally need the following lemma that seems to be folklore:

**Lemma 1.** *Let  $\alpha \in S_n$  be a cycle of length  $l \leq n$ . Then  $\alpha^x$  splits into  $\gcd(x, l)$  many disjoint cycles of length  $\frac{l}{\gcd(x, l)}$ .*

A proof can be found in [13]. All proofs of NP-hardness will start from one of the following problems:

### Problem 2 (3-SAT).

*Input: a finite set  $X$  of variables and a set  $C$  of clauses over  $X$  with  $|c| = 3$  for all  $c \in C$ .*

*Question: Is there a satisfying truth assignment for  $C$ ?*

### Problem 3 (Not-All-Equal 3SAT).

*Input: a finite set  $X$  of variables and a set  $C$  of clauses over  $X$  with  $|c| = 3$  for all  $c \in C$ .*

*Question: Is there a truth assignment for  $X$  such that each clause in  $C$  has at least one true literal and at least one false literal?*

### Problem 4 (X3HS).

*Input: a finite set  $X$  and a set  $\mathcal{B} \subseteq 2^X$  of subsets of  $X$  all of size 3.*

*Question: Is there a subset  $X' \subseteq X$  such that  $|X' \cap C| = 1$  for all  $C \in \mathcal{B}$ ?*

All of these problems are NP-complete [12]. For this also note that X3HS is the same problem as positive 1-in-3-SAT.

## 2.1 Permutations

We denote with  $S_n$  the set of all permutations on the set  $\{1, \dots, n\}$  for some integer  $n \geq 1$ . By  $\text{id}$  we denote the permutation that fixes all points. For a permutation  $\pi \in S_n$  and all  $i \in \{1, \dots, n\}$  we use  $i^\pi$  to denote the unique  $j \in \{1, \dots, n\}$  such that  $\pi(i) = j$ . Moreover we evaluate from left to right, i.e. for permutations  $\pi_1, \dots, \pi_m \in S_n$  and some  $a_0, a_1, \dots, a_m \in \{1, \dots, n\}$  we have  $a_0^{\pi_1 \cdots \pi_m} = a_m$  if and only if for  $i = 1, \dots, m-1$  we have  $a_{i-1}^{\pi_i \cdots \pi_m} = a_i^{\pi_{i+1} \cdots \pi_m}$  and  $a_{m-1}^{\pi_m} = a_m$ .

We assume that permutations are given in standard representation. There are two standard representations: the pointwise representation where a permutation  $\pi \in S_n$  is represented by a list

$[1^\pi, 2^\pi, \dots, n^\pi]$  and the cycle representation where  $\pi$  is represented by a list of its pairwise disjoint cycles. Fixed-points are usually not included in this list. The standard representations can be transformed into each other in log-space [7].

## 2.2 Notations

For a cycle  $\gamma$  we define

$$\text{act}(\gamma) = \begin{cases} \{i\} & \text{if } \gamma \text{ is a 1-cycle identifying the fixed-point } i^\gamma = i \\ \{i \mid i^\gamma \neq i\} & \text{if } \gamma \text{ has length at least 2.} \end{cases}$$

By  $\text{ord}(\alpha)$  where  $\alpha \in S_n$  we denote the order of  $\alpha$  i.e. the smallest non-negative integer  $i \geq 1$  such that  $\alpha^i = \text{id}$ . With  $\nu_p(n)$  we denote the  $p$ -adic valuation of the integer  $n \in \mathbb{Z}$ , i.e. the largest positive integer  $d$  such that  $n \equiv 0 \pmod{p^d}$ . We use the notation  $[i, j]$  to denote the set  $\{i, i+1, i+2, \dots, j\}$  for integers  $i \leq j$ . Moreover we use  $\llbracket i, j \rrbracket$  to denote the cycle  $(i, i+1, i+2, \dots, j) \in S_n$  for non-negative integers  $1 \leq i < j \leq n$ . We also use  $\llbracket i \rrbracket$  instead of  $\llbracket 1, i \rrbracket$  for a non-negative integer  $2 \leq i \leq n$ . For permutations  $\tau, \pi \in S_n$  and some non-negative integer  $p \geq 1$  we denote with  $p\text{-val}(\tau, \pi)$  the value

$$p\text{-val}(\tau, \pi) = \sum_{i=1}^n |i^\tau - i^\pi|^p.$$

Moreover for a permutation  $\omega \in S_n$  we denote by  $\vec{\omega}^z \in S_n^z$  the unique tuple of permutations in  $S_n^z$  that contains in each coordinate a copy of  $\omega$ . For a permutation  $\sigma \in S_n$  we denote with  $\text{lis}(\sigma)$  the length of the longest increasing subsequence in  $(1^\sigma, \dots, n^\sigma)$ . Let  $X$  be a set of variables and let  $\sigma$  be a truth assignment of these variables. With  $\hat{\sigma}$  we denote the extension of  $\sigma$  to literals which we denote by  $\tilde{x}$  for some variable  $x \in X$ . Then we have

$$\hat{\sigma}(\tilde{x}) = \begin{cases} 1 & \text{if } \tilde{x} = x \text{ and } \sigma(x) = 1 \text{ or } \tilde{x} = \bar{x} \text{ and } \sigma(x) = 0 \\ 0 & \text{if } \tilde{x} = x \text{ and } \sigma(x) = 0 \text{ or } \tilde{x} = \bar{x} \text{ and } \sigma(x) = 1. \end{cases}$$

## 3 Subgroup Distance Problem

In the following sections when we show NP-completeness results we only show the hardness since membership in NP has already been shown in [4] for all metrics from the introduction.

### 3.1 Hamming Distance

**Lemma 2.** *Let  $l \geq 2$  and  $0 \leq e \leq l-1$  be integers. Then  $\llbracket l \rrbracket^x$  and  $\llbracket l \rrbracket^e$  match at  $l$  positions if  $x \equiv e \pmod{l}$  and mismatch at  $l$  positions if  $x \not\equiv e \pmod{l}$ .*

*Proof.* Let  $1 \leq i \leq l$  and let  $0 \leq y \leq l-1$  be such that  $y \equiv x \pmod{l}$ . Then we have

$$i^{\llbracket l \rrbracket^x} = \begin{cases} i+y & \text{if } i+y \leq l \\ i+y-l & \text{otherwise} \end{cases}$$

and

$$i^{\llbracket l \rrbracket^e} = \begin{cases} i+e & \text{if } i+e \leq l \\ i+e-l & \text{otherwise.} \end{cases}$$

Therefore we have  $i^{\llbracket l \rrbracket^x} = i^{\llbracket l \rrbracket^e}$  if and only if  $i+y = i+e$  or  $i+y-l = i+e-l$  if and only if  $y = e$  if and only if  $x \equiv e \pmod{l}$ . Note that the cases  $i+y = i+e-l$  and  $i+y-l = i+e$  cannot occur since we would get  $y = e-l < 0$  and  $y = e+l > l-1$  which contradict  $0 \leq y \leq l-1$ .  $\square$

**Theorem 1.** *The SUBGROUP DISTANCE PROBLEM regarding the Hamming distance is NP-complete when the input group is cyclic.*

*Proof.* We give a log-space reduction from 3-SAT. Let  $X = \{x_1, \dots, x_n\}$  be a set of variables and let  $C = \{c_1, \dots, c_m\}$  be a set of clauses over  $X$  where  $c_j$  contains exactly 3 different literals for all  $j \in [1, m]$ . W.l.o.g. we can assume that no clause contains a positive and a negative literal regarding the same variable. For  $j \in [1, m]$  we define  $I_j \subseteq [1, n]$  as the set of all indices  $i$  such that  $c_j \cap \{x_i, \bar{x}_i\} \neq \emptyset$ . Let  $p_1, \dots, p_n$  be the first  $n$  odd primes. Moreover let  $q_j = \prod_{i \in I_j} p_i$  for  $j \in [1, m]$  and let  $N = 2 \sum_{i=1}^n p_i + 7 \sum_{j=1}^m q_j$ . We will work with the group  $G \leq S_N$  in which

$$G = \prod_{i=1}^n V_i \times \prod_{j=1}^m U_j$$

with  $V_i = S_{p_i}^2$  and  $U_j = S_{q_j}^7$ . We define the input group elements as

$$\begin{aligned} \tau &= (\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) \\ \pi &= (\gamma_1, \dots, \gamma_n, \delta_1, \dots, \delta_m) \end{aligned}$$

with  $\alpha_i = ([p_i], \text{id})$  and  $\gamma_i = ([p_i], [p_i])$  for  $i \in [1, n]$ . To define  $\beta_j$  and  $\delta_j$  for  $j \in [1, m]$  consider the clause  $c_j$ . There are 7 truth assignments of the variables occurring in this clause that satisfy this clause. Let  $\sigma_1, \dots, \sigma_7$  be the truth assignments of the variables occurring in this clause that satisfy the clause. Then we define for all  $j \in [1, m]$  and  $l \in [1, 7]$  numbers  $0 \leq z_{j,l} \leq q_j - 1$  as the smallest positive integers satisfying the congruences

$$z_{j,l} \equiv \sigma_l(x_i) \pmod{p_i}$$

for all  $i \in I_j$ . Then we define for  $j \in [1, m]$

$$\begin{aligned} \beta_j &= ([q_j]^{z_{j,1}}, [q_j]^{z_{j,2}}, [q_j]^{z_{j,3}}, [q_j]^{z_{j,4}}, [q_j]^{z_{j,5}}, [q_j]^{z_{j,6}}, [q_j]^{z_{j,7}}) \\ \delta_j &= ([q_j], [q_j], [q_j], [q_j], [q_j], [q_j], [q_j]). \end{aligned}$$

Finally we set  $k = \sum_{i=1}^n p_i + 6 \sum_{j=1}^m q_j$ . Now we show that  $C$  is satisfiable if and only if there is a number  $z \in \mathbb{N}$  such that  $H(\tau, \pi^z) \leq k$ . Suppose  $C$  is satisfiable and let  $\sigma$  be a truth assignment that satisfies  $C$ . Let  $0 \leq z \leq \prod_{i=1}^n p_i - 1$  be the smallest positive integer satisfying the congruence  $z \equiv \sigma(x_i) \pmod{p_i}$  for  $i \in [1, n]$ . Consider  $\alpha_i$  and  $\gamma_i$ . Clearly we have that  $([p_i], \text{id})$  and  $([p_i], [p_i])^z$  match at  $p_i$  positions. Now consider  $\beta_j$  and  $\delta_j$  for some  $j \in [1, m]$ . Since  $C$  is satisfied by  $\sigma$  there is an  $l \in [1, 7]$  such that  $\sigma_l(x_i) = \sigma(x_i)$  for  $i \in I_j$ . Hence we have  $z \equiv z_{j,l} \pmod{q_j}$ . Then we have  $[q_j]^z = [q_j]^{z_{j,l}}$  which gives us that

$$\delta_j^z = ([q_j]^{z_{j,l}}, [q_j]^{z_{j,l}}, [q_j]^{z_{j,l}}, [q_j]^{z_{j,l}}, [q_j]^{z_{j,l}}, [q_j]^{z_{j,l}}, [q_j]^{z_{j,l}})$$

and matches with

$$\beta_j = ([q_j]^{z_{j,1}}, [q_j]^{z_{j,2}}, [q_j]^{z_{j,3}}, [q_j]^{z_{j,4}}, [q_j]^{z_{j,5}}, [q_j]^{z_{j,6}}, [q_j]^{z_{j,7}})$$

at  $q_j$  positions. This gives us a total of  $\sum_{i=1}^n p_i + \sum_{j=1}^m q_j$  matching positions. Subtracting this number from the total number of positions gives us

$$H(\tau, \pi^z) = 2 \sum_{i=1}^n p_i + 7 \sum_{j=1}^m q_j - \left( \sum_{i=1}^n p_i + \sum_{j=1}^m q_j \right) = \sum_{i=1}^n p_i + 6 \sum_{j=1}^m q_j = k$$

mismatches.

Vice versa suppose  $H(\tau, \pi^z) \leq k$  for some  $z \in \mathbb{N}$ . Consider  $\alpha_i$  and  $\gamma_i$ . By Lemma 2 we have that  $([p_i], \text{id})$  and  $([p_i], [p_i])^z$  match at  $p_i$  positions if  $z \equiv 0, 1 \pmod{p_i}$  or at no position otherwise. Moreover

$$\begin{aligned} \delta_j^z &= ([q_j]^z, [q_j]^z, [q_j]^z, [q_j]^z, [q_j]^z, [q_j]^z, [q_j]^z) \\ \beta_j &= ([q_j]^{z_{j,1}}, [q_j]^{z_{j,2}}, [q_j]^{z_{j,3}}, [q_j]^{z_{j,4}}, [q_j]^{z_{j,5}}, [q_j]^{z_{j,6}}, [q_j]^{z_{j,7}}) \end{aligned}$$

match at  $q_j$  positions if  $z \equiv z_{j,1}, \dots, z_{j,7} \pmod{q_j}$  or at no position otherwise. By counting the number of possible matchings we find that we can match at most  $\sum_{i=1}^n p_i + \sum_{j=1}^m q_j$  positions. By noting that  $k + \sum_{i=1}^n p_i + \sum_{j=1}^m q_j$  equals the total number of positions we obtain that in every coordinate of  $G$  we need the maximal number of matchings. Therefore we have for all  $i \in [1, n]$  the congruence  $z \equiv 0, 1 \pmod{p_i}$ . Therefore  $z$  encodes a truth assignment of the variables. Since the  $z_{j,l}$  encode satisfying truth assignments of  $c_j$  we find that the truth assignment encoded by  $z$  satisfies all clauses. Therefore we obtain by

$$\sigma(x_i) = \begin{cases} 1 & \text{if } z \equiv 1 \pmod{p_i} \\ 0 & \text{if } z \equiv 0 \pmod{p_i} \end{cases}$$

a satisfying truth assignment for  $C$ . □

### 3.2 Cayley Distance

**Lemma 3.** *Let  $n \geq 1$  be an integer. Let us denote by  $\hat{p}_k$  the  $k^{\text{th}}$  prime, i.e.  $\hat{p}_1 = 2, \hat{p}_2 = 3, \dots$ . Then  $\hat{p}_{n^2+86}^3 > 6\hat{p}_{n^2+n+85}^2$ .*

*Proof.* We have

$$\hat{p}_k \geq k(\ln k + \ln \ln k - 1) \text{ for all } k \geq 2 \text{ by [10, Theorem 3]}. \quad (1)$$

Moreover we have

$$\hat{p}_k \leq k(\ln k + \ln \ln k) \text{ if } 6 \leq k \leq e^{95} \text{ by [18, Theorem 28]}$$

and

$$\hat{p}_k \leq k(\ln k + \ln \ln k - 0.9484) \text{ for all } k \geq 39017 \text{ by [10, Chapter 4]}$$

which gives us

$$\hat{p}_k \leq k(\ln k + \ln \ln k) \text{ for all } k \geq 6. \quad (2)$$

Using (1) we obtain

$$\hat{p}_{n^2+86}^3 \geq (n^2 + 86)^3 (\ln(n^2 + 86) + \ln \ln(n^2 + 86) - 1)^3$$

and (2) gives us

$$\hat{p}_{n^2+n+85}^2 \leq (n^2 + n + 85)^2 (\ln(n^2 + n + 85) + \ln \ln(n^2 + n + 85))^2.$$

From this it follows now that

$$\begin{aligned} \hat{p}_{n^2+86}^3 &\geq (n^2 + 86)^3 (\ln(n^2 + 86) + \ln \ln(n^2 + 86) - 1)^3 \\ &> (n^2 + 86)^3 \ln(n^2 + 86)^3 \\ &= (n^2 + 86) \ln(n^2 + 86) (n^2 + 86)^2 \ln(n^2 + 86)^2 \\ &> 384(n^2 + 86)^2 \ln(n^2 + 86)^2 \\ &= 6 \cdot 64(n^2 + 86)^2 \ln(n^2 + 86)^2 \\ &= 6 \cdot 4(n^2 + 86)^2 \cdot 16 \ln(n^2 + 86)^2 \\ &= 6(2(n^2 + 86))^2 (2 \ln(n^2 + 86) + 2 \ln(n^2 + 86))^2 \\ &> 6(n^2 + n + 85)^2 (\ln(n^2 + n + 85) + \ln \ln(n^2 + n + 85))^2 \\ &\geq 6\hat{p}_{n^2+n+85}^2 \end{aligned}$$

for all  $n \geq 1$  which shows the lemma. □

**Remark 1.** Although the estimation  $\hat{p}_{n^2+86}^3 > 6\hat{p}_{n^2+n+85}^2$  of Lemma 3 is not very accurate it is sufficient for our purposes. And in fact it can be shown that already  $\hat{p}_{n+8}^3 > 6\hat{p}_{2n+7}^2$  for all  $n \geq 1$  but a formal proof needs a more complicated technique.

**Theorem 2.** The SUBGROUP DISTANCE PROBLEM regarding the Cayley distance is NP-complete when the input group is cyclic.

*Proof.* We give a log-space reduction from X3HS. Let  $X$  be a finite set and  $\mathcal{B} \subseteq 2^X$  be a set of subsets of  $X$  all of size 3. W.l.o.g. assume that  $X = [1, n]$  and let  $\mathcal{B} = \{C_1, \dots, C_m\}$ . Let  $p_1 < \dots < p_n$  be the first  $n$  primes such that  $p_1^3 > 6p_n^2$ . Note that  $p_1, p_n \in O(n^2 \log n)$  by Lemma 3 and the prime number theorem. We define  $q_j = \prod_{i \in C_j} p_i$  for all  $j \in [1, m]$ . We will work with the group

$$G = \prod_{j=1}^m S_{q_j}^6$$

which naturally embeds into  $S_N$  for  $N = 6 \sum_{j=1}^m q_j$ . Moreover for  $j \in [1, m]$  and all  $d \in [1, 6]$  we define the number  $0 \leq s_{j,d} < q_j$  as the smallest positive integer satisfying the congruences in which we assume  $C_j = \{i_1, i_2, i_3\}$  with  $i_1 < i_2 < i_3$

$$\begin{array}{lll} s_{j,1} \equiv 1 \pmod{p_{i_1}} & s_{j,2} \equiv 0 \pmod{p_{i_1}} & s_{j,3} \equiv 0 \pmod{p_{i_1}} \\ s_{j,1} \equiv 0 \pmod{p_{i_2}} & s_{j,2} \equiv 1 \pmod{p_{i_2}} & s_{j,3} \equiv 0 \pmod{p_{i_2}} \\ s_{j,1} \equiv 0 \pmod{p_{i_3}} & s_{j,2} \equiv 0 \pmod{p_{i_3}} & s_{j,3} \equiv 1 \pmod{p_{i_3}} \end{array}$$

$$\begin{array}{lll} s_{j,4} \equiv 1 \pmod{p_{i_1}} & s_{j,5} \equiv 3 \pmod{p_{i_1}} & s_{j,6} \equiv 2 \pmod{p_{i_1}} \\ s_{j,4} \equiv 2 \pmod{p_{i_2}} & s_{j,5} \equiv 1 \pmod{p_{i_2}} & s_{j,6} \equiv 3 \pmod{p_{i_2}} \\ s_{j,4} \equiv 3 \pmod{p_{i_3}} & s_{j,5} \equiv 2 \pmod{p_{i_3}} & s_{j,6} \equiv 1 \pmod{p_{i_3}}. \end{array}$$

We define the input group elements  $\tau, \pi \in G$  as follows where  $j$  ranges over  $[1, m]$ :

$$\begin{aligned} \tau &= (\tau_1, \dots, \tau_m) \\ \tau_j &= ([q_j]^{s_{j,1}}, [q_j]^{s_{j,2}}, [q_j]^{s_{j,3}}, [q_j]^{s_{j,4}}, [q_j]^{s_{j,5}}, [q_j]^{s_{j,6}}) \\ \pi &= (\pi_1, \dots, \pi_m) \\ \pi_j &= ([q_j], [q_j], [q_j], [q_j], [q_j], [q_j]) \end{aligned}$$

and we define

$$k = N - \sum_{j=1}^m (q_j + 2 + \sum_{i \in C_j} p_i).$$

Now we will show there is  $x \in \mathbb{N}$  such that  $C(\tau, \pi^x) \leq k$  if and only if there is a subset  $X' \subseteq X$  such that  $|X' \cap C_j| = 1$  for all  $j \in [1, m]$ .

Suppose there is  $x \in \mathbb{N}$  such that  $C(\tau, \pi^x) \leq k$ . We define

$$X' = \{i \in [1, n] \mid x \equiv 1 \pmod{p_i}\}.$$

**Claim 1.** For all  $j \in [1, m]$  and all  $z \in \mathbb{Z}$  we have that  $\tau_j \pi_j^{-z}$  splits into exactly  $q_j + 2 + \sum_{i \in C_j} p_i$  cycles if there is  $a \in [1, 3]$  such that  $z \equiv s_{j,a} \pmod{q_j}$  or in strictly less than  $q_j + 2 + \sum_{i \in C_j} p_i$  cycles if  $z \not\equiv s_{j,a} \pmod{q_j}$  for all  $a \in [1, 3]$ .

Let  $j \in [1, m]$  and assume  $C_j = \{i_1, i_2, i_3\}$  with  $i_1 < i_2 < i_3$ . Note that for all  $d \in [1, 6]$  we have that  $[q_j]^{s_{j,d}-z}$  will split into  $\gcd(q_j, s_{j,d} - z)$  cycles of length  $\frac{q_j}{\gcd(q_j, s_{j,d} - z)}$  by Lemma 1.

Suppose there is an  $a \in [1, 3]$  such that  $z \equiv s_{j,a} \pmod{q_j}$ . Then clearly  $z \not\equiv s_{j,c} \pmod{q_j}$  for all  $c \in [1, 6] \setminus \{a\}$  since  $s_{j,e} \not\equiv s_{j,f} \pmod{q_j}$  for all  $e \neq f$ . Moreover we have for all  $b \in [1, 3] \setminus \{a\}$  and all  $c \in [1, 3]$

$$s_{j,b+3} - z \equiv s_{j,b+3} - s_{j,a} \not\equiv 0 \pmod{p_{i_c}}$$

and hence  $\llbracket q_j \rrbracket^{s_{j,b+3}-z}$  will not split into further cycles by Lemma 1. Moreover we have for all  $b \in [1, 3] \setminus \{a\}$

$$s_{j,b} - z \equiv s_{j,b} - s_{j,a} \begin{cases} \equiv 0 \pmod{p_{i_c}} & \text{if } c \in [1, 3] \setminus \{a, b\} \\ \not\equiv 0 \pmod{p_{i_c}} & \text{if } c \in \{a, b\} \end{cases}$$

and hence  $\llbracket q_j \rrbracket^{s_{j,b}-z}$  will split into  $p_{i_c}$  cycles by Lemma 1 with  $c \in [1, 3] \setminus \{a, b\}$ . Moreover we have

$$s_{j,a} - z \equiv s_{j,a} - s_{j,a} \equiv 0 \pmod{q_j}$$

and hence  $\llbracket q_j \rrbracket^{s_{j,a}-z}$  will split into  $q_j$  fixed points by Lemma 1. Finally we have

$$s_{j,a+3} - z \equiv s_{j,a+3} - s_{j,a} \equiv 1 - 1 \equiv 0 \pmod{p_{i_a}}$$

and for all  $b \in [1, 3] \setminus \{a\}$  we have

$$s_{j,a+3} - z \equiv s_{j,a+3} - s_{j,a} \equiv s_{j,a+3} - 0 \not\equiv 0 \pmod{p_{i_b}}$$

and hence  $\llbracket q_j \rrbracket^{s_{j,a+3}-z}$  will split into  $p_{i_a}$  cycles by Lemma 1. Thus the total number of cycles in  $\tau_j \pi_j^{-z}$  is

$$q_j + 2 + \sum_{i \in C_j} p_i.$$

Suppose  $z \not\equiv s_{j,a} \pmod{q_j}$  for all  $a \in [1, 3]$ . If also  $z \not\equiv s_{j,a} \pmod{q_j}$  for all  $a \in [4, 6]$  then  $\tau_j \pi_j^{-z}$  can only split into at most  $6p_n^2$  cycles which is strictly less than  $q_j + 2 + \sum_{i \in C_j} p_i$  since we already have

$$6p_n^2 < p_1^3 < q_j.$$

In the case  $z \equiv s_{j,a} \pmod{q_j}$  for some  $a \in [4, 6]$  we have  $z \not\equiv s_{j,c} \pmod{q_j}$  for all  $c \in [1, 6] \setminus \{a\}$  since  $s_{j,e} \not\equiv s_{j,f} \pmod{q_j}$  for all  $e \neq f$ . Moreover we have for all  $b \in [1, 3] \setminus \{a-3\}$  and all  $c \in [1, 3]$

$$s_{j,b} - z \equiv s_{j,b} - s_{j,a} \not\equiv 0 \pmod{p_{i_c}}$$

and hence  $\llbracket q_j \rrbracket^{s_{j,b}-z}$  will not split into further cycles by Lemma 1. Similarly we have for all  $b \in [4, 6] \setminus \{a\}$  and all  $c \in [1, 3]$

$$s_{j,b} - z \equiv s_{j,b} - s_{j,a} \not\equiv 0 \pmod{p_{i_c}}$$

and hence also in this case  $\llbracket q_j \rrbracket^{s_{j,b}-z}$  will not split into further cycles by Lemma 1. Moreover we have

$$s_{j,a} - z \equiv s_{j,a} - s_{j,a} \equiv 0 \pmod{q_j}$$

and hence  $\llbracket q_j \rrbracket^{s_{j,a}-z}$  will split into  $q_j$  fixed points by Lemma 1. Finally we have

$$s_{j,a-3} - z \equiv s_{j,a-3} - s_{j,a} \equiv 1 - 1 \equiv 0 \pmod{p_{i_{a-3}}}$$

and for all  $b \in [1, 3] \setminus \{a-3\}$  we have

$$s_{j,a-3} - z \equiv s_{j,a-3} - s_{j,a} \equiv 0 - s_{j,a} \not\equiv 0 \pmod{p_{i_b}}$$

and hence  $\llbracket q_j \rrbracket^{s_{j,a-3}-z}$  will split into  $p_{i_{a-3}}$  cycles by Lemma 1. This gives us a total of

$$4 + q_j + p_{i_{a-3}} < q_j + 2 + \sum_{i \in C_j} p_i$$

cycles. □



**Claim 2.** For all  $j \in [1, m]$  there is exactly one  $a \in [1, 3]$  such that  $x \equiv 1 \pmod{p_{i_a}}$  and  $x \equiv 0 \pmod{p_{i_b}}$  for all  $b \in [1, 3] \setminus \{a\}$  in which  $C_j = \{i_1, i_2, i_3\}$  with  $i_1 < i_2 < i_3$ .

By Claim 1 we find that summing up the largest possible amount of splitting cycles gives us

$$C(\tau, \pi^x) \geq N - \sum_{j=1}^m (q_j + 2 + \sum_{i \in C_j} p_i) = k$$

and hence  $C(\tau, \pi^x) = k$ . Thus for all  $j \in [1, m]$  the only possibility for  $x$  is to satisfy  $x \equiv s_{j,a} \pmod{q_j}$  for exactly one  $a \in [1, 3]$  which implies  $x \equiv 1 \pmod{p_{i_a}}$  and  $x \equiv 0 \pmod{p_{i_b}}$  for all  $b \in [1, 3] \setminus \{a\}$  as claimed.  $\square$

Now we will show  $|X' \cap C_j| = 1$  for all  $j \in [1, m]$ . Let  $C_j = \{i_1, i_2, i_3\}$  with  $i_1 < i_2 < i_3$ . Then by Claim 2 there is exactly one  $a \in [1, 3]$  such that  $x \equiv 1 \pmod{p_{i_a}}$  and  $x \equiv 0 \pmod{p_{i_b}}$  for all  $b \in [1, 3] \setminus \{a\}$ . Thus we have  $i_a \in X'$  and  $i_b \notin X'$  for all  $b \in [1, 3] \setminus \{a\}$  which finally gives us  $|X' \cap C_j| = 1$ .

Vice versa suppose there is a subset  $X' \subseteq X$  such that  $|X' \cap C_j| = 1$  for all  $j \in [1, m]$ . Then we define  $x$  as the smallest positive integer satisfying

$$x \equiv \begin{cases} 1 \pmod{p_i} & \text{if } i \in X' \\ 0 \pmod{p_i} & \text{if } i \notin X' \end{cases}$$

for all  $i \in [1, n]$ . Then we obtain for all  $j \in [1, m]$  and  $i \in [1, n]$

$$x \equiv \begin{cases} 1 \pmod{p_i} & \text{if } i \in X' \cap C_j \\ 0 \pmod{p_i} & \text{if } i \in C_j \setminus X' \end{cases}$$

from which it follows that  $x \equiv s_{j,a} \pmod{q_j}$  where  $a$  is the unique element in  $X' \cap C_j$ . Then  $\tau_j \pi_j^{-x}$  splits into exactly  $q_j + 2 + \sum_{i \in C_j} p_i$  cycles by Claim 1 for all  $j \in [1, m]$  which gives us

$$C(\tau, \pi^x) = N - \sum_{j=1}^m (q_j + 2 + \sum_{i \in C_j} p_i) = k.$$

This shows the theorem.  $\square$

### 3.3 $l_\infty$ Distance

#### 3.3.1 General Case

**Lemma 4.** Let  $p \geq 5$  be an odd prime and  $k \geq 2$  be a non-negative integer. Define

$$\delta = (1, k+1, 2k+1, \dots, \frac{p-1}{2}k+1, \frac{p-1}{2}k, \frac{p-3}{2}k, \frac{p-5}{2}k, \dots, k) \in S_{\frac{p-1}{2}k+1}$$

in which  $\delta$  is a cycle of length  $p$ . Then  $l_\infty((\delta, \text{id}), (\delta, \delta)^x) \leq k$  if and only if  $x \equiv 0, 1 \pmod{p}$ .

*Proof.* One direction is clear since the difference of two consecutive numbers of  $\delta$  is at most  $k$ . Now suppose  $l_\infty((\delta, \text{id}), (\delta, \delta)^x) \leq k$ . It suffices to show for all  $a \in [2, p-1]$  if  $x \equiv a \pmod{p}$  then  $l_\infty((\delta, \text{id}), (\delta, \delta)^x) > k$ . In the case  $2 \leq a \leq \frac{p-1}{2}$  we have  $(1, 1)^{(\delta, \text{id})} = (k+1, 1)$  and  $(1, 1)^{(\delta, \delta)^a} = (ak+1, ak+1)$ . Therefore the distance is at least  $ak+1-1 = ak \geq 2k$ . In the case  $\frac{p+1}{2} \leq a \leq p-2$  we have  $(1, 1)^{(\delta, \delta)^a} = (k(p-a), k(p-a))$ . In this case the distance is at least  $k(p-a)-1 \geq k(p-(p-2))-1 = 2k-1$ . In the case  $a = p-1$  we have  $(k+1, k+1)^{(\delta, \text{id})} = (2k+1, k+1)$  and  $(k+1, k+1)^{(\delta, \delta)^{p-1}} = (1, 1)$  which gives us a distance of  $2k+1-1 = 2k$ .  $\square$

**Theorem 3.** The SUBGROUP DISTANCE PROBLEM regarding the  $l_\infty$  distance is NP-complete when the input group is cyclic.

*Proof.* We give a log-space reduction from 3-SAT. Let  $X = \{x_1, \dots, x_n\}$  be a set of variables and let  $C = \{c_1, \dots, c_m\}$  be a set of clauses over  $X$  where  $c_j$  contains exactly 3 different literals for all  $j \in [1, m]$ . W.l.o.g. we can assume that no clause contains a positive and a negative literal regarding the same variable. For  $j = 1, \dots, m$  we define  $I_j \subseteq [1, n]$  as the set of all indices  $i$  such that  $c_j$  contains  $x_i$  or  $\bar{x}_i$ . Let  $p_1, \dots, p_n$  be the first  $n$  odd primes with  $p_1 \geq 5$ . Moreover let  $k = p_n^3$ ,  $q_j = \prod_{i \in I_j} p_i$  for  $j = 1, \dots, m$  and let  $N = \sum_{i=1}^n ((p_i - 1)k + 2) + m(k + 2)$ . We will work with the group  $G \leq S_N$  in which

$$G = \prod_{i=1}^n V_i \times \prod_{j=1}^m U_j$$

with  $V_i = S_{\frac{p_i-1}{2}k+1}^2$  and  $U_j = S_{k+2}$ . For  $i = 1, \dots, n$  we define the cycle  $\delta_i$  of length  $p_i$  by

$$\delta_i = (1, k+1, 2k+1, \dots, \frac{p_i-1}{2}k+1, \frac{p_i-1}{2}k, \frac{p_i-3}{2}k, \frac{p_i-5}{2}k, \dots, k).$$

Now we define the input group elements as

$$\begin{aligned} \tau &= (\zeta_1, \dots, \zeta_n, \mu_1, \dots, \mu_m) \\ \pi &= (\eta_1, \dots, \eta_m, \lambda_1, \dots, \lambda_m) \end{aligned}$$

with  $\zeta_i = (\delta_i, \text{id})$  and  $\eta_i = (\delta_i, \delta_i)$  for  $i \in [1, n]$ . To define  $\lambda_j$  and  $\mu_j$  for  $j \in [1, m]$  we first define some auxiliary permutations. Let  $j \in [1, m]$  and let  $d < e < f \in I_j$  be the indices of the variables that occur (negated or unnegated) in this clause. Then we define permutations that do not need to be constructed explicitly:

$$\begin{aligned} \alpha_j &= \prod_{r=1}^{p_f} \alpha_{j,r} & \beta_j &= \prod_{r=1}^{p_f} \beta_{j,r} & \gamma_j &= \prod_{s=1}^{p_e} \gamma_{j,s} \\ \alpha_{j,r} &= \prod_{s=1}^{p_e} \alpha_{j,r,s} & \beta_{j,r} &= \prod_{t=1}^{p_d} \beta_{j,r,t} & \gamma_{j,s} &= \prod_{t=1}^{p_d} \gamma_{j,s,t} \\ \alpha_{j,r,s} &= (\alpha_{j,r,s,1}, \dots, \alpha_{j,r,s,p_d}) & \beta_{j,r,t} &= (\beta_{j,r,t,1}, \dots, \beta_{j,r,t,p_e}) & \gamma_{j,s,t} &= (\gamma_{j,s,t,1}, \dots, \gamma_{j,s,t,p_f}) \end{aligned}$$

with  $\alpha_{j,r,s,t} \in [1, q_j]$  and  $\alpha_{j,r,s,t} \neq \alpha_{j,r',s',t'}$  for  $(r, s, t) \neq (r', s', t')$  and the constraint

$$\alpha_{j,r,s,t} = \beta_{j,r,t,s} = \gamma_{j,s,t,r} \quad (3)$$

for  $r \in [1, p_f]$ ,  $s \in [1, p_e]$  and  $t \in [1, p_d]$ . Note that  $\text{ord}(\alpha_j) = p_d$ ,  $\text{ord}(\beta_j) = p_e$  and  $\text{ord}(\gamma_j) = p_f$ . We fix the following 8 values:

$$\begin{aligned} \alpha_{j,1,1,2} &= 1 \\ \alpha_{j,1,1,1} &= 2 \\ \alpha_{j,1,p_e,2} &= 3 \\ \alpha_{j,p_f,1,2} &= 4 \\ \alpha_{j,p_f,p_e,2} &= 5 \\ \alpha_{j,p_f,1,1} &= 6 \\ \alpha_{j,1,p_e,1} &= 7 \\ \alpha_{j,p_f,p_e,1} &= 8. \end{aligned} \quad (4)$$

In the clause  $c_j$  there is exactly one truth assignment of the variables occurring in  $c_j$  that does not

satisfy this clause. Let  $\sigma_j$  denote this partial truth assignment. We define

$$w_j = \begin{cases} 1 & \text{if } \sigma_j(x_d) = 0, \sigma_j(x_e) = 0 \text{ and } \sigma_j(x_f) = 0 \\ 2 & \text{if } \sigma_j(x_d) = 1, \sigma_j(x_e) = 0 \text{ and } \sigma_j(x_f) = 0 \\ 3 & \text{if } \sigma_j(x_d) = 0, \sigma_j(x_e) = 1 \text{ and } \sigma_j(x_f) = 0 \\ 4 & \text{if } \sigma_j(x_d) = 0, \sigma_j(x_e) = 0 \text{ and } \sigma_j(x_f) = 1 \\ 5 & \text{if } \sigma_j(x_d) = 0, \sigma_j(x_e) = 1 \text{ and } \sigma_j(x_f) = 1 \\ 6 & \text{if } \sigma_j(x_d) = 1, \sigma_j(x_e) = 0 \text{ and } \sigma_j(x_f) = 1 \\ 7 & \text{if } \sigma_j(x_d) = 1, \sigma_j(x_e) = 1 \text{ and } \sigma_j(x_f) = 0 \\ 8 & \text{if } \sigma_j(x_d) = 1, \sigma_j(x_e) = 1 \text{ and } \sigma_j(x_f) = 1 \end{cases}$$

and finally we define  $\lambda_j = \alpha_j \beta_j \gamma_j(k+2, k)$  and  $\mu_j = (w_j, k+2)$ . Now we show that we can construct  $\alpha_j \beta_j \gamma_j$  in log-space.

**Claim 3.**  $\alpha_j, \beta_j, \gamma_j$  pairwise commute.

In the following we make use of Constraint (3) several times without explicit mentioning. We have

$$\begin{aligned} \alpha_{j,r,s,t}^{\beta_j \alpha_j} &= \beta_{j,r,t,s}^{\beta_j \alpha_j} = \begin{cases} \beta_{j,r,t,1}^{\alpha_j} & = \alpha_{j,r,1,t}^{\alpha_j} & \text{if } s = p_e \\ \beta_{j,r,t,s+1}^{\alpha_j} & = \alpha_{j,r,s+1,t}^{\alpha_j} & \text{if } 1 \leq s < p_e \end{cases} \\ &= \begin{cases} \alpha_{j,r,1,1} & = \beta_{j,r,1,1} & \text{if } t = p_d, s = p_e \\ \alpha_{j,r,1,t+1} & = \beta_{j,r,t+1,1} & \text{if } 1 \leq t < p_d, s = p_e \\ \alpha_{j,r,s+1,1} & = \beta_{j,r,1,s+1} & \text{if } t = p_d, 1 \leq s < p_e \\ \alpha_{j,r,s+1,t+1} & = \beta_{j,r,t+1,s+1} & \text{if } 1 \leq t < p_d, 1 \leq s < p_e \end{cases} \\ &= \begin{cases} \beta_{j,r,1,s}^{\beta_j} & = \alpha_{j,r,s,1}^{\beta_j} & \text{if } t = p_d \\ \beta_{j,r,t+1,s}^{\beta_j} & = \alpha_{j,r,s,t+1}^{\beta_j} & \text{if } 1 \leq t < p_d \end{cases} \\ &= \alpha_{j,r,s,t}^{\alpha_j \beta_j}. \end{aligned}$$

Analogously we obtain that  $\alpha_j, \gamma_j$  and  $\beta_j, \gamma_j$  commute.  $\square$

By Claim 3 we have  $\text{ord}(\alpha_j \beta_j \gamma_j) = p_d p_e p_f = q_j$  from which it follows that  $\alpha_j \beta_j \gamma_j$  is a cycle of length  $q_j$ . Now we give a mapping to construct  $\alpha_j \beta_j \gamma_j$  in log-space:

$$\begin{aligned} \alpha_{j,r,s,t}^{\alpha_j \beta_j \gamma_j} &= \begin{cases} \alpha_{j,r,s,1}^{\beta_j \gamma_j} & = \beta_{j,r,1,s}^{\beta_j \gamma_j} & \text{if } t = p_d \\ \alpha_{j,r,s,t+1}^{\beta_j \gamma_j} & = \beta_{j,r,t+1,s}^{\beta_j \gamma_j} & \text{if } 1 \leq t < p_d \end{cases} \\ &= \begin{cases} \beta_{j,r,1,1}^{\gamma_j} & = \gamma_{j,1,1,r}^{\gamma_j} & \text{if } t = p_d, s = p_e \\ \beta_{j,r,1,s+1}^{\gamma_j} & = \gamma_{j,s+1,1,r}^{\gamma_j} & \text{if } t = p_d, 1 \leq s < p_e \\ \beta_{j,r,t+1,1}^{\gamma_j} & = \gamma_{j,1,t+1,r}^{\gamma_j} & \text{if } 1 \leq t < p_d, s = p_e \\ \beta_{j,r,t+1,s+1}^{\gamma_j} & = \gamma_{j,s+1,t+1,r}^{\gamma_j} & \text{if } 1 \leq t < p_d, 1 \leq s < p_e \end{cases} \\ &= \begin{cases} \gamma_{j,1,1,1} & = \alpha_{j,1,1,1} & \text{if } t = p_d, s = p_e, r = p_f \\ \gamma_{j,1,1,r+1} & = \alpha_{j,r+1,1,1} & \text{if } t = p_d, s = p_e, 1 \leq r < p_f \\ \gamma_{j,s+1,1,1} & = \alpha_{j,1,s+1,1} & \text{if } t = p_d, 1 \leq s < p_e, r = p_f \\ \gamma_{j,s+1,1,r+1} & = \alpha_{j,r+1,s+1,1} & \text{if } t = p_d, 1 \leq s < p_e, 1 \leq r < p_f \\ \gamma_{j,1,t+1,1} & = \alpha_{j,1,t+1,1} & \text{if } 1 \leq t < p_d, s = p_e, r = p_f \\ \gamma_{j,1,t+1,r+1} & = \alpha_{j,r+1,t+1,1} & \text{if } 1 \leq t < p_d, s = p_e, 1 \leq r < p_f \\ \gamma_{j,s+1,t+1,1} & = \alpha_{j,1,s+1,t+1} & \text{if } 1 \leq t < p_d, 1 \leq s < p_e, r = p_f \\ \gamma_{j,s+1,t+1,r+1} & = \alpha_{j,r+1,s+1,t+1} & \text{if } 1 \leq t < p_d, 1 \leq s < p_e, 1 \leq r < p_f. \end{cases} \end{aligned}$$

Because  $\alpha_j \beta_j \gamma_j$  is a cycle we can start with an arbitrary triple  $(r, s, t)$  and write in the output the numbers from 9 up to  $q_j$ . When we obtain a triple where we already assigned a fixed value (see (4)) we write in the output that fixed value instead. By this procedure we clearly can write  $\alpha_j \beta_j \gamma_j$  in the output in log-space. Moreover  $\alpha_j \beta_j \gamma_j$  evaluates as follows

$$\begin{aligned}
1^{\alpha_j^0 \beta_j^0 \gamma_j^0} &= 1 \\
2^{\alpha_j^1 \beta_j^0 \gamma_j^0} &= 1 \\
3^{\alpha_j^0 \beta_j^1 \gamma_j^0} &= 1 \\
4^{\alpha_j^0 \beta_j^0 \gamma_j^1} &= 1 \\
5^{\alpha_j^0 \beta_j^1 \gamma_j^1} &= 1 \\
6^{\alpha_j^1 \beta_j^0 \gamma_j^1} &= 1 \\
7^{\alpha_j^1 \beta_j^1 \gamma_j^0} &= 1 \\
8^{\alpha_j^1 \beta_j^1 \gamma_j^1} &= 1
\end{aligned} \tag{5}$$

since

$$\begin{aligned}
1^{\alpha_j^0 \beta_j^0 \gamma_j^0} &= 1^{\text{id}} = 1 \\
2^{\alpha_j^1 \beta_j^0 \gamma_j^0} &= 2^{\alpha_j} = \alpha_{j,1,1,1}^{\alpha_j} = \alpha_{j,1,1,2} = 1 \\
3^{\alpha_j^0 \beta_j^1 \gamma_j^0} &= 3^{\beta_j} = \alpha_{j,1,p_e,2}^{\beta_j} = \beta_{j,1,2,p_e}^{\beta_j} = \beta_{j,1,2,1} = \alpha_{j,1,1,2} = 1 \\
4^{\alpha_j^0 \beta_j^0 \gamma_j^1} &= 4^{\gamma_j} = \alpha_{j,p_f,1,2}^{\gamma_j} = \gamma_{j,1,2,p_f}^{\gamma_j} = \gamma_{j,1,2,1} = \alpha_{j,1,1,2} = 1 \\
5^{\alpha_j^0 \beta_j^1 \gamma_j^1} &= 5^{\beta_j \gamma_j} = \alpha_{j,p_f,p_e,2}^{\beta_j \gamma_j} = \beta_{j,p_f,2,p_e}^{\beta_j \gamma_j} = \beta_{j,p_f,2,1}^{\gamma_j} = \gamma_{j,1,2,p_f}^{\gamma_j} = \gamma_{j,1,2,1} = \alpha_{j,1,1,2} = 1 \\
6^{\alpha_j^1 \beta_j^0 \gamma_j^1} &= 6^{\alpha_j \gamma_j} = \alpha_{j,p_f,1,1}^{\alpha_j \gamma_j} = \alpha_{j,1,2,p_f}^{\gamma_j} = \gamma_{j,1,2,p_f}^{\gamma_j} = \gamma_{j,1,2,1} = \alpha_{j,1,1,2} = 1 \\
7^{\alpha_j^1 \beta_j^1 \gamma_j^0} &= 7^{\alpha_j \beta_j} = \alpha_{j,1,p_e,1}^{\alpha_j \beta_j} = \alpha_{j,1,p_e,2}^{\beta_j} = \beta_{j,1,2,p_e}^{\beta_j} = \beta_{j,1,2,1} = \alpha_{j,1,1,2} = 1 \\
8^{\alpha_j^1 \beta_j^1 \gamma_j^1} &= 8^{\alpha_j \beta_j \gamma_j} = \alpha_{j,p_f,p_e,1}^{\alpha_j \beta_j \gamma_j} = \alpha_{j,p_f,p_e,2}^{\beta_j \gamma_j} = \beta_{j,p_f,2,p_e}^{\beta_j \gamma_j} = \beta_{j,p_f,2,1}^{\gamma_j} = \gamma_{j,1,2,p_f}^{\gamma_j} = \gamma_{j,1,2,1} = \alpha_{j,1,1,2} = 1.
\end{aligned}$$

Now we will show there is a  $z \in \mathbb{N}$  such that  $l_\infty(\tau, \pi^z) \leq k$  if and only if  $C$  is satisfiable. Suppose there is such a  $z$ . Consider the computations in  $V_i$ . By Lemma 4 we have  $l_\infty(\zeta_i, \eta_i^z) \leq k$  if and only if  $z \equiv 0, 1 \pmod{p_i}$ . Now we consider the computations in  $U_j$ . We have  $\lambda_j^z = (\alpha_j \beta_j \gamma_j)^z (k+2, k)^z$  and  $\mu_j = (w_j, k+2)$ . By Claim 3 we have that  $\alpha_j, \beta_j, \gamma_j$  pairwise commute which gives us  $(\alpha_j \beta_j \gamma_j)^z = \alpha_j^z \beta_j^z \gamma_j^z$ . Now let  $z_1, z_2, z_3 \in \{0, 1\}$  be such that  $z_1 \equiv z \pmod{p_d}, z_2 \equiv z \pmod{p_e}$  and  $z_3 \equiv z \pmod{p_f}$  in which  $d < e < f \in I_j$ . Such numbers exist since we have  $z \equiv 0, 1 \pmod{p_i}$  for all  $i \in [1, n]$ . Then we have  $\alpha_j^z \beta_j^z \gamma_j^z = \alpha_j^{z_1} \beta_j^{z_2} \gamma_j^{z_3}$ . By (5) there is a  $w \in [1, 8]$  such that  $w^{\alpha_j^{z_1} \beta_j^{z_2} \gamma_j^{z_3}} = 1$ . If  $w = w_j$  we get by  $w^{\mu_j} = w_j^{\mu_j} = k+2$  a distance of  $k+1$  contradicting  $l_\infty(\tau, \pi^z) \leq k$ . Therefore we have  $w \neq w_j$ . Since however  $w_j$  is associated with a truth assignment that does not satisfy  $c_j$  we obtain that  $z$  encodes a truth assignment that satisfies  $c_j$  for all  $j \in [1, m]$ . Therefore we obtain by

$$\sigma(x_i) = \begin{cases} 1 & \text{if } z \equiv 1 \pmod{p_i} \\ 0 & \text{if } z \equiv 0 \pmod{p_i} \end{cases}$$

a satisfying truth assignment  $\sigma$  for  $C$ .

Vice versa suppose  $C$  is satisfiable and let  $\sigma$  be a satisfying truth assignment. Let  $z \in \mathbb{N}$  be the smallest non-negative integer satisfying

$$\begin{aligned}
z &\equiv 1 \pmod{2} \\
z &\equiv \begin{cases} 1 \pmod{p_i} & \text{if } \sigma(x_i) = 1 \\ 0 \pmod{p_i} & \text{if } \sigma(x_i) = 0. \end{cases}
\end{aligned}$$

Then clearly  $l_\infty(\zeta_i, \eta_i^z) \leq k$  by Lemma 4. Now consider  $\lambda_j^z$  and  $\mu_j$ . We have  $(k+2)^{\lambda_j^z} = k$  and  $(k+2)^{\mu_j} = w_j$  giving us the distance  $k - w_j < k$ . Moreover we have  $k^{\lambda_j^z} = k+2$  and  $k^{\mu_j} = k$  with the distance  $k+2 - k = 2$ . Now consider  $(\alpha_j \beta_j \gamma_j)^z = \alpha_j^z \beta_j^z \gamma_j^z = \alpha_j^{z_1} \beta_j^{z_2} \gamma_j^{z_3}$  for some  $z_1, z_2, z_3 \in \{0, 1\}$ . By (5) there is a  $w \in [1, 8]$  such that  $w^{\alpha_j^{z_1} \beta_j^{z_2} \gamma_j^{z_3}} = 1$ . Then we have  $w \neq w_j$  because  $\sigma$  is a satisfying truth assignment that satisfies  $c_j$ . Therefore we have  $w_j^{\alpha_j^{z_1} \beta_j^{z_2} \gamma_j^{z_3}} \geq 2$  and  $w_j^{\mu_j} = k+2$  giving us a distance of  $k+2 - w_j^{\alpha_j^{z_1} \beta_j^{z_2} \gamma_j^{z_3}} \leq k$ . Moreover for all  $y \in [1, q_j] \setminus \{w_j\}$  we have  $y^{\alpha_j^{z_1} \beta_j^{z_2} \gamma_j^{z_3}} \in [1, q_j]$  and  $y^{\mu_j} = y$  giving us a distance of at most  $q_j - 1 < k$ . Finally  $\{k+1\} \cup [q_j+1, k-1]$  are fixed-points in both  $\lambda_j$  and  $\mu_j$ . Therefore we obtain  $l_\infty(\mu_j, \lambda_j^z) \leq k$  and thus  $l_\infty(\tau, \pi^z) \leq k$ .  $\square$

### 3.3.2 Fixed $k$

**Lemma 5.** *Let  $\alpha, \beta \in S_n$  and  $\alpha = \alpha_1 \cdots \alpha_d$  be the disjoint cycle decomposition of  $\alpha$  and let  $a_i$  denote the length of  $\alpha_i$ . Let  $X = \{x \in \mathbb{Z} \mid l_\infty(\beta, \alpha^x) \leq 1\}$ . Then for all  $i \in [1, d]$  there are at most two numbers  $0 \leq y_1, y_2 < a_i$  such that for all  $x \in X$  the following holds:  $x \equiv y_1 \pmod{a_i}$  or  $x \equiv y_2 \pmod{a_i}$ .*

*Proof.* Let  $i \in [1, d]$  and suppose  $\alpha_i = (i_1, \dots, i_{a_i})$  where we assume w.l.o.g.  $i_1 < i_j$  for all  $j \in [2, a_i]$ .

Case 1: There exists  $1 \leq h \leq a_i$  such that  $i_h^\beta = i_1$ . Then for all  $x \in X$  we have  $i_h^{\alpha_i^x} \in \{i_1, i_1+1\}$  which can hold only for at most two different values in  $[0, a_i - 1]$ .

Case 2: For all  $1 \leq h \leq a_i$  we have  $i_h^\beta \neq i_1$ . Then there is a value  $e \in [1, n] \setminus \{i_1, \dots, i_{a_i}\}$  such that  $e^\beta = i_1$ . Hence there is also a value  $g \in [1, a_i]$  such that  $i_g^\beta = f \notin \{i_1, \dots, i_{a_i}\}$ . Then for all  $x \in X$  we have  $i_g^{\alpha_i^x} \in \{f-1, f+1\} \cap \{i_1, \dots, i_{a_i}\}$  which can hold only for at most two different values in  $[0, a_i - 1]$ .  $\square$

**Theorem 4.** *Let  $\alpha, \beta \in S_n$  be given in standard representation. Then it can be decided in NL whether there is a number  $z \in \mathbb{N}$  such that  $l_\infty(\beta, \alpha^z) \leq 1$ .*

*Proof.* We will give a log-space reduction to 2-SAT which is NL-complete [16] and use the following notations:

1.  $x_1 \Rightarrow x_2$  for  $x_1 \vee \neg x_2$
2.  $x_1 \text{ xor } x_2$  for  $(x_1 \vee x_2) \wedge (\neg x_1 \vee \neg x_2)$ .

In the first step we check in log-space for every fixed point  $i^\alpha = i$  whether  $i \in \{i^\beta - 1, i^\beta, i^\beta + 1\}$ . In the following it therefore suffices to consider cycles of length at least 2. Since  $\alpha$  is given in standard representation we can compute in log-space the cycle representation of  $\alpha$  [7]. Let  $\alpha = \alpha_1 \cdots \alpha_m$  be the disjoint cycle decomposition (without fixed points) of  $\alpha$  and let  $a_i \geq 2$  denote the length of  $\alpha_i$ . For  $i = 1, \dots, m$  we define the ordered set

$$X_i = \{v \mid 0 \leq v < a_i, \forall j \in \text{act}(\alpha_i) : j^{\alpha_i^v} \in \{j^\beta - 1, j^\beta, j^\beta + 1\}\}$$

and  $X_{m+1} = \emptyset$ . By Lemma 5 we have  $|X_i| \leq 2$ . When we write  $X_i = \{v_1, v_2\}$  we mean  $v_1 < v_2$ . If there is an  $i \in [1, m]$  with  $|X_i| = 0$  there clearly is no such  $z$ . Therefore we assume in the following  $1 \leq |X_i| \leq 2$  for all  $i \in [1, m]$ . When we speak of the  $p$ -adic valuation of some  $a_i$  we always mean the case that  $\nu_p(a_i) \geq 1$ . For every prime power  $p^d \leq n$  with  $d \geq 1$  (there clearly are at most  $n$  such prime powers) we define  $i_{p,d} = \min(\{j \mid d = \nu_p(a_j)\} \cup \{m+1\})$  and define the ordered set

$$Y_{p,d} = \{u \in [0, p^d - 1] \mid \exists v \in X_{i_{p,d}} : v \equiv u \pmod{p^d}\}.$$

Note that we have  $0 \leq |Y_{p,d}| \leq 2$ . If  $|Y_{p,d}| = 0$  then there is no  $i \in [1, m]$  with  $d = \nu_p(a_i)$ . We use  $kY_{p,d}$  to denote the  $k^{\text{th}}$  element of  $Y_{p,d}$ . Now we introduce  $|Y_{p,d}| + 1$  variables  $x_{p,d,0}, \dots, x_{p,d,|Y_{p,d}|}$

for all  $p^d \leq n$  and define a 2-SAT formula by the following:

$$F_0 = \bigwedge_{p^d \leq n} \neg x_{p,d,0} \wedge \bigwedge_{\substack{p^d \leq n, \\ |Y_{p,d}|=2}} (x_{p,d,1} \text{ XOR } x_{p,d,2}) \wedge \bigwedge_{\substack{p^d \leq n, \\ |Y_{p,d}|=1}} x_{p,d,1}.$$

Moreover for every prime  $p \leq n$  we define

$$F'_p = \bigwedge_{p^d \leq n} \bigwedge_{\substack{p^e \leq n, \\ d \leq e}} \bigwedge_{k_1=1}^{|Y_{p,d}|} \bigwedge_{k_2=1}^{|Y_{p,e}|} \varphi(p, d, e, k_1, k_2)$$

in which we have

$$\varphi(p, d, e, k_1, k_2) = \begin{cases} x_{p,e,k_2} \Rightarrow x_{p,d,k_1} & \text{if } k_1 Y_{p,d} \equiv k_2 Y_{p,e} \pmod{p^d} \\ x_{p,e,k_2} \Rightarrow \neg x_{p,d,k_1} & \text{if } k_1 Y_{p,d} \not\equiv k_2 Y_{p,e} \pmod{p^d}. \end{cases}$$

Now for all  $i \in [1, m]$  and every prime power  $p^d \mid a_i$  with  $d = \nu_p(a_i)$  we define literals by the following: if  $X_i = \{v\}$  we define

$$\tilde{x}_{i,p,d,0} = \begin{cases} x_{p,d,1} & \text{if } |Y_{p,d}| = 1, 1Y_{p,d} \equiv v \pmod{p^d} \\ x_{p,d,1} & \text{if } |Y_{p,d}| = 2, 1Y_{p,d} \equiv v \pmod{p^d} \\ x_{p,d,2} & \text{if } |Y_{p,d}| = 2, 2Y_{p,d} \equiv v \pmod{p^d} \\ x_{p,d,0} & \text{otherwise} \end{cases}$$

and if  $X_i = \{v_1, v_2\}$  we define in the case  $v_1 \not\equiv v_2 \pmod{p^d}$

$$\tilde{x}_{i,p,d,1} = \begin{cases} x_{p,d,1} & \text{if } |Y_{p,d}| = 1, 1Y_{p,d} \equiv v_1 \pmod{p^d} \\ x_{p,d,1} & \text{if } |Y_{p,d}| = 2, 1Y_{p,d} \equiv v_1 \pmod{p^d} \\ x_{p,d,2} & \text{if } |Y_{p,d}| = 2, 2Y_{p,d} \equiv v_1 \pmod{p^d} \\ x_{p,d,0} & \text{otherwise} \end{cases}$$

and

$$\tilde{x}_{i,p,d,2} = \begin{cases} x_{p,d,1} & \text{if } |Y_{p,d}| = 1, 1Y_{p,d} \equiv v_2 \pmod{p^d} \\ x_{p,d,1} & \text{if } |Y_{p,d}| = 2, 1Y_{p,d} \equiv v_2 \pmod{p^d} \\ x_{p,d,2} & \text{if } |Y_{p,d}| = 2, 2Y_{p,d} \equiv v_2 \pmod{p^d} \\ x_{p,d,0} & \text{otherwise.} \end{cases}$$

If  $v_1 \equiv v_2 \pmod{p^d}$  we define

$$\tilde{x}_{i,p,d,0} = \begin{cases} x_{p,d,1} & \text{if } |Y_{p,d}| = 1, 1Y_{p,d} \equiv v_1 \pmod{p^d} \\ x_{p,d,1} & \text{if } |Y_{p,d}| = 2, 1Y_{p,d} \equiv v_1 \pmod{p^d} \\ x_{p,d,2} & \text{if } |Y_{p,d}| = 2, 2Y_{p,d} \equiv v_1 \pmod{p^d} \\ x_{p,d,0} & \text{otherwise} \end{cases}$$

and define the formula

$$F_i = \begin{cases} F_{i,1} & \text{if } |X_i| = 1 \\ F_{i,2} \wedge F_{i,3} & \text{if } |X_i| = 2 \end{cases}$$

in which

$$F_{i,1} = \bigwedge_{\substack{p^d \mid a_i \\ \text{with } d=\nu_p(a_i)}} \tilde{x}_{i,p,d,0}$$

and

$$F_{i,2} = \bigwedge_{\substack{p^d | a_i \\ \text{with } d=\nu_p(a_i), \\ v_1 \not\equiv v_2 \pmod{p^d}}} \bigwedge_{\substack{q^e | a_i \\ \text{with } e=\nu_q(a_i), \\ v_1 \not\equiv v_2 \pmod{q^e}}} (\tilde{x}_{i,p,d,1} \text{ XOR } \tilde{x}_{i,q,e,2})$$

and

$$F_{i,3} = \bigwedge_{\substack{p^d | a_i \\ \text{with } d=\nu_p(a_i), \\ v_1 \equiv v_2 \pmod{p^d}}} \tilde{x}_{i,p,d,0}$$

for all  $i \in [1, m]$ . Finally we define our 2-SAT formula  $F$  by

$$F = F_0 \wedge \bigwedge_{i=1}^m F_i \wedge \bigwedge_{p \leq n} F'_p.$$

Now we will show there is a number  $z \in \mathbb{N}$  such that  $l_\infty(\beta, \alpha^z) \leq 1$  if and only if  $F$  is satisfiable.

Suppose there is a number  $z \in \mathbb{N}$  such that  $l_\infty(\beta, \alpha^z) \leq 1$ . For all  $i \in [1, m]$  let  $0 \leq z_i < a_i$  be the smallest positive integer such that  $z_i \equiv z \pmod{a_i}$ . Then we have

$$\alpha^z = \prod_{i=1}^m \alpha_i^{z_i} = \prod_{i=1}^m \alpha_i^{z_i}.$$

Then clearly  $z_i \in X_i$  for all  $i \in [1, m]$ . Now we define a truth assignment  $\sigma$  by the following: for every prime power  $p^d \leq n$  with  $d \geq 1$  we define

$$\sigma(x_{p,d,0}) = 0.$$

Moreover for all prime powers  $p^d$  with  $1 \leq |Y_{p,d}| \leq 2$  we define

$$\sigma(x_{p,d,1}) = 1$$

if  $|Y_{p,d}| = 1$ . In the case  $|Y_{p,d}| = 2$  note that we have  $z_{i_{p,d}} \in X_{i_{p,d}}$  and hence we either have  $1Y_{p,d} \equiv z_{i_{p,d}} \pmod{p^d}$  or  $2Y_{p,d} \equiv z_{i_{p,d}} \pmod{p^d}$ . We define

$$\sigma(x_{p,d,1}) = \begin{cases} 1 & \text{if } 1Y_{p,d} \equiv z_{i_{p,d}} \pmod{p^d} \\ 0 & \text{if } 1Y_{p,d} \not\equiv z_{i_{p,d}} \pmod{p^d} \end{cases}$$

and

$$\sigma(x_{p,d,2}) = \begin{cases} 0 & \text{if } 2Y_{p,d} \not\equiv z_{i_{p,d}} \pmod{p^d} \\ 1 & \text{if } 2Y_{p,d} \equiv z_{i_{p,d}} \pmod{p^d}. \end{cases}$$

Note that we have  $\sigma(x_{p,d,1}) = 1$  if and only if  $\sigma(x_{p,d,2}) = 0$ . Now we will show that  $\sigma$  satisfies  $F$ .

**Claim 4.**  $\sigma$  satisfies  $F_0$ .

We have  $\sigma(x_{p,d,0}) = 0$  by definition. Moreover in the case  $|Y_{p,d}| = 1$  we have  $\sigma(x_{p,d,1}) = 1$  and if  $|Y_{p,d}| = 2$  then we have  $\sigma(x_{p,d,1}) = 1$  if and only if  $\sigma(x_{p,d,2}) = 0$ . Thus the subformula  $F_0$  clearly evaluates to true.  $\square$

**Claim 5.**  $\sigma$  satisfies  $F'_p$  for all primes  $p \leq n$ .

It suffices to consider the case  $\sigma(x_{p,e,k_2}) = 1$ . Since  $\sigma(x_{p,e,k_2}) = 1$  we have  $k_2 Y_{p,e} \equiv z_{i_{p,e}} \pmod{p^e}$ . If  $|Y_{p,e}| = 1$  this follows from the definition of  $Y_{p,e}$  and if  $|Y_{p,e}| = 2$  this follows from the definition of  $\sigma$ . In the case  $\varphi(p, d, e, k_1, k_2) = x_{p,e,k_2} \Rightarrow x_{p,d,k_1}$  we have  $\sigma(x_{p,d,k_1}) = 1$  if  $|Y_{p,d}| = 1$  by definition of  $\sigma$  and if  $|Y_{p,d}| = 2$  we have

$$z_{i_{p,d}} \equiv z_{i_{p,e}} \equiv k_2 Y_{p,e} \equiv k_1 Y_{p,d} \pmod{p^d}$$

and hence  $\sigma(x_{p,d,k_1}) = 1$  and  $\varphi(p, d, e, k_1, k_2)$  evaluates to true. Now we consider the case  $\varphi(p, d, e, k_1, k_2) = x_{p,e,k_2} \Rightarrow \neg x_{p,d,k_1}$ . Suppose  $|Y_{p,d}| = 1$ . Then we have  $\sigma(x_{p,d,k_1}) = 1$  by definition. Moreover since  $z_{i_{p,d}} \in X_{i_{p,d}}$  we have  $k_1 Y_{p,d} \equiv z_{i_{p,d}} \pmod{p^d}$  by definition of  $Y_{p,d}$ . Then we obtain on the one hand

$$k_2 Y_{p,e} \equiv z_{i_{p,e}} \equiv z_{i_{p,d}} \equiv k_1 Y_{p,d} \pmod{p^d}$$

and on the other hand

$$k_2 Y_{p,e} \not\equiv k_1 Y_{p,d} \pmod{p^d}$$

by definition of  $\varphi(p, d, e, k_1, k_2)$  which is a contradiction. Hence  $|Y_{p,d}| = 2$  and we finally obtain

$$z_{i_{p,d}} \equiv z_{i_{p,e}} \equiv k_2 Y_{p,e} \not\equiv k_1 Y_{p,d} \pmod{p^d}$$

which gives us  $\sigma(x_{p,d,k_1}) = 0$  and  $\varphi(p, d, e, k_1, k_2)$  evaluates to true. Note that  $z_{i_{p,e}} \equiv z_{i_{p,d}} \pmod{p^d}$  because  $d \leq e$ . Thus  $F'_p$  evaluates to true.  $\square$

**Claim 6.**  $\sigma$  satisfies  $F_i$  for all  $i \in [1, m]$ .

In the case  $X_i = \{v\}$  we have  $F_i = F_{i,1}$ . Since  $z_i \in X_i$  we have  $v = z_i$ . Moreover we have  $z_{i_{p,d}} \equiv z_i \pmod{p^d}$  for all prime powers  $p^d \mid a_i$  with  $d = \nu_p(a_i)$ . Hence there is a  $k \in [1, 2]$  such that  $v \equiv z_i \equiv z_{i_{p,d}} \equiv k Y_{p,d} \pmod{p^d}$ . From this it follows now that  $\tilde{x}_{i,p,d,0} = x_{p,d,k}$ . If  $|Y_{p,d}| = 1$  then  $k = 1$  and  $\sigma(x_{p,d,1}) = 1$  by definition and if  $|Y_{p,d}| = 2$  then  $z_{i_{p,d}} \equiv k Y_{p,d} \pmod{p^d}$  and hence  $\sigma(x_{p,d,k}) = 1$  by definition which satisfies  $F_{i,1}$ .

In the case  $X_i = \{v_1, v_2\}$  we have  $F_i = F_{i,2} \wedge F_{i,3}$ . Let  $p^d \mid a_i$  be such that  $d = \nu_p(a_i)$  and  $v_1 \equiv v_2 \pmod{p^d}$ . Since  $z_i \in X_i$  we have  $z_i \equiv v_1 \equiv v_2 \pmod{p^d}$ . Moreover we have  $z_{i_{p,d}} \equiv z_i \pmod{p^d}$  for all prime powers  $p^d \mid a_i$  with  $d = \nu_p(a_i)$ . Hence there is a  $k \in [1, 2]$  such that  $v_1 \equiv v_2 \equiv z_i \equiv z_{i_{p,d}} \equiv k Y_{p,d} \pmod{p^d}$ . From this it follows now that  $\tilde{x}_{i,p,d,0} = x_{p,d,k}$ . If  $|Y_{p,d}| = 1$  then  $k = 1$  and  $\sigma(x_{p,d,1}) = 1$  by definition and if  $|Y_{p,d}| = 2$  then  $z_{i_{p,d}} \equiv k Y_{p,d} \pmod{p^d}$  and hence  $\sigma(x_{p,d,k}) = 1$  by definition which satisfies  $F_{i,3}$ . Now let  $p^d \mid a_i$  be such that  $d = \nu_p(a_i)$  and  $v_1 \not\equiv v_2 \pmod{p^d}$  and let  $q^e \mid a_i$  be such that  $e = \nu_q(a_i)$  and  $v_1 \not\equiv v_2 \pmod{q^e}$ . Since  $z_i \in X_i$  there is an  $l \in [1, 2]$  such that  $z_i = v_l$ . Moreover we have  $z_{i_{p,d}} \equiv z_i \pmod{p^d}$  for all prime powers  $p^d \mid a_i$  with  $d = \nu_p(a_i)$ . Hence there is a  $k_1 \in [1, 2]$  such that  $v_l \equiv z_i \equiv z_{i_{p,d}} \equiv k_1 Y_{p,d} \pmod{p^d}$ . Furthermore we have  $z_{i_{q,e}} \equiv z_i \pmod{q^e}$  for all prime powers  $q^e \mid a_i$  with  $e = \nu_q(a_i)$ . Hence there is a  $k_2 \in [1, 2]$  such that  $v_l \equiv z_i \equiv z_{i_{q,e}} \equiv k_2 Y_{q,e} \pmod{q^e}$ . We then have

$$\tilde{x}_{i,p,d,1} = \begin{cases} x_{p,d,k_1} & \text{if } l = 1 \\ x_{p,d,3-k_1} & \text{if } l = 2, |Y_{p,d}| = 2, v_{3-l} \equiv (3 - k_1) Y_{p,d} \pmod{p^d} \\ x_{p,d,0} & \text{otherwise} \end{cases}$$

and

$$\tilde{x}_{i,q,e,2} = \begin{cases} x_{q,e,k_2} & \text{if } l = 2 \\ x_{q,e,3-k_2} & \text{if } l = 1, |Y_{q,e}| = 2, v_{3-l} \equiv (3 - k_2) Y_{q,e} \pmod{q^e} \\ x_{q,e,0} & \text{otherwise.} \end{cases}$$

By this we obtain one of the following four cases

$$\tilde{x}_{i,p,d,1} \text{ XOR } \tilde{x}_{i,q,e,2} = \begin{cases} x_{p,d,k_1} \text{ XOR } x_{q,e,0} \\ x_{p,d,k_1} \text{ XOR } x_{q,e,3-k_2} \\ x_{p,d,0} \text{ XOR } x_{q,e,k_2} \\ x_{p,d,3-k_1} \text{ XOR } x_{q,e,k_2} \end{cases}$$

We have  $\sigma(x_{q,e,0}) = 0$  and  $\sigma(x_{p,d,k_1}) = 1$  if  $|Y_{p,d}| = 1$  and if  $|Y_{p,d}| = 2$  we have  $\sigma(x_{p,d,k_1}) = 1$  because  $z_{i_{p,d}} \equiv k_1 Y_{p,d} \pmod{p^d}$ . Thus  $x_{p,d,k_1} \text{ XOR } x_{q,e,0}$  is satisfied. Since we have  $z_{i_{q,e}} \equiv k_2 Y_{q,e} \pmod{q^e}$  we clearly have  $z_{i_{q,e}} \not\equiv (3 - k_2) Y_{q,e} \pmod{q^e}$  and thus  $\sigma(x_{q,e,3-k_2}) = 0$  and  $x_{p,d,k_1} \text{ XOR } x_{q,e,3-k_2}$  is



satisfied. Moreover we have  $\sigma(x_{p,d,0}) = 0$  and  $\sigma(x_{q,e,k_2}) = 1$  if  $|Y_{q,e}| = 1$  and if  $|Y_{q,e}| = 2$  we have  $\sigma(x_{q,e,k_2}) = 1$  because  $z_{i_{q,e}} \equiv k_2 Y_{q,e} \pmod{q^e}$ . Thus  $x_{p,d,0} \text{ xor } x_{q,e,k_2}$  is satisfied. Since we have  $z_{i_{p,d}} \equiv k_1 Y_{p,d} \pmod{p^d}$  we clearly have  $z_{i_{p,d}} \not\equiv (3 - k_1) Y_{p,d} \pmod{p^d}$  and thus  $\sigma(x_{p,d,3-k_1}) = 0$  and  $x_{p,d,3-k_1} \text{ xor } x_{q,e,k_2}$  is satisfied. We finally obtain that  $F_i$  is satisfied.  $\square$

By Claim 4,5 and 6 it follows now that  $F$  is satisfied by  $\sigma$ .

Vice versa suppose  $F$  is satisfiable and let  $\sigma$  be a satisfying truth assignment. Then for every prime power  $p^d$  with  $|Y_{p,d}| > 0$  we define numbers  $b_{p,d}$  by the following

$$b_{p,d} = \begin{cases} 1Y_{p,d} & \text{if } |Y_{p,d}| = 1 \\ 1Y_{p,d} & \text{if } |Y_{p,d}| = 2, \sigma(x_{p,d,1}) = 1 \\ 2Y_{p,d} & \text{if } |Y_{p,d}| = 2, \sigma(x_{p,d,2}) = 1. \end{cases}$$

Note that by the subformula  $F_0$  we have if  $|Y_{p,d}| = 1$  then  $\sigma(x_{p,d,1}) = 1$  and if  $|Y_{p,d}| = 2$  then  $x_{p,d,1} \text{ xor } x_{p,d,2}$  gives us either  $\sigma(x_{p,d,1}) = 1$  or  $\sigma(x_{p,d,2}) = 1$ . Thus we have  $b_{p,d} = kY_{p,d}$  if and only if  $\sigma(x_{p,d,k}) = 1$  for some  $k \in [1, 2]$ . For all  $i \in [1, m]$  we define the number  $b_i$  as the smallest positive integer satisfying the congruences

$$b_i \equiv b_{p,d} \pmod{p^d}$$

for all prime powers  $p^d \mid a_i$  with  $d = \nu_p(a_i)$ . Then we have  $0 \leq b_i < a_i$ .

**Claim 7.** *For all  $i \in [1, m]$  we have  $b_i \in X_i$ .*

In the case  $X_i = \{v\}$  we have for every prime power  $p^d \mid a_i$  with  $d = \nu_p(a_i)$  that  $1 = \sigma(\tilde{x}_{i,p,d,0}) = \sigma(x_{p,d,k})$  for some  $k \in [1, 2]$  by  $F_{i,1}$  since  $F_0$  gives us  $\sigma(x_{p,d,0}) = 0$  and hence  $kY_{p,d} \equiv v \pmod{p^d}$ . Thus we obtain  $b_{p,d} = kY_{p,d}$  from which it follows now that

$$b_i \equiv b_{p,d} \equiv kY_{p,d} \equiv v \pmod{p^d}.$$

All congruences together now give us  $b_i \equiv v \pmod{a_i}$  and since  $0 \leq b_i, v < a_i$  we obtain  $b_i = v$ . In the case  $X_i = \{v_1, v_2\}$  we have for every prime power  $p^d \mid a_i$  with  $d = \nu_p(a_i)$  and  $v_1 \equiv v_2 \pmod{p^d}$  that  $1 = \sigma(\tilde{x}_{i,p,d,0}) = \sigma(x_{p,d,k})$  for some  $k \in [1, 2]$  by  $F_{i,3}$  and hence  $kY_{p,d} \equiv v_1 \equiv v_2 \pmod{p^d}$ . Thus we obtain  $b_{p,d} = kY_{p,d}$  from which it follows now that

$$b_i \equiv b_{p,d} \equiv kY_{p,d} \equiv v_1 \equiv v_2 \pmod{p^d}.$$

Moreover we either have  $\sigma(\tilde{x}_{i,p,d,1}) = 1$  and  $\sigma(\tilde{x}_{i,q,e,2}) = 0$  or  $\sigma(\tilde{x}_{i,p,d,1}) = 0$  and  $\sigma(\tilde{x}_{i,q,e,2}) = 1$  for every prime power  $p^d \mid a_i$  with  $d = \nu_p(a_i)$  and  $v_1 \not\equiv v_2 \pmod{p^d}$  and all  $q^e \mid a_i$  with  $e = \nu_q(a_i)$  and  $v_1 \not\equiv v_2 \pmod{q^e}$ . This follows from the following: let  $p_1^{d_1} \mid a_i$  with  $d_1 = \nu_{p_1}(a_i)$  and  $p_2^{d_2} \mid a_i$  with  $d_2 = \nu_{p_2}(a_i)$  be prime powers (we may have  $p_1 = p_2$ ) and assume  $\sigma(\tilde{x}_{i,p_1,d_1,1}) = c$  and  $\sigma(\tilde{x}_{i,p_2,d_2,2}) = c$  for some  $c \in \{0, 1\}$ . Then  $F_{i,2}$  gives us  $\tilde{x}_{i,p_1,d_1,1} \text{ xor } \tilde{x}_{i,p_2,d_2,2}$  which yields a contradiction. Now let  $l \in [1, 2]$  be such that  $\sigma(\tilde{x}_{i,p,d,l}) = 1$  for every prime power  $p^d \mid a_i$  with  $d = \nu_p(a_i)$  and  $v_1 \not\equiv v_2 \pmod{p^d}$  and let  $k \in [1, 2]$  be such that  $\tilde{x}_{i,p,d,l} = x_{p,d,k}$ . Note that  $k = 0$  is not possible since  $\sigma(\tilde{x}_{i,p,d,l}) = 1$  and  $\sigma(x_{p,d,0}) = 0$  by  $F_0$ . Then we have  $v_l \equiv kY_{p,d} \pmod{p^d}$  and  $\sigma(x_{p,d,k}) = 1$  from which it follows now that

$$b_i \equiv b_{p,d} \equiv kY_{p,d} \equiv v_l \pmod{p^d}.$$

All congruences together now give us  $b_i \equiv v_l \pmod{a_i}$  and since  $0 \leq b_i, v_l < a_i$  we obtain  $b_i = v_l$ .  $\square$

**Claim 8.** *There is  $b \in \mathbb{N}$  such that  $b \equiv b_i \pmod{a_i}$  for all  $i \in [1, m]$ .*

Let  $i \in [1, m]$  and  $j \in [1, m]$  be such that  $p^d \mid a_i$  is a prime power with  $d = \nu_p(a_i)$  and  $p^e \mid a_j$  is a prime power with  $e = \nu_p(a_j)$  and  $d \leq e$ . Then there are  $k_1, k_2 \in [1, 2]$  such that  $\sigma(x_{p,d,k_1}) = 1$  and  $\sigma(x_{p,e,k_2}) = 1$  because of  $F_0$ . Then we have  $b_{p,d} = k_1 Y_{p,d}$  and  $b_{p,e} = k_2 Y_{p,e}$ . Assume  $b_{p,d} \not\equiv b_{p,e} \pmod{p^d}$ . Then the subformula  $F'_p$  gives us

$$\varphi(p, d, e, k_1, k_2) = \begin{cases} x_{p,e,k_2} \Rightarrow x_{p,d,k_1} & \text{if } k_1 Y_{p,d} \equiv k_2 Y_{p,e} \pmod{p^d} \\ x_{p,e,k_2} \Rightarrow \neg x_{p,d,k_1} & \text{if } k_1 Y_{p,d} \not\equiv k_2 Y_{p,e} \pmod{p^d}. \end{cases}$$

We have

$$k_1 Y_{p,d} \equiv b_{p,d} \not\equiv b_{p,e} \equiv k_2 Y_{p,e} \pmod{p^d}$$

by assumption which gives us

$$\varphi(p, d, e, k_1, k_2) = x_{p,e,k_2} \Rightarrow \neg x_{p,d,k_1}.$$

Since we have  $\sigma(x_{p,d,k_1}) = 1$  and  $\sigma(x_{p,e,k_2}) = 1$  we obtain that  $F'_p$  evaluates to false which is a contradiction. Thus  $b_{p,d} \equiv b_{p,e} \pmod{p^d}$  and we can define  $b \equiv b_i \pmod{a_i}$  for all  $i \in [1, m]$ .  $\square$

By Claim 8 we can define  $0 \leq b < \text{ord}(\alpha)$  as the smallest positive integer satisfying  $b \equiv b_i \pmod{a_i}$  for all  $i \in [1, m]$ . Then we have

$$\alpha^b = \prod_{i=1}^m \alpha_i^b = \prod_{i=1}^m \alpha_i^{b_i}$$

in which by Claim 7 we have  $b_i \in X_i$  from which it finally follows that for all  $j \in [1, n]$  we have

$$j^{\alpha^b} \in \{j^\beta - 1, j^\beta, j^\beta + 1\}$$

and hence  $l_\infty(\beta, \alpha^b) \leq 1$ .  $\square$

**Lemma 6.** *Let  $l \geq 3$  be an integer and let  $a \in [0, l-1]$ . Then we have  $l_\infty(\llbracket l \rrbracket^a, \llbracket l \rrbracket^x) \leq 1$  if and only if  $x \equiv a \pmod{l}$ .*

*Proof.* One direction follows immediately since we clearly have  $l_\infty(\llbracket l \rrbracket^a, \llbracket l \rrbracket^a) = 0$ . Now suppose  $l_\infty(\llbracket l \rrbracket^a, \llbracket l \rrbracket^x) \leq 1$ . It suffices to show  $l_\infty(\llbracket l \rrbracket^a, \llbracket l \rrbracket^x) > 1$  if  $x \not\equiv a \pmod{l}$ . In the case  $b \in [1, l-2]$  we have  $(l-a)\llbracket l \rrbracket^a = l$  and  $(l-a)\llbracket l \rrbracket^{a+b} = b$  giving us a distance of at least 2. In the case  $b = l-1$  and  $a = 0$  we have  $1\llbracket l \rrbracket^0 = 1$  and  $1\llbracket l \rrbracket^{l-1} = l$  which gives us a distance of  $l-1$ . Finally consider the remaining case  $b = l-1$  and  $a \in [1, l-1]$ . We have  $(l-a+1)\llbracket l \rrbracket^a = 1$  and  $(l-a+1)\llbracket l \rrbracket^{a+(l-1)} = (l-a+1)\llbracket l \rrbracket^{a-1} = l$  which gives us also a distance of  $l-1$ .  $\square$

**Theorem 5.** *Let  $t \in \mathbb{N}$  be odd and let  $0 \leq t_1 < t_2 < t$  be such that  $t_1 \not\equiv t_2 \pmod{p}$  for all primes  $p$  with  $p \mid t$ . Then there is a cycle  $\alpha$  of length  $t$  and a permutation  $\beta$  in which  $\beta$  is a product of disjoint 2-cycles such that  $l_\infty(\beta, \alpha^{t_1}) \leq 1$  and  $l_\infty(\beta, \alpha^{t_2}) \leq 1$  and for all  $x \in [0, t-1]$  there is  $i \in [1, t]$  such that  $i^{\alpha^x} = i^\beta$  and  $j^{\alpha^x} \neq j^\beta$  for all  $j \in [1, t] \setminus \{i\}$ .*

*Proof.* We define

$$\omega = t_2 - t_1.$$

Then  $\omega$  is a generator of the additive group  $(\mathbb{Z}_t, +)$  since  $t_1 \not\equiv t_2 \pmod{p}$  for all primes  $p$  with  $p \mid t$  and in particular  $\omega$  and  $t$  are coprime and we can define  $0 \leq \psi < t$  as the smallest positive integer satisfying

$$\psi \equiv \omega^{-1}(t - t_1) \pmod{t}$$

since  $\omega^{-1} \pmod{t}$  exists. For  $i = 0, \dots, t-1$  we define  $0 \leq \omega_i < t$  as the smallest positive integer satisfying  $\omega_i \equiv i\omega \pmod{t}$ . Moreover for  $i = 0, \dots, t-1$  we define  $0 \leq \psi_i < t$  as the smallest positive integer satisfying  $\psi_i \equiv \psi + i \pmod{t}$ . Now we define the cycle  $\alpha = (\alpha_0, \dots, \alpha_{t-1})$  of length  $t$  by the following:

$$\alpha_{\omega_i} = \begin{cases} 2i+1 & \text{if } 0 \leq i \leq \frac{t-1}{2} \\ 2(t-i) & \text{if } \frac{t+1}{2} \leq i \leq t-1. \end{cases}$$

For  $i = 0, \dots, t-1$  we define  $0 \leq d_{i,1}, d_{i,2} < t$  as the smallest positive integers satisfying

$$d_{i,k} \equiv i + t_k \pmod{t}$$

for  $k \in [1, 2]$ . Then  $\alpha^{t_k}$  maps  $\alpha_i$  to  $\alpha_{d_{i,k}}$  for all  $i \in [0, t-1]$ .

**Claim 9.** Let  $i \in [0, t-1]$  and let  $j \in [0, t-1]$  be such that  $\omega_j = d_{i,1}$ . If  $j = t-1$  then  $d_{i,2} = \omega_0$  and if  $0 \leq j \leq t-2$  then  $d_{i,2} = \omega_{j+1}$ .

We have

$$\begin{aligned}
d_{i,1} &\equiv i + t_1 \pmod{t} \\
\Leftrightarrow i &\equiv d_{i,1} - t_1 \pmod{t} \\
\Leftrightarrow d_{i,2} \equiv i + t_2 &\equiv d_{i,1} - t_1 + t_2 \equiv d_{i,1} + \omega \pmod{t} \\
\Leftrightarrow d_{i,2} &\equiv \omega_j + \omega \pmod{t} \\
\Leftrightarrow d_{i,2} &\equiv j\omega + \omega \pmod{t} \\
\Leftrightarrow d_{i,2} &\equiv (j+1)\omega \pmod{t} \\
\Leftrightarrow d_{i,2} &\equiv \begin{cases} \omega_0 \pmod{t} & \text{if } j = t-1 \\ \omega_{j+1} \pmod{t} & \text{if } j \in [0, t-2]. \end{cases}
\end{aligned}$$

Since  $0 \leq d_{i,2} < t$  and  $0 \leq \omega_0, \omega_{j+1} < t$  we finally obtain

$$d_{i,2} = \begin{cases} \omega_0 & \text{if } j = t-1 \\ \omega_{j+1} & \text{if } j \in [0, t-2]. \end{cases}$$

□

By Claim 9 we have  $1 \leq |\alpha_{d_{i,1}} - \alpha_{d_{i,2}}| \leq 2$  for all  $i \in [0, t-1]$  and if  $|\alpha_{d_{i,1}} - \alpha_{d_{i,2}}| = 1$  then either  $\alpha_{d_{i,2}} = 1$  or  $\alpha_{d_{i,1}} = t$ . We define for all  $i \in [0, t-1]$

$$\alpha'_i = \begin{cases} \frac{\alpha_{d_{i,1}} + \alpha_{d_{i,2}}}{2} & \text{if } |\alpha_{d_{i,1}} - \alpha_{d_{i,2}}| = 2 \\ 1 & \text{if } |\alpha_{d_{i,1}} - \alpha_{d_{i,2}}| = 1 \text{ and } \alpha_{d_{i,2}} = 1 \\ t & \text{if } |\alpha_{d_{i,1}} - \alpha_{d_{i,2}}| = 1 \text{ and } \alpha_{d_{i,1}} = t. \end{cases}$$

Now we define the permutation  $\beta$  by the following:

$$\beta = \prod_{i=0}^{t-1} \beta_i$$

in which

$$\beta_i = \begin{cases} (\alpha_i, \alpha'_i) & \text{if } \alpha_i < \alpha'_i \\ \text{id} & \text{otherwise.} \end{cases}$$

**Claim 10.** For all  $i \in [0, t-1]$  we have  $d_{\omega_{\psi_i}, 1} = \omega_i$ .

We have

$$\begin{aligned}
d_{\omega_{\psi_i}, 1} &\equiv \omega_{\psi_i} + t_1 \pmod{t} \\
&\equiv \psi_i \omega + t_1 \pmod{t} \\
&\equiv ((t - t_1)\omega^{-1} + i)\omega + t_1 \pmod{t} \\
&\equiv t - t_1 + i\omega + t_1 \pmod{t} \\
&\equiv \omega_i \pmod{t}.
\end{aligned}$$

Since  $0 \leq d_{\omega_{\psi_i}, 1}, \omega_i < t$  we finally obtain  $d_{\omega_{\psi_i}, 1} = \omega_i$ .

□

**Claim 11.** For all  $i \in [0, t-1]$  we have  $\alpha'_{\omega_{\psi_i}} = \alpha_{\omega_{t-1-i}}$ .

Note that by Claim 10 we have  $d_{\omega_{\psi_i}, 1} = \omega_i$ . Then we have by Claim 9

$$d_{\omega_{\psi_i}, 2} = \begin{cases} \omega_{i+1} & \text{if } i \in [0, t-2] \\ \omega_0 & \text{if } i = t-1. \end{cases}$$

Case 1:  $i \in [0, \frac{t-3}{2}]$ . We have

$$\begin{aligned}
\alpha'_{\omega_{\psi_i}} &= \frac{\alpha_{d_{\omega_{\psi_i},1}} + \alpha_{d_{\omega_{\psi_i},2}}}{2} \\
&= \frac{\alpha_{\omega_i} + \alpha_{\omega_{i+1}}}{2} \\
&= \frac{2i+1 + 2(i+1) + 1}{2} \\
&= 2i+2 \\
&= 2(t - (t-1-i)) \\
&= \alpha_{\omega_{t-1-i}}.
\end{aligned}$$

Case 2:  $i = \frac{t-1}{2}$ . We have  $\alpha_{d_{\omega_{\psi_i},1}} = \alpha_{\omega_i} = t$  and hence

$$\alpha'_{\omega_{\psi_i}} = \alpha_{d_{\omega_{\psi_i},1}} = t = \alpha_{\omega_{t-1-\frac{t-1}{2}}}.$$

Case 3:  $i \in [\frac{t+1}{2}, t-2]$ . We have

$$\begin{aligned}
\alpha'_{\omega_{\psi_i}} &= \frac{\alpha_{d_{\omega_{\psi_i},1}} + \alpha_{d_{\omega_{\psi_i},2}}}{2} \\
&= \frac{\alpha_{\omega_i} + \alpha_{\omega_{i+1}}}{2} \\
&= \frac{2(t-i) + 2(t-(i+1))}{2} \\
&= 2(t-i) - 1 \\
&= 2(t-1-i) + 1 \\
&= \alpha_{\omega_{t-1-i}}.
\end{aligned}$$

Case 4:  $i = t-1$ . We have  $\alpha_{d_{\omega_{\psi_i},2}} = \alpha_{\omega_0} = 1$  and hence

$$\alpha'_{\omega_{\psi_i}} = \alpha_{d_{\omega_{\psi_i},2}} = 1 = \alpha_{\omega_{t-1-(t-1)}}.$$

□

**Claim 12.** For all  $i \in [0, t-1]$  and  $j \in [0, t-1]$  we have  $\alpha'_i = \alpha_j$  if and only if  $\alpha'_j = \alpha_i$ .

Suppose  $\alpha'_i = \alpha_j$  and let  $0 \leq e < t$  be such that  $i = \omega_{\psi_e}$ . Note that  $e$  exists. Since  $\omega$  is a generator there is  $c \in [0, t-1]$  such that  $i \equiv \omega_c \pmod{t}$  and we can choose  $e \equiv c - \psi \pmod{t}$ . By Claim 11 we have  $\alpha'_{\omega_{\psi_e}} = \alpha_{\omega_{t-1-e}}$  (i.e.  $j = \omega_{t-1-e}$ ). Claim 11 also gives us

$$\begin{aligned}
\alpha'_j &= \alpha'_{\omega_{t-1-e}} \\
&= \alpha'_{\omega_{\psi - \psi + t-1-e}} \\
&= \begin{cases} \alpha'_{\omega_{\psi_{t-1-e-\psi}}} & \text{if } \psi \leq t-1-e \\ \alpha'_{\omega_{\psi_{t-1-e+t-\psi}}} & \text{if } \psi > t-1-e \end{cases} \\
&= \begin{cases} \alpha_{\omega_{t-1-(t-1-e-\psi)}} & \text{if } \psi \leq t-1-e \\ \alpha_{\omega_{t-1-(t-1-e+t-\psi)}} & \text{if } \psi > t-1-e \end{cases} \\
&= \begin{cases} \alpha_{\omega_{e+\psi}} & \text{if } \psi \leq t-1-e \\ \alpha_{\omega_{e-t+\psi}} & \text{if } \psi > t-1-e \end{cases} \\
&= \alpha_{\omega_{\psi_e}} \\
&= \alpha_i.
\end{aligned}$$

Note that  $0 \leq \psi_e < t$  and hence  $\psi_e = e + \psi$  if  $\psi \leq t - 1 - e$  because  $e + \psi \leq t - 1$  and  $\psi_e = e - t + \psi$  if  $\psi > t - 1 - e$  because  $e + \psi \geq t$ .  $\square$

By Claim 12 it also follows that the cycles of  $\beta$  are disjoint: suppose  $\beta$  contains  $(\alpha_h, \alpha_i)$  and  $(\alpha_j, \alpha_i)$  for some pairwise different  $h, i, j \in [0, t - 1]$ . Then we have  $\alpha_h = \alpha'_i = \alpha_j$  which yields  $h = j$  contradicting  $h \neq j$ .

Now it suffices to show  $l_\infty(\beta, \alpha^{t_1}) \leq 1$  and  $l_\infty(\beta, \alpha^{t_2}) \leq 1$ . By Claim 9 we have for all  $i \in [0, t - 1]$  and all  $k \in [1, 2]$

$$\alpha_i^{\alpha^{t_k}} \in \{\alpha_j - 1, \alpha_j, \alpha_j + 1\}$$

for some  $j \in [0, t - 1]$ . Moreover we have  $\alpha'_i = \alpha_j$ . By Claim 12 we then have  $\alpha'_j = \alpha_i$  and hence

$$\alpha_j^{\alpha^{t_k}} \in \{\alpha_i - 1, \alpha_i, \alpha_i + 1\}.$$

Thus we either have  $\beta_i = (\alpha_i, \alpha_j)$  and  $\beta_j = \text{id}$  or  $\beta_i = \text{id}$  and  $\beta_j = (\alpha_i, \alpha_j)$  yielding a distance of at most 1 if  $i \neq j$ . In the case

$$\alpha_i^{\alpha^{t_k}} \in \{\alpha_i - 1, \alpha_i, \alpha_i + 1\}$$

we have that  $\alpha_i$  is a fixed point in  $\beta$  yielding a distance of at most 1. Thus we finally obtain  $l_\infty(\beta, \alpha^{t_1}) \leq 1$  and  $l_\infty(\beta, \alpha^{t_2}) \leq 1$ .

It remains to show the second part of the theorem. We define the distance  $\Delta : [0, t - 1]^2 \rightarrow [0, t - 1]$  as  $\Delta(i, j) = k$  in which  $0 \leq k \leq t - 1$  is the unique number such that  $i + \omega_k \equiv j \pmod t$ .

**Claim 13.** *Let  $i \in [0, t - 1]$  and  $j \in [0, t - 1]$  and let  $0 \leq g, h \leq t - 1$  be such that  $i = \omega_g$  and  $j = \omega_h$  then we have  $\Delta(i, j) = h - g$  if  $g \leq h$  and  $\Delta(i, j) = t - g + h$  if  $g > h$ .*

Suppose  $g \leq h$ . Then we have

$$\omega_g + \omega_{h-g} \equiv g\omega + (h - g)\omega \equiv h\omega \equiv \omega_h \pmod t$$

and hence  $\Delta(i, j) = h - g$ . Now suppose  $g > h$ . In this case we have

$$\omega_g + \omega_{t+h-g} \equiv g\omega + (t + h - g)\omega \equiv h\omega \equiv \omega_h \pmod t$$

and  $\Delta(i, j) = t + h - g$ .  $\square$

By Claim 11 we have  $\alpha'_{\omega_{\psi_i}} = \alpha_{\omega_{t-1-i}}$  for all  $i \in [0, t - 1]$ . Then  $\alpha^{\Delta(\omega_{\psi_i}, \omega_{t-1-i})\omega}$  maps  $\alpha_{\omega_{\psi_i}}$  to  $\alpha_{\omega_{t-1-i}}$  since clearly  $\alpha^{\omega_{t-1-i} - \omega_{\psi_i}}$  maps  $\alpha_{\omega_{\psi_i}}$  to  $\alpha_{\omega_{t-1-i}}$  and we have by Claim 13

$$\omega_{t-1-i} - \omega_{\psi_i} \equiv (t - 1 - i - \psi_i)\omega \equiv \Delta(\omega_{\psi_i}, \omega_{t-1-i})\omega \pmod t.$$

Thus we obtain

$$\left( \alpha^{\Delta(\omega_{\psi_i}, \omega_{t-1-i})\omega} \right)_{\alpha_{\omega_{\psi_i}}} = \alpha'_{\omega_{\psi_i}} = \alpha_{\omega_{\psi_i}}^\beta.$$

Hence it suffices to show  $\Delta(\omega_{\psi_i}, \omega_{t-1-i}) \neq \Delta(\omega_{\psi_j}, \omega_{t-1-j})$  if  $i \neq j$ . By Claim 13 we have

$$\begin{aligned} \Delta(\omega_{\psi_i}, \omega_{t-1-i}) &= \begin{cases} t - 1 - i - \psi_i & \text{if } \psi_i \leq t - 1 - i \\ t - \psi_i + t - 1 - i & \text{if } \psi_i > t - 1 - i \end{cases} \\ &= \begin{cases} t - 1 - 2i - \psi & \text{if } \psi_i \leq t - 1 - i \text{ and } \psi + i < t \\ 2t - 1 - 2i - \psi & \text{if } \psi_i \leq t - 1 - i \text{ and } \psi + i \geq t \\ & \text{or } \psi_i > t - 1 - i \text{ and } \psi + i < t \\ 3t - 1 - 2i - \psi & \text{if } \psi_i > t - 1 - i \text{ and } \psi + i \geq t. \end{cases} \end{aligned}$$

For the second equation note that  $\psi_i = \psi + i$  if  $\psi + i < t$  and  $\psi_i = \psi + i - t$  if  $\psi + i \geq t$ . Assuming  $\Delta(\omega_{\psi_i}, \omega_{t-1-i}) = \Delta(\omega_{\psi_j}, \omega_{t-1-j})$  for some  $j \in [0, t - 1] \setminus \{i\}$  gives us one of the following cases:

$$\begin{aligned} t - 1 - 2i - \psi &= t - 1 - 2j - \psi && \text{if and only if } i = j \\ t - 1 - 2i - \psi &= 2t - 1 - 2j - \psi && \text{if and only if } 2(j - i) = t \\ t - 1 - 2i - \psi &= 3t - 1 - 2j - \psi && \text{if and only if } j = t + i \end{aligned}$$

$$\begin{aligned}
2t - 1 - 2i - \psi &= t - 1 - 2j - \psi \text{ if and only if } 2(i - j) = t \\
2t - 1 - 2i - \psi &= 2t - 1 - 2j - \psi \text{ if and only if } i = j \\
2t - 1 - 2i - \psi &= 3t - 1 - 2j - \psi \text{ if and only if } 2(j - i) = t
\end{aligned}$$

$$\begin{aligned}
3t - 1 - 2i - \psi &= t - 1 - 2j - \psi \text{ if and only if } i = t + j \\
3t - 1 - 2i - \psi &= 2t - 1 - 2j - \psi \text{ if and only if } 2(i - j) = t \\
3t - 1 - 2i - \psi &= 3t - 1 - 2j - \psi \text{ if and only if } i = j.
\end{aligned}$$

This gives us a contradiction in all cases since  $i = j$  contradicts  $j \in [0, t - 1] \setminus \{i\}$ ,  $2(j - i) = t$  and  $2(j - i) = t$  contradict the fact that  $t$  is odd and  $j = t + i$  and  $i = t + j$  contradict  $0 \leq i, j < t$ . Hence  $\Delta(\omega_{\psi_i}, \omega_{t-1-i}) \neq \Delta(\omega_{\psi_j}, \omega_{t-1-j})$ . We finally obtain

$$\alpha_{\omega_{\psi_j}}^{\left(\alpha^{\Delta(\omega_{\psi_i}, \omega_{t-1-i})\omega}\right)} \neq \alpha_{\omega_{\psi_j}}^{\left(\alpha^{\Delta(\omega_{\psi_j}, \omega_{t-1-j})\omega}\right)} = \alpha'_{\omega_{\psi_j}} = \alpha_{\omega_{\psi_j}}^\beta$$

for all  $j \in [0, t - 1] \setminus \{i\}$ .  $\square$

**Corollary 1.** *Let  $t \in \mathbb{N}$  be odd and let  $0 \leq t_1 < t_2 < t$  be such that  $t_1 \not\equiv t_2 \pmod{p}$  for all primes  $p$  with  $p \mid t$ . Moreover let  $d \geq 3$  be an integer with  $\gcd(d, t) = 1$  and let  $0 \leq d_0 < d$ . Then there are permutations  $\gamma, \delta \in S_{t+d}$  such that  $l_\infty(\delta, \gamma^{a_1}) \leq 1$  and  $l_\infty(\delta, \gamma^{a_2}) \leq 1$  in which  $a_r$  satisfies the congruences  $a_r \equiv d_0 \pmod{d}$  and  $a_r \equiv t_r \pmod{t}$  for  $r \in [1, 2]$ .*

*Proof.* Let  $\alpha$  and  $\beta$  be the permutations that Theorem 5 yields regarding the numbers  $t_1, t_2, t$ . Moreover let  $\varepsilon = \llbracket d \rrbracket$ . We define  $\gamma = (\alpha, \varepsilon) \in S_t \times S_d$  and  $\delta = (\beta, \varepsilon^{d_0}) \in S_t \times S_d$ . Then we have  $l_\infty(\delta, \gamma^{a_1}) \leq 1$  and  $l_\infty(\delta, \gamma^{a_2}) \leq 1$  since  $\gamma^{a_r} = (\alpha^{a_r}, \varepsilon^{a_r}) = (\alpha^{t_r}, \varepsilon^{d_0})$  with  $r \in [1, 2]$  and clearly  $l_\infty(\varepsilon^{d_0}, \varepsilon^{d_0}) \leq 1$  and  $l_\infty(\beta, \alpha^{t_r}) \leq 1$  follows from Theorem 5.  $\square$

**Theorem 6.** *The SUBGROUP DISTANCE PROBLEM regarding the  $l_\infty$  distance is NP-complete when the input group is abelian and given by two generators and  $k = 1$ .*

*Proof.* We give a log-space reduction from X3HS. Let  $X$  be a finite set and  $\mathcal{B} \subseteq 2^X$  be a set of subsets of  $X$  all of size 3. W.l.o.g. assume that  $X = [1, n]$  and let  $\mathcal{B} = \{C_1, \dots, C_m\}$ . For  $i \in X$  we denote by  $D_i \subseteq [1, m]$  the ordered set of all numbers  $j$  such that  $i \in C_j$ . For  $k \in [1, |D_i|]$  we denote by  $kD_i$  the  $k^{\text{th}}$  element of  $D_i$ . For  $i \in [1, n]$  and  $j \in [0, m]$  let  $p_{i,j}$  be the  $(jn + i)^{\text{th}}$  odd prime. We define  $q_j = \prod_{i \in C_j} p_{i,j}$ . Moreover let  $N = \sum_{i=1}^n p_{i,0} p_{i,m} |D_i| + 2 \sum_{j=1}^m (p_{n,j}^2 + p_{n,j})$ . We will work with the group

$$G = \prod_{i=1}^n V_i \times \prod_{j=1}^m U_j$$

with  $V_i = S_{p_{i,0} p_{i,m}}^{|D_i|}$  and  $U_j = S_{p_{n,j}^2 + p_{n,j}}^2$  which naturally embeds into  $S_N$ . We define auxiliary permutations by the following: for  $i \in [1, n]$  and  $k \in [1, |D_i|]$  let  $\alpha_{i,kD_i}$  and  $\beta_{i,kD_i}$  be the permutations that Theorem 5 yields regarding the solutions  $0 \leq x_{i,k,1}, x_{i,k,2} < p_{i,0} p_{i,kD_i}$  with

$$\begin{aligned}
x_{i,k,1} &\equiv 0 \pmod{p_{i,0}} \\
x_{i,k,1} &\equiv 0 \pmod{p_{i,kD_i}}
\end{aligned}$$

and

$$\begin{aligned}
x_{i,k,2} &\equiv 1 \pmod{p_{i,0}} \\
x_{i,k,2} &\equiv 1 \pmod{p_{i,kD_i}}
\end{aligned}$$

in which  $\alpha_{i,kD_i}$  is a cycle of length  $p_{i,0} p_{i,kD_i}$  and  $\beta_{i,kD_i}$  is a product of 2-cycles. Moreover we define the following: for  $j \in [1, m]$  let  $\gamma_{j,1}, \delta_{j,1}$  be the permutations that Corollary 1 yields regarding the

solutions  $0 \leq y_{j,1}, y_{j,2} < q_j$  with

$$\begin{aligned} y_{j,1} &\equiv 1 \pmod{p_{i_1,j}} \\ y_{j,1} &\equiv 0 \pmod{p_{i_2,j}} \\ y_{j,1} &\equiv 0 \pmod{p_{i_3,j}} \end{aligned}$$

and

$$\begin{aligned} y_{j,2} &\equiv 0 \pmod{p_{i_1,j}} \\ y_{j,2} &\equiv 1 \pmod{p_{i_2,j}} \\ y_{j,2} &\equiv 0 \pmod{p_{i_3,j}} \end{aligned}$$

in which  $i_1 < i_2 < i_3 \in C_j$  are the elements of  $C_j$ . Furthermore for  $j \in [1, m]$  let  $\gamma_{j,2}, \delta_{j,2}$  be the permutations that Corollary 1 yields regarding the solutions  $0 \leq z_{j,1}, z_{j,2} < q_j$  with

$$\begin{aligned} z_{j,1} &\equiv 0 \pmod{p_{i_1,j}} \\ z_{j,1} &\equiv 0 \pmod{p_{i_2,j}} \\ z_{j,1} &\equiv 0 \pmod{p_{i_3,j}} \end{aligned}$$

and

$$\begin{aligned} z_{j,2} &\equiv 1 \pmod{p_{i_1,j}} \\ z_{j,2} &\equiv 0 \pmod{p_{i_2,j}} \\ z_{j,2} &\equiv -1 \pmod{p_{i_3,j}} \end{aligned}$$

in which  $i_1 < i_2 < i_3 \in C_j$  are the elements of  $C_j$ . Note that these permutations can be constructed in log-space. Also note that these solutions are the only solutions by Lemma 5 and Lemma 6. We define the input group elements  $\tau, \pi_1, \pi_2 \in G$  as follows where  $i$  ranges over  $[1, n]$ ,  $j$  ranges over  $[1, m]$  and  $k$  ranges over  $[1, |D_i|]$ :

$$\begin{aligned} \tau &= (\tau_1, \dots, \tau_n, \tau'_1, \dots, \tau'_m) \text{ with} \\ \tau_i &= (\tau_{i,1}, \dots, \tau_{i,|D_i|}) \\ \tau_{i,k} &= \beta_{i,kD_i} \\ \tau'_j &= (\delta_{j,1}, \delta_{j,2}) \end{aligned}$$

$$\begin{aligned} \pi_1 &= (\rho_{1,1}, \dots, \rho_{1,n}, \sigma_{1,1}, \dots, \sigma_{1,m}) \text{ with} \\ \rho_{1,i} &= (\rho_{1,i,1}, \dots, \rho_{1,i,|D_i|}) \\ \rho_{1,i,k} &= \alpha_{i,kD_i} \\ \sigma_{1,j} &= (\gamma_{j,1}, \text{id}) \end{aligned}$$

and

$$\begin{aligned} \pi_2 &= (\rho_{2,1}, \dots, \rho_{2,n}, \sigma_{2,1}, \dots, \sigma_{2,m}) \text{ with} \\ \rho_{2,i} &= (\rho_{2,i,1}, \dots, \rho_{2,i,|D_i|}) \\ \rho_{2,i,k} &= \text{id} \\ \sigma_{2,j} &= (\gamma_{j,1}, \gamma_{j,2}). \end{aligned}$$

Note that  $\pi_1$  and  $\pi_2$  commute.

Now we will show there are  $x_1, x_2 \in \mathbb{N}$  such that  $l_\infty(\tau, \pi_1^{x_1} \pi_2^{x_2}) \leq 1$  if and only if there is a subset  $X' \subseteq X$  such that  $|X' \cap C_j| = 1$  for all  $j \in [1, m]$ .

Suppose there are  $x_1, x_2 \in \mathbb{N}$  such that  $l_\infty(\tau, \pi_1^{x_1} \pi_2^{x_2}) \leq 1$ . Then we define

$$X' = \{i \mid x_1 \equiv 1 \pmod{p_{i,0}}\}.$$

**Claim 14.** For all  $i \in [1, n]$  and all  $k \in [1, |D_i|]$  the following holds:  $x_1 \equiv 0, 1 \pmod{p_{i,kD_i}}$  and  $x_1 \equiv 0, 1 \pmod{p_{i,0}}$ . Moreover  $x_1 \equiv 1 \pmod{p_{i,0}}$  if and only if  $x_1 \equiv 1 \pmod{p_{i,kD_i}}$ .

The first part follows from the fact that  $l_\infty(\tau_{i,k}, \rho_{1,i,k}^{x_1} \rho_{2,i,k}^{x_2}) = l_\infty(\beta_{i,kD_i}, \alpha_{i,kD_i}^{x_1}) \leq 1$  if and only if  $x_1 \equiv x_{i,k,1}, x_{i,k,2} \pmod{p_{i,0}p_{i,kD_i}}$ . The second part follows from the definitions of  $x_{i,k,1}$  and  $x_{i,k,2}$ .  $\square$

**Claim 15.** For all  $j \in [1, m]$  there is exactly one  $a \in C_j$  such that  $x_1 \equiv 1 \pmod{p_{a,j}}$  and  $x_1 \equiv 0 \pmod{p_{b,j}}$  for all  $b \in C_j \setminus \{a\}$ .

Consider the projection onto the factor  $U_j$ . We have  $l_\infty(\tau'_j, \sigma_{1,j}^{x_1} \sigma_{2,j}^{x_2}) \leq 1$  which gives us the two statements

$$l_\infty(\delta_{j,1}, \gamma_{j,1}^{x_1} \gamma_{j,1}^{x_2}) \leq 1 \quad (6)$$

and

$$l_\infty(\delta_{j,2}, \gamma_{j,2}^{x_2}) \leq 1. \quad (7)$$

By (7) we obtain  $x_2 \equiv z_{j,1}, z_{j,2} \pmod{q_j}$ . Moreover  $l_\infty(\delta_{j,1}, \gamma_{j,1}^x) \leq 1$  holds if and only if  $x \equiv y_{j,1}, y_{j,2} \pmod{q_j}$ . Hence by (6) we obtain  $x_1 + x_2 \equiv y_{j,1}, y_{j,2} \pmod{q_j}$ . If  $x_2 \equiv z_{j,1} \equiv 0 \pmod{q_j}$  we obtain  $x_1 \equiv y_{j,1}, y_{j,2} \pmod{q_j}$ . If  $x_2 \equiv z_{j,2} \pmod{q_j}$  we obtain the following

$$\begin{aligned} x_1 + x_2 &\equiv x_1 + 1 \pmod{p_{i_1,j}} \\ x_1 + x_2 &\equiv x_1 + 0 \pmod{p_{i_2,j}} \\ x_1 + x_2 &\equiv x_1 - 1 \pmod{p_{i_3,j}} \end{aligned}$$

in which  $i_1 < i_2 < i_3 \in C_j$  are the elements of  $C_j$ . In the case  $x_1 + x_2 \equiv y_{j,2} \pmod{q_j}$  we obtain

$$\begin{aligned} x_1 + 1 &\equiv 0 \pmod{p_{i_1,j}} \\ x_1 + 0 &\equiv 1 \pmod{p_{i_2,j}} \\ x_1 - 1 &\equiv 0 \pmod{p_{i_3,j}} \end{aligned}$$

which gives us by

$$\begin{aligned} x_1 &\equiv -1 \pmod{p_{i_1,j}} \\ x_1 &\equiv 1 \pmod{p_{i_2,j}} \\ x_1 &\equiv 1 \pmod{p_{i_3,j}} \end{aligned}$$

a contradiction since  $x_1 \equiv -1 \pmod{p_{i_1,j}}$  is not possible by Claim 14. For this also note that  $p_{i,j} \geq 3$ . Thus  $x_1 + x_2 \equiv y_{j,1} \pmod{q_j}$  and

$$\begin{aligned} x_1 + 1 &\equiv 1 \pmod{p_{i_1,j}} \\ x_1 + 0 &\equiv 0 \pmod{p_{i_2,j}} \\ x_1 - 1 &\equiv 0 \pmod{p_{i_3,j}} \end{aligned}$$

which gives us

$$\begin{aligned} x_1 &\equiv 0 \pmod{p_{i_1,j}} \\ x_1 &\equiv 0 \pmod{p_{i_2,j}} \\ x_1 &\equiv 1 \pmod{p_{i_3,j}}. \end{aligned}$$

Now we define  $0 \leq y_{j,3} < q_j$  as the smallest positive integer satisfying the congruences

$$\begin{aligned} y_{j,3} &\equiv 0 \pmod{p_{i_1,j}} \\ y_{j,3} &\equiv 0 \pmod{p_{i_2,j}} \\ y_{j,3} &\equiv 1 \pmod{p_{i_3,j}}. \end{aligned}$$



Hence there is exactly one  $a \in [1, 3]$  such that  $x_1 \equiv y_{j,a} \equiv 1 \pmod{p_{i_a,j}}$  and for all  $b \in [1, 3] \setminus \{a\}$  we have  $x_1 \equiv y_{j,a} \equiv 0 \pmod{p_{i_b,j}}$  which proves the claim. For this also note that the congruence for  $x_2$  can be chosen suitably for every  $j \in [1, m]$ . This does not interfere other congruences since  $q_{j_1}$  and  $q_{j_2}$  are coprime for  $j_1 \neq j_2$ .  $\square$

Now we show  $|X' \cap C_j| = 1$  for all  $j \in [1, m]$ . Let  $j \in [1, m]$ . By Claim 15 there is exactly one  $a \in C_j$  such that  $x_1 \equiv 1 \pmod{p_{a,j}}$  and  $x_1 \equiv 0 \pmod{p_{b,j}}$  for all  $b \in C_j \setminus \{a\}$ . By Claim 14 we have  $x_1 \equiv 1 \pmod{p_{i,a}}$  if and only if  $x_1 \equiv 1 \pmod{p_{a,0}}$ . Hence  $a \in X'$ . Moreover by Claim 14  $x_1 \equiv 0 \pmod{p_{b,j}}$  if and only if  $x_1 \equiv 0 \pmod{p_{b,0}}$  and by this  $b \notin X'$  for all  $b \in C_j \setminus \{a\}$ . Hence  $|X' \cap C_j| = 1$ .

Vice versa suppose there is a subset  $X' \subseteq X$  such that  $|X' \cap C_j| = 1$  for all  $j \in [1, m]$ . Then we define  $x_1 \in \mathbb{N}$  as the smallest positive integer satisfying the congruences

$$x_1 \equiv \begin{cases} 1 \pmod{p_{i,0}p_{i,kD_i}} & \text{if } i \in X' \\ 0 \pmod{p_{i,0}p_{i,kD_i}} & \text{if } i \notin X' \end{cases}$$

for all  $i \in [1, n]$  and all  $k \in [1, |D_i|]$ . Then by projecting onto the factor  $V_i$  we clearly have  $l_\infty(\tau_{i,k}, \rho_{1,i,k}^{x_1} \rho_{2,i,k}^{x_2}) = l_\infty(\beta_{i,k}, \alpha_{i,kD_i}^{x_1}) \leq 1$  because  $x_1 \equiv x_{i,k,1} \pmod{p_{i,0}p_{i,kD_i}}$  or  $x_1 \equiv x_{i,k,2} \pmod{p_{i,0}p_{i,kD_i}}$ . Since  $|X' \cap C_j| = 1$  for all  $j \in [1, m]$  there is exactly one  $a \in C_j$  such that  $x_1 \equiv 1 \pmod{p_{a,j}}$  and  $x_1 \equiv 0 \pmod{p_{b,j}}$  for all  $b \in C_j \setminus \{a\}$  and thus  $x_1 \equiv y_{j,a} \pmod{q_j}$ . Hence we can define  $x_2 \in \mathbb{N}$  as the smallest positive integer satisfying the congruences

$$x_2 \equiv \begin{cases} z_{j,1} \pmod{q_j} & \text{if } x_1 \equiv y_{j,1}, y_{j,2} \pmod{q_j} \\ z_{j,2} \pmod{q_j} & \text{if } x_1 \equiv y_{j,3} \pmod{q_j}. \end{cases}$$

Then by projecting onto the factor  $U_j$  we have

$$l_\infty(\delta_{j,1}, \gamma_{j,1}^{x_1} \gamma_{j,1}^{x_2}) \leq 1$$

and

$$l_\infty(\delta_{j,2}, \gamma_{j,2}^{x_2}) \leq 1$$

because  $x_2 \equiv z_{j,1} \pmod{q_j}$  or  $x_2 \equiv z_{j,2} \pmod{q_j}$  and  $x_1 + x_2 \equiv y_{j,3} + z_{j,2} \equiv y_{j,1} \pmod{q_j}$  or  $x_1 + x_2 \equiv x_1 + z_{j,1} \equiv x_1 \equiv y_{j,1}, y_{j,2} \pmod{q_j}$  which gives us  $l_\infty(\tau'_j, \sigma_{1,j}^{x_1} \sigma_{2,j}^{x_2}) \leq 1$  from which it follows now that  $l_\infty(\tau, \pi_1^{x_1} \pi_2^{x_2}) \leq 1$ .  $\square$

### 3.4 $l_p$ Distance and Lee Distance

Let  $p \geq 1$  be any fixed non-negative integer throughout this section.

**Lemma 7.** *Let  $t, q \in \mathbb{N}$  be odd primes with  $t \neq q$  and let  $a \in [0, tq - 1]$ . Moreover let  $\delta \in S_{tq}$  be the cycle defined by*

$$\delta = (1, 3, 5, \dots, tq, tq - 1, tq - 3, \dots, 2).$$

*Then the following holds*

$$p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^a\right) = \begin{cases} (tq - 1)^p + 2 \sum_{i=0}^{\frac{tq-3}{2}} (2i + 1)^p & \text{if } a \in \{0, 1\} \\ (2a - 1) \cdot |tq - 2a + 1|^p + 2 \sum_{i=0}^{\frac{tq-1}{2}-a} (2i + 1)^p & \text{if } a \in [2, \frac{tq-1}{2}] \\ 0 & \text{if } a = \frac{tq+1}{2} \\ (2tq - 2a + 1) \cdot |tq - 2a + 1|^p + 2 \sum_{i=0}^{a-\frac{tq+3}{2}} (2i + 1)^p & \text{if } a \in [\frac{tq+3}{2}, tq - 1]. \end{cases}$$

*Proof.* Clearly  $p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^a\right) = 0$  if  $a = \frac{tq+1}{2}$ . Now suppose  $a \neq \frac{tq+1}{2}$ .

Case 1:  $a \in \{0, 1\}$ . Suppose  $a = 0$ . For all  $i \in [0, \frac{tq-3}{2}]$  we have  $(2i + 1)^{\delta^{\frac{tq+1}{2}}} = tq - (2i + 1)$  and  $(2i + 1)^{\delta^0} = 2i + 1$  which gives us a distance of

$$|tq - (2i + 1) - (2i + 1)|^p = |tq - 4i - 2|^p. \quad (8)$$

Moreover for all  $i \in [0, \frac{tq-3}{2}]$  we have  $(2i+2)^{\delta^{\frac{tq+1}{2}}} = tq - 2i$  and  $(2i+2)^{\delta^0} = 2i+2$  which gives us a distance of

$$|tq - 2i - (2i+2)|^p = |tq - 4i - 2|^p. \quad (9)$$

Moreover  $tq^{\delta^{\frac{tq+1}{2}}} = 1$  and  $tq^{\delta^0} = tq$  with the distance

$$|tq - 1|^p. \quad (10)$$

Summing over (8),(9) and (10) gives us

$$\begin{aligned} p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^0\right) &= |tq - 1|^p + 2 \sum_{i=0}^{\frac{tq-3}{2}} |tq - 4i - 2|^p \\ &= (tq - 1)^p + 2 \sum_{i=0}^{\frac{tq-3}{2}} (2i + 1)^p. \end{aligned}$$

Suppose  $a = 1$ . For all  $i \in [0, \frac{tq-3}{2}]$  we have  $(2i+1)^{\delta^{\frac{tq+1}{2}}} = tq - (2i+1)$  and  $(2i+1)^{\delta^1} = 2i+3$  which gives us a distance of

$$|tq - (2i+1) - (2i+3)|^p = |tq - 4i - 4|^p. \quad (11)$$

Moreover for all  $i \in [0, \frac{tq-5}{2}]$  we have  $(2i+4)^{\delta^{\frac{tq+1}{2}}} = tq - 2i - 2$  and  $(2i+4)^{\delta^1} = 2i+2$  which gives us a distance of

$$|tq - 2i - 2 - (2i+2)|^p = |tq - 4i - 4|^p. \quad (12)$$

Moreover  $tq^{\delta^{\frac{tq+1}{2}}} = 1$  and  $tq^{\delta^1} = tq - 1$  and  $2^{\delta^{\frac{tq+1}{2}}} = tq$  and  $2^{\delta^1} = 1$  with the distance

$$|tq - 2|^p + |tq - 1|^p. \quad (13)$$

Summing over (11),(12) and (13) gives us

$$\begin{aligned} p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^1\right) &= |tq - 2|^p + |tq - 1|^p + 2 \sum_{i=0}^{\frac{tq-5}{2}} |tq - 4i - 4|^p + |tq - 2|^p \\ &= (tq - 1)^p + 2 \sum_{i=0}^{\frac{tq-3}{2}} (2i + 1)^p. \end{aligned}$$

Case 2:  $a \in [2, \frac{tq-1}{2}]$ . For all  $i \in [0, \frac{tq-1}{2} - a]$  we have  $(2i+1)^{\delta^{\frac{tq+1}{2}}} = tq - (2i+1)$  and  $(2i+1)^{\delta^a} = 2i+1+2a$  which gives us a distance of

$$|tq - (2i+1) - (2i+1+2a)|^p = |tq - 4i - 2 - 2a|^p. \quad (14)$$

Moreover for all  $i \in [\frac{tq+1}{2} - a, \frac{tq-3}{2}]$  we have  $(2i+1)^{\delta^{\frac{tq+1}{2}}} = tq - (2i+1)$  and  $(2i+1)^{\delta^a} = 2tq - 2a - 2i$  which gives us a distance of

$$|2tq - 2a - 2i - (tq - (2i+1))|^p = |tq - 2a + 1|^p. \quad (15)$$

Moreover  $tq^{\delta^{\frac{tq+1}{2}}} = 1$  and  $tq^{\delta^a} = tq - 2a + 1$  with the distance

$$|tq - 2a|^p. \quad (16)$$

Moreover for all  $i \in [0, \frac{tq-3}{2} - a]$  we have  $(tq - (2i+1))^{\delta^{\frac{tq+1}{2}}} = 2i+3$  and  $(tq - (2i+1))^{\delta^a} = tq - (2i+1) - 2a$  which gives us a distance of

$$|tq - (2i+1) - 2a - (2i+3)|^p = |tq - 4i - 4 - 2a|^p. \quad (17)$$

Moreover for all  $i \in [\frac{tq-1}{2} - a, \frac{tq-3}{2}]$  we have  $(tq - (2i+1))^{\delta^{\frac{tq+1}{2}}} = 2i+3$  and  $(tq - (2i+1))^{\delta^a} = -tq + 2a + 2i + 2$  which gives us a distance of

$$|2i+3 - (-tq + 2a + 2i + 2)|^p = |tq - 2a + 1|^p. \quad (18)$$

Summing over (14),(15),(16),(17) and (18) gives us

$$\begin{aligned} p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^a\right) &= \left(\frac{tq-3}{2} - \left(\frac{tq+1}{2} - a\right) + 1\right) |tq - 2a + 1|^p + |tq - 2a|^p \\ &\quad + \left(\frac{tq-3}{2} - \left(\frac{tq-1}{2} - a\right) + 1\right) |tq - 2a + 1|^p \\ &\quad + \sum_{i=0}^{\frac{tq-1}{2}-a} |tq - 4i - 2 - 2a|^p + \sum_{i=0}^{\frac{tq-3}{2}-a} |tq - 4i - 4 - 2a|^p \\ &= (2a-1)|tq - 2a + 1|^p + 2|tq - 2a|^p + 2 \sum_{i=0}^{\frac{tq-3}{2}-a} |tq - 4i - 2 - 2a|^p \\ &= (2a-1)|tq - 2a + 1|^p + 2 \sum_{i=0}^{\frac{tq-1}{2}-a} (2i+1)^p. \end{aligned}$$

Case 3:  $a \in [\frac{tq+3}{2}, tq-1]$ . For all  $i \in [0, tq-a-1]$  we have  $(2i+1)^{\delta^{\frac{tq+1}{2}}} = tq - (2i+1)$  and  $(2i+1)^{\delta^a} = 2tq - 2a - 2i$  which gives us a distance of

$$|2tq - 2a - 2i - (tq - (2i+1))|^p = |tq - 2a + 1|^p. \quad (19)$$

Moreover for all  $i \in [tq-a, \frac{tq-3}{2}]$  we have  $(2i+1)^{\delta^{\frac{tq+1}{2}}} = tq - (2i+1)$  and  $(2i+1)^{\delta^a} = 2a + 2i - 2tq + 1$  which gives us a distance of

$$|tq - (2i+1) - (2a + 2i - 2tq + 1)|^p = |3tq - 2 - 4i - 2a|^p. \quad (20)$$

Moreover  $tq^{\delta^{\frac{tq+1}{2}}} = 1$  and  $tq^{\delta^a} = 2a - tq$  with the distance

$$|1 - 2a + tq|^p. \quad (21)$$

Moreover for all  $i \in [0, tq-a-1]$  we have  $(tq - (2i+1))^{\delta^{\frac{tq+1}{2}}} = 2i+3$  and  $(tq - (2i+1))^{\delta^a} = 2a + 2i + 2 - tq$  which gives us a distance of

$$|2i+3 - (2a + 2i + 2 - tq)|^p = |tq - 2a + 1|^p. \quad (22)$$

Moreover for all  $i \in [tq-a, \frac{tq-3}{2}]$  we have  $(tq - (2i+1))^{\delta^{\frac{tq+1}{2}}} = 2i+3$  and  $(tq - (2i+1))^{\delta^a} = 3tq - 2a - 2i - 1$  which gives us a distance of

$$|3tq - 2a - 2i - 1 - (2i+3)|^p = |3tq - 4 - 4i - 2a|^p. \quad (23)$$

Summing over (19),(20),(21),(22) and (23) gives us

$$\begin{aligned}
p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^a\right) &= (2tq - 2a + 1)|tq - 2a + 1|^p \\
&+ \sum_{i=tq-a}^{\frac{tq-3}{2}} |3tq - 2 - 4i - 2a|^p + \sum_{i=tq-a}^{\frac{tq-3}{2}} |3tq - 4 - 4i - 2a|^p \\
&= (2tq - 2a + 1)|tq - 2a + 1|^p \\
&+ \sum_{i=0}^{a-\frac{tq+3}{2}} |2a - tq - 4i - 2|^p + \sum_{i=0}^{a-\frac{tq+3}{2}} |2a - tq - 4i - 4|^p \\
&= (2tq - 2a + 1)|tq - 2a + 1|^p + 2 \sum_{i=0}^{a-\frac{tq+3}{2}} |tq - 4i - 2 - 2a|^p \\
&= (2tq - 2a + 1)|tq - 2a + 1|^p + 2 \sum_{i=0}^{a-\frac{tq+3}{2}} (2i + 1)^p.
\end{aligned}$$

□

**Lemma 8.** Let  $t, q \geq 3$  be primes with  $t \neq q$ . Let  $0 \leq r, s < tq$  be the smallest positive integers satisfying

$$\begin{aligned}
s &\equiv 1 \pmod{t} & r &\equiv 0 \pmod{t} \\
s &\equiv 0 \pmod{q} & r &\equiv 1 \pmod{q}
\end{aligned}$$

and let  $\delta \in S_{tq}$  be the cycle defined by

$$\delta = (1, 3, 5, \dots, tq, tq - 1, tq - 3, \dots, 2).$$

Then the following holds

$$\begin{aligned}
p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^r\right) &= p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^s\right) = (tq - |s - r|) \cdot |s - r|^p + 2 \sum_{i=0}^{\frac{|s-r|}{2}-1} (2i + 1)^p \\
&< (tq - 1)^p + 2 \sum_{i=0}^{\frac{tq-3}{2}} (2i + 1)^p \\
&= p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^0\right) = p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^1\right).
\end{aligned}$$

*Proof.* We clearly have  $r \neq s$ . Moreover because of the above congruences we have  $r, s \notin \{0, 1\}$  and since  $1 < r, s < tq$  we obtain  $r + s = tq + 1$  which gives us  $r = tq + 1 - s$  and  $s = tq + 1 - r$ . In the case  $r < s$  we have  $1 < r < \frac{tq+1}{2}$  and  $\frac{tq+1}{2} < s < tq - 1$  and obtain by Lemma 7

$$p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^r\right) = (2r - 1) \cdot |tq - 2r + 1|^p + 2 \sum_{i=0}^{\frac{tq-1}{2}-r} (2i + 1)^p$$

and

$$p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^s\right) = (2tq - 2s + 1) \cdot |tq - 2s + 1|^p + 2 \sum_{i=0}^{s-\frac{tq+3}{2}} (2i + 1)^p.$$

Now we use  $r = tq + 1 - s$  and  $s = tq + 1 - r$  and obtain

$$\begin{aligned}
p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^r\right) &= (2r-1) \cdot |tq-2r+1|^p + 2 \sum_{i=0}^{\frac{tq-1}{2}-r} (2i+1)^p \\
&= (r+tq-(tq+1-r)) \cdot |-r+(tq+1-r)|^p + 2 \sum_{i=0}^{\frac{(tq+1-r)-r-2}{2}} (2i+1)^p \\
&= (r+tq-s) \cdot |-r+s|^p + 2 \sum_{i=0}^{\frac{s-r}{2}-1} (2i+1)^p \\
&= (tq-|s-r|) \cdot |s-r|^p + 2 \sum_{i=0}^{\frac{|s-r|}{2}-1} (2i+1)^p
\end{aligned}$$

and

$$\begin{aligned}
p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^s\right) &= (2tq-2s+1) \cdot |tq-2s+1|^p + 2 \sum_{i=0}^{s-\frac{tq+3}{2}} (2i+1)^p \\
&= (tq-s+(tq+1-s)) \cdot |-s+(tq+1-s)|^p + 2 \sum_{i=0}^{\frac{s-(tq+1-s)-2}{2}} (2i+1)^p \\
&= (tq-s+r) \cdot |-s+r|^p + 2 \sum_{i=0}^{\frac{s-r}{2}-1} (2i+1)^p \\
&= (tq-|s-r|) \cdot |s-r|^p + 2 \sum_{i=0}^{\frac{|s-r|}{2}-1} (2i+1)^p.
\end{aligned}$$

In the case  $r > s$  we have  $\frac{tq+1}{2} < r < tq-1$  and  $1 < s < \frac{tq+1}{2}$  and obtain by Lemma 7

$$p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^r\right) = (2tq-2r+1) \cdot |tq-2r+1|^p + 2 \sum_{i=0}^{r-\frac{tq+3}{2}} (2i+1)^p$$

and

$$p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^s\right) = (2s-1) \cdot |tq-2s+1|^p + 2 \sum_{i=0}^{\frac{tq-1}{2}-s} (2i+1)^p.$$

Now we use  $r = tq + 1 - s$  and  $s = tq + 1 - r$  and as above we analogously obtain

$$p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^s\right) = (tq-|r-s|) \cdot |r-s|^p + 2 \sum_{i=0}^{\frac{|r-s|}{2}-1} (2i+1)^p = p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^r\right).$$

By noting that  $|r-s| = |s-r|$  we finally obtain

$$p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^s\right) = (tq-|s-r|) \cdot |s-r|^p + 2 \sum_{i=0}^{\frac{|s-r|}{2}-1} (2i+1)^p = p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^r\right).$$

Furthermore by Lemma 7 we have

$$p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^0\right) = p\text{-val}\left(\delta^{\frac{tq+1}{2}}, \delta^1\right) = (tq-1)^p + 2 \sum_{i=0}^{\frac{tq-3}{2}} (2i+1)^p.$$

Moreover we have  $s - r \equiv 1 \pmod t$  and  $s - r \equiv -1 \pmod q$ . Thus  $|s - r| \not\equiv 1, -1 \pmod{tq}$  and hence  $2 \leq |s - r| \leq tq - 2$  from which it finally follows that

$$(tq - |s - r|) \cdot |s - r|^p + 2 \sum_{i=0}^{\frac{|s-r|}{2}-1} (2i+1)^p < (tq - 1)^p + 2 \sum_{i=0}^{\frac{tq-3}{2}} (2i+1)^p. \quad (24)$$

This is seen as follows: Inequation (24) holds if and only if

$$(tq - |s - r|) \cdot |s - r|^p < (tq - 1)^p + 2 \sum_{i=\frac{|s-r|}{2}}^{\frac{tq-3}{2}} (2i+1)^p.$$

We clearly have  $(tq - 1)^p > |s - r|^p$  and  $(2i + 1)^p > |s - r|^p$  for all  $i \in [\frac{|s-r|}{2}, \frac{tq-3}{2}]$ . Moreover we add up  $1 + 2(\frac{tq-3}{2} - \frac{|s-r|}{2} + 1) = tq - |s - r|$  numbers all of which are greater than  $|s - r|^p$ . Thus Inequation (24) is true.  $\square$

**Lemma 9.** *Let  $t \in \mathbb{N}$  be odd and let  $0 \leq t_1 < t_2 < t$  be such that  $t_1 \not\equiv t_2 \pmod q$  for all primes  $q$  with  $q \mid t$ . Moreover let  $\alpha, \beta \in S_t$  be the permutations that Theorem 5 yields regarding the solutions  $t_1, t_2$  i.e.  $l_\infty(\beta, \alpha^{t_1}) \leq 1$  and  $l_\infty(\beta, \alpha^{t_2}) \leq 1$ . Then*

$$p\text{-val}(\beta, \alpha^x) \begin{cases} = t - 1 & \text{if } x \equiv t_1, t_2 \pmod t \\ \geq 2^p(t - 1) & \text{if } x \not\equiv t_1, t_2 \pmod t. \end{cases}$$

*Proof.* Suppose  $x \equiv t_1, t_2 \pmod t$ . Then we have  $l_\infty(\beta, \alpha^x) \leq 1$ . The second part of Theorem 5 states that there is exactly one point  $i \in [1, t]$  such that  $i^{\alpha^x} = i^\beta$  and hence

$$p\text{-val}(\beta, \alpha^x) = t - 1.$$

Now suppose  $x \not\equiv t_1, t_2 \pmod t$ . For all  $i \in [1, t]$  there are at most 2 possible mappings such that the distance is exactly 1 namely if  $i^\beta = j$  then the distance is 1 if and only if  $i^{\alpha^x} \in \{j - 1, j + 1\}$ . However in the cases  $j = 1$  and  $j = t$  there is only one possible mapping such that the distance is 1. This gives a total of  $2(t - 2) + 2$  mappings where the distance is 1. However  $\alpha^{t_1}$  and  $\alpha^{t_2}$  cover  $t - 1$  of these mappings each giving us a total of  $2(t - 1)$  matches. Hence we have  $|i^{\alpha^x} - i^\beta| \geq 2$  except for the single point where the distance is 0 since the second part of Theorem 5 states that this single point exists for every exponent. By this we obtain

$$p\text{-val}(\beta, \alpha^x) = \sum_{i=1}^t |i^{\alpha^x} - i^\beta|^p \geq 2^p(t - 1) + 0^p = 2^p(t - 1).$$

$\square$

**Theorem 7.** *The SUBGROUP DISTANCE PROBLEM regarding the  $l_p$  distance and the SUBGROUP DISTANCE PROBLEM regarding the Lee distance are NP-complete when the input group is cyclic.*

*Proof.* Obviously the  $l_1$  distance reduces to the Lee distance by embedding  $S_n$  into  $S_{2n}$ . Then clearly  $|i^\tau - i^\pi| < 2n - |i^\tau - i^\pi|$  for all  $\tau, \pi \in S_n$ . Hence it suffices to show NP-completeness for the  $l_p$  distance.

We give a log-space reduction from Not-All-Equal 3SAT. Let  $X = \{x_1, \dots, x_n\}$  be a finite set of variables and  $C = \{c_1, \dots, c_m\}$  be a set of clauses over  $X$  in which every clause contains three different literals. Throughout the proof when we write  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  we always assume  $i_1 < i_2 < i_3$ . Let  $p_1 < \dots < p_n$  be the first  $n$  primes with  $p_1 \geq 3$ . Moreover let  $\bar{p}_1 < \dots < \bar{p}_n$  be the next  $n$  primes with  $\bar{p}_1 > p_n$ . We associate  $x_i$  with  $p_i$  and  $\bar{x}_i$  with  $\bar{p}_i$  for all  $i \in [1, n]$ . For all

$j \in [1, m]$  we define numbers  $r_{j,1}, r_{j,2}, r_{j,3}, s_{j,1}, s_{j,2}, s_{j,3}$  as the smallest positive integers satisfying the congruences

$$\begin{aligned} s_{j,1} &\equiv 1 \pmod{\tilde{p}_{i_2}} & r_{j,1} &\equiv 0 \pmod{\tilde{p}_{i_2}} \\ s_{j,1} &\equiv 0 \pmod{\tilde{p}_{i_3}} & r_{j,1} &\equiv 1 \pmod{\tilde{p}_{i_3}} \\ \\ s_{j,2} &\equiv 1 \pmod{\tilde{p}_{i_1}} & r_{j,2} &\equiv 0 \pmod{\tilde{p}_{i_1}} \\ s_{j,2} &\equiv 0 \pmod{\tilde{p}_{i_3}} & r_{j,2} &\equiv 1 \pmod{\tilde{p}_{i_3}} \\ \\ s_{j,3} &\equiv 1 \pmod{\tilde{p}_{i_1}} & r_{j,3} &\equiv 0 \pmod{\tilde{p}_{i_1}} \\ s_{j,3} &\equiv 0 \pmod{\tilde{p}_{i_2}} & r_{j,3} &\equiv 1 \pmod{\tilde{p}_{i_2}} \end{aligned}$$

in which we assume  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  and define

$$\tilde{p}_{i_l} = \begin{cases} p_{i_l} & \text{if } \tilde{x}_{i_l} = x_{i_l} \\ \bar{p}_{i_l} & \text{if } \tilde{x}_{i_l} = \bar{x}_{i_l}. \end{cases}$$

Moreover for all  $i \in [1, n]$  we define numbers  $r_i, s_i$  as the smallest positive integers satisfying

$$\begin{aligned} s_i &\equiv 1 \pmod{p_i} & r_i &\equiv 0 \pmod{p_i} \\ s_i &\equiv 0 \pmod{\bar{p}_i} & r_i &\equiv 1 \pmod{\bar{p}_i}. \end{aligned}$$

We will work with the group

$$G = \prod_{i=1}^n V_i \times \prod_{j=1}^m U_j$$

in which  $V_i = S_{p_i}^d \times S_{\bar{p}_i}^d \times S_{p_i \bar{p}_i}$  and  $U_j = S_{\tilde{p}_{i_2} \tilde{p}_{i_3}}^{b_{j,2} b_{j,3}} \times S_{\tilde{p}_{i_1} \tilde{p}_{i_3}}^{b_{j,1} b_{j,3}} \times S_{\tilde{p}_{i_1} \tilde{p}_{i_2}}^{b_{j,1} b_{j,2}}$  with  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  and the following

$$\begin{aligned} a_{j,1} &= (\tilde{p}_{i_2} \tilde{p}_{i_3} - |s_{j,1} - r_{j,1}|) \cdot |s_{j,1} - r_{j,1}|^p + 2 \sum_{i=0}^{\frac{|s_{j,1} - r_{j,1}|}{2} - 1} (2i+1)^p \\ a_{j,2} &= (\tilde{p}_{i_1} \tilde{p}_{i_3} - |s_{j,2} - r_{j,2}|) \cdot |s_{j,2} - r_{j,2}|^p + 2 \sum_{i=0}^{\frac{|s_{j,2} - r_{j,2}|}{2} - 1} (2i+1)^p \\ a_{j,3} &= (\tilde{p}_{i_1} \tilde{p}_{i_2} - |s_{j,3} - r_{j,3}|) \cdot |s_{j,3} - r_{j,3}|^p + 2 \sum_{i=0}^{\frac{|s_{j,3} - r_{j,3}|}{2} - 1} (2i+1)^p \end{aligned}$$

and

$$\begin{aligned} b_{j,1} &= (\tilde{p}_{i_2} \tilde{p}_{i_3} - 1)^p + 2 \sum_{i=0}^{\frac{\tilde{p}_{i_2} \tilde{p}_{i_3} - 3}{2}} (2i+1)^p - a_{j,1} \\ b_{j,2} &= (\tilde{p}_{i_1} \tilde{p}_{i_3} - 1)^p + 2 \sum_{i=0}^{\frac{\tilde{p}_{i_1} \tilde{p}_{i_3} - 3}{2}} (2i+1)^p - a_{j,2} \\ b_{j,3} &= (\tilde{p}_{i_1} \tilde{p}_{i_2} - 1)^p + 2 \sum_{i=0}^{\frac{\tilde{p}_{i_1} \tilde{p}_{i_2} - 3}{2}} (2i+1)^p - a_{j,3} \end{aligned}$$

and

$$d = \left\lceil \frac{\sum_{i=1}^n (p_i \bar{p}_i - 1) + \sum_{j=1}^m (a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} + b_{j,1} b_{j,2} b_{j,3})}{2^p - 1} \right\rceil$$

Note that  $b_{j,l} > 0$  by Lemma 8 and  $s_{j,l} - r_{j,l}$  is even for all  $l \in [1, 3]$ . The latter is seen as follows: since we have  $2 \leq s_{j,l}, r_{j,l} < \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}}{\tilde{p}_{i_l}}$  and  $s_{j,l} + r_{j,l} \equiv 1 \pmod{\frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}}{\tilde{p}_{i_l}}}$  we obtain  $s_{j,l} + r_{j,l} = 1 + \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}}{\tilde{p}_{i_l}}$  and thus  $s_{j,l} - r_{j,l} = 1 + \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}}{\tilde{p}_{i_l}} - 2r_{j,l}$ .  $G$  naturally embeds into  $S_N$  for

$$N = \sum_{i=1}^n (d(p_i + \bar{p}_i) + p_i \bar{p}_i) + \sum_{c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\} \in C} (\tilde{p}_{i_2} \tilde{p}_{i_3} b_{j,2} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_3} b_{j,1} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_2} b_{j,1} b_{j,2}).$$

Before we define the input group elements let us define auxiliary permutations as follows: for all  $i \in [1, n]$  we define permutations that Theorem 5 yields such that

$$l_\infty(\eta_{i,1}, \zeta_{i,1}^0) \leq 1 \text{ and } l_\infty(\eta_{i,1}, \zeta_{i,1}^1) \leq 1 \text{ in which } \zeta_{i,1}, \eta_{i,1} \in S_{p_i}$$

$$l_\infty(\eta_{i,2}, \zeta_{i,2}^0) \leq 1 \text{ and } l_\infty(\eta_{i,2}, \zeta_{i,2}^1) \leq 1 \text{ in which } \zeta_{i,2}, \eta_{i,2} \in S_{\bar{p}_i}$$

and

$$l_\infty(\eta_{i,3}, \zeta_{i,3}^{r_i}) \leq 1 \text{ and } l_\infty(\eta_{i,3}, \zeta_{i,3}^{s_i}) \leq 1 \text{ in which } \zeta_{i,3}, \eta_{i,3} \in S_{p_i \bar{p}_i}.$$

Note that these permutations can be constructed in log-space. Now we define the input group elements  $\tau, \pi \in G$  as follows where  $i$  ranges over  $[1, n]$  and  $j$  ranges over  $[1, m]$  and  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ :

$$\tau = (\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$$

with

$$\begin{aligned} \alpha_i &= (\bar{\alpha}_{i,1}^d, \bar{\alpha}_{i,2}^d, \alpha_{i,3}) & \beta_j &= (\bar{\beta}_{j,1}^{b_{j,2} b_{j,3}}, \bar{\beta}_{j,2}^{b_{j,1} b_{j,3}}, \bar{\beta}_{j,3}^{b_{j,1} b_{j,2}}) \\ \alpha_{i,1} &= \eta_{i,1} & \beta_{j,1} &= (1, 3, 5, \dots, \tilde{p}_{i_2} \tilde{p}_{i_3}, \tilde{p}_{i_2} \tilde{p}_{i_3} - 1, \tilde{p}_{i_2} \tilde{p}_{i_3} - 3, \dots, 2)^{\frac{\tilde{p}_{i_2} \tilde{p}_{i_3} + 1}{2}} \\ \alpha_{i,2} &= \eta_{i,2} & \beta_{j,2} &= (1, 3, 5, \dots, \tilde{p}_{i_1} \tilde{p}_{i_3}, \tilde{p}_{i_1} \tilde{p}_{i_3} - 1, \tilde{p}_{i_1} \tilde{p}_{i_3} - 3, \dots, 2)^{\frac{\tilde{p}_{i_1} \tilde{p}_{i_3} + 1}{2}} \\ \alpha_{i,3} &= \eta_{i,3} & \beta_{j,3} &= (1, 3, 5, \dots, \tilde{p}_{i_1} \tilde{p}_{i_2}, \tilde{p}_{i_1} \tilde{p}_{i_2} - 1, \tilde{p}_{i_1} \tilde{p}_{i_2} - 3, \dots, 2)^{\frac{\tilde{p}_{i_1} \tilde{p}_{i_2} + 1}{2}} \end{aligned}$$

and

$$\pi = (\gamma_1, \dots, \gamma_n, \delta_1, \dots, \delta_m)$$

with

$$\begin{aligned} \gamma_i &= (\bar{\gamma}_{i,1}^d, \bar{\gamma}_{i,2}^d, \gamma_{i,3}) & \delta_j &= (\bar{\delta}_{j,1}^{b_{j,2} b_{j,3}}, \bar{\delta}_{j,2}^{b_{j,1} b_{j,3}}, \bar{\delta}_{j,3}^{b_{j,1} b_{j,2}}) \\ \gamma_{i,1} &= \zeta_{i,1} & \delta_{j,1} &= (1, 3, 5, \dots, \tilde{p}_{i_2} \tilde{p}_{i_3}, \tilde{p}_{i_2} \tilde{p}_{i_3} - 1, \tilde{p}_{i_2} \tilde{p}_{i_3} - 3, \dots, 2) \\ \gamma_{i,2} &= \zeta_{i,2} & \delta_{j,2} &= (1, 3, 5, \dots, \tilde{p}_{i_1} \tilde{p}_{i_3}, \tilde{p}_{i_1} \tilde{p}_{i_3} - 1, \tilde{p}_{i_1} \tilde{p}_{i_3} - 3, \dots, 2) \\ \gamma_{i,3} &= \zeta_{i,3} & \delta_{j,3} &= (1, 3, 5, \dots, \tilde{p}_{i_1} \tilde{p}_{i_2}, \tilde{p}_{i_1} \tilde{p}_{i_2} - 1, \tilde{p}_{i_1} \tilde{p}_{i_2} - 3, \dots, 2) \end{aligned}$$

and finally we define

$$k = \sum_{i=1}^n (d(p_i - 1) + d(\bar{p}_i - 1) + p_i \bar{p}_i - 1) + \sum_{j=1}^m (a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} + b_{j,1} b_{j,2} b_{j,3}).$$

To ensure that the  $p^{\text{th}}$  root will be an integer we add  $k^{p-1} - 1$  copies. Then we clearly have that there is  $x \in \mathbb{N}$  such that  $l_p \left( \bar{\pi}^{(k^{p-1})}, \left( \bar{\pi}^{(k^{p-1})} \right)^x \right) \leq k$  if and only if there is  $x \in \mathbb{N}$  such that  $p\text{-val}(\tau, \pi^x) \leq k$ . Now we will show there is  $x \in \mathbb{N}$  such that  $p\text{-val}(\tau, \pi^x) \leq k$  if and only if  $X, C$  is a positive instance of **Not-All-Equal 3SAT**.

Suppose there is  $x \in \mathbb{N}$  such that  $p\text{-val}(\tau, \pi^x) \leq k$ .



**Claim 16.** For all  $i \in [1, n]$  we have  $x \equiv 0, 1 \pmod{p_i}$  and  $x \equiv 0, 1 \pmod{\bar{p}_i}$  and

$$\begin{aligned} p\text{-val}(\bar{\alpha}_{i,1}^d, (\bar{\gamma}_{i,1}^d)^x) &= d(p_i - 1) \\ p\text{-val}(\bar{\alpha}_{i,2}^d, (\bar{\gamma}_{i,2}^d)^x) &= d(\bar{p}_i - 1). \end{aligned}$$

We have by Lemma 9

$$p\text{-val}(\alpha_{i,1}, \gamma_{i,1}^x) = \begin{cases} = p_i - 1 & \text{if } x \equiv 0, 1 \pmod{p_i} \\ \geq 2^p(p_i - 1) & \text{if } x \not\equiv 0, 1 \pmod{p_i} \end{cases}$$

and

$$p\text{-val}(\alpha_{i,2}, \gamma_{i,2}^x) = \begin{cases} = \bar{p}_i - 1 & \text{if } x \equiv 0, 1 \pmod{\bar{p}_i} \\ \geq 2^p(\bar{p}_i - 1) & \text{if } x \not\equiv 0, 1 \pmod{\bar{p}_i}. \end{cases}$$

From this we obtain

$$p\text{-val}(\bar{\alpha}_{i,1}^d, (\bar{\gamma}_{i,1}^d)^x) \begin{cases} = d(p_i - 1) & \text{if } x \equiv 0, 1 \pmod{p_i} \\ \geq 2^p d(p_i - 1) & \text{if } x \not\equiv 0, 1 \pmod{p_i} \end{cases}$$

and

$$p\text{-val}(\bar{\alpha}_{i,2}^d, (\bar{\gamma}_{i,2}^d)^x) \begin{cases} = d(\bar{p}_i - 1) & \text{if } x \equiv 0, 1 \pmod{\bar{p}_i} \\ \geq 2^p d(\bar{p}_i - 1) & \text{if } x \not\equiv 0, 1 \pmod{\bar{p}_i}. \end{cases}$$

Now suppose there is an  $e \in [1, n]$  such that  $x \not\equiv 0, 1 \pmod{p_e}$  or  $x \not\equiv 0, 1 \pmod{\bar{p}_e}$ . Then

$$\begin{aligned} p\text{-val}(\bar{\alpha}_{e,1}^d, (\bar{\gamma}_{e,1}^d)^x) &\geq 2^p d(p_e - 1) = (2^p - 1)d(p_e - 1) + d(p_e - 1) \\ \text{or } p\text{-val}(\bar{\alpha}_{e,2}^d, (\bar{\gamma}_{e,2}^d)^x) &\geq 2^p d(\bar{p}_e - 1) = (2^p - 1)d(\bar{p}_e - 1) + d(\bar{p}_e - 1). \end{aligned}$$

By using the above lower bounds and the following trivial lower bounds  $p\text{-val}(\alpha_{i,3}, \gamma_{i,3}^x) \geq 0$  for all  $i \in [1, n]$  and  $p\text{-val}(\beta_{j,l}, \delta_{j,l}^x) \geq 0$  and hence

$$p\text{-val}\left(\bar{\beta}_{j,l}^{\frac{b_{j,1}b_{j,2}b_{j,3}}{b_{j,l}}}, \left(\bar{\delta}_{j,l}^{\frac{b_{j,1}b_{j,2}b_{j,3}}{b_{j,l}}}\right)^x\right) \geq 0$$

for all  $j \in [1, m]$  and  $l \in [1, 3]$  we obtain in the case  $x \not\equiv 0, 1 \pmod{p_e}$

$$\begin{aligned} p\text{-val}(\tau, \pi^x) &\geq \sum_{i=1}^n (d(p_i - 1) + d(\bar{p}_i - 1)) + (2^p - 1)d(p_e - 1) \\ &\geq \sum_{i=1}^n (d(p_i - 1) + d(\bar{p}_i - 1)) \\ &\quad + (p_e - 1)\left(\sum_{i=1}^n (p_i \bar{p}_i - 1) + \sum_{j=1}^m (a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3})\right) \\ &= \sum_{i=1}^n (d(p_i - 1) + d(\bar{p}_i - 1) + (p_i \bar{p}_i - 1)) \\ &\quad + \sum_{j=1}^m (a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3}) \\ &\quad + (p_e - 2)\left(\sum_{i=1}^n (p_i \bar{p}_i - 1) + \sum_{j=1}^m (a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3})\right) \\ &= k + (p_e - 2)\left(\sum_{i=1}^n (p_i \bar{p}_i - 1) + \sum_{j=1}^m (a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3})\right) \\ &> k \end{aligned}$$

which is a contradiction. In the case  $x \not\equiv 0, 1 \pmod{\bar{p}_e}$  we analogously obtain  $p\text{-val}(\tau, \pi^x) > k$  and by this a contradiction in both cases. Thus  $x \equiv 0, 1 \pmod{p_i}$  and  $x \equiv 0, 1 \pmod{\bar{p}_i}$  and

$$\begin{aligned} p\text{-val}(\bar{\alpha}_{i,1}^d, (\bar{\gamma}_{i,1}^d)^x) &= d(p_i - 1) \\ p\text{-val}(\bar{\alpha}_{i,2}^d, (\bar{\gamma}_{i,2}^d)^x) &= d(\bar{p}_i - 1) \end{aligned}$$

for all  $i \in [1, n]$ . □

**Claim 17.** For all  $j \in [1, m]$  we have

$$p\text{-val}(\beta_j, \delta_j^x) = \begin{cases} a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + 3b_{j,1}b_{j,2}b_{j,3} & \text{if } x \equiv 0, 1 \pmod{\tilde{p}_{i_1}\tilde{p}_{i_2}\tilde{p}_{i_3}} \\ a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3} & \text{if } x \not\equiv 0, 1 \pmod{\tilde{p}_{i_1}\tilde{p}_{i_2}\tilde{p}_{i_3}} \end{cases}$$

in which  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ .

Suppose  $x \equiv 0, 1 \pmod{\tilde{p}_{i_1}\tilde{p}_{i_2}\tilde{p}_{i_3}}$ . Then we have for all  $l \in [1, 3]$  by Lemma 8

$$\begin{aligned} p\text{-val}(\beta_{j,l}, \delta_{j,l}^x) &= p\text{-val}\left(\delta_{j,l}^{\frac{\tilde{p}_{i_1}\tilde{p}_{i_2}\tilde{p}_{i_3} + \tilde{p}_{i_l}}{2\tilde{p}_{i_l}}}, \delta_{j,l}^x\right) \\ &= \left(\frac{\tilde{p}_{i_1}\tilde{p}_{i_2}\tilde{p}_{i_3}}{\tilde{p}_{i_l}} - 1\right)^p + 2 \sum_{i=0}^{\frac{\tilde{p}_{i_1}\tilde{p}_{i_2}\tilde{p}_{i_3} - 3\tilde{p}_{i_l}}{2\tilde{p}_{i_l}}} (2i+1)^p \\ &= a_{j,l} + b_{j,l}. \end{aligned}$$

Thus

$$p\text{-val}\left(\beta_{j,l}^{\frac{b_{j,1}b_{j,2}b_{j,3}}{b_{j,l}}}, \left(\delta_{j,l}^{\frac{b_{j,1}b_{j,2}b_{j,3}}{b_{j,l}}}\right)^x\right) = \frac{b_{j,1}b_{j,2}b_{j,3}}{b_{j,l}}(a_{j,l} + b_{j,l})$$

from which it follows now that

$$\begin{aligned} p\text{-val}(\beta_j, \delta_j^x) &= b_{j,2}b_{j,3}(a_{j,1} + b_{j,1}) + b_{j,1}b_{j,3}(a_{j,2} + b_{j,2}) + b_{j,1}b_{j,2}(a_{j,3} + b_{j,3}) \\ &= a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + 3b_{j,1}b_{j,2}b_{j,3}. \end{aligned}$$

Now suppose  $x \not\equiv 0, 1 \pmod{\tilde{p}_{i_1}\tilde{p}_{i_2}\tilde{p}_{i_3}}$ . By Claim 16 we have  $x \equiv 0, 1 \pmod{\tilde{p}_i}$  for all  $i \in [1, n]$ . Thus there are  $g, h \in [1, 3]$  and  $c \in \{0, 1\}$  with  $g \neq h$  such that  $x \equiv c \pmod{\tilde{p}_{i_g}}$  and  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$  and let w.l.o.g.  $f \in [1, 3] \setminus \{g, h\}$  be such that  $x \equiv c \pmod{\tilde{p}_{i_f}}$ . Then we obtain by Lemma 8

$$\begin{aligned} p\text{-val}(\beta_{j,h}, \delta_{j,h}^x) &= p\text{-val}\left(\delta_{j,h}^{\frac{\tilde{p}_{i_g}\tilde{p}_{i_f} + 1}{2}}, \delta_{j,h}^x\right) \\ &= p\text{-val}\left(\delta_{j,h}^{\frac{\tilde{p}_{i_g}\tilde{p}_{i_f} + 1}{2}}, \delta_{j,h}^c\right) \\ &= (\tilde{p}_{i_g}\tilde{p}_{i_f} - 1)^p + 2 \sum_{i=0}^{\frac{\tilde{p}_{i_g}\tilde{p}_{i_f} - 3}{2}} (2i+1)^p \\ &= a_{j,h} + b_{j,h}. \end{aligned}$$

Moreover we have  $x \equiv s_{j,f} \pmod{\tilde{p}_{i_g}\tilde{p}_{i_h}}$  and  $x \equiv s_{j,g} \pmod{\tilde{p}_{i_f}\tilde{p}_{i_h}}$  or  $x \equiv r_{j,f} \pmod{\tilde{p}_{i_g}\tilde{p}_{i_h}}$  and  $x \equiv r_{j,g} \pmod{\tilde{p}_{i_f}\tilde{p}_{i_h}}$ . Then Lemma 8 gives us

$$\begin{aligned} p\text{-val}(\beta_{j,f}, \delta_{j,f}^x) &= p\text{-val}\left(\delta_{j,f}^{\frac{\tilde{p}_{i_g}\tilde{p}_{i_h} + 1}{2}}, \delta_{j,f}^x\right) \\ &= (\tilde{p}_{i_g}\tilde{p}_{i_h} - |s_{j,f} - r_{j,f}|) \cdot |s_{j,f} - r_{j,f}|^p + 2 \sum_{i=0}^{\frac{|s_{j,f} - r_{j,f}| - 1}{2}} (2i+1)^p \\ &= a_{j,f} \end{aligned}$$

and

$$\begin{aligned}
p\text{-val}(\beta_{j,g}, \delta_{j,g}^x) &= p\text{-val}\left(\delta_{j,g}^{\frac{\bar{p}_{i_f}\bar{p}_{i_h}+1}{2}}, \delta_{j,g}^x\right) \\
&= (\tilde{p}_{i_f}\tilde{p}_{i_h} - |s_{j,g} - r_{j,g}|) \cdot |s_{j,g} - r_{j,g}|^p + 2 \sum_{i=0}^{\frac{|s_{j,g}-r_{j,g}|-1}{2}} (2i+1)^p \\
&= a_{j,g}.
\end{aligned}$$

Thus

$$\begin{aligned}
p\text{-val}\left(\bar{\beta}_{j,h}^{b_{j,f}b_{j,g}}, \left(\bar{\delta}_{j,h}^{b_{j,f}b_{j,g}}\right)^x\right) &= b_{j,f}b_{j,g}(a_{j,h} + b_{j,h}) \\
p\text{-val}\left(\bar{\beta}_{j,f}^{b_{j,h}b_{j,g}}, \left(\bar{\delta}_{j,f}^{b_{j,h}b_{j,g}}\right)^x\right) &= b_{j,h}b_{j,g}a_{j,f}
\end{aligned}$$

and

$$p\text{-val}\left(\bar{\beta}_{j,g}^{b_{j,h}b_{j,f}}, \left(\bar{\delta}_{j,g}^{b_{j,h}b_{j,f}}\right)^x\right) = b_{j,h}b_{j,f}a_{j,g}.$$

From this it finally follows that

$$\begin{aligned}
p\text{-val}(\beta_j, \delta_j^x) &= b_{j,f}b_{j,g}(a_{j,h} + b_{j,h}) + b_{j,h}b_{j,g}a_{j,f} + b_{j,h}b_{j,f}a_{j,g} \\
&= a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3}.
\end{aligned}$$

□

**Claim 18.** For all  $i \in [1, n]$  we have  $x \equiv 1 \pmod{p_i}$  and  $x \equiv 0 \pmod{\bar{p}_i}$  or  $x \equiv 0 \pmod{p_i}$  and  $x \equiv 1 \pmod{\bar{p}_i}$ .

Suppose there is an  $e \in [1, n]$  for which the contrary holds. By Claim 16 we have  $x \equiv 0, 1 \pmod{p_e}$  and  $x \equiv 0, 1 \pmod{\bar{p}_e}$ . Therefore it suffices to consider the cases  $x \equiv 0, 1 \pmod{p_e\bar{p}_e}$ . Then by Lemma 9 we have  $p\text{-val}(\alpha_{e,3}, \gamma_{e,3}^x) \geq 2^p(p_e\bar{p}_e - 1)$ . Summing over all lower bounds Claim 16, 17 and Lemma 9 yield we obtain

$$\begin{aligned}
p\text{-val}(\tau, \pi^x) &\geq \sum_{i=1}^n (d(2p_i - 1) + d(2\bar{p}_i - 1) + p_i\bar{p}_i - 1) - (p_e\bar{p}_e - 1) + 2^p(p_e\bar{p}_e - 1) \\
&\quad + \sum_{j=1}^m (a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3}) \\
&= \sum_{i=1}^n (d(2p_i - 1) + d(2\bar{p}_i - 1) + p_i\bar{p}_i - 1) + (2^p - 1)(p_e\bar{p}_e - 1) \\
&\quad + \sum_{j=1}^m (a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3}) \\
&= k + (2^p - 1)(p_e\bar{p}_e - 1) \\
&> k
\end{aligned}$$

which is a contradiction. □

**Claim 19.** For every clause  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  the following holds: If there are  $f, g \in [1, 3]$  with  $f \neq g$  and  $c \in \{0, 1\}$  such that  $x \equiv c \pmod{\tilde{p}_{i_f}}$  and  $x \equiv c \pmod{\tilde{p}_{i_g}}$  then  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$  where  $h$  is the unique element in  $[1, 3] \setminus \{f, g\}$ .

Suppose there is a clause  $c_e = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  such that  $x \equiv c \pmod{\tilde{p}_{i_l}}$  for all  $l \in [1, 3]$  and some  $c \in \{0, 1\}$ . Then we have by Claim 17

$$p\text{-val}(\beta_e, \delta_e^x) = a_{e,1}b_{e,2}b_{e,3} + a_{e,2}b_{e,1}b_{e,3} + a_{e,3}b_{e,1}b_{e,2} + 3b_{e,1}b_{e,2}b_{e,3}.$$

Summing over all lower bounds Claim 16,17 and Lemma 9 yield we obtain

$$\begin{aligned}
p\text{-val}(\tau, \pi^x) &\geq \sum_{i=1}^n (d(p_i - 1) + d(\bar{p}_i - 1) + p_i \bar{p}_i - 1) \\
&\quad + \sum_{j=1}^m (a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} + b_{j,1} b_{j,2} b_{j,3}) \\
&\quad - (a_{e,1} b_{e,2} b_{e,3} + a_{e,2} b_{e,1} b_{e,3} + a_{e,3} b_{e,1} b_{e,2} + b_{e,1} b_{e,2} b_{e,3}) \\
&\quad + (a_{e,1} b_{e,2} b_{e,3} + a_{e,2} b_{e,1} b_{e,3} + a_{e,3} b_{e,1} b_{e,2} + 3b_{e,1} b_{e,2} b_{e,3}) \\
&= k + 2b_{e,1} b_{e,2} b_{e,3} \\
&> k
\end{aligned}$$

which is a contradiction. Hence we obtain for every clause  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ : If there are  $f, g \in [1, 3]$  with  $f \neq g$  and  $c \in \{0, 1\}$  such that  $x \equiv c \pmod{\tilde{p}_{i_f}}$  and  $x \equiv c \pmod{\tilde{p}_{i_g}}$  then  $x \not\equiv c \pmod{\tilde{p}_{i_h}}$  where  $h$  is the unique element in  $[1, 3] \setminus \{f, g\}$ . Since by Claim 16 we have  $x \equiv 0, 1 \pmod{\tilde{p}_{i_h}}$  we finally obtain  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$ .  $\square$

Now we define a truth assignment  $\sigma$  by the following:

$$\sigma(x_i) = \begin{cases} 1 & \text{if } x \equiv 1 \pmod{p_i} \\ 0 & \text{if } x \equiv 0 \pmod{p_i} \end{cases}$$

for all  $i \in [1, n]$ . Let  $\hat{\sigma}$  be the extension of  $\sigma$  to literals. Now we will show for every clause  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  there are pairwise different numbers  $f, g, h \in [1, 3]$  and  $c \in \{0, 1\}$  such that

$$\begin{aligned}
\hat{\sigma}(\tilde{x}_{i_f}) &= c \\
\hat{\sigma}(\tilde{x}_{i_g}) &= c \\
\hat{\sigma}(\tilde{x}_{i_h}) &= 1 - c.
\end{aligned}$$

By Claim 16 we have  $x \equiv 0, 1 \pmod{p_i}$  and  $x \equiv 0, 1 \pmod{\bar{p}_i}$  for all  $i \in [1, n]$ . Hence there clearly are  $f, g \in [1, 3]$  with  $f \neq g$  and  $c \in \{0, 1\}$  such that  $x \equiv c \pmod{\tilde{p}_{i_f}}$  and  $x \equiv c \pmod{\tilde{p}_{i_g}}$ . In the case  $\tilde{p}_{i_f} = p_{i_f}$  we obtain  $\sigma(x_{i_f}) = c$  and hence  $\hat{\sigma}(\tilde{x}_{i_f}) = c$ . In the case  $\tilde{p}_{i_f} = \bar{p}_{i_f}$  we have  $x \equiv 1 - c \pmod{p_{i_f}}$  by Claim 18. Thus  $\sigma(x_{i_f}) = 1 - c$  and  $\hat{\sigma}(\tilde{x}_{i_f}) = c$ . Analogously we obtain  $\hat{\sigma}(\tilde{x}_{i_g}) = c$ . Since we have  $x \equiv c \pmod{\tilde{p}_{i_f}}$  and  $x \equiv c \pmod{\tilde{p}_{i_g}}$  we obtain  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$  by Claim 19. As above we then analogously obtain  $\hat{\sigma}(\tilde{x}_{i_h}) = 1 - c$  which eventually shows that  $X, C$  is a positive instance of Not-All-Equal 3SAT.

Vice versa suppose  $X, C$  is a positive instance of Not-All-Equal 3SAT and let  $\sigma$  be a truth assignment such that for every clause  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  there are pairwise different numbers  $f, g, h \in [1, 3]$  and  $c \in \{0, 1\}$  such that

$$\begin{aligned}
\hat{\sigma}(\tilde{x}_{i_f}) &= c \\
\hat{\sigma}(\tilde{x}_{i_g}) &= c \\
\hat{\sigma}(\tilde{x}_{i_h}) &= 1 - c.
\end{aligned}$$

Then we define  $x$  as the smallest positive integer satisfying  $x \equiv \sigma(x_i) \pmod{p_i}$  and  $x \equiv 1 - \sigma(x_i) \pmod{\bar{p}_i}$  for all  $i \in [1, n]$ . Then we have  $x \equiv s_i, r_i \pmod{p_i \bar{p}_i}$  for all  $i \in [1, n]$ . Then by Lemma 9 we obtain

$$\begin{aligned}
p\text{-val}(\alpha_{i,1}, \gamma_{i,1}^x) &= p_i - 1 \\
p\text{-val}(\alpha_{i,2}, \gamma_{i,2}^x) &= \bar{p}_i - 1
\end{aligned}$$

and

$$p\text{-val}(\alpha_{i,3}, \gamma_{i,3}^x) = p_i \bar{p}_i - 1.$$

Thus

$$\begin{aligned} p\text{-val}(\bar{\alpha}_{i,1}^d, (\bar{\gamma}_{i,1}^d)^x) &= d(p_i - 1) \\ p\text{-val}(\bar{\alpha}_{i,2}^d, (\bar{\gamma}_{i,2}^d)^x) &= d(\bar{p}_i - 1) \end{aligned}$$

and

$$p\text{-val}(\alpha_i, \gamma_i^x) = d(p_i - 1) + d(\bar{p}_i - 1) + p_i \bar{p}_i - 1. \quad (25)$$

Let  $j \in [1, m]$  and suppose  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ . Then there are pairwise different numbers  $f, g, h \in [1, 3]$  and  $c \in \{0, 1\}$  such that

$$\begin{aligned} \hat{\sigma}(\tilde{x}_{i_f}) &= c \\ \hat{\sigma}(\tilde{x}_{i_g}) &= c \\ \hat{\sigma}(\tilde{x}_{i_h}) &= 1 - c. \end{aligned}$$

By definition we have  $x \equiv \sigma(x_i) \pmod{p_i}$  and  $x \equiv 1 - \sigma(x_i) \pmod{\bar{p}_i}$  for all  $i \in [1, n]$  which gives us

$$x \equiv \begin{cases} \sigma(x_{i_f}) \equiv \hat{\sigma}(x_{i_f}) \equiv c \pmod{p_{i_f}} & \text{if } \tilde{x}_{i_f} = x_{i_f} \\ 1 - \sigma(x_{i_f}) \equiv \hat{\sigma}(\tilde{x}_{i_f}) \equiv c \pmod{\bar{p}_{i_f}} & \text{if } \tilde{x}_{i_f} = \tilde{x}_{i_f} \end{cases}$$

and hence  $x \equiv c \pmod{\tilde{p}_{i_f}}$ . Analogously we obtain  $x \equiv c \pmod{\tilde{p}_{i_g}}$  and  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$ . Then we have  $x \equiv s_{j,f}, r_{j,f} \pmod{\tilde{p}_{i_f}}$  and  $x \equiv s_{j,g}, r_{j,g} \pmod{\tilde{p}_{i_g}}$  and we obtain by Lemma 8

$$\begin{aligned} p\text{-val}(\beta_{j,f}, \delta_{j,f}^x) &= p\text{-val}\left(\delta_{j,f}^{\frac{\tilde{p}_{i_g} \tilde{p}_{i_h} + 1}{2}}, \delta_{j,f}^x\right) \\ &= (\tilde{p}_{i_g} \tilde{p}_{i_h} - |s_{j,f} - r_{j,f}|) \cdot |s_{j,f} - r_{j,f}|^p + 2 \sum_{i=0}^{\frac{|s_{j,f} - r_{j,f}|}{2} - 1} (2i + 1)^p \\ &= a_{j,f} \end{aligned}$$

and

$$\begin{aligned} p\text{-val}(\beta_{j,g}, \delta_{j,g}^x) &= p\text{-val}\left(\delta_{j,g}^{\frac{\tilde{p}_{i_f} \tilde{p}_{i_h} + 1}{2}}, \delta_{j,g}^x\right) \\ &= (\tilde{p}_{i_f} \tilde{p}_{i_h} - |s_{j,g} - r_{j,g}|) \cdot |s_{j,g} - r_{j,g}|^p + 2 \sum_{i=0}^{\frac{|s_{j,g} - r_{j,g}|}{2} - 1} (2i + 1)^p \\ &= a_{j,g} \end{aligned}$$

and

$$\begin{aligned} p\text{-val}(\beta_{j,h}, \delta_{j,h}^x) &= p\text{-val}\left(\delta_{j,h}^{\frac{\tilde{p}_{i_g} \tilde{p}_{i_f} + 1}{2}}, \delta_{j,h}^x\right) \\ &= p\text{-val}\left(\delta_{j,h}^{\frac{\tilde{p}_{i_g} \tilde{p}_{i_f} + 1}{2}}, \delta_{j,h}^c\right) \\ &= (\tilde{p}_{i_g} \tilde{p}_{i_f} - 1)^p + 2 \sum_{i=0}^{\frac{\tilde{p}_{i_g} \tilde{p}_{i_f} - 3}{2}} (2i + 1)^p \\ &= a_{j,h} + b_{j,h}. \end{aligned}$$

By this we obtain

$$\begin{aligned} p\text{-val}\left(\bar{\beta}_{j,f}^{b_{j,g} b_{j,h}}, \left(\bar{\delta}_{j,f}^{b_{j,g} b_{j,h}}\right)^x\right) &= b_{j,g} b_{j,h} a_{j,f} \\ p\text{-val}\left(\bar{\beta}_{j,g}^{b_{j,f} b_{j,h}}, \left(\bar{\delta}_{j,g}^{b_{j,f} b_{j,h}}\right)^x\right) &= b_{j,f} b_{j,h} a_{j,g} \end{aligned}$$

and

$$p\text{-val}\left(\bar{\beta}_{j,h}^{b_{j,f}b_{j,g}}, \left(\bar{\delta}_{j,h}^{b_{j,f}b_{j,g}}\right)^x\right) = b_{j,f}b_{j,g}(a_{j,h} + b_{j,h}).$$

From this it follows now that

$$\begin{aligned} p\text{-val}(\beta_j, \delta_j^x) &= b_{j,g}b_{j,h}a_{j,f} + b_{j,f}b_{j,h}a_{j,g} + b_{j,f}b_{j,g}(a_{j,h} + b_{j,h}) \\ &= a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3}. \end{aligned} \quad (26)$$

Using (25) and (26) and summing up we finally obtain

$$\begin{aligned} p\text{-val}(\tau, \pi^x) &= \sum_{i=1}^n (d(p_i - 1) + d(\bar{p}_i - 1) + p_i\bar{p}_i - 1) \\ &\quad + \sum_{j=1}^m (a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3}) \\ &= k. \end{aligned}$$

□

### 3.5 Kendall's tau Distance

**Lemma 10.** *Let  $p, q \geq 3$  be primes with  $p \neq q$ . Let  $0 \leq r, s < pq$  be the smallest positive integers satisfying*

$$\begin{aligned} s &\equiv 1 \pmod{p} & r &\equiv 0 \pmod{p} \\ s &\equiv 0 \pmod{q} & r &\equiv 1 \pmod{q}. \end{aligned}$$

*Then the following holds:*

$$\frac{pq+1}{2} < pq - \left| \frac{pq+1}{2} - r \right| = pq - \left| \frac{pq+1}{2} - s \right|.$$

*Proof.* Note that because of the congruences we clearly have  $r, s \notin \{0, 1\}$ . Moreover note that because of  $r + s \equiv 1 \pmod{pq}$  and  $2 \leq r, s < pq$  it follows that  $r + s = pq + 1$  which gives us  $s = pq + 1 - r$  and  $r = pq + 1 - s$ . If  $r \leq \frac{pq+1}{2}$  we have

$$pq - \left| \frac{pq+1}{2} - r \right| = pq - \frac{pq+1}{2} + r = \frac{pq-1}{2} + r \geq \frac{pq-1}{2} + 2 > \frac{pq+1}{2}$$

and

$$pq - \left| \frac{pq+1}{2} - s \right| = pq - \left| \frac{pq+1}{2} - (pq+1-r) \right| = pq - \left| -\frac{pq+1}{2} + r \right| = pq - \frac{pq+1}{2} + r = pq - \left| \frac{pq+1}{2} - r \right|.$$

If  $r > \frac{pq+1}{2}$  we have  $s < \frac{pq+1}{2}$  which gives us

$$pq - \left| \frac{pq+1}{2} - s \right| = pq - \frac{pq+1}{2} + s = \frac{pq-1}{2} + s \geq \frac{pq-1}{2} + 2 > \frac{pq+1}{2}$$

and

$$pq - \left| \frac{pq+1}{2} - r \right| = pq - \left| \frac{pq+1}{2} - (pq+1-s) \right| = pq - \left| -\frac{pq+1}{2} + s \right| = pq - \frac{pq+1}{2} + s = pq - \left| \frac{pq+1}{2} - s \right|.$$

□

**Lemma 11.** Let  $q, p \geq 3$  be primes with  $p \neq q$ . Let  $0 \leq r, s < qp$  be the smallest positive integers satisfying

$$\begin{aligned} s &\equiv 1 \pmod{p} & r &\equiv 0 \pmod{p} \\ s &\equiv 0 \pmod{q} & r &\equiv 1 \pmod{q}. \end{aligned}$$

Then the following holds:

$$(pq - |\frac{pq+1}{2} - s|)|\frac{pq+1}{2} - s| = (pq - |\frac{pq+1}{2} - r|)|\frac{pq+1}{2} - r| < \frac{pq+1}{2} \frac{pq-1}{2}.$$

*Proof.* Equality follows from the equation

$$|\frac{pq+1}{2} - r| = |\frac{pq+1}{2} - s|$$

by Lemma 10. Furthermore because of the above congruences we have  $s, r \notin \{0, 1\}$ . Moreover we have  $s + r \equiv 1 \pmod{pq}$  and since  $2 \leq r, s < qp$  we obtain  $s + r = 1 + pq$ . In the case  $s \leq \frac{pq+1}{2}$  we use  $s > 1$  to obtain

$$\begin{aligned} (pq - |\frac{pq+1}{2} - s|)|\frac{pq+1}{2} - s| &= \frac{pq+1}{2} \frac{pq-1}{2} - s(s-1) \\ &< \frac{pq+1}{2} \frac{pq-1}{2}. \end{aligned}$$

In the case  $s > \frac{pq+1}{2}$  we then have  $r < \frac{pq+1}{2}$  and use  $r > 1$  to obtain

$$\begin{aligned} (pq - |\frac{pq+1}{2} - r|)|\frac{pq+1}{2} - r| &= \frac{pq+1}{2} \frac{pq-1}{2} - r(r-1) \\ &< \frac{pq+1}{2} \frac{pq-1}{2}. \end{aligned}$$

□

**Lemma 12.** Let  $n \geq 2$  and  $0 \leq a, b < n$  be integers. Then

$$K(\llbracket n \rrbracket^a, \llbracket n \rrbracket^b) = |a - b|(n - |a - b|).$$

*Proof.* If  $a = b$  then clearly  $K(\llbracket n \rrbracket^a, \llbracket n \rrbracket^b) = 0$ . Now suppose  $a \neq b$ . Case 1:  $a < b$ . We partition the set  $[1, n]$  into 3 sets as follows

$$T_1 = [1, n - b] \quad T_2 = [n - b + 1, n - a] \quad T_3 = [n - a + 1, n].$$

Then we have for  $i \in T_1$

$$\begin{aligned} i\llbracket n \rrbracket^a &= i + a \in [a + 1, n - b + a] \\ i\llbracket n \rrbracket^b &= i + b \in [b + 1, n] \end{aligned}$$

and for  $i \in T_2$

$$\begin{aligned} i\llbracket n \rrbracket^a &= i + a \in [n - b + a + 1, n] \\ i\llbracket n \rrbracket^b &= i + b - n \in [1, b - a] \end{aligned}$$

and for  $i \in T_3$

$$\begin{aligned} i\llbracket n \rrbracket^a &= i + a - n \in [1, a] \\ i\llbracket n \rrbracket^b &= i + b - n \in [b - a + 1, b]. \end{aligned}$$

By this we obtain

$$\begin{aligned} K(\llbracket n \rrbracket^a, \llbracket n \rrbracket^b) &= |\{(i, j) \mid i \in T_1, j \in T_2\}| + |\{(i, j) \mid i \in T_3, j \in T_2\}| \\ &= (n-b)(b-a) + a(b-a) \\ &= |a-b|(n-|a-b|). \end{aligned}$$

Case 2:  $a > b$ . In this case we partition the set  $[1, n]$  into 3 sets as follows

$$T_1 = [1, n-a] \quad T_2 = [n-a+1, n-b] \quad T_3 = [n-b+1, n]$$

and analogously obtain

$$\begin{aligned} K(\llbracket n \rrbracket^a, \llbracket n \rrbracket^b) &= |\{(i, j) \mid i \in T_2, j \in T_1\}| + |\{(i, j) \mid i \in T_2, j \in T_3\}| \\ &= (a-b)(n-a) + (a-b)b \\ &= |a-b|(n-|a-b|). \end{aligned}$$

□

**Lemma 13.** *Let  $n \geq 3$  be odd and  $0 \leq a < n$  be an integer. Then*

$$K(\llbracket \frac{n+1}{2} \rrbracket, n, \llbracket n \rrbracket^a) \begin{cases} = \frac{n-1}{2} & \text{if } a \in \{0, 1\} \\ \geq \frac{n+1}{2} & \text{if } 2 \leq a < n. \end{cases}$$

*Proof.* Suppose  $a \in \{0, 1\}$ . We partition the set  $[1, n]$  into 3 sets as follows

$$T_1 = [1, \frac{n-1}{2}] \quad T_2 = [\frac{n+1}{2}, n-1] \quad T_3 = \{n\}.$$

Then we have for  $i \in T_1$

$$i[\llbracket \frac{n+1}{2} \rrbracket, n] = i \in [1, \frac{n-1}{2}]$$

and

$$\begin{aligned} i[\llbracket n \rrbracket^0] &= i \in [1, \frac{n-1}{2}] \\ i[\llbracket n \rrbracket^1] &= i+1 \in [2, \frac{n+1}{2}]. \end{aligned}$$

Moreover for  $i \in T_2$

$$i[\llbracket \frac{n+1}{2} \rrbracket, n] = i+1 \in [\frac{n+3}{2}, n]$$

and

$$\begin{aligned} i[\llbracket n \rrbracket^0] &= i \in [\frac{n+1}{2}, n-1] \\ i[\llbracket n \rrbracket^1] &= i+1 \in [\frac{n+3}{2}, n]. \end{aligned}$$

Moreover for  $i \in T_3$

$$i[\llbracket \frac{n+1}{2} \rrbracket, n] = \frac{n+1}{2}$$

and

$$\begin{aligned} i[\llbracket n \rrbracket^0] &= n \\ i[\llbracket n \rrbracket^1] &= 1. \end{aligned}$$



By this we obtain

$$\begin{aligned} K(\lfloor \frac{n+1}{2}, n \rfloor, \llbracket n \rrbracket^0) &= |\{(i, j) \mid i \in T_3, j \in T_2\}| = \frac{n-1}{2} \\ K(\lfloor \frac{n+1}{2}, n \rfloor, \llbracket n \rrbracket^1) &= |\{(i, j) \mid i \in T_1, j \in T_3\}| = \frac{n-1}{2}. \end{aligned}$$

Now suppose  $2 \leq a < n$ . In the case  $2 \leq a \leq \frac{n+1}{2}$  we have for all  $i \in [1, \frac{n-1}{2}]$

$$i \llbracket \frac{n+1}{2}, n \rrbracket = i < \frac{n+1}{2} = n \llbracket \frac{n+1}{2}, n \rrbracket$$

and

$$i \llbracket n \rrbracket^a = i + a > a = n \llbracket n \rrbracket^a.$$

Moreover we have

$$n \llbracket \frac{n+1}{2}, n \rrbracket = \frac{n+1}{2} < n - a + 2 = (n - a + 1) \llbracket \frac{n+1}{2}, n \rrbracket$$

and

$$n \llbracket n \rrbracket^a = a > 1 = (n - a + 1) \llbracket n \rrbracket^a.$$

Thus we obtain

$$K(\lfloor \frac{n+1}{2}, n \rfloor, \llbracket n \rrbracket^a) \geq \frac{n+1}{2}.$$

In the case  $\frac{n+3}{2} \leq a \leq n-1$  we have for all  $j \in [\frac{n+1}{2}, n-1]$

$$n \llbracket \frac{n+1}{2}, n \rrbracket = \frac{n+1}{2} < j + 1 = j \llbracket \frac{n+1}{2}, n \rrbracket$$

and

$$n \llbracket n \rrbracket^a = a > j + a - n = j \llbracket n \rrbracket^a.$$

Moreover we have

$$1 \llbracket \frac{n+1}{2}, n \rrbracket = 1 < \frac{n+1}{2} = n \llbracket \frac{n+1}{2}, n \rrbracket$$

and

$$1 \llbracket n \rrbracket^a = a + 1 > a = n \llbracket n \rrbracket^a.$$

Thus we obtain also in this case

$$K(\lfloor \frac{n+1}{2}, n \rfloor, \llbracket n \rrbracket^a) \geq \frac{n+1}{2}.$$

□

**Theorem 8.** *The SUBGROUP DISTANCE PROBLEM regarding Kendall's tau distance is NP-complete when the input group is cyclic.*

*Proof.* We give a log-space reduction from Not-All-Equal 3SAT. Let  $X = \{x_1, \dots, x_n\}$  be a finite set of variables and  $C = \{c_1, \dots, c_m\}$  be a set of clauses over  $X$  in which every clause contains three different literals. Throughout the proof when we write  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  we always assume  $i_1 < i_2 < i_3$ . Let  $p_1 < \dots < p_n$  be the first  $n$  primes with  $p_1 \geq 3$ . Moreover let  $\bar{p}_1 < \dots < \bar{p}_n$  be the next  $n$  primes with  $\bar{p}_1 > p_n$ . We associate  $x_i$  with  $p_i$  and  $\bar{x}_i$  with  $\bar{p}_i$  for all  $i \in [1, n]$ . For all  $j \in [1, m]$  we define numbers  $r_{j,1}, r_{j,2}, r_{j,3}, s_{j,1}, s_{j,2}, s_{j,3}$  as the smallest positive integers satisfying the congruences

$$\begin{aligned} s_{j,1} &\equiv 1 \pmod{\tilde{p}_{i_2}} & r_{j,1} &\equiv 0 \pmod{\tilde{p}_{i_2}} \\ s_{j,1} &\equiv 0 \pmod{\tilde{p}_{i_3}} & r_{j,1} &\equiv 1 \pmod{\tilde{p}_{i_3}} \end{aligned}$$

$$\begin{aligned}
s_{j,2} &\equiv 1 \pmod{\tilde{p}_{i_1}} & r_{j,2} &\equiv 0 \pmod{\tilde{p}_{i_1}} \\
s_{j,2} &\equiv 0 \pmod{\tilde{p}_{i_3}} & r_{j,2} &\equiv 1 \pmod{\tilde{p}_{i_3}} \\
\\ 
s_{j,3} &\equiv 1 \pmod{\tilde{p}_{i_1}} & r_{j,3} &\equiv 0 \pmod{\tilde{p}_{i_1}} \\
s_{j,3} &\equiv 0 \pmod{\tilde{p}_{i_2}} & r_{j,3} &\equiv 1 \pmod{\tilde{p}_{i_2}}
\end{aligned}$$

in which we assume  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  and define

$$\tilde{p}_{i_l} = \begin{cases} p_{i_l} & \text{if } \tilde{x}_{i_l} = x_{i_l} \\ \bar{p}_{i_l} & \text{if } \tilde{x}_{i_l} = \bar{x}_{i_l}. \end{cases}$$

Moreover for all  $i \in [1, n]$  we define numbers  $r_i, s_i$  as the smallest positive integers satisfying

$$\begin{aligned}
s_i &\equiv 1 \pmod{p_i} & r_i &\equiv 0 \pmod{p_i} \\
s_i &\equiv 0 \pmod{\bar{p}_i} & r_i &\equiv 1 \pmod{\bar{p}_i}.
\end{aligned}$$

We will work with the group

$$G = \prod_{i=1}^n V_i \times \prod_{j=1}^m U_j$$

in which  $V_i = S_{p_i}^d \times S_{\bar{p}_i}^d \times S_{p_i \bar{p}_i}$  and  $U_j = S_{\tilde{p}_{i_2} \tilde{p}_{i_3}}^{b_{j,2} b_{j,3}} \times S_{\tilde{p}_{i_1} \tilde{p}_{i_3}}^{b_{j,1} b_{j,3}} \times S_{\tilde{p}_{i_1} \tilde{p}_{i_2}}^{b_{j,1} b_{j,2}}$  with  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  and the following

$$\begin{aligned}
a_{j,1} &= \left| \frac{\tilde{p}_{i_2} \tilde{p}_{i_3} + 1}{2} - s_{j,1} \right| (\tilde{p}_{i_2} \tilde{p}_{i_3} - \left| \frac{\tilde{p}_{i_2} \tilde{p}_{i_3} + 1}{2} - s_{j,1} \right|) \\
a_{j,2} &= \left| \frac{\tilde{p}_{i_1} \tilde{p}_{i_3} + 1}{2} - s_{j,2} \right| (\tilde{p}_{i_1} \tilde{p}_{i_3} - \left| \frac{\tilde{p}_{i_1} \tilde{p}_{i_3} + 1}{2} - s_{j,2} \right|) \\
a_{j,3} &= \left| \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} + 1}{2} - s_{j,3} \right| (\tilde{p}_{i_1} \tilde{p}_{i_2} - \left| \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} + 1}{2} - s_{j,3} \right|)
\end{aligned}$$

and

$$\begin{aligned}
b_{j,1} &= \frac{\tilde{p}_{i_2} \tilde{p}_{i_3} + 1}{2} \frac{\tilde{p}_{i_2} \tilde{p}_{i_3} - 1}{2} - a_{j,1} \\
b_{j,2} &= \frac{\tilde{p}_{i_1} \tilde{p}_{i_3} + 1}{2} \frac{\tilde{p}_{i_1} \tilde{p}_{i_3} - 1}{2} - a_{j,2} \\
b_{j,3} &= \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} + 1}{2} \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} - 1}{2} - a_{j,3}
\end{aligned}$$

and

$$\begin{aligned}
d &= 1 + \sum_{i=1}^n \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right) \\
&\quad + \sum_{j=1}^m (a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} + b_{j,1} b_{j,2} b_{j,3}).
\end{aligned}$$

Note that  $b_{j,l} > 0$  by Lemma 11.  $G$  naturally embeds into  $S_N$  for

$$N = \sum_{i=1}^n (d(p_i + \bar{p}_i) + p_i \bar{p}_i) + \sum_{c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\} \in C} (\tilde{p}_{i_2} \tilde{p}_{i_3} b_{j,2} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_3} b_{j,1} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_2} b_{j,1} b_{j,2}).$$

Now we define the input group elements  $\tau, \pi \in G$  as follows where  $i$  ranges over  $[1, n]$  and  $j$  ranges over  $[1, m]$  and  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ :

$$\tau = (\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$$

with

$$\begin{aligned}
\alpha_i &= (\bar{\alpha}_{i,1}^d, \bar{\alpha}_{i,2}^d, \alpha_{i,3}) & \beta_j &= (\bar{\beta}_{j,1}^{b_{j,2}b_{j,3}}, \bar{\beta}_{j,2}^{b_{j,1}b_{j,3}}, \bar{\beta}_{j,3}^{b_{j,1}b_{j,2}}) \\
\alpha_{i,1} &= \llbracket \frac{p_i + 1}{2}, p_i \rrbracket & \beta_{j,1} &= \llbracket \tilde{p}_{i_2} \tilde{p}_{i_3} \rrbracket^{\frac{\tilde{p}_{i_2} \tilde{p}_{i_3} + 1}{2}} \\
\alpha_{i,2} &= \llbracket \frac{\bar{p}_i + 1}{2}, \bar{p}_i \rrbracket & \beta_{j,2} &= \llbracket \tilde{p}_{i_1} \tilde{p}_{i_3} \rrbracket^{\frac{\tilde{p}_{i_1} \tilde{p}_{i_3} + 1}{2}} \\
\alpha_{i,3} &= \llbracket p_i \bar{p}_i \rrbracket^{\frac{p_i \bar{p}_i + 1}{2}} & \beta_{j,3} &= \llbracket \tilde{p}_{i_1} \tilde{p}_{i_2} \rrbracket^{\frac{\tilde{p}_{i_1} \tilde{p}_{i_2} + 1}{2}}
\end{aligned}$$

and

$$\pi = (\gamma_1, \dots, \gamma_n, \delta_1, \dots, \delta_m)$$

with

$$\begin{aligned}
\gamma_i &= (\bar{\gamma}_{i,1}^d, \bar{\gamma}_{i,2}^d, \gamma_{i,3}) & \delta_j &= (\bar{\delta}_{j,1}^{b_{j,2}b_{j,3}}, \bar{\delta}_{j,2}^{b_{j,1}b_{j,3}}, \bar{\delta}_{j,3}^{b_{j,1}b_{j,2}}) \\
\gamma_{i,1} &= \llbracket p_i \rrbracket & \delta_{j,1} &= \llbracket \tilde{p}_{i_2} \tilde{p}_{i_3} \rrbracket \\
\gamma_{i,2} &= \llbracket \bar{p}_i \rrbracket & \delta_{j,2} &= \llbracket \tilde{p}_{i_1} \tilde{p}_{i_3} \rrbracket \\
\gamma_{i,3} &= \llbracket p_i \bar{p}_i \rrbracket & \delta_{j,3} &= \llbracket \tilde{p}_{i_1} \tilde{p}_{i_2} \rrbracket
\end{aligned}$$

and finally we define

$$\begin{aligned}
k &= \sum_{i=1}^n \left( d \frac{p_i - 1}{2} + d \frac{\bar{p}_i - 1}{2} + \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right) \right) \\
&+ \sum_{j=1}^m (a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} + b_{j,1} b_{j,2} b_{j,3}).
\end{aligned}$$

Now we will show there is  $x \in \mathbb{N}$  such that  $K(\tau, \pi^x) \leq k$  if and only if  $X, C$  is a positive instance of Not-All-Equal 3SAT.

Suppose there is  $x \in \mathbb{N}$  such that  $K(\tau, \pi^x) \leq k$ .

**Claim 20.** *For all  $i \in [1, n]$  we have  $x \equiv 0, 1 \pmod{p_i}$  and  $x \equiv 0, 1 \pmod{\bar{p}_i}$  and*

$$\begin{aligned}
K(\bar{\alpha}_{i,1}^d, (\bar{\gamma}_{i,1}^d)^x) &= d \frac{p_i - 1}{2} \\
K(\bar{\alpha}_{i,2}^d, (\bar{\gamma}_{i,2}^d)^x) &= d \frac{\bar{p}_i - 1}{2}.
\end{aligned}$$

Suppose there is  $e \in [1, n]$  such that  $x \not\equiv 0, 1 \pmod{p_e}$ . Then we have by Lemma 13

$$\begin{aligned}
K(\alpha_{e,1}, \gamma_{e,1}^x) &= K(\llbracket \frac{p_e + 1}{2}, p_e \rrbracket, \llbracket p_e \rrbracket^x) \\
&\geq \frac{p_e + 1}{2}
\end{aligned}$$

by which we obtain

$$K(\bar{\alpha}_{e,1}^d, (\bar{\gamma}_{e,1}^d)^x) \geq d \frac{p_e + 1}{2} = d \frac{p_e - 1}{2} + d.$$

By Lemma 13 we have for all  $i \in [1, n]$

$$\begin{aligned}
K(\alpha_{i,1}, \gamma_{i,1}^x) &\geq \frac{p_i - 1}{2} \\
K(\alpha_{i,2}, \gamma_{i,2}^x) &\geq \frac{\bar{p}_i - 1}{2}
\end{aligned}$$

and hence

$$\begin{aligned} K(\bar{\alpha}_{i,1}^d, (\bar{\gamma}_{i,1}^d)^x) &\geq d \frac{p_i - 1}{2} \\ K(\bar{\alpha}_{i,2}^d, (\bar{\gamma}_{i,2}^d)^x) &\geq d \frac{\bar{p}_i - 1}{2}. \end{aligned}$$

By using the above lower bounds and the following trivial lower bounds

$$K(\alpha_{i,3}, \gamma_{i,3}^x) \geq 0$$

for all  $i \in [1, n]$  and

$$K(\beta_{j,l}, \delta_{j,l}^x) \geq 0$$

for all  $j \in [1, m]$  and  $l \in [1, 3]$  we obtain

$$\begin{aligned} K(\tau, \pi^x) &\geq \sum_{i=1}^n \left( d \frac{p_i - 1}{2} + d \frac{\bar{p}_i - 1}{2} \right) - \left( d \frac{p_e - 1}{2} \right) + \left( d \frac{p_e - 1}{2} + d \right) \\ &= \sum_{i=1}^n \left( d \frac{p_i - 1}{2} + d \frac{\bar{p}_i - 1}{2} \right) + d \\ &= \sum_{i=1}^n \left( d \frac{p_i - 1}{2} + d \frac{\bar{p}_i - 1}{2} + \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right) \right) \\ &\quad + \sum_{j=1}^m (a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} + b_{j,1} b_{j,2} b_{j,3}) + 1 \\ &= k + 1 \\ &> k \end{aligned}$$

which is a contradiction. By this we obtain  $x \equiv 0, 1 \pmod{p_i}$ . Analogously we obtain  $x \equiv 0, 1 \pmod{\bar{p}_i}$ . Finally by Lemma 13 we obtain

$$\begin{aligned} K(\bar{\alpha}_{i,1}^d, (\bar{\gamma}_{i,1}^d)^x) &= d \frac{p_i - 1}{2} \\ K(\bar{\alpha}_{i,2}^d, (\bar{\gamma}_{i,2}^d)^x) &= d \frac{\bar{p}_i - 1}{2}. \end{aligned}$$

□

**Claim 21.** For all  $j \in [1, m]$  we have

$$K(\beta_j, \delta_j^x) = \begin{cases} a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} + 3b_{j,1} b_{j,2} b_{j,3} & \text{if } x \equiv 0, 1 \pmod{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}} \\ a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} + b_{j,1} b_{j,2} b_{j,3} & \text{if } x \not\equiv 0, 1 \pmod{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}}. \end{cases}$$

in which  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ .

Suppose  $x \equiv 0, 1 \pmod{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}}$ . Then we have for all  $l \in [1, 3]$  by Lemma 12

$$\begin{aligned} K(\beta_{j,l}, \delta_{j,l}^x) &= K \left( \left\lfloor \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}}{\tilde{p}_{i_l}} \right\rfloor^{\frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3} + \tilde{p}_{i_l}}{2\tilde{p}_{i_l}}}, \left\lfloor \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}}{\tilde{p}_{i_l}} \right\rfloor^x \right) \\ &= \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3} + \tilde{p}_{i_l}}{2\tilde{p}_{i_l}} \cdot \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3} - \tilde{p}_{i_l}}{2\tilde{p}_{i_l}} \\ &= a_{j,l} + b_{j,l}. \end{aligned}$$

Thus

$$K \left( \frac{b_{j,1} b_{j,2} b_{j,3}}{\beta_{j,l}^{b_{j,l}}}, \left( \frac{b_{j,1} b_{j,2} b_{j,3}}{\delta_{j,l}^{b_{j,l}}} \right)^x \right) = \frac{b_{j,1} b_{j,2} b_{j,3}}{b_{j,l}} (a_{j,l} + b_{j,l})$$

from which it follows now that

$$\begin{aligned} K(\beta_j, \delta_j^x) &= b_{j,2}b_{j,3}(a_{j,1} + b_{j,1}) + b_{j,1}b_{j,3}(a_{j,2} + b_{j,2}) + b_{j,1}b_{j,2}(a_{j,3} + b_{j,3}) \\ &= a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + 3b_{j,1}b_{j,2}b_{j,3}. \end{aligned}$$

Now suppose  $x \not\equiv 0, 1 \pmod{\tilde{p}_{i_1}\tilde{p}_{i_2}\tilde{p}_{i_3}}$ . By Claim 20 we have  $x \equiv 0, 1 \pmod{p_i}$  and  $x \equiv 0, 1 \pmod{\tilde{p}_i}$  for all  $i \in [1, n]$ . Thus there are  $g, h \in [1, 3]$  and  $c \in \{0, 1\}$  with  $g \neq h$  such that  $x \equiv c \pmod{\tilde{p}_{i_g}}$  and  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$  and let w.l.o.g.  $f \in [1, 3] \setminus \{g, h\}$  be such that  $x \equiv c \pmod{\tilde{p}_{i_f}}$ . Then we obtain by Lemma 12

$$\begin{aligned} K(\beta_{j,h}, \delta_{j,h}^x) &= K\left(\llbracket \tilde{p}_{i_g}\tilde{p}_{i_f} \rrbracket^{\frac{\tilde{p}_{i_g}\tilde{p}_{i_f}+1}{2}}, \llbracket \tilde{p}_{i_g}\tilde{p}_{i_f} \rrbracket^x\right) \\ &= K\left(\llbracket \tilde{p}_{i_g}\tilde{p}_{i_f} \rrbracket^{\frac{\tilde{p}_{i_g}\tilde{p}_{i_f}+1}{2}}, \llbracket \tilde{p}_{i_g}\tilde{p}_{i_f} \rrbracket^c\right) \\ &= \frac{\tilde{p}_{i_g}\tilde{p}_{i_f} + 1}{2} \cdot \frac{\tilde{p}_{i_g}\tilde{p}_{i_f} - 1}{2} \\ &= a_{j,h} + b_{j,h}. \end{aligned}$$

Moreover we have  $x \equiv s_{j,f} \pmod{\tilde{p}_{i_g}\tilde{p}_{i_h}}$  and  $x \equiv s_{j,g} \pmod{\tilde{p}_{i_f}\tilde{p}_{i_h}}$  or  $x \equiv r_{j,f} \pmod{\tilde{p}_{i_g}\tilde{p}_{i_h}}$  and  $x \equiv r_{j,g} \pmod{\tilde{p}_{i_f}\tilde{p}_{i_h}}$ . By Lemma 10 we have

$$\begin{aligned} \left| \frac{\tilde{p}_{i_g}\tilde{p}_{i_h} + 1}{2} - r_{j,f} \right| &= \left| \frac{\tilde{p}_{i_g}\tilde{p}_{i_h} + 1}{2} - s_{j,f} \right| \\ \left| \frac{\tilde{p}_{i_f}\tilde{p}_{i_h} + 1}{2} - r_{j,g} \right| &= \left| \frac{\tilde{p}_{i_f}\tilde{p}_{i_h} + 1}{2} - s_{j,g} \right| \end{aligned}$$

and hence Lemma 12 gives us

$$\begin{aligned} K(\beta_{j,f}, \delta_{j,f}^x) &= K\left(\llbracket \tilde{p}_{i_g}\tilde{p}_{i_h} \rrbracket^{\frac{\tilde{p}_{i_g}\tilde{p}_{i_h}+1}{2}}, \llbracket \tilde{p}_{i_g}\tilde{p}_{i_h} \rrbracket^x\right) \\ &= \left| \frac{\tilde{p}_{i_g}\tilde{p}_{i_h} + 1}{2} - s_{j,f} \right| \left( \tilde{p}_{i_g}\tilde{p}_{i_h} - \left| \frac{\tilde{p}_{i_g}\tilde{p}_{i_h} + 1}{2} - s_{j,f} \right| \right) \\ &= a_{j,f} \end{aligned}$$

and

$$\begin{aligned} K(\beta_{j,g}, \delta_{j,g}^x) &= K\left(\llbracket \tilde{p}_{i_f}\tilde{p}_{i_h} \rrbracket^{\frac{\tilde{p}_{i_f}\tilde{p}_{i_h}+1}{2}}, \llbracket \tilde{p}_{i_f}\tilde{p}_{i_h} \rrbracket^x\right) \\ &= \left| \frac{\tilde{p}_{i_f}\tilde{p}_{i_h} + 1}{2} - s_{j,g} \right| \left( (\tilde{p}_{i_f}\tilde{p}_{i_h} - \left| \frac{\tilde{p}_{i_f}\tilde{p}_{i_h} + 1}{2} - s_{j,g} \right|) \right) \\ &= a_{j,g}. \end{aligned}$$

Thus

$$\begin{aligned} K\left(\vec{\beta}_{j,h}^{b_{j,f}b_{j,g}}, \left(\vec{\delta}_{j,h}^{b_{j,f}b_{j,g}}\right)^x\right) &= b_{j,f}b_{j,g}(a_{j,h} + b_{j,h}) \\ K\left(\vec{\beta}_{j,f}^{b_{j,h}b_{j,g}}, \left(\vec{\delta}_{j,f}^{b_{j,h}b_{j,g}}\right)^x\right) &= b_{j,h}b_{j,g}a_{j,f} \end{aligned}$$

and

$$K\left(\vec{\beta}_{j,g}^{b_{j,h}b_{j,f}}, \left(\vec{\delta}_{j,g}^{b_{j,h}b_{j,f}}\right)^x\right) = b_{j,h}b_{j,f}a_{j,g}.$$

From this it finally follows that

$$\begin{aligned} K(\beta_j, \delta_j^x) &= b_{j,f}b_{j,g}(a_{j,h} + b_{j,h}) + b_{j,h}b_{j,g}a_{j,f} + b_{j,h}b_{j,f}a_{j,g} \\ &= a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3}. \end{aligned}$$

□

**Claim 22.** For all  $i \in [1, n]$  we have

$$K(\alpha_{i,3}, \gamma_{i,3}^x) = \begin{cases} \frac{p_i \bar{p}_i + 1}{2} \cdot \frac{p_i \bar{p}_i - 1}{2} & \text{if } x \equiv 0, 1 \pmod{p_i \bar{p}_i} \\ \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| (p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right|) & \text{if } x \not\equiv 0, 1 \pmod{p_i \bar{p}_i}. \end{cases}$$

Suppose  $x \equiv 0, 1 \pmod{p_i \bar{p}_i}$ . Then we have by Lemma 12

$$\begin{aligned} K(\alpha_{i,3}, \gamma_{i,3}^x) &= K\left(\llbracket p_i \bar{p}_i \rrbracket^{\frac{p_i \bar{p}_i + 1}{2}}, \llbracket p_i \bar{p}_i \rrbracket^x\right) \\ &= \frac{p_i \bar{p}_i + 1}{2} \cdot \frac{p_i \bar{p}_i - 1}{2} \end{aligned}$$

Now suppose  $x \not\equiv 0, 1 \pmod{p_i \bar{p}_i}$ . By Claim 20 we have  $x \equiv 0, 1 \pmod{p_i}$  and  $x \equiv 0, 1 \pmod{\bar{p}_i}$  for all  $i \in [1, n]$ . Thus  $x \equiv s_i \pmod{p_i \bar{p}_i}$  or  $x \equiv r_i \pmod{p_i \bar{p}_i}$ . By Lemma 10 we have

$$\left| \frac{p_i \bar{p}_i + 1}{2} - r_i \right| = \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right|$$

and by Lemma 12 we finally obtain

$$\begin{aligned} K(\alpha_{i,3}, \gamma_{i,3}^x) &= K\left(\llbracket p_i \bar{p}_i \rrbracket^{\frac{p_i \bar{p}_i + 1}{2}}, \llbracket p_i \bar{p}_i \rrbracket^x\right) \\ &= \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right). \end{aligned}$$

□

**Claim 23.** For all  $i \in [1, n]$  we have  $x \equiv 1 \pmod{p_i}$  and  $x \equiv 0 \pmod{\bar{p}_i}$  or  $x \equiv 0 \pmod{p_i}$  and  $x \equiv 1 \pmod{\bar{p}_i}$ .

Suppose there is an  $e \in [1, n]$  for which the contrary holds. By Claim 20 we have  $x \equiv 0, 1 \pmod{p_e}$  and  $x \equiv 0, 1 \pmod{\bar{p}_e}$ . Therefore it suffices to consider the cases  $x \equiv 0, 1 \pmod{p_e \bar{p}_e}$ . Then by Lemma 12 we have  $K(\alpha_{e,3}, \gamma_{e,3}^x) = \frac{p_e \bar{p}_e + 1}{2} \cdot \frac{p_e \bar{p}_e - 1}{2}$ . Summing over all lower bounds Claim 20, 21, 22 and Lemma 13 yield we obtain

$$\begin{aligned} K(\tau, \pi^x) &\geq \sum_{i=1}^n \left( d \frac{p_i - 1}{2} + d \frac{\bar{p}_i - 1}{2} + \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right) \right) \\ &\quad - \left| \frac{p_e \bar{p}_e + 1}{2} - s_e \right| \left( p_e \bar{p}_e - \left| \frac{p_e \bar{p}_e + 1}{2} - s_e \right| \right) + \frac{p_e \bar{p}_e + 1}{2} \cdot \frac{p_e \bar{p}_e - 1}{2} \\ &\quad + \sum_{j=1}^m (a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} + b_{j,1} b_{j,2} b_{j,3}) \\ &> \sum_{i=1}^n \left( d \frac{p_i - 1}{2} + d \frac{\bar{p}_i - 1}{2} + \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right) \right) \\ &\quad - \left| \frac{p_e \bar{p}_e + 1}{2} - s_e \right| \left( p_e \bar{p}_e - \left| \frac{p_e \bar{p}_e + 1}{2} - s_e \right| \right) + \left| \frac{p_e \bar{p}_e + 1}{2} - s_e \right| \left( p_e \bar{p}_e - \left| \frac{p_e \bar{p}_e + 1}{2} - s_e \right| \right) \\ &\quad + \sum_{j=1}^m (a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} + b_{j,1} b_{j,2} b_{j,3}) \\ &= \sum_{i=1}^n \left( d \frac{p_i - 1}{2} + d \frac{\bar{p}_i - 1}{2} + \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right) \right) \\ &\quad + \sum_{j=1}^m (a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} + b_{j,1} b_{j,2} b_{j,3}) \\ &= k \end{aligned}$$

which is a contradiction. For this also note that

$$\frac{p_i \bar{p}_i + 1}{2} \cdot \frac{p_i \bar{p}_i - 1}{2} > \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right)$$

by Lemma 11 and hence Claim 22 gives us the lower bound

$$\left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right).$$

□

**Claim 24.** For every clause  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  the following holds: If there are  $f, g \in [1, 3]$  with  $f \neq g$  and  $c \in \{0, 1\}$  such that  $x \equiv c \pmod{\tilde{p}_{i_f}}$  and  $x \equiv c \pmod{\tilde{p}_{i_g}}$  then  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$  where  $h$  is the unique element in  $[1, 3] \setminus \{f, g\}$ .

Suppose there is a clause  $c_e = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  such that  $x \equiv c \pmod{\tilde{p}_{i_l}}$  for all  $l \in [1, 3]$  and some  $c \in \{0, 1\}$ . Then we have by Claim 21

$$K(\beta_e, \delta_e^x) = a_{e,1}b_{e,2}b_{e,3} + a_{e,2}b_{e,1}b_{e,3} + a_{e,3}b_{e,1}b_{e,2} + 3b_{e,1}b_{e,2}b_{e,3}.$$

Summing over all lower bounds Claim 20,21,22 and Lemma 13 yield we obtain

$$\begin{aligned} K(\tau, \pi^x) &\geq \sum_{i=1}^n \left( d \frac{p_i - 1}{2} + d \frac{\bar{p}_i - 1}{2} + \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right) \right) \\ &\quad + \sum_{j=1}^m (a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3}) \\ &\quad - (a_{e,1}b_{e,2}b_{e,3} + a_{e,2}b_{e,1}b_{e,3} + a_{e,3}b_{e,1}b_{e,2} + b_{e,1}b_{e,2}b_{e,3}) \\ &\quad + (a_{e,1}b_{e,2}b_{e,3} + a_{e,2}b_{e,1}b_{e,3} + a_{e,3}b_{e,1}b_{e,2} + 3b_{e,1}b_{e,2}b_{e,3}) \\ &= \sum_{i=1}^n \left( d \frac{p_i - 1}{2} + d \frac{\bar{p}_i - 1}{2} + \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right) \right) \\ &\quad + \sum_{j=1}^m (a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3}) + 2b_{e,1}b_{e,2}b_{e,3} \\ &= k + 2b_{e,1}b_{e,2}b_{e,3} \\ &> k \end{aligned}$$

which is a contradiction. As above we use

$$\frac{p_i \bar{p}_i + 1}{2} \cdot \frac{p_i \bar{p}_i - 1}{2} > \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right)$$

by Lemma 11. Hence we obtain for every clause  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ : If there are  $f, g \in [1, 3]$  with  $f \neq g$  and  $c \in \{0, 1\}$  such that  $x \equiv c \pmod{\tilde{p}_{i_f}}$  and  $x \equiv c \pmod{\tilde{p}_{i_g}}$  then  $x \not\equiv c \pmod{\tilde{p}_{i_h}}$  where  $h$  is the unique element in  $[1, 3] \setminus \{f, g\}$ . Since by Claim 20 we have  $x \equiv 0, 1 \pmod{\tilde{p}_{i_h}}$  we finally obtain  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$ . □

Now we define a truth assignment  $\sigma$  by the following:

$$\sigma(x_i) = \begin{cases} 1 & \text{if } x \equiv 1 \pmod{p_i} \\ 0 & \text{if } x \equiv 0 \pmod{p_i} \end{cases}$$

for all  $i \in [1, n]$ . Let  $\hat{\sigma}$  be the extension of  $\sigma$  to literals. Now we will show for every clause  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  there are pairwise different numbers  $f, g, h \in [1, 3]$  and  $c \in \{0, 1\}$  such that

$$\begin{aligned} \hat{\sigma}(\tilde{x}_{i_f}) &= c \\ \hat{\sigma}(\tilde{x}_{i_g}) &= c \\ \hat{\sigma}(\tilde{x}_{i_h}) &= 1 - c. \end{aligned}$$

By Claim 20 we have  $x \equiv 0, 1 \pmod{\tilde{p}_i}$  for all  $i \in [1, n]$ . Hence there clearly are  $f, g \in [1, 3]$  with  $f \neq g$  and  $c \in \{0, 1\}$  such that  $x \equiv c \pmod{\tilde{p}_{i_f}}$  and  $x \equiv c \pmod{\tilde{p}_{i_g}}$ . In the case  $\tilde{p}_{i_f} = p_{i_f}$  we obtain  $\sigma(x_{i_f}) = c$  and hence  $\hat{\sigma}(x_{i_f}) = c$ . In the case  $\tilde{p}_{i_f} = \bar{p}_{i_f}$  we have  $x \equiv 1 - c \pmod{p_{i_f}}$  by Claim 23. Thus  $\sigma(x_{i_f}) = 1 - c$  and  $\hat{\sigma}(\bar{x}_{i_f}) = c$ . Analogously we obtain  $\hat{\sigma}(\bar{x}_{i_g}) = c$ . Since we have  $x \equiv c \pmod{\tilde{p}_{i_f}}$  and  $x \equiv c \pmod{\tilde{p}_{i_g}}$  we obtain  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$  by Claim 24. As above we then analogously obtain  $\hat{\sigma}(\bar{x}_{i_h}) = 1 - c$  which eventually shows that  $X, C$  is a positive instance of Not-All-Equal 3SAT.

Vice versa suppose  $X, C$  is a positive instance of Not-All-Equal 3SAT and let  $\sigma$  be a truth assignment such that for every clause  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  there are pairwise different numbers  $f, g, h \in [1, 3]$  and  $c \in \{0, 1\}$  such that

$$\begin{aligned}\hat{\sigma}(\tilde{x}_{i_f}) &= c \\ \hat{\sigma}(\tilde{x}_{i_g}) &= c \\ \hat{\sigma}(\tilde{x}_{i_h}) &= 1 - c.\end{aligned}$$

Then we define  $x$  as the smallest positive integer satisfying  $x \equiv \sigma(x_i) \pmod{p_i}$  and  $x \equiv 1 - \sigma(x_i) \pmod{\bar{p}_i}$  for all  $i \in [1, n]$ . Then we have  $x \equiv s_i, r_i \pmod{p_i \bar{p}_i}$  for all  $i \in [1, n]$ . Then by Lemma 12 and 13 we obtain

$$\begin{aligned}K(\alpha_{i,1}, \gamma_{i,1}^x) &= \frac{p_i - 1}{2} \\ K(\alpha_{i,2}, \gamma_{i,2}^x) &= \frac{\bar{p}_i - 1}{2}\end{aligned}$$

and

$$K(\alpha_{i,3}, \gamma_{i,3}^x) = \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right).$$

Thus

$$\begin{aligned}K(\bar{\alpha}_{i,1}^d, (\bar{\gamma}_{i,1}^d)^x) &= d \frac{p_i - 1}{2} \\ K(\bar{\alpha}_{i,2}^d, (\bar{\gamma}_{i,2}^d)^x) &= d \frac{\bar{p}_i - 1}{2}\end{aligned}$$

and

$$K(\alpha_i, \gamma_i^x) = d \frac{p_i - 1}{2} + d \frac{\bar{p}_i - 1}{2} + \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right). \quad (27)$$

Let  $j \in [1, m]$  and suppose  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ . Then there are pairwise different numbers  $f, g, h \in [1, 3]$  and  $c \in \{0, 1\}$  such that

$$\begin{aligned}\hat{\sigma}(\tilde{x}_{i_f}) &= c \\ \hat{\sigma}(\tilde{x}_{i_g}) &= c \\ \hat{\sigma}(\tilde{x}_{i_h}) &= 1 - c.\end{aligned}$$

By definition we have  $x \equiv \sigma(x_i) \pmod{p_i}$  and  $x \equiv 1 - \sigma(x_i) \pmod{\bar{p}_i}$  for all  $i \in [1, n]$  which gives us

$$x \equiv \begin{cases} \sigma(x_{i_f}) \equiv \hat{\sigma}(x_{i_f}) \equiv c \pmod{p_{i_f}} & \text{if } \tilde{x}_{i_f} = x_{i_f} \\ 1 - \sigma(x_{i_f}) \equiv \hat{\sigma}(\bar{x}_{i_f}) \equiv c \pmod{\bar{p}_{i_f}} & \text{if } \tilde{x}_{i_f} = \bar{x}_{i_f} \end{cases}$$

and hence  $x \equiv c \pmod{\tilde{p}_{i_f}}$ . Analogously we obtain  $x \equiv c \pmod{\tilde{p}_{i_g}}$  and  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$ . Then we have  $x \equiv s_{j,f}, r_{j,f} \pmod{\tilde{p}_{i_f}}$  and  $x \equiv s_{j,g}, r_{j,g} \pmod{\tilde{p}_{i_g}}$  and since by Lemma 10 we have

$$\left| \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3} + \tilde{p}_{i_l}}{2\tilde{p}_{i_l}} - r_{j,l} \right| = \left| \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3} + \tilde{p}_{i_l}}{2\tilde{p}_{i_l}} - s_{j,l} \right|$$



for all  $l \in [1, 3]$  we obtain by Lemma 12

$$\begin{aligned}
K(\beta_{j,f}, \delta_{j,f}^x) &= K\left(\llbracket \tilde{p}_{i_g} \tilde{p}_{i_h} \rrbracket^{\frac{\tilde{p}_{i_g} \tilde{p}_{i_h} + 1}{2}}, \llbracket \tilde{p}_{i_g} \tilde{p}_{i_h} \rrbracket^x\right) \\
&= \left| \frac{\tilde{p}_{i_g} \tilde{p}_{i_h} + 1}{2} - s_{j,f} \right| \left( \tilde{p}_{i_g} \tilde{p}_{i_h} - \left| \frac{\tilde{p}_{i_g} \tilde{p}_{i_h} + 1}{2} - s_{j,f} \right| \right) \\
&= a_{j,f}
\end{aligned}$$

and

$$\begin{aligned}
K(\beta_{j,g}, \delta_{j,g}^x) &= K\left(\llbracket \tilde{p}_{i_f} \tilde{p}_{i_h} \rrbracket^{\frac{\tilde{p}_{i_f} \tilde{p}_{i_h} + 1}{2}}, \llbracket \tilde{p}_{i_f} \tilde{p}_{i_h} \rrbracket^x\right) \\
&= \left| \frac{\tilde{p}_{i_f} \tilde{p}_{i_h} + 1}{2} - s_{j,g} \right| \left( \tilde{p}_{i_f} \tilde{p}_{i_h} - \left| \frac{\tilde{p}_{i_f} \tilde{p}_{i_h} + 1}{2} - s_{j,g} \right| \right) \\
&= a_{j,g}
\end{aligned}$$

and

$$\begin{aligned}
K(\beta_{j,h}, \delta_{j,h}^x) &= K\left(\llbracket \tilde{p}_{i_f} \tilde{p}_{i_g} \rrbracket^{\frac{\tilde{p}_{i_f} \tilde{p}_{i_g} + 1}{2}}, \llbracket \tilde{p}_{i_f} \tilde{p}_{i_g} \rrbracket^x\right) \\
&= K\left(\llbracket \tilde{p}_{i_f} \tilde{p}_{i_g} \rrbracket^{\frac{\tilde{p}_{i_f} \tilde{p}_{i_g} + 1}{2}}, \llbracket \tilde{p}_{i_f} \tilde{p}_{i_g} \rrbracket^c\right) \\
&= \frac{\tilde{p}_{i_f} \tilde{p}_{i_g} + 1}{2} \cdot \frac{\tilde{p}_{i_f} \tilde{p}_{i_g} - 1}{2} \\
&= a_{j,h} + b_{j,h}.
\end{aligned}$$

By this we obtain

$$\begin{aligned}
K\left(\tilde{\beta}_{j,f}^{b_{j,g}b_{j,h}}, \left(\tilde{\delta}_{j,f}^{b_{j,g}b_{j,h}}\right)^x\right) &= b_{j,g}b_{j,h}a_{j,f} \\
K\left(\tilde{\beta}_{j,g}^{b_{j,f}b_{j,h}}, \left(\tilde{\delta}_{j,g}^{b_{j,f}b_{j,h}}\right)^x\right) &= b_{j,f}b_{j,h}a_{j,g}
\end{aligned}$$

and

$$K\left(\tilde{\beta}_{j,h}^{b_{j,f}b_{j,g}}, \left(\tilde{\delta}_{j,h}^{b_{j,f}b_{j,g}}\right)^x\right) = b_{j,f}b_{j,g}(a_{j,h} + b_{j,h}).$$

From this it follows now that

$$\begin{aligned}
K(\beta_j, \delta_j^x) &= b_{j,g}b_{j,h}a_{j,f} + b_{j,f}b_{j,h}a_{j,g} + b_{j,f}b_{j,g}(a_{j,h} + b_{j,h}) \\
&= a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3}.
\end{aligned} \tag{28}$$

Using (27) and (28) and summing up we finally obtain

$$\begin{aligned}
K(\tau, \pi^x) &= \sum_{i=1}^n \left( d \frac{p_i - 1}{2} + d \frac{\bar{p}_i - 1}{2} + \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \left( p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right) \right) \\
&\quad + \sum_{j=1}^m (a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} + b_{j,1}b_{j,2}b_{j,3}) \\
&= k.
\end{aligned}$$

□

### 3.6 Ulam's Distance

**Lemma 14.** *Let  $n \geq 3$  be odd and  $0 \leq b < n$  be an integer. Then*

$$\max\{n - |\frac{n+1}{2} - b|, |\frac{n+1}{2} - b|\} = \begin{cases} \frac{n+1}{2} & \text{if } b \in \{0, 1\} \\ n - |\frac{n+1}{2} - b| & \text{if } b \in [2, n-1]. \end{cases}$$

*Proof.* We clearly have

$$n - |\frac{n+1}{2} - 0| = \frac{n-1}{2} < \frac{n+1}{2} = |\frac{n+1}{2} - 0|$$

and

$$n - |\frac{n+1}{2} - 1| = \frac{n+1}{2} > \frac{n-1}{2} = |\frac{n+1}{2} - 1|.$$

In the case  $2 \leq b \leq \frac{n+1}{2}$  we have

$$n - |\frac{n+1}{2} - b| = n - \frac{n+1}{2} + b > \frac{n+1}{2} > \frac{n+1}{2} - b = |\frac{n+1}{2} - b|.$$

In the case  $\frac{n+3}{2} \leq b \leq n-1$  we have

$$n - |\frac{n+1}{2} - b| = \frac{3n+1}{2} - b \geq \frac{n+3}{2} > \frac{n-3}{2} \geq b - \frac{n+1}{2} = |\frac{n+1}{2} - b|.$$

□

**Lemma 15.** *Let  $n \geq 3$  be odd and  $0 \leq a, b < n$  be integers. Then*

$$\text{lis}(\llbracket n \rrbracket^{a-b}) = \max\{n - |a - b|, |a - b|\}.$$

*Proof.* If  $a = b$  then  $\llbracket n \rrbracket^{a-b} = \text{id}$  and

$$(1^{\text{id}}, \dots, n^{\text{id}}) = (1, \dots, n).$$

Thus clearly  $\text{lis}(\llbracket n \rrbracket^{a-b}) = n$ . Now suppose  $a \neq b$ . If  $a > b$  then  $(1^{\llbracket n \rrbracket^{a-b}}, \dots, n^{\llbracket n \rrbracket^{a-b}})$  contains two increasing subsequences namely

$$\begin{aligned} (1^{\llbracket n \rrbracket^{a-b}}, \dots, n^{\llbracket n \rrbracket^{a-b}}) &= (1^{\llbracket n \rrbracket^{a-b}}, \dots, (n-a+b)^{\llbracket n \rrbracket^{a-b}}, (n-a+b+1)^{\llbracket n \rrbracket^{a-b}}, \dots, n^{\llbracket n \rrbracket^{a-b}}) \\ &= (1+a-b, \dots, n, 1, \dots, a-b) \end{aligned}$$

giving us the two sequences  $1+a-b, \dots, n$  and  $1, \dots, a-b$  with lengths  $n-(a-b)$  and  $a-b$  and hence  $\text{lis}(\llbracket n \rrbracket^{a-b}) = \max\{n - |a - b|, |a - b|\}$ . If  $a < b$  we similarly obtain by

$$\begin{aligned} (1^{\llbracket n \rrbracket^{a-b}}, \dots, n^{\llbracket n \rrbracket^{a-b}}) &= (1^{\llbracket n \rrbracket^{a-b}}, \dots, (-a+b)^{\llbracket n \rrbracket^{a-b}}, (-a+b+1)^{\llbracket n \rrbracket^{a-b}}, \dots, n^{\llbracket n \rrbracket^{a-b}}) \\ &= (1+n+a-b, \dots, n, 1, \dots, n+a-b) \end{aligned}$$

the two sequences  $1+n+a-b, \dots, n$  and  $1, \dots, n+a-b$  with lengths  $-a+b = |a-b|$  and  $n+a-b = n-|a-b|$ . Thus  $\text{lis}(\llbracket n \rrbracket^{a-b}) = \max\{n - |a - b|, |a - b|\}$ . □

**Theorem 9.** *The SUBGROUP DISTANCE PROBLEM regarding Ulam's distance is NP-complete when the input group is cyclic.*

*Proof.* We give a log-space reduction from Not-All-Equal 3SAT. Let  $X = \{x_1, \dots, x_n\}$  be a finite set of variables and  $C = \{c_1, \dots, c_m\}$  be a set of clauses over  $X$  in which every clause contains three different literals. Throughout the proof when we write  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  we always assume  $i_1 < i_2 < i_3$ . Let  $p_1 < \dots < p_n$  be the first  $n$  primes with  $p_1 \geq 5$ . Moreover let  $\bar{p}_1 < \dots < \bar{p}_n$  be the next  $n$  primes with  $\bar{p}_1 > p_n$ . We associate  $x_i$  with  $p_i$  and  $\bar{x}_i$  with  $\bar{p}_i$  for all  $i \in [1, n]$ . For all

$j \in [1, m]$  we define numbers  $r_{j,1}, r_{j,2}, r_{j,3}, s_{j,1}, s_{j,2}, s_{j,3}$  as the smallest positive integers satisfying the congruences

$$\begin{aligned} s_{j,1} &\equiv 1 \pmod{\tilde{p}_{i_2}} & r_{j,1} &\equiv 0 \pmod{\tilde{p}_{i_2}} \\ s_{j,1} &\equiv 0 \pmod{\tilde{p}_{i_3}} & r_{j,1} &\equiv 1 \pmod{\tilde{p}_{i_3}} \\ \\ s_{j,2} &\equiv 1 \pmod{\tilde{p}_{i_1}} & r_{j,2} &\equiv 0 \pmod{\tilde{p}_{i_1}} \\ s_{j,2} &\equiv 0 \pmod{\tilde{p}_{i_3}} & r_{j,2} &\equiv 1 \pmod{\tilde{p}_{i_3}} \\ \\ s_{j,3} &\equiv 1 \pmod{\tilde{p}_{i_1}} & r_{j,3} &\equiv 0 \pmod{\tilde{p}_{i_1}} \\ s_{j,3} &\equiv 0 \pmod{\tilde{p}_{i_2}} & r_{j,3} &\equiv 1 \pmod{\tilde{p}_{i_2}} \end{aligned}$$

in which we assume  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  and define

$$\tilde{p}_{i_l} = \begin{cases} p_{i_l} & \text{if } \tilde{x}_{i_l} = x_{i_l} \\ \bar{p}_{i_l} & \text{if } \tilde{x}_{i_l} = \bar{x}_{i_l}. \end{cases}$$

Moreover for all  $i \in [1, n]$  we define numbers  $r_i, s_i$  as the smallest positive integers satisfying

$$\begin{aligned} s_i &\equiv 1 \pmod{p_i} & r_i &\equiv 0 \pmod{p_i} \\ s_i &\equiv 0 \pmod{\bar{p}_i} & r_i &\equiv 1 \pmod{\bar{p}_i}. \end{aligned}$$

We will work with the group

$$G = \prod_{i=1}^n V_i \times \prod_{j=1}^m U_j$$

in which  $V_i = S_{p_i}^{2d} \times S_{\bar{p}_i}^{2d} \times S_{p_i \bar{p}_i}$  and  $U_j = S_{\tilde{p}_{i_2} \tilde{p}_{i_3}}^{b_{j,2} b_{j,3}} \times S_{\tilde{p}_{i_1} \tilde{p}_{i_3}}^{b_{j,1} b_{j,3}} \times S_{\tilde{p}_{i_1} \tilde{p}_{i_2}}^{b_{j,1} b_{j,2}}$  with  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  and the following

$$d = \left\lceil \frac{\sum_{i=1}^n p_i \bar{p}_i + \sum_{c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\} \in C} (\tilde{p}_{i_2} \tilde{p}_{i_3} b_{j,2} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_3} b_{j,1} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_2} b_{j,1} b_{j,2})}{2} \right\rceil$$

and

$$\begin{aligned} a_{j,1} &= \tilde{p}_{i_2} \tilde{p}_{i_3} - \left\lfloor \frac{\tilde{p}_{i_2} \tilde{p}_{i_3} + 1}{2} - s_{j,1} \right\rfloor & b_{j,1} &= a_{j,1} - \frac{\tilde{p}_{i_2} \tilde{p}_{i_3} + 1}{2} \\ a_{j,2} &= \tilde{p}_{i_1} \tilde{p}_{i_3} - \left\lfloor \frac{\tilde{p}_{i_1} \tilde{p}_{i_3} + 1}{2} - s_{j,2} \right\rfloor & b_{j,2} &= a_{j,2} - \frac{\tilde{p}_{i_1} \tilde{p}_{i_3} + 1}{2} \\ a_{j,3} &= \tilde{p}_{i_1} \tilde{p}_{i_2} - \left\lfloor \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} + 1}{2} - s_{j,3} \right\rfloor & b_{j,3} &= a_{j,3} - \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} + 1}{2}. \end{aligned}$$

Note that  $b_{j,l} > 0$  by Lemma 10.  $G$  naturally embeds into  $S_N$  for

$$N = \sum_{i=1}^n (2d(p_i + \bar{p}_i) + p_i \bar{p}_i) + \sum_{c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\} \in C} (\tilde{p}_{i_2} \tilde{p}_{i_3} b_{j,2} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_3} b_{j,1} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_2} b_{j,1} b_{j,2}).$$

We define the input group elements  $\tau, \pi \in G$  as follows where  $i$  ranges over  $[1, n]$  and  $j$  ranges over  $[1, m]$  and  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ :

$$\tau = (\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$$

with

$$\begin{aligned}
\alpha_i &= (\bar{\alpha}_{i,1}^d, \bar{\alpha}_{i,2}^d, \alpha_{i,3}) & \beta_j &= (\bar{\beta}_{j,1}^{b_{j,2}b_{j,3}}, \bar{\beta}_{j,2}^{b_{j,1}b_{j,3}}, \bar{\beta}_{j,3}^{b_{j,1}b_{j,2}}) \\
\alpha_{i,1} &= (\llbracket p_i \rrbracket, \text{id}) & \beta_{j,1} &= \llbracket \tilde{p}_{i_2} \tilde{p}_{i_3} \rrbracket^{\frac{\tilde{p}_{i_2} \tilde{p}_{i_3} + 1}{2}} \\
\alpha_{i,2} &= (\llbracket \bar{p}_i \rrbracket, \text{id}) & \beta_{j,2} &= \llbracket \tilde{p}_{i_1} \tilde{p}_{i_3} \rrbracket^{\frac{\tilde{p}_{i_1} \tilde{p}_{i_3} + 1}{2}} \\
\alpha_{i,3} &= \llbracket p_i \bar{p}_i \rrbracket^{\frac{p_i \bar{p}_i + 1}{2}} & \beta_{j,3} &= \llbracket \tilde{p}_{i_1} \tilde{p}_{i_2} \rrbracket^{\frac{\tilde{p}_{i_1} \tilde{p}_{i_2} + 1}{2}}
\end{aligned}$$

and

$$\pi = (\gamma_1, \dots, \gamma_n, \delta_1, \dots, \delta_m)$$

with

$$\begin{aligned}
\gamma_i &= (\bar{\gamma}_{i,1}^d, \bar{\gamma}_{i,2}^d, \gamma_{i,3}) & \delta_j &= (\bar{\delta}_{j,1}^{b_{j,2}b_{j,3}}, \bar{\delta}_{j,2}^{b_{j,1}b_{j,3}}, \bar{\delta}_{j,3}^{b_{j,1}b_{j,2}}) \\
\gamma_{i,1} &= (\llbracket p_i \rrbracket, \llbracket p_i \rrbracket) & \delta_{j,1} &= \llbracket \tilde{p}_{i_2} \tilde{p}_{i_3} \rrbracket \\
\gamma_{i,2} &= (\llbracket \bar{p}_i \rrbracket, \llbracket p_i \rrbracket) & \delta_{j,2} &= \llbracket \tilde{p}_{i_1} \tilde{p}_{i_3} \rrbracket \\
\gamma_{i,3} &= \llbracket p_i \bar{p}_i \rrbracket & \delta_{j,3} &= \llbracket \tilde{p}_{i_1} \tilde{p}_{i_2} \rrbracket
\end{aligned}$$

and finally we define

$$\begin{aligned}
k &= N - \sum_{i=1}^n \left( d(2p_i - 1) + d(2\bar{p}_i - 1) + p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right) \\
&\quad - \sum_{j=1}^m (a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} - b_{j,1} b_{j,2} b_{j,3}).
\end{aligned}$$

Now we will show there is  $x \in \mathbb{N}$  such that  $U(\tau, \pi^x) \leq k$  if and only if  $X, C$  is a positive instance of **Not-All-Equal 3SAT**.

Suppose there is  $x \in \mathbb{N}$  such that  $U(\tau, \pi^x) \leq k$ .

**Claim 25.** *For all  $i \in [1, n]$  we have  $x \equiv 0, 1 \pmod{p_i}$  and  $x \equiv 0, 1 \pmod{\bar{p}_i}$  and*

$$\begin{aligned}
\text{lis}(\bar{\alpha}_{i,1}^d (\bar{\gamma}_{i,1}^d)^{-x}) &= d(2p_i - 1) \\
\text{lis}(\bar{\alpha}_{i,2}^d (\bar{\gamma}_{i,2}^d)^{-x}) &= d(2\bar{p}_i - 1).
\end{aligned}$$

Consider  $\alpha_i \gamma_i^{-x}$ . Let  $0 \leq b < p_i$  be the smallest positive integer such that  $x \equiv b \pmod{p_i}$ . Then we have

$$\alpha_{i,1} \gamma_{i,1}^{-x} = \alpha_{i,1} \gamma_{i,1}^{-b} = (\llbracket p_i \rrbracket^{1-b}, \llbracket p_i \rrbracket^{0-b})$$

and

$$\text{lis}(\alpha_{i,1} \gamma_{i,1}^{-x}) = \text{lis}(\llbracket p_i \rrbracket^{1-b}) + \text{lis}(\llbracket p_i \rrbracket^{0-b}).$$

We obtain by Lemma 15

$$\begin{aligned}
\text{lis}(\llbracket p_i \rrbracket^{1-b}) &= \max\{p_i - |1 - b|, |1 - b|\} \\
\text{lis}(\llbracket p_i \rrbracket^{0-b}) &= \max\{p_i - |0 - b|, |0 - b|\}.
\end{aligned}$$

In the case  $0 \leq b \leq 1$  we obtain  $\max\{p_i - |1 - b|, |1 - b|\} = p_i - |1 - b| = p_i - 1 + b$  and  $\max\{p_i - |0 - b|, |0 - b|\} = p_i - |0 - b| = p_i - b$ . By this we obtain

$$\text{lis}(\alpha_{i,1} \gamma_{i,1}^{-x}) = p_i - 1 + b + p_i - b = 2p_i - 1.$$

In the case  $2 \leq b \leq \frac{p_i-1}{2}$  we obtain  $\max\{p_i - |1 - b|, |1 - b|\} = p_i - |1 - b| = p_i + 1 - b$  and  $\max\{p_i - |0 - b|, |0 - b|\} = p_i - |0 - b| = p_i - b$  and

$$\text{lis}(\alpha_{i,1} \gamma_{i,1}^{-x}) = p_i + 1 - b + p_i - b \leq 2p_i - 3.$$

For  $b = \frac{p_i+1}{2}$  we obtain  $\max\{p_i - |1-b|, |1-b|\} = p_i - |1-b| = p_i + 1 - b$  and  $\max\{p_i - |0-b|, |0-b|\} = |0-b| = b$  and

$$\text{lis}(\alpha_{i,1}\gamma_{i,1}^{-x}) = p_i + 1 - b + b = p_i + 1 \leq 2p_i - 3$$

since  $p_i \geq 5$ . In the case  $\frac{p_i+3}{2} \leq b \leq p_i - 1$  we obtain  $\max\{p_i - |1-b|, |1-b|\} = |1-b| = b - 1$  and  $\max\{p_i - |0-b|, |0-b|\} = |0-b| = b$  and

$$\text{lis}(\alpha_{i,1}\gamma_{i,1}^{-x}) = b - 1 + b \leq 2p_i - 3.$$

Analogously we obtain  $\text{lis}(\alpha_{i,2}\gamma_{i,2}^{-x}) = 2\bar{p}_i - 1$  if  $x \equiv 0, 1 \pmod{\bar{p}_i}$  and  $\text{lis}(\alpha_{i,2}\gamma_{i,2}^{-x}) \leq 2\bar{p}_i - 3$  if  $x \not\equiv 0, 1 \pmod{\bar{p}_i}$ . From this we obtain

$$\text{lis}(\bar{\alpha}_{i,1}^d(\bar{\gamma}_{i,1}^d)^{-x}) \begin{cases} = d(2p_i - 1) & \text{if } x \equiv 0, 1 \pmod{p_i} \\ \leq d(2p_i - 3) & \text{if } x \not\equiv 0, 1 \pmod{p_i} \end{cases}$$

and

$$\text{lis}(\bar{\alpha}_{i,2}^d(\bar{\gamma}_{i,2}^d)^{-x}) \begin{cases} = d(2\bar{p}_i - 1) & \text{if } x \equiv 0, 1 \pmod{\bar{p}_i} \\ \leq d(2\bar{p}_i - 3) & \text{if } x \not\equiv 0, 1 \pmod{\bar{p}_i}. \end{cases}$$

Now suppose there is an  $e \in [1, n]$  such that  $x \not\equiv 0, 1 \pmod{p_e}$  or  $x \not\equiv 0, 1 \pmod{\bar{p}_e}$ . Then

$$\begin{aligned} \text{lis}(\bar{\alpha}_{e,1}^d(\bar{\gamma}_{e,1}^d)^{-x}) &\leq d(2p_e - 3) = d(2p_e - 1) - 2d \\ \text{or } \text{lis}(\bar{\alpha}_{e,2}^d(\bar{\gamma}_{e,2}^d)^{-x}) &\leq d(2\bar{p}_e - 3) = d(2\bar{p}_e - 1) - 2d. \end{aligned}$$

By using the above upper bounds and the following trivial upper bounds  $\text{lis}\left(\llbracket p_i \bar{p}_i \rrbracket^{\frac{p_i \bar{p}_i + 1}{2} - x}\right) \leq p_i \bar{p}_i$

for all  $i \in [1, n]$  and  $\text{lis}\left(\llbracket \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}}{\tilde{p}_{i_l}} \rrbracket^{\frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3} + 1}{2\tilde{p}_{i_l}} - x}\right) \leq \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}}{\tilde{p}_{i_l}}$  and hence

$$\text{lis}\left(\bar{\beta}_{j,l}^{\frac{b_{j,1}b_{j,2}b_{j,3}}{b_{j,l}}} \left(\bar{\delta}_{j,l}^{\frac{b_{j,1}b_{j,2}b_{j,3}}{b_{j,l}}}\right)^{-x}\right) \leq \frac{b_{j,1}b_{j,2}b_{j,3}}{b_{j,l}} \cdot \frac{\tilde{p}_{i_1}\tilde{p}_{i_2}\tilde{p}_{i_3}}{\tilde{p}_{i_l}}$$

for all  $j \in [1, m]$  and  $l \in [1, 3]$  where  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  we obtain

$$\begin{aligned} \text{lis}(\tau\pi^{-x}) &\leq \sum_{i=1}^n (d(2p_i - 1) + d(2\bar{p}_i - 1) + p_i \bar{p}_i) - 2d \\ &\quad + \sum_{c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\} \in C} (\tilde{p}_{i_2} \tilde{p}_{i_3} b_{j,2} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_3} b_{j,1} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_2} b_{j,1} b_{j,2}). \end{aligned}$$

From this it follows now that

$$\begin{aligned}
U(\tau, \pi^x) &= N - \text{lis}(\tau \pi^{-x}) \\
&\geq N - \sum_{i=1}^n (d(2p_i - 1) + d(2\bar{p}_i - 1) + p_i \bar{p}_i) + 2d \\
&\quad - \sum_{c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\} \in C} (\tilde{p}_{i_2} \tilde{p}_{i_3} b_{j,2} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_3} b_{j,1} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_2} b_{j,1} b_{j,2}) \\
&\geq N - \sum_{i=1}^n (d(2p_i - 1) + d(2\bar{p}_i - 1) + p_i \bar{p}_i) \\
&\quad + \sum_{i=1}^n p_i \bar{p}_i + \sum_{c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\} \in C} (\tilde{p}_{i_2} \tilde{p}_{i_3} b_{j,2} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_3} b_{j,1} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_2} b_{j,1} b_{j,2}) \\
&\quad - \sum_{c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\} \in C} (\tilde{p}_{i_2} \tilde{p}_{i_3} b_{j,2} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_3} b_{j,1} b_{j,3} + \tilde{p}_{i_1} \tilde{p}_{i_2} b_{j,1} b_{j,2}) \\
&= N - \sum_{i=1}^n (d(2p_i - 1) + d(2\bar{p}_i - 1)) \\
&> k
\end{aligned}$$

which is a contradiction. Thus  $x \equiv 0, 1 \pmod{p_i}$  and  $x \equiv 0, 1 \pmod{\bar{p}_i}$  and

$$\begin{aligned}
\text{lis}(\bar{\alpha}_{i,1}^d (\gamma_{i,1}^d)^{-x}) &= d(2p_i - 1) \\
\text{lis}(\bar{\alpha}_{i,2}^d (\gamma_{i,2}^d)^{-x}) &= d(2\bar{p}_i - 1)
\end{aligned}$$

for all  $i \in [1, n]$ . □

**Claim 26.** For all  $j \in [1, m]$  we have

$$\text{lis}(\beta_j \delta_j^{-x}) = \begin{cases} a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} - 3b_{j,1} b_{j,2} b_{j,3} & \text{if } x \equiv 0, 1 \pmod{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}} \\ a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} - b_{j,1} b_{j,2} b_{j,3} & \text{if } x \not\equiv 0, 1 \pmod{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}} \end{cases}$$

in which  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ .

Suppose  $x \equiv 0, 1 \pmod{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}}$ . Then we have for all  $l \in [1, 3]$  by Lemmas 14 and 15

$$\begin{aligned}
\text{lis}(\beta_{j,l} \delta_{j,l}^{-x}) &= \text{lis} \left( \left\lfloor \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}}{\tilde{p}_{i_l}} \right\rfloor^{\frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3} + \tilde{p}_{i_l}}{2\tilde{p}_{i_l}} - x} \right) \\
&= \max \left\{ \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3}}{\tilde{p}_{i_l}} - \left\lfloor \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3} + \tilde{p}_{i_l}}{2\tilde{p}_{i_l}} - x \right\rfloor, \left\lfloor \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3} + \tilde{p}_{i_l}}{2\tilde{p}_{i_l}} - x \right\rfloor \right\} \\
&= \frac{\tilde{p}_{i_1} \tilde{p}_{i_2} \tilde{p}_{i_3} + \tilde{p}_{i_l}}{2\tilde{p}_{i_l}} \\
&= a_{j,l} - b_{j,l}.
\end{aligned}$$

Thus

$$\text{lis} \left( \frac{\beta_{j,l}^{\frac{b_{j,1} b_{j,2} b_{j,3}}{b_{j,l}}}}{\delta_{j,l}^{\frac{b_{j,1} b_{j,2} b_{j,3}}{b_{j,l}}}} \right)^{-x} = \frac{b_{j,1} b_{j,2} b_{j,3}}{b_{j,l}} (a_{j,l} - b_{j,l})$$

from which it follows now that

$$\begin{aligned}
\text{lis}(\beta_j \delta_j^{-x}) &= b_{j,2} b_{j,3} (a_{j,1} - b_{j,1}) + b_{j,1} b_{j,3} (a_{j,2} - b_{j,2}) + b_{j,1} b_{j,2} (a_{j,3} - b_{j,3}) \\
&= a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} - 3b_{j,1} b_{j,2} b_{j,3}.
\end{aligned}$$

Now suppose  $x \not\equiv 0, 1 \pmod{\tilde{p}_{i_1}\tilde{p}_{i_2}\tilde{p}_{i_3}}$ . By Claim 25 we have  $x \equiv 0, 1 \pmod{p_i}$  and  $x \equiv 0, 1 \pmod{\tilde{p}_i}$  for all  $i \in [1, n]$ . Thus there are  $g, h \in [1, 3]$  and  $c \in \{0, 1\}$  with  $g \neq h$  such that  $x \equiv c \pmod{\tilde{p}_{i_g}}$  and  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$  and let w.l.o.g.  $f \in [1, 3] \setminus \{g, h\}$  be such that  $x \equiv c \pmod{\tilde{p}_{i_f}}$ . Then we obtain by Lemmas 14 and 15

$$\begin{aligned}
\text{lis}(\beta_{j,h}\delta_{j,h}^{-x}) &= \text{lis}\left(\llbracket \tilde{p}_{i_g}\tilde{p}_{i_f} \rrbracket^{\frac{\tilde{p}_{i_g}\tilde{p}_{i_f}+1}{2}} - x\right) \\
&= \text{lis}\left(\llbracket \tilde{p}_{i_g}\tilde{p}_{i_f} \rrbracket^{\frac{\tilde{p}_{i_g}\tilde{p}_{i_f}+1}{2}} - c\right) \\
&= \max\{\tilde{p}_{i_g}\tilde{p}_{i_f} - |\frac{\tilde{p}_{i_g}\tilde{p}_{i_f}+1}{2} - c|, |\frac{\tilde{p}_{i_g}\tilde{p}_{i_f}+1}{2} - c|\} \\
&= \frac{\tilde{p}_{i_g}\tilde{p}_{i_f}+1}{2} \\
&= a_{j,h} - b_{j,h}.
\end{aligned}$$

Moreover we have  $x \equiv s_{j,f} \pmod{\tilde{p}_{i_g}\tilde{p}_{i_h}}$  and  $x \equiv s_{j,g} \pmod{\tilde{p}_{i_f}\tilde{p}_{i_h}}$  or  $x \equiv r_{j,f} \pmod{\tilde{p}_{i_g}\tilde{p}_{i_h}}$  and  $x \equiv r_{j,g} \pmod{\tilde{p}_{i_f}\tilde{p}_{i_h}}$ . By Lemma 10 we have

$$\begin{aligned}
|\frac{\tilde{p}_{i_g}\tilde{p}_{i_h}+1}{2} - r_{j,f}| &= |\frac{\tilde{p}_{i_g}\tilde{p}_{i_h}+1}{2} - s_{j,f}| \\
|\frac{\tilde{p}_{i_f}\tilde{p}_{i_h}+1}{2} - r_{j,g}| &= |\frac{\tilde{p}_{i_f}\tilde{p}_{i_h}+1}{2} - s_{j,g}|
\end{aligned}$$

and hence Lemmas 14 and 15 give us

$$\begin{aligned}
\text{lis}(\beta_{j,f}\delta_{j,f}^{-x}) &= \text{lis}\left(\llbracket \tilde{p}_{i_g}\tilde{p}_{i_h} \rrbracket^{\frac{\tilde{p}_{i_g}\tilde{p}_{i_h}+1}{2}} - x\right) \\
&= \max\{\tilde{p}_{i_g}\tilde{p}_{i_h} - |\frac{\tilde{p}_{i_g}\tilde{p}_{i_h}+1}{2} - s_{j,f}|, |\frac{\tilde{p}_{i_g}\tilde{p}_{i_h}+1}{2} - s_{j,f}|\} \\
&= \tilde{p}_{i_g}\tilde{p}_{i_h} - |\frac{\tilde{p}_{i_g}\tilde{p}_{i_h}+1}{2} - s_{j,f}| \\
&= a_{j,f}
\end{aligned}$$

and

$$\begin{aligned}
\text{lis}(\beta_{j,g}\delta_{j,g}^{-x}) &= \text{lis}\left(\llbracket \tilde{p}_{i_f}\tilde{p}_{i_h} \rrbracket^{\frac{\tilde{p}_{i_f}\tilde{p}_{i_h}+1}{2}} - x\right) \\
&= \max\{\tilde{p}_{i_f}\tilde{p}_{i_h} - |\frac{\tilde{p}_{i_f}\tilde{p}_{i_h}+1}{2} - s_{j,g}|, |\frac{\tilde{p}_{i_f}\tilde{p}_{i_h}+1}{2} - s_{j,g}|\} \\
&= \tilde{p}_{i_f}\tilde{p}_{i_h} - |\frac{\tilde{p}_{i_f}\tilde{p}_{i_h}+1}{2} - s_{j,g}| \\
&= a_{j,g}.
\end{aligned}$$

Thus

$$\begin{aligned}
\text{lis}\left(\bar{\beta}_{j,h}^{b_{j,f}b_{j,g}}\left(\bar{\delta}_{j,h}^{b_{j,f}b_{j,g}}\right)^{-x}\right) &= b_{j,f}b_{j,g}(a_{j,h} - b_{j,h}) \\
\text{lis}\left(\bar{\beta}_{j,f}^{b_{j,h}b_{j,g}}\left(\bar{\delta}_{j,f}^{b_{j,h}b_{j,g}}\right)^{-x}\right) &= b_{j,h}b_{j,g}a_{j,f}
\end{aligned}$$

and

$$\text{lis}\left(\bar{\beta}_{j,g}^{b_{j,h}b_{j,f}}\left(\bar{\delta}_{j,g}^{b_{j,h}b_{j,f}}\right)^{-x}\right) = b_{j,h}b_{j,f}a_{j,g}.$$

From this it finally follows that

$$\begin{aligned}
\text{lis}(\beta_j\delta_j^{-x}) &= b_{j,f}b_{j,g}(a_{j,h} - b_{j,h}) + b_{j,h}b_{j,g}a_{j,f} + b_{j,h}b_{j,f}a_{j,g} \\
&= a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} - b_{j,1}b_{j,2}b_{j,3}.
\end{aligned}$$

□

**Claim 27.** For all  $i \in [1, n]$  we have

$$\text{lis}(\alpha_{i,3}\gamma_{i,3}^{-x}) = \begin{cases} \frac{p_i\bar{p}_i+1}{2} & \text{if } x \equiv 0, 1 \pmod{p_i\bar{p}_i} \\ p_i\bar{p}_i - \left| \frac{p_i\bar{p}_i+1}{2} - s_i \right| & \text{if } x \not\equiv 0, 1 \pmod{p_i\bar{p}_i}. \end{cases}$$

Suppose  $x \equiv 0, 1 \pmod{p_i\bar{p}_i}$ . Then we have by Lemmas 14 and 15

$$\begin{aligned} \text{lis}(\alpha_{i,3}\gamma_{i,3}^{-x}) &= \text{lis}\left(\left\lfloor p_i\bar{p}_i \right\rfloor^{\frac{p_i\bar{p}_i+1}{2}-x}\right) \\ &= \max\left\{p_i\bar{p}_i - \left| \frac{p_i\bar{p}_i+1}{2} - x \right|, \left| \frac{p_i\bar{p}_i+1}{2} - x \right|\right\} \\ &= \frac{p_i\bar{p}_i+1}{2}. \end{aligned}$$

Now suppose  $x \not\equiv 0, 1 \pmod{p_i\bar{p}_i}$ . By Claim 25 we have  $x \equiv 0, 1 \pmod{p_i}$  and  $x \equiv 0, 1 \pmod{\bar{p}_i}$  for all  $i \in [1, n]$ . Thus  $x \equiv s_i \pmod{p_i\bar{p}_i}$  or  $x \equiv r_i \pmod{p_i\bar{p}_i}$ . By Lemma 10 we have

$$\left| \frac{p_i\bar{p}_i+1}{2} - r_i \right| = \left| \frac{p_i\bar{p}_i+1}{2} - s_i \right|$$

and by Lemmas 14 and 15 we finally obtain

$$\begin{aligned} \text{lis}(\alpha_{i,3}\gamma_{i,3}^{-x}) &= \text{lis}\left(\left\lfloor p_i\bar{p}_i \right\rfloor^{\frac{p_i\bar{p}_i+1}{2}-x}\right) \\ &= \max\left\{p_i\bar{p}_i - \left| \frac{p_i\bar{p}_i+1}{2} - s_i \right|, \left| \frac{p_i\bar{p}_i+1}{2} - s_i \right|\right\} \\ &= p_i\bar{p}_i - \left| \frac{p_i\bar{p}_i+1}{2} - s_i \right|. \end{aligned}$$

□

**Claim 28.** For all  $i \in [1, n]$  we have  $x \equiv 1 \pmod{p_i}$  and  $x \equiv 0 \pmod{\bar{p}_i}$  or  $x \equiv 0 \pmod{p_i}$  and  $x \equiv 1 \pmod{\bar{p}_i}$ .

Suppose there is an  $e \in [1, n]$  for which the contrary holds. By Claim 25 we have  $x \equiv 0, 1 \pmod{p_e}$  and  $x \equiv 0, 1 \pmod{\bar{p}_e}$ . Therefore it suffices to consider the cases  $x \equiv 0, 1 \pmod{p_e\bar{p}_e}$ . Then by Claim 27 we have  $\text{lis}(\alpha_{e,3}\gamma_{e,3}^{-x}) = \frac{p_e\bar{p}_e+1}{2}$ . Summing over all upper bounds Claim 25, 26 and 27 yield we obtain

$$\begin{aligned} U(\tau, \pi^x) &= N - \text{lis}(\tau\pi^{-x}) \\ &\geq N - \sum_{i=1}^n \left( d(2p_i - 1) + d(2\bar{p}_i - 1) + p_i\bar{p}_i - \left| \frac{p_i\bar{p}_i+1}{2} - s_i \right| \right) \\ &\quad + p_e\bar{p}_e - \left| \frac{p_e\bar{p}_e+1}{2} - s_e \right| - \frac{p_e\bar{p}_e+1}{2} \\ &\quad - \sum_{j=1}^m (a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} - b_{j,1}b_{j,2}b_{j,3}) \\ &> k \end{aligned}$$

since  $\frac{p_e\bar{p}_e+1}{2} < p_e\bar{p}_e - \left| \frac{p_e\bar{p}_e+1}{2} - s_e \right|$  by Lemma 10 which is a contradiction. □

**Claim 29.** For every clause  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  the following holds: If there are  $f, g \in [1, 3]$  with  $f \neq g$  and  $c \in \{0, 1\}$  such that  $x \equiv c \pmod{\tilde{p}_{i_f}}$  and  $x \equiv c \pmod{\tilde{p}_{i_g}}$  then  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$  where  $h$  is the unique element in  $[1, 3] \setminus \{f, g\}$ .

Suppose there is a clause  $c_e = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  such that  $x \equiv c \pmod{\tilde{p}_{i_l}}$  for all  $l \in [1, 3]$  and some  $c \in \{0, 1\}$ . Then we have by Claim 26

$$\text{lis}(\beta_e\delta_e^{-x}) = a_{e,1}b_{e,2}b_{e,3} + a_{e,2}b_{e,1}b_{e,3} + a_{e,3}b_{e,1}b_{e,2} - 3b_{e,1}b_{e,2}b_{e,3}.$$



Summing over all upper bounds Claim 25,26 and 27 yield we obtain

$$\begin{aligned}
U(\tau, \pi^x) &= N - \text{lis}(\tau \pi^{-x}) \\
&\geq N - \sum_{i=1}^n \left( d(2p_i - 1) + d(2\bar{p}_i - 1) + p_i \bar{p}_i - \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right| \right) \\
&\quad - \sum_{j=1}^m (a_{j,1} b_{j,2} b_{j,3} + a_{j,2} b_{j,1} b_{j,3} + a_{j,3} b_{j,1} b_{j,2} - b_{j,1} b_{j,2} b_{j,3}) \\
&\quad + (a_{e,1} b_{e,2} b_{e,3} + a_{e,2} b_{e,1} b_{e,3} + a_{e,3} b_{e,1} b_{e,2} - b_{e,1} b_{e,2} b_{e,3}) \\
&\quad - (a_{e,1} b_{e,2} b_{e,3} + a_{e,2} b_{e,1} b_{e,3} + a_{e,3} b_{e,1} b_{e,2} - 3b_{e,1} b_{e,2} b_{e,3}) \\
&> k
\end{aligned}$$

which is a contradiction. Hence we obtain for every clause  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ : If there are  $f, g \in [1, 3]$  with  $f \neq g$  and  $c \in \{0, 1\}$  such that  $x \equiv c \pmod{\tilde{p}_{i_f}}$  and  $x \equiv c \pmod{\tilde{p}_{i_g}}$  then  $x \not\equiv c \pmod{\tilde{p}_{i_h}}$  where  $h$  is the unique element in  $[1, 3] \setminus \{f, g\}$ . Since by Claim 25 we have  $x \equiv 0, 1 \pmod{\tilde{p}_{i_h}}$  we finally obtain  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$ .  $\square$

Now we define a truth assignment  $\sigma$  by the following:

$$\sigma(x_i) = \begin{cases} 1 & \text{if } x \equiv 1 \pmod{p_i} \\ 0 & \text{if } x \equiv 0 \pmod{p_i} \end{cases}$$

for all  $i \in [1, n]$ . Let  $\hat{\sigma}$  be the extension of  $\sigma$  to literals. Now we will show for every clause  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  there are pairwise different numbers  $f, g, h \in [1, 3]$  and  $c \in \{0, 1\}$  such that

$$\begin{aligned}
\hat{\sigma}(\tilde{x}_{i_f}) &= c \\
\hat{\sigma}(\tilde{x}_{i_g}) &= c \\
\hat{\sigma}(\tilde{x}_{i_h}) &= 1 - c.
\end{aligned}$$

By Claim 25 we have  $x \equiv 0, 1 \pmod{p_i}$  and  $x \equiv 0, 1 \pmod{\bar{p}_i}$  for all  $i \in [1, n]$ . Hence there clearly are  $f, g \in [1, 3]$  with  $f \neq g$  and  $c \in \{0, 1\}$  such that  $x \equiv c \pmod{\tilde{p}_{i_f}}$  and  $x \equiv c \pmod{\tilde{p}_{i_g}}$ . In the case  $\tilde{p}_{i_f} = p_{i_f}$  we obtain  $\sigma(x_{i_f}) = c$  and hence  $\hat{\sigma}(\tilde{x}_{i_f}) = c$ . In the case  $\tilde{p}_{i_f} = \bar{p}_{i_f}$  we have  $x \equiv 1 - c \pmod{p_{i_f}}$  by Claim 28. Thus  $\sigma(x_{i_f}) = 1 - c$  and  $\hat{\sigma}(\tilde{x}_{i_f}) = c$ . Analogously we obtain  $\hat{\sigma}(\tilde{x}_{i_g}) = c$ . Since we have  $x \equiv c \pmod{\tilde{p}_{i_f}}$  and  $x \equiv c \pmod{\tilde{p}_{i_g}}$  we obtain  $x \equiv 1 - c \pmod{\tilde{p}_{i_h}}$  by Claim 29. As above we then analogously obtain  $\hat{\sigma}(\tilde{x}_{i_h}) = 1 - c$  which eventually shows that  $X, C$  is a positive instance of Not-All-Equal 3SAT.

Vice versa suppose  $X, C$  is a positive instance of Not-All-Equal 3SAT and let  $\sigma$  be a truth assignment such that for every clause  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$  there are pairwise different numbers  $f, g, h \in [1, 3]$  and  $c \in \{0, 1\}$  such that

$$\begin{aligned}
\hat{\sigma}(\tilde{x}_{i_f}) &= c \\
\hat{\sigma}(\tilde{x}_{i_g}) &= c \\
\hat{\sigma}(\tilde{x}_{i_h}) &= 1 - c.
\end{aligned}$$

Then we define  $x$  as the smallest positive integer satisfying

$$\begin{aligned}
x &\equiv \sigma(x_i) \pmod{p_i} \\
x &\equiv 1 - \sigma(x_i) \pmod{\bar{p}_i}
\end{aligned}$$

for all  $i \in [1, n]$ . Then we have  $x \equiv s_i, r_i \pmod{p_i \bar{p}_i}$  for all  $i \in [1, n]$  and because

$$\left| \frac{p_i \bar{p}_i + 1}{2} - r_i \right| = \left| \frac{p_i \bar{p}_i + 1}{2} - s_i \right|$$

by Lemma 10 we obtain by Lemmas 14 and 15

$$\begin{aligned}\text{lis}(\alpha_{i,1}\gamma_{i,1}^{-x}) &= \text{lis}(\llbracket p_i \rrbracket^{1-x}) + \text{lis}(\llbracket p_i \rrbracket^{0-x}) \\ &= \max\{p_i - |1-x|, |1-x|\} + \max\{p_i - |0-x|, |0-x|\} \\ &= 2p_i - 1\end{aligned}$$

$$\begin{aligned}\text{lis}(\alpha_{i,2}\gamma_{i,2}^{-x}) &= \text{lis}(\llbracket \bar{p}_i \rrbracket^{1-x}) + \text{lis}(\llbracket \bar{p}_i \rrbracket^{0-x}) \\ &= \max\{\bar{p}_i - |1-x|, |1-x|\} + \max\{\bar{p}_i - |0-x|, |0-x|\} \\ &= 2\bar{p}_i - 1\end{aligned}$$

and

$$\begin{aligned}\text{lis}(\alpha_{i,3}\gamma_{i,3}^{-x}) &= \text{lis}\left(\llbracket p_i \bar{p}_i \rrbracket^{\frac{p_i \bar{p}_i + 1}{2} - x}\right) \\ &= \max\{p_i \bar{p}_i - |\frac{p_i \bar{p}_i + 1}{2} - x|, |\frac{p_i \bar{p}_i + 1}{2} - x|\} \\ &= p_i \bar{p}_i - |\frac{p_i \bar{p}_i + 1}{2} - s_i|.\end{aligned}$$

Thus

$$\begin{aligned}\text{lis}(\bar{\alpha}_{i,1}^d(\bar{\gamma}_{i,1}^d)^{-x}) &= d(2p_i - 1) \\ \text{lis}(\bar{\alpha}_{i,2}^d(\bar{\gamma}_{i,2}^d)^{-x}) &= d(2\bar{p}_i - 1)\end{aligned}$$

and

$$\text{lis}(\alpha_i \gamma_i^{-x}) = d(2p_i - 1) + d(2\bar{p}_i - 1) + p_i \bar{p}_i - |\frac{p_i \bar{p}_i + 1}{2} - s_i|. \quad (29)$$

Let  $j \in [1, m]$  and suppose  $c_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ . Then there are pairwise different numbers  $f, g, h \in [1, 3]$  and  $c \in \{0, 1\}$  such that

$$\begin{aligned}\hat{\sigma}(\tilde{x}_{i_f}) &= c \\ \hat{\sigma}(\tilde{x}_{i_g}) &= c \\ \hat{\sigma}(\tilde{x}_{i_h}) &= 1 - c.\end{aligned}$$

By definition we have  $x \equiv \sigma(x_i) \bmod p_i$  and  $x \equiv 1 - \sigma(x_i) \bmod \bar{p}_i$  for all  $i \in [1, n]$  which gives us

$$x \equiv \begin{cases} \sigma(x_{i_f}) \equiv \hat{\sigma}(\tilde{x}_{i_f}) \equiv c \bmod p_{i_f} & \text{if } \tilde{x}_{i_f} = x_{i_f} \\ 1 - \sigma(x_{i_f}) \equiv \hat{\sigma}(\tilde{x}_{i_f}) \equiv c \bmod \bar{p}_{i_f} & \text{if } \tilde{x}_{i_f} = \bar{x}_{i_f} \end{cases}$$

and hence  $x \equiv c \bmod \tilde{p}_{i_f}$ . Analogously we obtain  $x \equiv c \bmod \tilde{p}_{i_g}$  and  $x \equiv 1 - c \bmod \tilde{p}_{i_h}$ . Then we have  $x \equiv s_{j,f}, r_{j,f} \bmod \tilde{p}_{i_f}$  and  $x \equiv s_{j,g}, r_{j,g} \bmod \tilde{p}_{i_g}$  and we obtain by Lemmas 14 and 15

$$\begin{aligned}\text{lis}(\beta_{j,f}\delta_{j,f}^{-x}) &= \text{lis}\left(\llbracket \tilde{p}_{i_g} \tilde{p}_{i_h} \rrbracket^{\frac{\tilde{p}_{i_g} \tilde{p}_{i_h} + 1}{2} - x}\right) \\ &= \max\{\tilde{p}_{i_g} \tilde{p}_{i_h} - |\frac{\tilde{p}_{i_g} \tilde{p}_{i_h} + 1}{2} - x|, |\frac{\tilde{p}_{i_g} \tilde{p}_{i_h} + 1}{2} - x|\} \\ &= \tilde{p}_{i_g} \tilde{p}_{i_h} - |\frac{\tilde{p}_{i_g} \tilde{p}_{i_h} + 1}{2} - s_{j,f}| \\ &= a_{j,f}\end{aligned}$$

$$\begin{aligned}
\text{lis}(\beta_{j,g}\delta_{j,g}^{-x}) &= \text{lis}\left(\left\lfloor \tilde{p}_{i_f}\tilde{p}_{i_h} \right\rfloor^{\frac{\tilde{p}_{i_f}\tilde{p}_{i_h}+1}{2}-x}\right) \\
&= \max\{\tilde{p}_{i_f}\tilde{p}_{i_h} - \left|\frac{\tilde{p}_{i_f}\tilde{p}_{i_h}+1}{2} - x\right|, \left|\frac{\tilde{p}_{i_f}\tilde{p}_{i_h}+1}{2} - x\right|\} \\
&= \tilde{p}_{i_f}\tilde{p}_{i_h} - \left|\frac{\tilde{p}_{i_f}\tilde{p}_{i_h}+1}{2} - s_{j,g}\right| \\
&= a_{j,g}
\end{aligned}$$

and

$$\begin{aligned}
\text{lis}(\beta_{j,h}\delta_{j,h}^{-x}) &= \text{lis}\left(\left\lfloor \tilde{p}_{i_f}\tilde{p}_{i_g} \right\rfloor^{\frac{\tilde{p}_{i_f}\tilde{p}_{i_g}+1}{2}-x}\right) \\
&= \text{lis}\left(\left\lfloor \tilde{p}_{i_f}\tilde{p}_{i_g} \right\rfloor^{\frac{\tilde{p}_{i_f}\tilde{p}_{i_g}+1}{2}-c}\right) \\
&= \max\{\tilde{p}_{i_f}\tilde{p}_{i_g} - \left|\frac{\tilde{p}_{i_f}\tilde{p}_{i_g}+1}{2} - c\right|, \left|\frac{\tilde{p}_{i_f}\tilde{p}_{i_g}+1}{2} - c\right|\} \\
&= \frac{\tilde{p}_{i_f}\tilde{p}_{i_g}+1}{2} \\
&= a_{j,h} - b_{j,h}.
\end{aligned}$$

By this we obtain

$$\begin{aligned}
\text{lis}\left(\tilde{\beta}_{j,f}^{b_{j,g}b_{j,h}}\left(\tilde{\delta}_{j,f}^{b_{j,g}b_{j,h}}\right)^{-x}\right) &= b_{j,g}b_{j,h}a_{j,f} \\
\text{lis}\left(\tilde{\beta}_{j,g}^{b_{j,f}b_{j,h}}\left(\tilde{\delta}_{j,g}^{b_{j,f}b_{j,h}}\right)^{-x}\right) &= b_{j,f}b_{j,h}a_{j,g}
\end{aligned}$$

and

$$\text{lis}\left(\tilde{\beta}_{j,h}^{b_{j,f}b_{j,g}}\left(\tilde{\delta}_{j,h}^{b_{j,f}b_{j,g}}\right)^{-x}\right) = b_{j,f}b_{j,g}(a_{j,h} - b_{j,h}).$$

From this it follows now that

$$\begin{aligned}
\text{lis}(\beta_j\delta_j^{-x}) &= b_{j,g}b_{j,h}a_{j,f} + b_{j,f}b_{j,h}a_{j,g} + b_{j,f}b_{j,g}(a_{j,h} - b_{j,h}) \\
&= a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} - b_{j,1}b_{j,2}b_{j,3}.
\end{aligned} \tag{30}$$

Using (29) and (30) and summing up we obtain

$$\begin{aligned}
\text{lis}(\tau\pi^{-x}) &= \sum_{i=1}^n \left( d(2p_i - 1) + d(2\bar{p}_i - 1) + p_i\bar{p}_i - \left|\frac{p_i\bar{p}_i + 1}{2} - s_i\right| \right) \\
&\quad + \sum_{j=1}^m (a_{j,1}b_{j,2}b_{j,3} + a_{j,2}b_{j,1}b_{j,3} + a_{j,3}b_{j,1}b_{j,2} - b_{j,1}b_{j,2}b_{j,3})
\end{aligned}$$

which finally gives us

$$U(\tau, \pi^x) = N - \text{lis}(\tau\pi^{-x}) = k.$$

□

## 4 Conclusion

We have shown that the SUBGROUP DISTANCE PROBLEM is **NP**-complete in cyclic permutation groups for all metrics mentioned in the introduction. This paper only focuses on the SUBGROUP DISTANCE PROBLEM but in the literature also the maximum subgroup distance problem was studied in [4] and the weight problem and further variants were studied in [6]. Further research could

try to show also for these problems NP-completeness when the input group is cyclic or at least given by a few generators since NP-completeness is not necessarily obtainable for cyclic groups. Although the SUBGROUP DISTANCE PROBLEM is NP-complete in cyclic permutation groups for all metrics mentioned in the introduction this does not necessarily hold for the minimum weight problem in cyclic groups. We give an example: consider the minimum weight problem regarding the Hamming weight (i.e.  $w_H(\tau) = |\{i \mid i^\tau \neq i\}|$ ). It can be decided in polynomial time whether there is a number  $z \in \mathbb{N}$  with  $z \not\equiv 0 \pmod{\text{ord}(\tau)}$  such that  $w_H(\tau^z) \leq k$  for some  $\tau \in S_n$  by simply checking whether there is a prime  $p \mid \text{ord}(\tau)$  such that  $w_H\left(\tau^{\frac{\text{ord}(\tau)}{p}}\right) \leq k$ . Note that such primes are relatively small since  $\text{ord}(\tau) \mid n!$  and hence  $p \leq n$ . On the other hand in [13] it was shown that it is NP-complete to decide whether for some given  $\alpha, \beta \in S_n$  the coset  $\beta\langle\alpha\rangle$  contains a fixed-point-free element  $\beta\alpha^z$  for some  $z \in \mathbb{N}$ . This problem is equivalent to asking whether there is  $z \in \mathbb{N}$  such that  $H(\beta, \alpha^{-z}) \geq n$ . This is seen as follows: for all  $i \in [1, n]$  we have  $i^{\beta\alpha^z} \neq i$  if and only if for all  $i \in [1, n]$  we have  $i^\beta = i^{\beta\alpha^z\alpha^{-z}} \neq i^{\alpha^{-z}}$ . By this the maximum subgroup distance problem regarding the Hamming distance is NP-complete when the input group is cyclic.

## 4.1 Open Problems

We have shown that it can be decided in NL whether for given permutations  $\alpha, \beta \in S_n$  there is  $x \in \mathbb{N}$  such that  $l_\infty(\beta, \alpha^x) \leq 1$ . We do not know if this problem is NL-complete or can even be solved in deterministic log-space. Moreover this problem becomes NP-complete when the input group is abelian and given by at least 2 generators. However we were only able to proof NP-completeness for the problem  $l_\infty(\beta, \alpha^x) \leq k$  when  $k$  is part of the input rather than a fixed value. Therefore it remains open whether the SUBGROUP DISTANCE PROBLEM regarding the  $l_\infty$  distance is NP-complete in cyclic permutation groups for any fixed  $k \geq 2$ .

## References

- [1] V. Arvind. The parameterized complexity of some permutation group problems. arXiv:1301.0379, 2013.
- [2] V. Arvind and P. S. Joglekar. Algorithmic Problems for Metrics on Permutation Groups. In *SOFSEM 2008: Theory and Practice of Computer Science*. Lecture Notes in Computer Science, volume 4910, pages 136–147, Springer, Berlin, Heidelberg, 2008.
- [3] L. Babai, E. M. Luks, and Á. Seress. Permutation groups in NC. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, STOC 1987*, pages 409–420, ACM, 1987.
- [4] C. Buchheim, P. J. Cameron and T. Wu. On the subgroup distance problem. *Discrete Mathematics*, 309(4): 962–968, 2009.
- [5] C. Buchheim and M. Jünger. Linear optimization over permutation groups. *Discrete Optimization*, 2(4): 308–319, 2005.
- [6] P. J. Cameron and T. Wu. The complexity of the weight problem for permutation and matrix groups. *Discrete Mathematics*, 310(3): 408–416, 2010.
- [7] S. A. Cook and P. McKenzie. Problems complete for deterministic logarithmic space. *Journal of Algorithms*, 8(3): 385–394, 1987.
- [8] M. Deza and T. Huang. Metrics on permutations: A survey. *Journal of Combinatorics, Information & System Sciences*, 23: 173–185, 1998.
- [9] P. Diaconis. Group representations in probability and statistics. *Institute of Mathematical Statistics*, 1988.

- [10] P. Dusart. The  $k^{\text{th}}$  prime is greater than  $k(\ln k + \ln \ln k - 1)$  for  $k \geq 2$ . *Mathematics of Computation*, 68(225): 411–415, 1999.
- [11] M. L. Furst, J. E. Hopcroft, and E. M. Luks. Polynomial-time algorithms for permutation groups. In *Proceedings of the 21st Annual Symposium on Foundations of Computer Science, FOCS 1980*, pages 36–41, IEEE Computer Society, 1980.
- [12] M. R. Garey and D. S. Johnson. Computers and Intractability: A Guide to the Theory of NP-completeness. *Freeman*, 1979.
- [13] M. Lohrey and A. Rosowski. Finding cycle types in permutation groups with few generators. arXiv:2503.02864, 2025.
- [14] A. Lucchini, F. Menegazzo, and M. Morigi. Generating permutation groups. *Communications in Algebra*, 32(5): 1729–1746, 2004.
- [15] C. B. Onur. A Zero-Knowledge Proof of Knowledge for Subgroup Distance Problem. arXiv:2408.00395, 2024.
- [16] C. H. Papadimitriou. Computational complexity. *Addison-Wesley*, 1994.
- [17] R. G. E. Pinch. *The distance of a permutation from a subgroup of  $S_n$* . Combinatorics and Probability, Cambridge University Press, pages 473–479, 2007.
- [18] J. B. Rosser. Explicit bounds for some functions of prime numbers. *American Journal of Mathematics*, 63(1): 211–232, 1941.
- [19] Á. Seress. *Permutation Group Algorithms*. Cambridge Tracts in Mathematics. Cambridge University Press, 2003.
- [20] C. C. Sims. Computational methods in the study of permutation groups. In *Computational Problems in Abstract Algebra*, pages 169–183, Pergamon, 1970.