Finding Cycle Types in Permutation Groups with Few Generators

Markus Lohrey[0000−0002−4680−7198] and Andreas Rosowski

Universität Siegen, Department ETI, 57076 Siegen, Germany
{lohrey,rosowski}@eti.uni-siegen.de

Abstract. The problem whether a given permutation group contains a permutation with a given cycle type is studied. This problem is known to be NP-complete. In this paper it is shown that the problem can be solved in logspace for a cyclic permutation group and that it is NP-complete for a 2-generated abelian permutation group. In addition it is shown that it is NP-complete whether a 2-generated abelian permutation group contains a fixpoint-free permutation.

Keywords: Permutation groups · Algorithmic group theory · NP-completeness

1 Introduction

Permutations are ubiquitous objects in combinatorics [4] and group theory [6]. The set of all permutations on a set Ω forms a group $\mathsf{Sym}(\Omega)$ (the *symmetric group* on Ω) under composition. A subgroup of a symmetric group is called a *permutation group*. Cayley's famous theorem states that every group is isomorphic to a permutation group via the right regular representation. Here, we only deal with the case that Ω is finite and write $\mathsf{Sym}(n)$ for $\mathsf{Sym}(\Omega)$ if $|\Omega| = n$.

Having group elements represented as permutations can be often exploited algorithmically. For instance, the subgroup membership problem for symmetric groups (Does a given permutation $\pi \in \mathsf{Sym}(n)$ belong to the subgroup generated by given permutations $\pi_1, \ldots, \pi_k \in \mathsf{Sym}(n)$?) can be solved in polynomial time [10,15,16] and even in NC [3]. Another problem that has an extremely simple algorithm in symmetric groups is the conjugacy problem: given permutations $\pi, \rho \in \mathsf{Sym}(n)$, does there exist $\tau \in \mathsf{Sym}(n)$ such that $\pi = \tau^{-1}\rho\tau$? This is equivalent to say that π and ρ have the same *cycle type*. The cycle type of a permutation $\pi \in \mathsf{Sym}(n)$ specifies for every $\ell \leq n$ the number of cycles of length ℓ when π is written (uniquely) as a product of pairwise disjoint cycles.

In this paper we are interested in the problem whether a given permutation group $G \leq \mathsf{Sym}(n)$ (specified by a list of generators) contains a permutation of a given cycle type. Or equivalently: does G contain an element that is conjugated to a given permutation π? We call this problem CycleType.

Cameron and Wu showed in [8] that CycleType is NP-complete. Moreover, NP-hardness already holds for the case where G is an elementary abelian 2-group (i.e., an abelian group where every non-identity element has order two). Here we further pinpoint the borderline between tractability and non-tractability: We show that if the input permutation group G is cyclic and given by a single generator then $\mathsf{CycleType}$ can be solved in logarithmic space on a deterministic Turing machine (and hence belongs to the complexity class P). On the other hand, we show that $\mathsf{CycleType}$ is already NP-complete for the case where G is generated by two commuting permutations, i.e., $G = \langle \pi, \tau \rangle$ with $\pi\tau = \tau\pi$. Moreover, our proof shows that it is already NP-complete whether for two given commuting permutations π and τ the coset $\pi\langle\tau\rangle$ (a coset of a cyclic group) contains a permutation with a given cycle type.

In the last section of the paper, we consider the problem $\mathsf{FixpointFree}$ that asks whether a given permutation group contains a fixpoint-free permutation, i.e., a permutation π such that $\pi(a) \neq a$ for all a. It was shown in [5,8] that $\mathsf{FixpointFree}$ is NP-complete and as for $\mathsf{CycleType}$, NP-hardness holds already for elementary abelian 2-groups. The restriction of $\mathsf{FixpointFree}$ to cyclic permutation groups is not interesting ($\langle\pi\rangle$ contains a fixpoint-free permutation if and only if π is fixpoint-free). We show that the restriction of $\mathsf{FixpointFree}$ to 2-generated abelian permutation groups $\langle \pi, \tau \rangle$ is NP-complete. Moreover, it is also NP-complete to check whether a coset $\pi\langle\tau\rangle$ of a cyclic permutation group, where in addition $\pi\tau = \tau\pi$, contains a fixpoint-free permutation.

Related work. Fixpoint-free permutations are also known as *derangements* and they have received a lot of attention in combinatorics and group theory; see [7] for a survey. Jordan proved in 1872 that every permutation group G that acts transitively on a finite set Ω of size at least two contains a derangement [14]. Arvind proved that in this situation one can compute in polynomial time a derangement in G [2]. In the same paper, Arvind shows that the problem whether a given permutation group G contains a permutation with at least k non-fixpoints is fixed parameter tractable with respect to the parameter k.

2 Preliminaries

2.1 General notations

For integers $1 \leq i \leq j$ we write $[i, j]$ for the set $\{i, i+1, \ldots, j\}$ and $[j]$ for $[1, j]$. For a prime p and an integer n we denote with $\nu_p(n)$ the largest positive integer d such that $p^d \mid n$ (it is also called the p-adic valuation of n). The greatest common divisor of integers $n_1, \ldots, n_k$ is denoted by $\gcd(n_1, \ldots, n_k)$ and the least common multiple is denoted by $\mathrm{lcm}(n_1, \ldots, n_k)$.

We assume that the reader is familiar with basic concepts of complexity theory; see [1] for more details. With L (also known as *logspace*) we denote the class of all problems that can be solved on a deterministic Turing machine in logarithmic space. It is a subset of P (deterministic polynomial time).

2.2 Permutations

For $n \geq 1$ we denote with $\mathsf{Sym}(n)$ the group of all permutations on $[n]$. The identity permutation is denoted by id. For $\pi \in \mathsf{Sym}(n)$ and $a \in [n]$ we also write $a\pi$ for $\pi(a)$. There are two standard representations for a permutation $\pi \in \mathsf{Sym}(n)$:

- The *pointwise representation* of π is the tuple $[\pi(1), \pi(2), \ldots, \pi(n)]$.
- The *cycle representation* is a list $\gamma_1\gamma_2 \cdots \gamma_k$ of pairwise disjoint cycles. Every cycle γ_i is written as a list $(a_0, a_1, \ldots, a_{\ell-1})$ (with $a_i \in [n]$) meaning that $a_k\pi = a_{k+1 \bmod \ell}$. Fixpoints (cycles of the form (i)) are usually omitted in the cycle representation, but sometimes we will explicitly list them.

Note that every cycle $(a_0, a_1, \ldots, a_{\ell-1})$ can be replaced by a cyclic rotation. Moreover since disjoint cycles commute, the order of the cycles γ_i is not relevant.

Computing the pointwise representation from the cycle representation is possible in uniform AC^0 (this is a very small circuit complexity class contained in L). On the other hand, the cycle representation can be computed in logspace from the pointwise representation and no better complexity bound is known [9]. Therefore, as long as one works with complexity classes that contain L (which will be the case in this paper), there is no reason to specify which of the above two representations of permutations is chosen.

Let $\mathsf{fpf}(n) = \{\pi \in \mathsf{Sym}(n) \mid a\pi \neq a \text{ for all } a \in [n]\}$ be the set of all *fixpoint-free* permutations. For $\pi_1, \ldots, \pi_k \in \mathsf{Sym}(n)$ we write $\langle \pi_1, \ldots, \pi_k \rangle \leq \mathsf{Sym}(n)$ for the permutation group generated by $\pi_1, \ldots, \pi_k$. The order $\mathrm{ord}(\pi)$ of $\pi \in \mathsf{Sym}(n)$ is the smallest integer $i \geq 1$ such that $\pi^i = \mathrm{id}$. If $\gamma_1 \cdots \gamma_k$ is the cycle representation of π and every cycle γ_i has length ℓ_i then the multiset $\mathsf{ct}(\pi) := \{\!\{\ell_1, \ldots, \ell_k\}\!\}$ is the *cycle type* of π. Note that in this situation we have

$$\mathrm{ord}(\pi) = \mathrm{lcm}(\ell_1, \ldots, \ell_k). \tag{1}$$

The following lemma is well known, see e.g. [6]:

Lemma 1. *For $\pi, \rho \in Sym(n)$ we have $\mathsf{ct}(\pi) = \mathsf{ct}(\rho)$ if and only if there is a $\sigma \in \mathsf{Sym}(n)$ such that $\pi = \sigma^{-1}\rho\sigma$.*

Also the following lemma seems to be folklore. For completeness we give a proof.

Lemma 2. *Let $x \in \mathbb{N}$ and γ be a single cycle of length ℓ. Then the cycle representation of γ^x consists of $\gcd(x, \ell)$ many disjoint cycles of length $\ell / \gcd(x, \ell)$.*

Proof (Proof of Lemma 2.). Let us first consider the case where $\gcd(x, \ell) = 1$. Then there is a $y \in \mathbb{N}$ with $xy \equiv 1 \bmod \ell$. If γ^x consists of at least two cycles of length strictly smaller than ℓ, then the same holds for every power of γ^x. This contradicts $(\gamma^x)^y = \gamma^{xy} = \gamma$. This shows the statement of the lemma for the case $\gcd(x, \ell) = 1$.

For the general case let $m = \gcd(x, \ell), k = \ell/m$ and $z = x/m$. Then we can write the cycle γ as $\gamma = (a_0, \ldots, a_{mk-1})$ for some pairwise different $a_i \in [n]$.

For all $i \in [0, m-1]$ and $d \in [0, k-1]$ we have $a_{dm+i}\gamma^m = a_{(d+1)m+i}$ where all arithmetics in the indices is done modulo $\ell = mk$. We obtain

$$\gamma^x = (\gamma^m)^z = \prod_{i=0}^{m-1} (a_i, a_{m+i}, a_{2m+i}, \dots, a_{(k-1)m+i})^z.$$

Since $\gcd(z, k) = 1$ we obtain from the above case $\gcd(x, \ell) = 1$ that

$$(a_i, a_{m+i}, a_{2m+i}, \dots, a_{(k-1)m+i})^z$$

is a cycle of length k. Hence, γ^x splits into m disjoint cycles of length k. $\square$

For integers $1 \le i < j \le n$ we denote with $([i, j])$ the cycle $(i, i+1, \dots, j) \in \mathsf{Sym}(n)$. We also use $([i])$ instead of $([1, i])$ for $2 \le i \le n$.

We will consider the following two computational problems in this paper:

Problem 1. CycleType is the following problem:
- input: $\pi_1, \dots, \pi_m, \rho \in \mathsf{Sym}(n)$
- question: Is there an element $\pi \in \langle \pi_1, \dots, \pi_m \rangle$ such that $\mathsf{ct}(\pi) = \mathsf{ct}(\rho)$?

Problem 2. FixpointFree is the following problem:
- input: $\pi_1, \dots, \pi_m \in \mathsf{Sym}(n)$
- question: Does $\mathsf{fpf}(n) \cap \langle \pi_1, \dots, \pi_m \rangle \neq \emptyset$ hold?

Note that the unary encoding of n (from $\mathsf{Sym}(n)$) is implicitly part of the inputs for CycleType and FixpointFree. It is easy to see that CycleType and FixpointFree are in NP: on input $\pi_1, \dots, \pi_m, \rho \in \mathsf{Sym}(n)$ we guess a permutation $\pi \in \mathsf{Sym}(n)$ and then check in polynomial time whether (i) $\pi \in \langle \pi_1, \dots, \pi_m \rangle$ [3] and (ii) $\mathsf{ct}(\pi) = \mathsf{ct}(\rho)$ (resp., $\pi \in \mathsf{fpf}(n)$).

For a given number k we denote with $\mathsf{CycleType}(k)$ the restriction of CycleType where $m \le k$ holds. In other words, the input permutation group is generated by k permutations. Moreover, if the input permutations $\pi_1, \dots, \pi_k$ pairwise commute, then we write $\mathsf{CycleType}(\mathsf{ab}, k)$ (ab stands for "abelian"). Analogous restrictions are defined for FixpointFree.

3 Cycle type in cyclic permutation groups

In this section, we study the problem $\mathsf{CycleType}(1)$, i.e., CycleType for cyclic permutation groups. Let us fix a symmetric group $\mathsf{Sym}(n)$. We assume that n is given in unary encoding for the following. Note that a brute-force algorithm that iterates over all elements $\pi \in \langle \pi_1 \rangle$ and thereby checks whether $\mathsf{ct}(\pi) = \mathsf{ct}(\rho)$ holds, needs exponential time. In [13, Lemma 2.1] it is shown that for every sufficiently large $n \in \mathbb{N}$, there exists a permutation $\pi_1 \in \mathsf{Sym}(\lfloor 2n^2 \ln n \rfloor)$ such that $\langle \pi_1 \rangle$ has size greater than 2^n.

Let P_n be the set of all primes in $[n]$. One can easily produce a list $p_1 < p_2 < \cdots < p_r$ of all those primes in logspace. For this, one only needs the fact that integer division for unary encoded integers can be done in logspace (actually, integer division of binary encoded integers can be also done in logspace [12] but this is not needed here). We will only consider numbers where all prime divisors are from P_n. For such a number a we denote with $\mathsf{pe}(a)$ (for prime exponents) the tuple $(e_1, \ldots, e_r)$ such that $a = \prod_{i=1}^{r} p_i^{e_i}$ is the prime factorizaton of a. We will represent the exponents e_i in unary notation. From the unary representation of the number $a \in [n]$ one can easily compute in logspace the tuple $\mathsf{pe}(a)$. We need the following fact:

Lemma 3. *From a given permutation $\pi \in \mathsf{Sym}(n)$ one can compute in logspace the tuple $\mathsf{pe}(\mathrm{ord}(\pi))$.*

Proof. Assume that the cycle representation $\pi = \gamma_1\gamma_2 \cdots \gamma_k$ is given. Let $\ell_i \in [n]$ be the length of the cycle γ_i. We then compute in logspace the tuple $\mathsf{pe}(\ell_i) = (e_{i,1}, \ldots, e_{i,r})$. Since $\mathrm{ord}(\pi) = \mathrm{lcm}(\ell_1, \ell_2, \ldots, \ell_k)$ we have

$$\mathsf{pe}(\mathrm{ord}(\pi)) = (e_1, \ldots, e_r)$$

with $e_i = \max\{e_{1,i}, \ldots, e_{k,i}\}$. Clearly, these exponents e_i can be computed in logspace. $\square$

Lemma 4. *For given permutations $\pi, \rho \in \mathsf{Sym}(n)$ one can check in logspace, whether $\mathrm{ord}(\rho) \mid \mathrm{ord}(\pi)$ holds.*

Proof. Let $\mathsf{pe}(\mathrm{ord}(\rho)) = (e_1, \ldots, e_r)$ and $\mathsf{pe}(\mathrm{ord}(\pi)) = (e'_1, \ldots, e'_r)$. Then $\mathrm{ord}(\rho) \mid \mathrm{ord}(\pi)$ if and only if $e_i \leq e'_i$ for all $i \in [r]$. Therefore, the statement of the lemma follows from Lemma 3. $\square$

Lemma 5. *There is a logspace algorithm with the following specification:*
- *input: $\pi, \rho \in \mathsf{Sym}(n)$ such that $\mathrm{ord}(\rho) \mid \mathrm{ord}(\pi)$ and $a \in [n]$.*
- *output: $a\pi^d \in [n]$ where $d = \mathrm{ord}(\pi)/\mathrm{ord}(\rho)$*

Proof. By Lemma 3 we can produce in logspace the tuples

$$\mathsf{pe}(\mathrm{ord}(\rho)) = (e_1, \ldots, e_r) \text{ and}$$
$$\mathsf{pe}(\mathrm{ord}(\pi)) = (e'_1, \ldots, e'_r).$$

Since $\mathrm{ord}(\rho) \mid \mathrm{ord}(\pi)$ we have $e_i \leq e'_i$ for all $i \in [r]$. We then have $\mathsf{pe}(d) = (f_1, \ldots, f_r)$ with $f_i = e'_i - e_i$ and this tuple can be also produced in logspace.

Let $\gamma_1\gamma_2 \cdots \gamma_k$ be the cycle representation of π. We then compute in logspace the length $\ell \in [n]$ of the unique cycle γ_i that contains $a \in [n]$. We have $a\pi^d = a\pi^{d \bmod \ell}$. Since all primes p_i and exponents f_i are given in unary notation, we can compute in logspace the value $d \bmod \ell$ by going over the prime factorization $\prod_{i=1}^{r} p_i^{f_i}$ and making $\sum_{i=1}^{r} f_i$ many multiplications modulo ℓ. Once $d \bmod \ell$ is computed, we can finally compute $a\pi^{d \bmod \ell}$ in logspace. $\square$

Lemma 6. *Let $\pi, \rho \in \mathsf{Sym}(n)$. Then the following holds:*
- *If $\mathsf{ct}(\pi) = \mathsf{ct}(\rho)$ then $\mathrm{ord}(\pi) = \mathrm{ord}(\rho)$.*
- *For all $i \in \mathbb{N}$ we have $\mathrm{ord}(\pi) = \mathrm{ord}(\pi^i)$ if and only if $\mathsf{ct}(\pi) = \mathsf{ct}(\pi^i)$.*

Proof. For the first statement note that if $\{\!\{\ell_1, \ell_2, \ldots, \ell_k\}\!\}$ is the common cycle type of π and ρ then $\mathrm{ord}(\pi) = \mathrm{lcm}(\ell_1, \ell_1, \ldots, \ell_k) = \mathrm{ord}(\rho)$ by (1). Therefore we only have to show that if $\mathrm{ord}(\pi) = \mathrm{ord}(\pi^i)$ then $\mathsf{ct}(\pi) = \mathsf{ct}(\pi^i)$. Let $\pi = \gamma_1 \cdots \gamma_k$ be the cycle representation of π. Then we have $\pi^i = \gamma_1^i \cdots \gamma_k^i$. Since $\mathrm{ord}(\pi) = \mathrm{ord}(\pi^i)$ we obtain $\gcd(\mathrm{ord}(\pi), i) = 1$. Because of $\mathrm{ord}(\gamma_j) \mid \mathrm{ord}(\pi)$ we get $\gcd(\mathrm{ord}(\gamma_j), i) = 1$ for all $j \in [k]$. By Lemma 2, γ_j and γ_j^i are cycles of the same length and thus π and π^i have the same cycle type. ☐

Theorem 1. $\mathsf{CycleType}(1)$ *is in* L.

Proof. Let $\pi, \rho \in \mathsf{Sym}(n)$ be the two input permutations of $\mathsf{CycleType}(1)$. It is asked whether there is a $q \in \mathbb{N}$ such that $\mathsf{ct}(\pi^q) = \mathsf{ct}(\rho)$. By Lemma 4 we can check in logspace whether $\mathrm{ord}(\rho) \mid \mathrm{ord}(\pi)$ holds. If this is not the case, then by the first statement of Lemma 6 there is no q such that $\mathsf{ct}(\pi^q) = \mathsf{ct}(\rho)$ and we can immediately reject. Let us now assume that $\mathrm{ord}(\rho) \mid \mathrm{ord}(\pi)$ and let $d = \mathrm{ord}(\pi)/\,\mathrm{ord}(\rho)$ in the following. Note that $\mathrm{ord}(\pi^d) = \mathrm{ord}(\rho)$.

Claim 1. There is a $q \in \mathbb{N}$ such that $\mathsf{ct}(\pi^q) = \mathsf{ct}(\rho)$ if and only if $\mathsf{ct}(\pi^d) = \mathsf{ct}(\rho)$.

Proof of Claim 1. The direction from right to left is trivial. Hence, let us assume that there is a q such that $\mathsf{ct}(\pi^q) = \mathsf{ct}(\rho)$. By Lemma 6, we have $\mathrm{ord}(\pi^q) = \mathrm{ord}(\rho)$. We get $\mathrm{ord}(\pi^d) = \mathrm{ord}(\rho) = \mathrm{ord}(\pi^q)$. Since $\langle \pi \rangle$ has exactly one subgroup of order $\mathrm{ord}(\rho)$ it follows that $\langle \pi^q \rangle = \langle \pi^d \rangle$. Let $\pi^q = (\pi^d)^i$ for $i \in \mathbb{N}$. Since $\mathrm{ord}(\pi^d) = \mathrm{ord}(\pi^q) = \mathrm{ord}((\pi^d)^i)$, the second statement of Lemma 6 implies that π^q and π^d (and hence ρ and π^d) have the same cycle type. This shows Claim 1.

By Claim 1, it suffices to check in logspace whether $\mathsf{ct}(\pi^d) = \mathsf{ct}(\rho)$. By Lemma 5 we can compute in logspace the pointwise representation and hence the cycle representation of π^d. From the cycle representation of a permutation we can of course compute in logspace the cycle type. ☐

4 Cycle type in the 2-generated abelian case

In this section we show that $\mathsf{CycleType}$ becomes NP-complete if the input permutation group is abelian and generated by two elements.

Theorem 2. $\mathsf{CycleType}(\mathsf{ab}, 2)$ *is* NP*-complete.*

Proof. Since $\mathsf{CycleType}$ is in NP (see the remark at the end of Section 2.2), it remains to show NP-hardness. For this we exhibit a logspace reduction from $\mathsf{X3HS}$ (exact 3-hitting set), which is the following problem:

- Input: a finite set S and a set $\mathcal{B} \subseteq 2^S$ of subsets of S all of size 3.
- Question: Is there a subset $T \subseteq S$ such that $|T \cap C| = 1$ for all $C \in \mathcal{B}$?

Note that $\mathsf{X3HS}$ is the same problem as positive $\mathsf{1\text{-}in\text{-}3\text{-}SAT}$, which is a well-known NP-complete problem; see [11] for more details.

Let S be a finite set and $\mathcal{B} \subseteq 2^S$ be a set of subsets of S all of size 3. W.l.o.g. assume that $S = [n]$ and let $\mathcal{B} = \{C_1, \ldots, C_m\}$. Let $p_1 < \cdots < p_{2n}$ be the first

$2n$ primes with $p_1 > 3$. Moreover let $q_1 < \cdots < q_m$ be the next m primes with $p_{2n} < q_1$. We associate $i \in S$ with the prime p_i and $C_j \in \mathcal{B}$ with the prime q_j. We will work with the group

$$G = \prod_{i=1}^{n} \mathsf{Sym}(p_i p_{n+i}) \times \prod_{j=1}^{m} \mathsf{Sym}(p_n^3 q_j)^6$$

which naturally embedds into $\mathsf{Sym}(N)$ for

$$N = \sum_{i=1}^{n} p_i p_{n+i} + 6 \sum_{j=1}^{m} p_n^3 q_j.$$

Let $f : G \to \mathsf{Sym}(N)$ be this embedding. When we talk of the cycle type of an element $g \in G$, we always refer to the cycle type of the permutation $f(g) \in \mathsf{Sym}(N)$. If $g = (\pi_1, \ldots, \pi_n, \rho_1, \ldots, \rho_{6m}) \in G$, then this cycle type is obtained by taking the disjoint union (of multisets) of the cycle types of all the π_i and ρ_j.

For $j \in [m]$ we define $r_j = q_j \cdot \prod_{i \in C_j} p_i$. Moreover for $j \in [m]$ and all $d \in [6]$ we define the number $s_{j,d} \in [0, r_j - 1]$ as the smallest positive integer satisfying the following congruences in which we assume $C_j = \{i_1, i_2, i_3\}$ with $i_1 < i_2 < i_3$:

$$\begin{array}{lll}
s_{j,1} \equiv -1 \bmod p_{i_1} & s_{j,2} \equiv 0 \bmod p_{i_1} & s_{j,3} \equiv 0 \bmod p_{i_1} \\
s_{j,1} \equiv 0 \bmod p_{i_2} & s_{j,2} \equiv -1 \bmod p_{i_2} & s_{j,3} \equiv 0 \bmod p_{i_2} \\
s_{j,1} \equiv 0 \bmod p_{i_3} & s_{j,2} \equiv 0 \bmod p_{i_3} & s_{j,3} \equiv -1 \bmod p_{i_3} \\
s_{j,1} \equiv 1 \bmod q_j & s_{j,2} \equiv 1 \bmod q_j & s_{j,3} \equiv 1 \bmod q_j \\
\\
s_{j,4} \equiv -1 \bmod p_{i_1} & s_{j,5} \equiv -3 \bmod p_{i_1} & s_{j,6} \equiv -2 \bmod p_{i_1} \\
s_{j,4} \equiv -2 \bmod p_{i_2} & s_{j,5} \equiv -1 \bmod p_{i_2} & s_{j,6} \equiv -3 \bmod p_{i_2} \\
s_{j,4} \equiv -3 \bmod p_{i_3} & s_{j,5} \equiv -2 \bmod p_{i_3} & s_{j,6} \equiv -1 \bmod p_{i_3} \\
s_{j,4} \equiv 1 \bmod q_j & s_{j,5} \equiv 1 \bmod q_j & s_{j,6} \equiv 1 \bmod q_j
\end{array}$$

Moreover, we define the number $t_j \in [0, r_j - 1]$ as the smallest positive integer satisfying

$$t_j \equiv 1 \bmod p_{i_a} \text{ for all } a \in [3] \text{ and } t_j \equiv 0 \bmod q_j.$$

We define the input group elements $\rho, \pi_1, \pi_2 \in G$ as follows, where i ranges over $[n]$, j ranges over $[m]$ and $i_1 < i_2 < i_3$ are the elements of C_j (recall that $([m])$ denotes the cycle $(1, 2, \ldots, m)$):

$$\begin{aligned}
\rho &= (\zeta_1, \ldots, \zeta_n, \eta_1, \ldots, \eta_m) \\
\zeta_i &= ([p_i p_{n+i}]) \\
\eta_j &= (([r_j])^{p_{i_1} p_{i_2} p_{i_3}}, ([r_j])^{p_{i_1}}, ([r_j])^{p_{i_2}}, ([r_j])^{p_{i_3}}, ([r_j]), ([r_j])) \\
\pi_1 &= (\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) \\
\alpha_i &= ([p_i p_{n+i}]) \\
\beta_j &= (([r_j])^{s_{j,1}}, ([r_j])^{s_{j,2}}, ([r_j])^{s_{j,3}}, ([r_j])^{s_{j,4}}, ([r_j])^{s_{j,5}}, ([r_j])^{s_{j,6}})
\end{aligned}$$

$$\pi_2 = (\gamma_1, \dots, \gamma_n, \delta_1, \dots, \delta_m)$$
$$\gamma_i = \mathrm{id}$$
$$\delta_j = (([r_j])^{t_j}, ([r_j])^{t_j}, ([r_j])^{t_j}, ([r_j])^{t_j}, ([r_j])^{t_j}, ([r_j])^{t_j})$$

Note that π_1 and π_2 commute.

We will show there are $x_1, x_2 \in \mathbb{N}$ such that $\mathsf{ct}(\rho) = \mathsf{ct}(\pi_1^{x_1}\pi_2^{x_2})$ if and only if there is a subset $T \subseteq S$ such that $|T \cap C_j| = 1$ for all $j \in [m]$.

First suppose that there are $x_1, x_2 \in \mathbb{N}$ with $\mathsf{ct}(\rho) = \mathsf{ct}(\pi_1^{x_1}\pi_2^{x_2})$. We define

$$T = \{i \in [n] \mid x_2 \not\equiv 0 \bmod p_i\}. \tag{2}$$

Claim 2. For all $i \in [n]$ and $j \in [m]$ we have $x_1 \not\equiv 0 \bmod p_i$, $x_1 \not\equiv 0 \bmod p_{n+i}$ and $x_1 \not\equiv 0 \bmod q_j$.

Proof of Claim 2. The claim follows from Lemma 2 and the following facts:
- ζ_i and α_i are cycles of length $p_i p_{n+i}$.
- π_2 does not contain any cycle whose length is a multiple of p_{n+i}.
- $t_j \equiv 0 \bmod q_j$ and hence π_2 also does not contain any cycle whose length is a multiple of q_j.
- ρ and π_1 both contain 6 pairwise disjoint permutations of the form $([r_j])^z$, where z is not a multiple of q_j. □

Claim 3. For all $C_j = \{i_1, i_2, i_3\} \in \mathcal{B}$ there is a (necessarily unique) $a \in [3]$ such that $x_2 \not\equiv 0 \bmod p_{i_a}$ and $x_2 \equiv 0 \bmod p_{i_b}$ for all $b \in [3] \setminus \{a\}$.

Proof of Claim 3. Let $j \in [m]$ and assume $C_j = \{i_1, i_2, i_3\}$ with $i_1 < i_2 < i_3$. Consider η_j. By Lemma 2 $([r_j])^{p_{i_1}p_{i_2}p_{i_3}}$ consists of $p_{i_1}p_{i_2}p_{i_3}$ cycles of length q_j and these are the only cycles of length q_j in ρ. Hence, $\beta_j^{x_1}\delta_j^{x_2}$ must contain exactly $p_{i_1}p_{i_2}p_{i_3}$ cycles of length q_j. By Lemma 2 this can only be achieved if there is a unique $a \in [6]$ such that

$$\forall c \in [3] : x_1 s_{j,a} + x_2 t_j \equiv 0 \bmod p_{i_c}. \tag{3}$$

Also note that

$$\forall b \in [6] : x_1 s_{j,b} + x_2 t_j \equiv x_1 \not\equiv 0 \bmod q_j$$

by Claim 2 and

$$\forall c \in [3] : x_2 t_j \equiv x_2 \bmod p_{i_c}.$$

We want to show that $a \in [3]$. In order to get a contradiction, suppose that $a \in \{4, 5, 6\}$. The congruence $x_1 s_{j,a} + x_2 t_j \equiv 0 \bmod p_{i_c}$ from (3) gives us

$$\forall c \in [3] : x_2 \equiv -x_1 s_{j,a} \bmod p_{i_c}.$$

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

$$x_1 s_{j,b} + x_2 t_j \equiv x_1 s_{j,b} - x_1 s_{j,a} \equiv x_1(-1 - s_{j,a}) \not\equiv 0 \bmod p_{i_b},$$

where $x_1 \not\equiv 0 \bmod p_{i_b}$ by Claim 2 and $-1-s_{j,a} \not\equiv 0 \bmod p_{i_b}$ since $s_{j,a} \not\equiv -1 \bmod p_{i_b}$ for $b \neq a-3$ (also note that $p_{i_b} > 2$). Similarly, for all $b \in [3] \setminus \{a-3\}$ we get

$$x_1 s_{j,3+b} + x_2 t_j \equiv x_1 s_{j,3+b} - x_1 s_{j,a} \equiv x_1(s_{j,3+b} - s_{j,a}) \not\equiv 0 \bmod p_{i_b},$$

where as above $x_1 \not\equiv 0 \bmod p_{i_b}$ by Claim 2 and $s_{j,3+b} - s_{j,a} \not\equiv 0 \bmod p_{i_b}$ since $a \neq 3+b$ and $s_{j,a} \not\equiv s_{j,3+b} \bmod p_{i_c}$ for all $c \in [3]$.

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

$$x_1 s_{j,b} + x_2 t_j \equiv x_1 s_{j,b} - x_1 s_{j,a} \equiv -x_1 s_{j,a} \not\equiv 0 \bmod p_{i_c} \text{ and}$$
$$x_1 s_{j,3+b} + x_2 t_j \equiv x_1 s_{j,3+b} - x_1 s_{j,a} \equiv x_1(s_{j,3+b} - s_{j,a}) \not\equiv 0 \bmod p_{i_c}.$$

Finally, for all $b \in [6]$ we have $x_1 s_{j,b} + x_2 t_j \not\equiv 0 \bmod q_j$ as pointed out above. Taken together, these congruences yield for all $b \in [3] \setminus \{a-3\}$:

$$\gcd(x_1 s_{j,b} + x_2 t_j, r_j) = \gcd(x_1 s_{j,3+b} + x_2 t_j, r_j) = 1.$$

Hence, by Lemma 2, $\beta_j^{x_1} \delta_j^{x_2}$ contains at least 4 cycles of length r_j. However η_j contains only 2 cycles of length r_j and ρ does not contain any other cycles of length r_j, which gives us a contradiction. Thus we obtain $a \in [3]$ and by this

$$x_2 \equiv -x_1 s_{j,a} \equiv x_1 \not\equiv 0 \bmod p_{i_a},$$

where $x_1 \not\equiv 0 \bmod p_{i_a}$ holds by Claim 2. Moreover, for all $b \in [3] \setminus \{a\}$ we obtain

$$x_2 \equiv -x_1 s_{j,a} \equiv 0 \bmod p_{i_b}.$$

This shows Claim 3. $\square$

We can now show that $|T \cap C_j| = 1$ for all $j \in [m]$. Let $j \in [m]$. By Claim 3 there is a unique $i \in C_j$ such that $x_2 \not\equiv 0 \bmod p_i$. Thus $i \in T$ by (2). Moreover for all $h \in C_j \setminus \{i\}$ we have $x_2 \equiv 0 \bmod p_h$ by Claim 3 and hence $h \notin T$. Thus, we get $|T \cap C_j| = 1$.

For the other direction, suppose there is a subset $T \subseteq [n]$ such that $|T \cap C_j| = 1$ for all $j \in [m]$. We define $x_1 = 1$ and x_2 as the smallest positive integer satisfying the congruences

$$x_2 \equiv \begin{cases} 1 \bmod p_i & \text{if } i \in T \\ 0 \bmod p_i & \text{if } i \notin T \end{cases}$$

for all $i \in [n]$. Since $x_1 = 1$, ρ and $\pi_1^{x_1} \pi_2^{x_2}$ both contain a unique cycle of length $p_i p_{n+i}$ for all $i \in [n]$. All other cycles in ρ and $\pi_1^{x_1} \pi_2^{x_2}$ result from powers of $([r_j])$ for some $j \in [m]$. Consider a $j \in [m]$ and let $C_j = \{i_1, i_2, i_3\}$ with $i_1 < i_2 < i_3$. By Lemma 2, η_j consists of

(i) $p_{i_1} p_{i_2} p_{i_3}$ cycles of length q_j,
(ii) p_{i_1} cycles of length $p_{i_2} p_{i_3} q_j$,
(iii) p_{i_2} cycles of length $p_{i_1} p_{i_3} q_j$,
(iv) p_{i_3} cycles of length $p_{i_1} p_{i_2} q_j$ and

(v) 2 cycles of length r_j.

We have to show that

$$\beta_j \delta_j^{x_2} = (([r_j])^{s_{j,1}+x_2 t_j}, ([r_j])^{s_{j,2}+x_2 t_j}, ([r_j])^{s_{j,3}+x_2 t_j},$$
$$([r_j])^{s_{j,4}+x_2 t_j}, ([r_j])^{s_{j,5}+x_2 t_j}, ([r_j])^{s_{j,6}+x_2 t_j})$$

contains the same cycle lengths with the same multiplicities as in (i)–(v). Note that $s_{j,d} + x_2 t_j \equiv 1 \bmod q_j$ for all $d \in [6]$. Let $a \in [3]$ be the unique element with $i_a \in T$. Then $x_2 \equiv 1 \bmod p_{i_a}$ and $x_2 \equiv 0 \bmod p_{i_b}$ for all $b \in [3] \setminus \{a\}$. We obtain

$$s_{j,a} + x_2 t_j \equiv -1 + 1 \equiv 0 \bmod p_{i_a} \text{ and}$$
$$s_{j,a} + x_2 t_j \equiv 0 + 0 \equiv 0 \bmod p_{i_b} \text{ for all } b \in [3] \setminus \{a\}.$$

By Lemma 2, $([r_j])^{s_{j,a}+x_2 t_j}$ consists of $p_{i_1} p_{i_2} p_{i_3}$ cycles of length q_j. Moreover

$$s_{j,3+a} + x_2 t_j \equiv -1 + 1 \equiv 0 \bmod p_{i_a} \text{ and}$$
$$s_{j,3+a} + x_2 t_j \equiv s_{j,3+a} + 0 \not\equiv 0 \bmod p_{i_b} \text{ for all } b \in [3] \setminus \{a\}$$

(for the second point we use the fact that all primes p_i are larger than 3). By Lemma 2, $([r_j])^{s_{j,3+a}+x_2 t_j}$ consists of p_{i_a} cycles of length $q_j \prod_{b \in [3] \setminus \{a\}} p_{i_b}$. For all $b \in [3] \setminus \{a\}$ we have

$$s_{j,b} + x_2 t_j \equiv 0 + 1 \equiv 1 \bmod p_{i_a},$$
$$s_{j,b} + x_2 t_j \equiv s_{j,b} + 0 \equiv -1 \bmod p_{i_b} \text{ and}$$
$$s_{j,b} + x_2 t_j \equiv s_{j,b} + 0 \equiv 0 \bmod p_{i_c}, \text{where } \{c\} = [3] \setminus \{a, b\}.$$

By Lemma 2, $([r_j])^{s_{j,b}+x_2 t_j}$ consists of p_{i_c} cycles of length $q_j p_{i_a} p_{i_b}$ with $\{c\} = [3] \setminus \{a, b\}$. Finally, for all $b \in [3] \setminus \{a\}$ we have

$$s_{j,3+b} + x_2 t_j \equiv s_{j,3+b} + 1 \not\equiv 0 \bmod p_{i_a} \text{ and}$$
$$s_{j,3+b} + x_2 t_j \equiv s_{j,3+b} + 0 \not\equiv 0 \bmod p_{i_c} \text{ for all } c \in [3] \setminus \{a\}.$$

Hence, $([r_j])^{s_{j,3+b}+x_2 t_j}$ is a single cycle of length r_j. This shows that $\mathsf{ct}(\eta_j) = \mathsf{ct}(\beta_j \delta_j^{x_2})$ and concludes the proof of the theorem. □

The construction from the previous proof yields the following additional result:

Corollary 1. *The following problem is* NP*-complete:*
- *input:* $\rho, \pi_1, \pi_2 \in \mathsf{Sym}(n)$ *such that* π_1 *and* π_2 *commute*
- *question: Is there is a* $\pi \in \pi_1 \langle \pi_2 \rangle$ *such that* $\mathsf{ct}(\rho) = \mathsf{ct}(\pi)$*?*

Proof. The instance ρ, π_1, π_2 of $\mathsf{CycleType}(\mathsf{ab}, 2)$ that we constructed in the proof of Theorem 2 has the property that there are $x_1, x_2 \in \mathbb{N}$ such that ρ and $\pi_1^{x_1} \pi_2^{x_2}$ have the same cycle type if and only if there is $x_2 \in \mathbb{N}$ such that ρ and $\pi_1 \pi_2^{x_2}$ have the same cycle type. This yields the corollary. □

Whereas it can be decided in logspace whether a cyclic permutation group $\langle \pi_1 \rangle$ contains a permutation with a given cycle type (Theorem 1), the same problem for cosets of cyclic permutation groups is NP-complete (Corollary 1).

5 Fixpoint freeness in the 2-generated abelian case

Our main result for the problem $\mathsf{FixpointFree}$ is:

Theorem 3. $\mathsf{FixpointFree}(\mathsf{ab}, 2)$ *is* NP*-complete.*

Proof. We give a logspace reduction from 3-SAT (the satisfiability problem for conjunctions of clauses, where every clause consists of exactly three literals and a literal is either a boolean variable x or a negated boolean variable $\bar{x}$). For this take a finite set of variables $X = \{x_1, \ldots, x_n\}$ and a set of clauses $\mathcal{C} = \{C_1, \ldots, C_m\}$. Every $C_j \in \mathcal{C}$ is a set of three literals. When we write C_j as $C_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$, every $\tilde{x}_{i_k}$ is either x_{i_k} or $\bar{x}_{i_k}$ and we always assume that $i_1 < i_2 < i_3$. A truth assignment $\sigma : X \to \{0, 1\}$ is implicitly extended to all literals by setting $\sigma(\bar{x}_i) = 1 - \sigma(x_i)$.

Let $p_1, \ldots, p_n, \bar{p}_1, \ldots, \bar{p}_n$ be the first $2n$ primes. We associate the positive literal x_i with p_i and the negative literal $\bar{x}_i$ with $\bar{p}_i$ and define

$$\tilde{p}_i = \begin{cases} p_i & \text{if } \tilde{x}_i = x_i, \\ \bar{p}_i & \text{if } \tilde{x}_i = \bar{x}_i. \end{cases}$$

For the clause $C_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ define $r_j = \tilde{p}_{i_1}\tilde{p}_{i_2}\tilde{p}_{i_3}$. Moreover, for all $i \in [n], l \in [p_i - 1]$ and $k \in [\bar{p}_i - 1]$ let $s_{i,l,k}$ be the unique number in $[p_i\bar{p}_i - 1]$ with

$$s_{i,l,k} \equiv l \bmod p_i \quad \text{and} \quad s_{i,l,k} \equiv k \bmod \bar{p}_i.$$

We will work with the group

$$G = \prod_{i=1}^{n} \Big(\mathsf{Sym}(p_i) \times \mathsf{Sym}(\bar{p}_i) \times \mathsf{Sym}(p_i\bar{p}_i)^{(p_i-1)(\bar{p}_i-1)+1}\Big) \times \prod_{j=1}^{m} \mathsf{Sym}(r_j).$$

The group G naturally embeds into $\mathsf{Sym}(N)$ for

$$N = \sum_{i=1}^{n}(p_i + \bar{p}_i + p_i\bar{p}_i((p_i - 1)(\bar{p}_i - 1) + 1)) + \sum_{j=1}^{m} r_j.$$

Now we define the input permutations π_1 and π_2 as follows, where i ranges over $[n]$, l ranges over $[p_i - 1]$, k ranges over $[\bar{p}_i - 1]$ and j ranges over $[m]$:

$$\begin{aligned}
\pi_1 &= (\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) \text{ with} \\
\alpha_i &= (\alpha_{i,1}, \alpha_{i,2}, \alpha_{i,3}, \alpha_{i,1,1}, \ldots, \alpha_{i,p_i-1,\bar{p}_i-1}) \\
\alpha_{i,1} &= ([p_i]) \\
\alpha_{i,2} &= ([\bar{p}_i]) \\
\alpha_{i,3} &= \mathrm{id} \\
\alpha_{i,l,k} &= ([p_i\bar{p}_i])^{s_{i,l,k}} \\
\beta_j &= \mathrm{id}
\end{aligned}$$

$$\begin{aligned}
\pi_2 &= (\gamma_1, \dots, \gamma_n, \delta_1, \dots, \delta_m) \text{ with} \\
\gamma_i &= (\gamma_{i,1}, \gamma_{i,2}, \gamma_{i,3}, \gamma_{i,1,1}, \dots, \gamma_{i,p_i-1,\bar{p}_i-1}) \\
\gamma_{i,1} &= \gamma_{i,2} = \mathrm{id} \\
\gamma_{i,3} &= \gamma_{i,l,k} = ([p_i\bar{p}_i]) \\
\delta_j &= ([r_j])
\end{aligned}$$

Note that π_1 and π_2 commute. We will show that $\mathcal{C}$ is satisfiable if and only if there are $z_1, z_2 \in \mathbb{N}$ such that $\pi_1^{z_1}\pi_2^{z_2} \in \mathsf{fpf}(N)$.

First, suppose that there are $z_1, z_2 \in \mathbb{N}$ such that $\pi_1^{z_1}\pi_2^{z_2} \in \mathsf{fpf}(N)$.

Claim 4. For all $i \in [n]$ we have $z_1 \not\equiv 0 \bmod p_i$ and $z_1 \not\equiv 0 \bmod \bar{p}_i$.

We have $\alpha_{i,1}^{z_1}\gamma_{i,1}^{z_2} = \alpha_{i,1}^{z_1} = ([p_i])^{z_1}$ and hence by Lemma 2 we obtain $z_1 \not\equiv 0 \bmod p_i$. Analogously we obtain $z_1 \not\equiv 0 \bmod \bar{p}_i$. □

Claim 5. For all $i \in [n]$ we have $z_2 \equiv 0 \bmod p_i$ if and only if $z_2 \not\equiv 0 \bmod \bar{p}_i$.

Assume that $z_2 \equiv 0 \bmod p_i$ and $z_2 \equiv 0 \bmod \bar{p}_i$. Then we obtain by

$$\alpha_{i,3}^{z_1}\gamma_{i,3}^{z_2} = \gamma_{i,3}^{z_2} = ([p_i\bar{p}_i])^{z_2} = \mathrm{id}$$

a contradiction. Now assume that $z_2 \not\equiv 0 \bmod p_i$ and $z_2 \not\equiv 0 \bmod \bar{p}_i$. Since by Claim 4 we have $z_1 \not\equiv 0 \bmod p_i$ and $z_1 \not\equiv 0 \bmod \bar{p}_i$ we can define $l \in [p_i - 1]$ and $k \in [\bar{p}_i - 1]$ as the smallest positive integers satisfying the congruences

$$l \equiv -z_2 z_1^{-1} \bmod p_i \quad \text{ and } \quad k \equiv -z_2 z_1^{-1} \bmod \bar{p}_i.$$

From this we obtain $s_{i,l,k} \equiv -z_2 z_1^{-1} \bmod p_i\bar{p}_i$ and hence

$$\alpha_{i,l,k}^{z_1}\gamma_{i,l,k}^{z_2} = ([p_i\bar{p}_i])^{s_{i,l,k}\cdot z_1}([p_i\bar{p}_i])^{z_2} = ([p_i\bar{p}_i])^{-z_2}([p_i\bar{p}_i])^{z_2} = \mathrm{id},$$

which is again a contradiction. This shows Claim 5 □

Claim 6. For all $j \in [m]$ there is an $a \in [3]$ such that $z_2 \not\equiv 0 \bmod \tilde{p}_{i_a}$, where $C_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$.

Since we must have $\beta_j^{z_1}\delta_j^{z_2} = \delta_j^{z_2} = ([r_j])^{z_2} \in \mathsf{fpf}(r_j)$ we must have $z_2 \not\equiv 0 \bmod r_j = \tilde{p}_{i_1}\tilde{p}_{i_2}\tilde{p}_{i_3}$. Hence, there is an $a \in [3]$ such that $z_2 \not\equiv 0 \bmod \tilde{p}_{i_a}$. □

We define the truth assignment $\sigma : X \to \{0, 1\}$ by

$$\sigma(x_i) = \begin{cases} 1 & \text{if } z_2 \not\equiv 0 \bmod p_i \\ 0 & \text{if } z_2 \equiv 0 \bmod p_i \end{cases}$$

for all $i \in [n]$ and show that every clause in $\mathcal{C}$ contains a literal that is mapped to 1 by σ. Let $j \in [m]$ and $C_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$. By Claim 6 there is an $a \in [3]$ such that $z_2 \not\equiv 0 \bmod \tilde{p}_{i_a}$. If $\tilde{x}_{i_a} = x_{i_a}$, then $\tilde{p}_{i_a} = p_{i_a}$ and $1 = \sigma(x_{i_a}) = \sigma(\tilde{x}_{i_a})$. On the other hand, if $\tilde{x}_{i_a} = \bar{x}_{i_a}$, then $\tilde{p}_{i_a} = \bar{p}_{i_a}$ and $z_2 \equiv 0 \bmod p_{i_a}$ by Claim 5. We obtain $1 = 1 - \sigma(x_{i_a}) = \sigma(\bar{x}_{i_a}) = \sigma(\tilde{x}_{i_a})$. Hence, $\sigma(\tilde{x}_{i_a}) = 1$ in both cases.

Vice versa suppose that there is a truth assignment $\sigma : X \to \{0, 1\}$ such that every clause in $\mathcal{C}$ contains a literal that is mapped to 1 by σ. We define $z_1 = 1$ and $z_2 \in \mathbb{N}$ as the smallest positive integer satisfying the congruences

$$z_2 \equiv \sigma(x_i) \bmod p_i \quad \text{and} \quad z_2 \equiv 1 - \sigma(x_i) \bmod \bar{p}_i \tag{4}$$

for all $i \in [n]$. Then $\pi_1^{z_1}\pi_2^{z_2} \in \mathsf{fpf}(N)$ follows from the following points, where $i \in [n]$, $l \in [p_i - 1]$, $k \in [\bar{p}_i - 1]$, and $j \in [m]$ are arbitrary:

- $\alpha_{i,1}^{z_1}\gamma_{i,1}^{z_2} = ([p_i])$, $\alpha_{i,2}^{z_1}\gamma_{i,2}^{z_2} = ([\bar{p}_i])$ and $\alpha_{i,3}^{z_1}\gamma_{i,3}^{z_2} = \gamma_{i,3}^{z_2} = ([p_i\bar{p}_i])^{z_2}$ are fixpoint-free.
- $\alpha_{i,l,k}^{z_1}\gamma_{i,l,k}^{z_2} = ([p_i\bar{p}_i])^{s_{i,l,k}+z_2}$ is fixpoint-free since $s_{i,l,k} + z_2 \equiv l \not\equiv 0 \bmod p_i$ if $\sigma(x_i) = 0$ and $s_{i,l,k} + z_2 \equiv k \not\equiv 0 \bmod \bar{p}_i$ if $\sigma(x_i) = 1$.
- $\beta_j^{z_1}\delta_j^{z_2} = \delta_j^{z_2} = ([r_j])^{z_2}$ is fixpoint-free. To see this let $C_j = \{\tilde{x}_{i_1}, \tilde{x}_{i_2}, \tilde{x}_{i_3}\}$ and $a \in [3]$ be such that $\sigma(\tilde{x}_{i_a}) = 1$. Then (4) yields $z_2 \equiv \sigma(\tilde{x}_{i_a}) \equiv 1 \bmod \tilde{p}_{i_a}$ and hence $z_2 \not\equiv 0 \bmod r_j$. □

Corollary 2. *It is* NP*-complete to check whether* $\pi_1\langle\pi_2\rangle \cap \mathsf{fpf}(n) \neq \emptyset$ *holds for given* $\pi_1, \pi_2 \in \mathsf{Sym}(n)$ *with* $\pi_1\pi_2 = \pi_2\pi_1$.

Proof. For π_1 and π_2 from the proof of Theorem 3, there are $z_1, z_2 \in \mathbb{N}$ with $\pi_1^{z_1}\pi_2^{z_2} \in \mathsf{fpf}(n)$ if and only if there is $z \in \mathbb{N}$ with $\pi_1\pi_2^{z} \in \mathsf{fpf}(n)$. □

6 Conclusion

We proved NP-completeness of the following two problem:

- Does a given 2-generated abelian permutation group contain a permutation with a given cycle type (Theorem 2)?
- Does a given 2-generated abelian permutation group contain a fixpoint-free permutation (Theorem 3)?

One might consider the problems $\mathsf{CycleType}$ and $\mathsf{FixpointFree}$ also for other classes of permutation groups. Whereas $\mathsf{FixpointFree}$ is trivial for transitive permuation groups (by Jordan's theorem [14]), the complexity of $\mathsf{CycleType}$ for transitive permuation groups seems to be open.

Acknowledgments. This work has been supported by the DFG research project LO 748/15-1.

References

1. Arora, S., Barak, B.: Computational Complexity - A Modern Approach. Cambridge University Press (2009). https://doi.org/10.1017/CBO9780511804090
2. Arvind, V.: The parameterized complexity of fixpoint free elements and bases in permutation groups. In: Proceedings of the 8th International Symposium on Parameterized and Exact Computation, IPEC 2013. Lecture Notes in Computer Science, vol. 8246, pp. 4–15. Springer (2013). https://doi.org/10.1007/978-3-319-03898-8_2

3. Babai, L., Luks, E.M., Seress, Á.: Permutation groups in NC. In: Proceedings of the 19th Annual ACM Symposium on Theory of Computing, STOC 1987. pp. 409–420. ACM (1987). https://doi.org/10.1145/28395.28439
4. Bóna, M.: Combinatorics of Permutations, Third Edition. Discrete mathematics and its applications, CRC Press (2022). https://doi.org/10.1201/9780429274107
5. Buchheim, C., Jünger, M.: Linear optimization over permutation groups. Discret. Optim. **2**(4), 308–319 (2005). https://doi.org/10.1016/J.DISOPT.2005.08.005
6. Cameron, P.J.: Permutation groups. Cambridge University Press (2010). https://doi.org/10.1017/CBO9780511623677
7. Cameron, P.J.: Lectures on derangements. In: Pretty Structures Conference in Paris. vol. 654 (2011)
8. Cameron, P.J., Wu, T.: The complexity of the weight problem for permutation and matrix groups. Discrete Mathematics **310**(3), 408–416 (2010). https://doi.org/10.1016/J.DISC.2009.03.005
9. Cook, S.A., McKenzie, P.: Problems complete for deterministic logarithmic space. Journal of Algorithms **8**(3), 385–394 (1987). https://doi.org/10.1016/0196-6774(87)90018-6
10. Furst, M.L., Hopcroft, J.E., Luks, E.M.: Polynomial-time algorithms for permutation groups. In: Proceedings of the 21st Annual Symposium on Foundations of Computer Science, FOCS 1980. pp. 36–41. IEEE Computer Society (1980). https://doi.org/10.1109/SFCS.1980.34
11. Garey, M.R., Johnson, D.S.: Computers and Intractability: A Guide to the Theory of NP–completeness. Freeman (1979)
12. Hesse, W., Allender, E., Barrington, D.A.M.: Uniform constant-depth threshold circuits for division and iterated multiplication. Journal of Computer and System Sciences **65**(4), 695–716 (2002). https://doi.org/10.1016/S0022-0000(02)00025-9
13. Jerrum, M.: The complexity of finding minimum-length generator sequences. Theoretical Computer Science **36**, 265–289 (1985). https://doi.org/10.1016/0304-3975(85)90047-7
14. Jordan, C.: Recherches sur les substitutions. Journal de Mathématiques Pures et Appliquées **17**, 351–387 (1872), http://eudml.org/doc/234268
15. Sims, C.C.: Computational methods in the study of permutation groups. In: Computational Problems in Abstract Algebra, pp. 169–183. Pergamon (1970). https://doi.org/10.1016/B978-0-08-012975-4.50020-5
16. Sims, C.C.: Computation with permutation groups. In: Proceedings of the 2nd ACM Symposium on Symbolic and Algebraic Manipulation, SYMSAC 1971. pp. 23–28. ACM (1971). https://doi.org/10.1145/800204.806264