Two-closure of odd permutation group in polynomial time

Sergei Evdokimov\textsuperscript{a,}* , Ilia Ponomarenko\textsuperscript{b}

\textsuperscript{a}St. Petersburg Institute for Informatics and Automation, Academy of Sciences of Russia, 14th Liniya 39, St. Petersburg, 199178, Russia
\textsuperscript{b}V.A. Steklov Institute of Mathematics, Academy of Sciences of Russia, St. Petersburg, Russia

Abstract

The $k$-closure $G^{(k)}$ of a permutation group $G$ on a finite set $V$ is by definition the largest permutation group on $V$ having the same orbits on $V^k$ as $G$. We prove that if the order of $G$ is odd, then a set of generators of $G^{(2)}$ can be found in polynomial time in the cardinality of $V$. If in addition $G$ is primitive, then given $k \geq 1$ we can list all elements of $G^{(k)}$ within the same time. © 2001 Elsevier Science B.V. All rights reserved.

1. Introduction

The method of invariant relations was first applied to permutation group theory by Wielandt in [12]. In [13] it was identified along with the theory of centralizer rings and the character theory as one of the three basic tools for studying permutation groups. The essence of the method is the existence of, for each positive integer $k$, a Galois correspondence between permutation groups on a finite set $V$ and partitions of $V^k$ (see [5]). Namely, to each permutation group $G$ on $V$ we associate a partition $\text{Orb}_k(G)$ which is the partition of $V^k$ into $k$-orbits of $G$, i.e., the orbits of the permutation group on $V^k$ induced by $G$. On the other hand, to each partition $P$ of $V^k$ we associate its automorphism group $\text{Aut}(P)$ by definition consisting of all permutations of $V$ preserving any class of $P$. Denoting by $\geq$ the natural partial orders on the set of all permutation groups on $V$ and the set of all partitions of $V^k$ we have

$$\text{Aut}(\text{Orb}_k(G)) \geq G, \quad \text{Orb}_k(\text{Aut}(P)) \geq P,$$

which expresses the correspondence.

\textsuperscript{*}Research partially supported by the Volkswagen–Stiftung Program on Computational Complexity and RFFI grant 99-01-00098.

*Corresponding author.

\textit{E-mail addresses:} evdokim@pdmi.ras.ru (S. Evdokimov), inp@pdmi.ras.ru (I. Ponomarenko).
In the context of computational complexity theory, the above correspondence leads to two natural problems: given a partition $P$ find $\text{Orb}_2(\text{Aut}(P))$ and given a permutation group $G$ find $\text{Aut}(\text{Orb}(G))$. It is well known that for $k = 2$, the first problem is equivalent to the Graph Isomorphism Problem (the modern state of which can be found in [2]). In this paper we are interested in the second problem.

According to [12] we define the $k$-closure $G^{(k)}$ of a permutation group $G$ to be $\text{Aut}(\text{Orb}(G))$ and say that $G$ is $k$-closed if $G = G^{(k)}$. It is easy to see that $G^{(k)}$ coincides with the intersection of all $k$-closed permutation groups on $V$ containing $G$.

**k-closure problem.** Given a permutation group $G$ and a positive integer $k$, find a set of generators of $G^{(k)}$.

The case $k = 1$ is trivial because the 1-closure of a permutation group $G$ is the direct product of symmetric groups acting on the orbits of $G$. Since the 2-closure problem is reduced to the Graph Isomorphism Problem, the 2-closure of any permutation group can be constructed in moderately exponential time (see [2]). We also mention a quasipolynomial algorithm from [3] constructing the automorphism group of a tournament (and so solving the 2-closure problem for permutation groups of odd order) in time $n^{O(\log n)}$ where $n$ is the cardinality of $V$. It should be noted that the technique from [3] and the inclusion $G^{(k)} \leq G^{(2)}$ valid for $k \geq 2$ provide an $n^{O(k)}$ reduction of the $k$-closure problem to the 2-closure problem if $G^{(2)}$ is a solvable group.

The setting of the 2-closure problem appeared in [8] where a polynomial-time algorithm for nilpotent permutation groups was described. It was based on the technique of [3] mentioned above and exploited the fact that the 2-closure of a nilpotent permutation group is solvable. The main obstacle to extending the result to solvable groups is the observation that the 2-closure of a solvable group is not necessarily solvable: there are 2-transitive solvable groups. It was remarked in [8] that the next interesting case is that of groups of odd order. This class is closed with respect to taking 2-closure and by the famous Feit–Thompson theorem consists of solvable groups. The main result of the paper is a polynomial-time solution to the 2-closure problem in this case.

**Theorem 1.1.** The 2-closure problem for a permutation group of odd order on $V$ can be solved in polynomial time in the cardinality of $V$.

It was proved in [9] that each primitive group of odd order is 4-closed. Combining this result and the above reduction of the $k$-closure problem to the 2-closure problem we obtain by Theorem 1.1 the following statement.

**Theorem 1.2.** For any positive integer $k \geq 1$ the $k$-closure problem for a primitive permutation group of odd order on $V$ can be solved in polynomial time in the cardinality of $V$.

Let us discuss the basic ideas of the proof. First, using the standard permutation group techniques we recursively reduce the 2-closure problem for permutation groups...
of odd order to that for primitive ones. Here we make use of the fact that the intransitive action of the direct product as well as the imprimitive action of the wreath product preserve the property ‘to be 2-closed’.

To manage with primitive permutation groups of odd order we make use of Suprunenko’s theory [10]. In this case, a one-point stabilizer $G_v, v \in V$, can be viewed as an irreducible linear group over a prime field $\text{GF}(p)$ for some $p > 2$. Using the algorithm BLOCK (see Section 5) we proceed depending on imprimitivity or primitivity of this group. If it is imprimitive we construct an imbedding of $G$ into the wreath product in primitive action of two smaller permutation groups of odd order (see Section 4.2) and apply the recursion. This is possible since the property ‘to be 2-closed’ is preserved by the primitive action of the wreath product.

If $G_v$ is a primitive linear group, then there are two possibilities: either $G = G^{(2)}$ or $G$ is permutationally equivalent to a subgroup of odd order of the group $\text{AGL}(1, p^d)$ consisting of all semilinear affine transformations of $\text{GF}(p^d)$. In the first case we are done. In the second one, the algorithm IMBED (see Section 5) constructs the required imbedding and we can find $G^{(2)}$ using the 2-closedness of the odd part of $\text{AGL}(1, p^d)$.

The paper consists of seven sections. In Section 2 we give some definitions concerning permutation and linear groups. The wreath product and its actions compose the subject of Section 3. We prove Proposition 3.1 where the behavior of 2-closure with respect to these actions is studied. In Section 4 we apply Suprunenko’s theory to a primitive permutation group of odd order. Some algorithmic tools and the MAIN ALGORITHM are described in Section 5 and Section 6, respectively. The latter also contains the proof of Theorem 1.1. A brief discussion of the problems concentrated around the $k$-closure problem is presented in Section 7.

A preliminary version of this paper is [4].

**Notation.** As usual, $\text{GF}(p^d)$ denotes a finite field with $p^d$ elements ($p$ is a prime).

Throughout the paper $V$ denotes a finite set with $n = |V|$ elements. If $E$ is an equivalence (i.e., reflexive, symmetric and transitive relation) on $V$, then $V/E$ denotes the set of all equivalence classes modulo $E$.

The group of all permutations of $V$ is denoted by $\text{Sym}(V)$. The unity of $\text{Sym}(V)$ is denoted by $\text{id}_V$. (In all our algorithms a subgroup of $\text{Sym}(V)$ will be given by a set of at most $n^2$ generators; for this fact and the standard permutation group algorithms see [6].)

If $G$ is a group, then $H \leq G$ means that $H$ is a subgroup of $G$.

### 2. Permutation and linear groups

All undefined terms below concerning permutation and linear groups can be found in [11] and [10], respectively.
2.1. By a permutation group on a set $V$ we mean a subgroup of $\text{Sym}(V)$. Let $G \leq \text{Sym}(V)$, $G' \leq \text{Sym}(V')$ be permutation groups and $\varphi : V \to V'$ be a bijection. We say that $\varphi$ produces an imbedding $G \hookrightarrow G'$ of $G$ into $G'$, if $G^\varphi \leq G'$ where $G^\varphi$ is the image of $G$ with respect to the isomorphism from $\text{Sym}(V)$ onto $\text{Sym}(V')$ induced by $\varphi$.

For two permutation groups $G_1 \leq \text{Sym}(V_1)$ and $G_2 \leq \text{Sym}(V_2)$ we define their direct sum $G_1 \oplus G_2$ and direct product $G_1 \otimes G_2$ as permutation groups on the disjoint union $V_1 \sqcup V_2$ and the Cartesian product $V_1 \times V_2$ given by the natural actions of the group $G_1 \times G_2$ on these sets.

Let $k$ be a positive integer. Given a permutation group $G \leq \text{Sym}(V)$ denote by $\text{Orb}_k(G)$ the set of all orbits of the componentwise action of $G$ on $V^k$. Set

$$G^{(k)} = \{ g \in \text{Sym}(V) : O^g = O \text{ for all } O \in \text{Orb}_k(G) \}.$$ 

This permutation group is called the $k$-closure of $G$ (see [12]). It is well-known that

$$G^{(1)} \geq G^{(2)} \geq \cdots \geq G^{(n)} = G$$

and $H \leq G$ implies $H^{(k)} \leq G^{(k)}$ for all $k$. The group $G$ is called $k$-closed if $G^{(k)} = G$.

Let $U$ be a subset of $V$. Denote by $G_U$ and $G^U$ the setwise stabilizer of $U$ in $G$ and the restriction of $G_U$ to $U$, respectively. Thus $G_U \leq \text{Sym}(V)$ and $G^U \leq \text{Sym}(U)$.

If $U = \{v\}$, we write $G_v$ instead of $G_{\{v\}}$.

Let $G$ be transitive, i.e., $\text{Orb}_1(G) = \{V\}$. A non-empty subset $U \subset V$ is called a $G$-block if for each $g \in G$ either $U^g = U$ or $U^g \cap U = \emptyset$. $G$-blocks $V$ and $\{v\}$ for $v \in V$ are called trivial. If every $G$-block is trivial, then $G$ is called primitive. Otherwise, it is called imprimitive.

To each $G$-block $U$ we associate a $G$-invariant equivalence $E = E(U)$ on $V$ with $V/E = \{U^g : g \in G\}$. The induced action of $G$ on $V/E$ defines a permutation group on this set denoted by $G^E$.

2.2. Let $V$ be a linear space over a field $F$. As usual, we denote by $\text{GL}(V)$ the group of all non-degenerate linear transformations of $V$, by $T(V)$ the group of all translations of $V$ and by $\text{AGL}(V) = \text{GL}(V) T(V) = T(V) \text{GL}(V)$ the group of all affine transformations of $V$. Sometimes we will view these groups as subgroups of $\text{Sym}(V)$.

Let $\Gamma \leq \text{GL}(V)$ be an irreducible linear group over $V$. A linear subspace $U \subset V$ is called a $\Gamma$-block if

$$V = \sum_{U^g, g \in \Gamma} U^g$$

and the sum is direct. The group $\Gamma$ is called primitive (as a linear group) if each $\Gamma$-block is trivial, i.e., coincides with $V$. Otherwise, it is called imprimitive.

For a $\Gamma$-block $U$ set $V/\delta = \{U^g : g \in \Gamma\}$ where $\delta = \delta(U)$ is decomposition (1). There is a natural group homomorphism from $\Gamma$ to $\text{Sym}(V/\delta)$ mapping $h \in \Gamma$ to the permutation $U^g \mapsto U^{gh}$, $g \in \Gamma$. Let us denote its image by $\Gamma^\delta$. We also associate to $U$ a linear group $\Gamma^U \leq \text{GL}(U)$ consisting of all restrictions to $U$ of those $g \in \Gamma$ for which $U^g = U$. 

\[ \text{(1)} \]
3. Wreath product and its properties

3.1. Let $G$ be a group and $K \leq \text{Sym}(X)$ be a permutation group. Set

$$G \wr K = \{(g_x, x, k) : g_x \in G, k \in K\}.$$ 

Then the multiplication defined by

$$(g_x, x, k)(g'_x, x', k') = (g_x g'_x x, k k')$$

turns the set $G \wr K$ into a group called the wreath product of $G$ and $K$. It is easy to see that it is isomorphic to the semidirect product of the groups $G^X$ and $K$ with respect to the action of $K$ on $G^X$ by permutations of coordinates. The action of $K$ on $X$ induces a natural action of $G \wr K$ on $X$ with kernel $G^X$.

3.2. Let $G \leq \text{Sym}(V)$ be a permutation group. There are two natural actions of the wreath product $G \wr K$ on the sets $V \times X$ and $V^X$ defined as follows:

The imprimitive action is given by

$$(v, x)(g_x, k) = (v g_x^{x^{-1}} x, k), \quad v \in V, x \in X,$$

and defines a permutation group on $V \times X$ denoted by $G \downarrow K$. The term ‘imprimitive’ is explained by the fact that if $G$ is a transitive group, $E$ is a $G$-invariant equivalence on $V$ and $U \in V/E$, then there exists an imbedding $G \hookrightarrow \varphi_U (U \downarrow G) \wr G^E$ for a suitable bijection $\varphi_U : V \rightarrow U \times V/E$. This bijection $\varphi_U$ can be efficiently constructed but is not uniquely determined.

The primitive action is given by

$$\{v_x\}(g_x, k) = \{v'_x g_x^{x^{-1}}\}, \quad v_x \in V, x \in X,$$

and defines a permutation group on $V^X$ denoted by $G \uparrow K$. If $G$ is primitive, non-cyclic and $K$ is transitive, then $G \uparrow K$ is primitive (see [5]), which explains the term ‘primitive’.

3.3. Let $V$ be a linear space and $\Gamma \leq \text{GL}(V)$ be a group. Taking into account the natural injection of $\text{GL}(V)$ into $\text{Sym}(V)$ we consider $\Gamma$ as a permutation group on $V$. Further, let us endow the set $V^X$ with the linear structure of direct sum so that $V^X = \bigoplus_{x \in X} V$. Then the permutation group $\Gamma \uparrow K$ becomes a subgroup of $\text{GL}(V^X)$ coinciding with the wreath product of a linear group and a permutation group as defined in [10, Section 15]).

3.4. In the following statement we give the properties of the permutation group operations related to 2-closure.

**Proposition 3.1.** Given permutation groups $G_1, G_2$ and $G \leq \text{Sym}(V)$, $K \leq \text{Sym}(X)$ the following statements hold:

1. $$(G_1 \boxtimes G_2)(2) = G_1(2) \boxtimes G_2(2);$$
2. $$(G_1 \otimes G_2)(2) = G_1(2) \otimes G_2(2);$$
3. $$(G \downarrow K)(2) = G(2) \downarrow K(2);$$
4. $$(G \uparrow K)(2) \leq G(2) \uparrow K(2)$$ unless $G(2) = \text{Sym}(V)$. 
Besides, conclude that a counterexample is given by Remark 3.2. The inverse inclusion in statement (4) is not always true. A for all $S$ $gx$ for all $G$.

Proof. Since the first three statements can be treated in a similar way, we will prove only the third one. It is easy to see that the groups on both sides of (3) have the same 2-orbits. So $G^{(2)} \downarrow K^{(2)} \leq (G \downarrow K)^{(2)}$. On the other hand,

$$(G \downarrow K)^{(2)} \leq \text{Sym}(V) \downarrow \text{Sym}(X).$$

Let $(\{g_x\}, k) \in (G \downarrow K)^{(2)}$. Then this permutation stabilizes all binary relations on $V \times X$ of the form $(J_V, S)$, $S \in \text{Orb}_2(K)$ and $(R, I_X)$, $R \in \text{Orb}_2(G)$, where $J_V = V \times V$ and $I_X = \{(x,x) : x \in X\}$. This implies that $k \in K^{(2)}$ and $g_x \in G^{(2)}$ for all $x$, which completes the proof of (3).

We start the proof of (4) with some constructions. For $x_1, x_2 \in X$ set

$$\Delta(x_1, x_2) = \{(v_x, v'_x) : (v_x, v'_x) \in R_1, (v_x, v'_x) \in R_2$$

where $R_1, R_2 \in \text{Orb}_2(G)$, $R_1 \neq R_2$, $R_1, R_2 \subset V^2 \setminus I_V$. (The existence of $R_1$ and $R_2$ follows from the hypothesis.) The definition implies that

$$\Delta(x_1, x_2)^{(g_x, k)} = \Delta(x'_1, x'_2), \quad k \in \text{Sym}(X). \quad (2)$$

Besides,

$$\Delta(x_1, x_2) \cap \Delta(x'_1, x'_2) = \emptyset \quad \text{if} \quad (x_1, x_2) \neq (x'_1, x'_2). \quad (3)$$

For $S \in \text{Orb}_2(K)$ set

$$\Delta(S) = \bigcup_{(x_1, x_2) \in S} \Delta(x_1, x_2).$$

It follows from (2) that $\Delta(S)$ is a union of 2-orbits of $G \uparrow K$ and $\Delta(S_k) = \Delta(S)^{(g_x, k)}$ for all $g_x \in G$, $k \in K$. Moreover, the mapping $S \mapsto \Delta(S)$ is a bijection by (3).

Now we prove the fourth statement. Since $G \uparrow K \leq \text{Sym}(V) \uparrow \text{Sym}(X)$ and the last permutation group is 2-closed by [5], we have $(G \uparrow K)^{(2)} \leq (\text{Sym}(V) \uparrow \text{Sym}(X))^{(2)}$. Let $(\{g_x\}, k)$ stabilize each 2-orbit of $G \uparrow K$ where $g_x \in \text{Sym}(V)$, $k \in \text{Sym}(X)$. Then

$$\Delta(S) = \Delta(S^k) = \Delta(S)^{(g_x, k)}$$

for all $S \in \text{Orb}_2(K)$ (see above). By the injectivity of the mapping $S \mapsto \Delta(S)$ we conclude that $S = S^k$, i.e., $k \in K^{(2)}$. Finally, since the set $\{R\}_{x \in X} \subset V^X \times V^X$ is a 2-orbit of $G \uparrow K$ for all $R \in \text{Orb}_2(G)$, by the definition of the action we have $R^{g_x} = R$ for all $R$ and $x$. So $g_x \in G^{(2)}$ for all $x \in X$. □

Remark 3.2. The inverse inclusion in statement (4) is not always true. A counterexample is given by $G = \{\text{id}_V\}$ and any $K$ with $K \neq K^{(2)}$ and $|X| \leq n$.

Corollary 3.3. If the permutation groups $G_1, G_2, G, K$ are 2-closed, then so are the permutation groups $G_1 \boxplus G_2, G_1 \otimes G_2, G \downarrow K$ and for $G \neq \text{Sym}(V)$ also $G \uparrow K$.

3.5. Below we mainly deal with groups of odd order called for brevity as odd groups. By the Feit–Thompson theorem they are solvable. The class of odd permutation groups is obviously closed with respect to taking direct sums and direct and wreath products.
It was proved in [12] that the $k$-closure of an odd permutation group is also odd if $k \geq 2$. Thus, the condition of statement (4) of Proposition 3.1 is satisfied for such a group.

4. Primitive odd permutation groups

4.1. All facts cited in this subsection can be found for instance in [10]. Let $G \leq \text{Sym}(V)$ be a solvable primitive permutation group. Then $G$ has a uniquely determined normal subgroup $H$ isomorphic to an elementary Abelian $p$-group of order $p^d$ for some prime $p$. Moreover, the permutation group $H$ is regular on $V$, i.e., transitive with $H_v = \{\text{id}_V\}, v \in V$. In particular, $n = |H| = p^d$.

For each $v \in V$, the set $V$ can be endowed with the structure of a linear space over $\text{GF}(p)$ with zero $v$ so that $G_v$ can be viewed as an irreducible linear group on $V$. Moreover,

$$G = G_v H \leq \text{AGL}(V), \quad H = T(V).$$

Below we study $G$ depending on primitivity or imprimitivity of $G_v$ as a linear group.

4.2. Let $\Gamma \leq \text{GL}(V)$ be an irreducible linear group and $U$ be a $\Gamma$-block. Set $X = V/\mathcal{E}$ where $\mathcal{E}$ is the decomposition (1). For each $U' \in X$ choose $g \in \Gamma$ with $U^g = U$. Then $\varphi' = g^{-1}|_{U'}$ is a linear isomorphism from $U'$ onto $U$. Collecting all $\varphi'$ we obtain a linear isomorphism $\varphi_U : V \to U^X$ producing a linear imbedding $\Gamma \hookrightarrow \varphi_U, \Gamma^U \uparrow \Gamma^\mathcal{E}$ (cf. [10]).

**Proposition 4.1.** Let $G \leq \text{Sym}(V)$ be a solvable primitive permutation group and $U$ be a $G_v$-block, $v \in V$. Then the bijection $\varphi_U$ (for $\Gamma = G_v$) produces an imbedding $G \hookrightarrow \varphi_U, G^U \uparrow K$ where $K = (G_v)^\mathcal{E}$.

**Proof.** Set $\varphi = \varphi_U$. Since $\varphi(v) = (v, \ldots, v)$, we have

$$(G^U \uparrow K)_{\varphi(v)} = (G^U)_v \uparrow K = (G_v)^U \uparrow K.$$ By the definition of $\varphi$ this gives an imbedding $G_v \hookrightarrow (G^U \uparrow K)_{\varphi(v)}$. On the other hand, $T(V)^\varphi = T(U^X) = T(U)^X$. Thus the required statement follows from (4). □

4.3. Let us denote by $G(p, d)$ the group of all permutations of a finite field $F = \text{GF}(p^d)$ of the form

$$x \mapsto ax^a + b, \quad a, b \in F, \quad a \neq 0, \quad \sigma \in \text{Aut}(F).$$

This group is solvable and has a uniquely determined maximal subgroup of odd order, $G_{\text{odd}}(p, d)$. The group $G(p, d)$ is obviously 2-transitive. On the contrary, $G_{\text{odd}}(p, d)$ is a maximal odd subgroup of $\text{Sym}(F)$ (see [1]) and so 2-closed by Section 3.5. We say that a permutation group $G \leq \text{Sym}(V)$ is *cycloctic* if $G \hookrightarrow \varphi, G(p, d)$ for some bijection $\varphi : V \to F$.

4.4. Here we consider primitive groups with primitive one-point stabilizers.
Proposition 4.2. Let $G \leqslant \text{Sym}(V)$ be a primitive odd permutation group with primitive $G_v \leqslant \text{GL}(V)$, $v \in V$. Then $G = G^{(2)}$, unless $G$ is cyclotomic.

Proof. Set $\tilde{G} = G^{(2)}$. Since $\tilde{G} \geqslant G$, $\tilde{G}$ is a primitive permutation group and $\tilde{G}_v$ is a primitive linear group. On the other hand, if $G$ is not cyclotomic, then $\tilde{G}_v$ cannot be imbedded into $\tilde{G}(p,d)_0$ (equal to $I(1, p^d)$ in notation of [9]). Then by [9, Theorem 2.12] there exists $U \in \text{Orb}_1(\tilde{G}_v)$ for which the permutation group $(\tilde{G}_v)^U$ is regular. Moreover, the groups $G_v$ and $\tilde{G}_v$ being primitive linear groups, act faithfully on $U$. Since $\text{Orb}_1(G_v) = \text{Orb}_1(\tilde{G}_v)$ and $G_v \leqslant \tilde{G}_v$, it follows that $|\tilde{G}_v| = |G_v| = |U|$. Thus $\tilde{G} = G$. □

We note that if $G$ is a cyclotomic group satisfying the hypothesis of Proposition 4.2, then $G_v$ has a uniquely determined maximal normal Abelian subgroup $A$. Moreover, $A$ is cyclic and its linear span $[A]$ in $\text{End}_{\mathbb{F}(p)}(V)$ is a finite field of cardinality $n$.

4.5. In the following statement we summarize the results of the section to clarify the logic of the main algorithm.

Proposition 4.3. Let $G$ be a primitive odd permutation group. Then at least one of the following statements holds:
1. $G \hookrightarrow H \uparrow K$ for some odd permutation groups $H,K$ with $H \neq G$;
2. $G$ is cyclotomic;
3. $G$ is 2-closed.

5. Algorithmic tools

5.1. Let $G \leqslant \text{Sym}(V)$ be a primitive solvable permutation group and $\Gamma = G_v$. Below we will show how to find in polynomial time in $n$ the minimal $\Gamma$-block $U = U(S)$ containing a non-empty set $S \subset V$ different from $\{v\}$. Note that $\Gamma$ is an imprimitive linear group iff $U(\{w\}) \neq V$ for some $w \in V \setminus \{v\}$. Besides, within the same time one can find the set $V/\delta$ and the permutation group $\Gamma^\delta$ where $\delta = \delta(U)$ is the decomposition (1). According to [7] we have $|G| \leqslant n^4$, so the permutation group $G^U$ can be found within the same time by exhaustive search.

Let us describe how to find the minimal $\Gamma$-block $U(S)$ where $\Gamma \leqslant \text{GL}(V)$ is an irreducible linear group and $V$ is a finite-dimensional linear space over a field $F$. Let $\Delta$ be a generating set of $\Gamma$, $L \neq \{0\}$ be a subspace of $V$ and $M$ be a non-empty subset of $\Gamma$ such that the sum $L^M = \sum_{g \in M} L^g$ is direct. For recursion purpose, we define $\text{BLOCK}(\Delta,L,M)$ to be the minimal $\Gamma$-block containing $L$. In this notation $U(S) = \text{BLOCK}(\Delta, \langle S \rangle, \{1\})$ where $\langle S \rangle$ is the linear span of $S$. It is easy to see that the following procedure correctly finds $\text{BLOCK}(\Delta,L,M)$ and can be implemented in polynomial time in $|\Delta|$ and dim$_F(V)$.
BLOCK

Step 1: If \( L^M = V \), then output \( L \).

Step 2: If there exist \( g \in M \) and \( h \in \Delta \) such that the sum \( L^M \cup \{ gh \} = L^M + L^g h \) is direct, then output BLOCK(\( \Delta, L', M \cup \{ gh \} \)).

Step 3: Choose \( g \in M \) and \( h \in \Delta \) such that \( L^g h \not\subset L^M \). Output BLOCK(\( \{ V \}, L', \{ 1 \} \)) where \( L' = L + \sum_{\gamma \in M'} L^\gamma h^{-1} g^{-1} \) with \( M' = \{ g' \in M : L^g h \cap L^M \neq L^g h \cap L^M \} \).

5.2. Here we construct in polynomial time an explicit imbedding (if it exists) of a primitive solvable permutation group into the group of all semilinear affine transformations of the corresponding finite field.

IMBED

Input: a primitive solvable group \( G \leq \text{Sym}(V) \) with \( n = p^d \) and primitive \( G_v \leq \text{GL}(V), \ v \in V \).

Output: ‘\( G \) is not cyclotomic’ or a bijection \( \varphi : V \rightarrow \text{GF}(p^d) \) producing an imbedding \( G \hookrightarrow \varphi G(\text{odd}(p,d)) \).

Step 1: By exhaustive search find a maximal normal cyclic subgroup \( A \) of \( G_v \). If it is not uniquely determined or \( |K| \neq n \) where \( K = [A] \subseteq \text{End}(\text{GF}(p))(V) \) is the linear span of \( A \), then output ‘\( G \) is not cyclotomic’.

Step 2: Choose \( w \in V \setminus \{ v \} \) and output \( \psi = \varphi^{-1} \) where \( \psi : K \rightarrow V \) is a bijection defined by \( x \mapsto x(w) \). (In fact, \( K \cong \text{GF}(p^d) \) and \( \varphi(0) = v, \ \varphi(1) = w \).)

Claim. The algorithm IMBED is correct and runs in polynomial time in \( n \).

Proof. The time upper bound is clear from the inequality \( |G| \leq n^4 \) (see [7]). If \( G \) appears as an input of Step 2, then it is cyclotomic by [10, Section 19, Corollary 2] and so \( \varphi \) is the required bijection. This proves the correctness of the algorithm for a non-cyclotomic \( G \) and after taking into account the end of Section 4.4 also for a cyclotomic one. □

Remark. If \( G \) is an odd cyclotomic group, then the bijection \( \varphi \) produces an imbedding \( G \hookrightarrow \varphi G(\text{odd}(p,d)) \).

5.3. The following construction is the basic auxiliary tool of the main algorithm. Let \( G \leq \text{Sym}(V) \) and \( G' \leq \text{Sym}(V') \) be permutation groups and \( \varphi : V \rightarrow V' \) be a bijection. Set

\[
\text{CLOSURE}(G, G', \varphi) = ((G^\varphi)^{(2)} \cap G')^{\varphi^{-1}}.
\]

Claim. If \( G' \) is a solvable group, then the permutation group CLOSURE\( (G, G', \varphi) \) can be found in polynomial time in \( n \).

Proof. Without loss of generality we assume that \( V = V' \) and \( \varphi = \text{id}_V \). Denote by \( \Gamma \) the edge colored graph with \( V \) as a vertex set, \( V \times V \) as an edge set and \( \text{Orb}_2(G) \) as
the set of colored classes. Then clearly $G^{(2)} = \text{Aut}(\Gamma)$. Since the group $G'$ is solvable, the claim follows from [3, Corollary 3.6]. □

6. Proof of Theorem 1.1

We start with the description of the algorithm.

**Main Algorithm**

*Input:* an odd permutation group $G \leq \text{Sym}(V)$.

*Output:* the permutation group $G^{(2)}$.

**Step 1:** If $G$ is intransitive and $U \in \text{Orb}_1(G)$, then output

$$\text{CLOSURE}(G, (G^U)^{(2)}) \boxplus (G^{V\setminus U})^{(2)}, \varphi_U),$$

where $(G^U)^{(2)}$ and $(G^{V\setminus U})^{(2)}$ are found recursively and $\varphi_U : V \to U \sqcup (V \setminus U)$ is a natural bijection.

**Step 2:** If $G$ is imprimitive and $U$ is a non-trivial $G$-block, then output

$$\text{CLOSURE}(G, (G^U)^{(2)} \downarrow (G^E)^{(2)}, \varphi_U)$$

where $(G^U)^{(2)}$ and $(G^E)^{(2)}$ are found recursively, $E = E(U)$ is the equivalence from Section 2.1 and $\varphi_U : V \to U \times V/E$ is the bijection from Section 3.2.

**Step 3:** If $G$ is primitive, $G_v \leq \text{GL}(V)$ is imprimitive and $U$ is a non-trivial $G_v$-block found by the procedure BLOCK (see Section 5.1), then output

$$\text{CLOSURE}(G, (G^U)^{(2)} \uparrow ((G_v)^{\varphi})^{(2)}, \varphi_U),$$

where $(G^U)^{(2)}$ and $((G_v)^{\varphi})^{(2)}$ are found recursively, $\varphi = \varphi(U)$ is the decomposition (1) and $\varphi_U : V \to U^{V/\varphi}$ is the bijection from Section 4.2.

**Step 4:** If $G$ is cyclotomic and $\varphi : V \to \text{GF}(p^d)$ is the bijection found by the algorithm IMBED, then output

$$\text{CLOSURE}(G, G_{\text{odd}}(p, d), \varphi).$$

**Step 5:** Output $G$.

To prove the correctness of the algorithm, it suffices to check that the output of each of its steps coincides with $G^{(2)}$. For Step 5, this follows from Proposition 4.2. For Steps 1–3 (resp. Step 4) the statement is easily deduced from the fact that by Corollary 3.3 (resp. Section 4.3) the second argument of CLOSURE is a 2-closed group containing $G^U$ (resp. $G^\varphi$).

To estimate the running time of the algorithm we note that the number of recursive calls is polynomial in $n$. Besides, since the 2-closure of an odd group is also odd, each computation of CLOSURE throughout the algorithm can be done in time $n^{O(1)}$ by the Claim of Section 5.3. Finally, the bijections $\varphi_U$ and $\varphi$ at Steps 2–4 can be found in time $n^{O(1)}$ (see Sections 3.2, 4.2, 5.2, respectively).
7. Discussion

The 2-closure problem seems to be easier than the Graph Isomorphism Problem. However, we do not know a polynomial-time solution to it even for solvable groups. As far as an arbitrary \( k \) is concerned the difficulties arise even for Abelian groups. Despite the fact that the 2-closure of an Abelian group can be found efficiently, we cannot construct its \( k \)-closure in time depending on \( k \) polynomially. In particular, the problem of finding the smallest \( k \) for which such a group is \( k \)-closed seems to be hard.

It is well known that the Graph Isomorphism Problem is polynomially reduced to the problem of finding the automorphism group of a graph. The natural question arises: what knowledge of the automorphism group could help to find it? More exactly, we state the following problem:

**Problem 7.1.** Given a colored graph \( \Gamma \) and a permutation group \( G \leqslant \text{Aut}(\Gamma) \) find a set of generators of \( \text{Aut}(\Gamma) \).

If \( G \) is the identity group, the problem is equivalent to the Graph Isomorphism Problem. If \( G \) and \( \text{Aut}(\Gamma) \) are 2-equivalent (i.e., have the same 2-orbits), we come to the 2-closure problem, which is solved in this paper for an odd \( G \). It would be interesting to extend this result to the case when \( G \) and \( \text{Aut}(\Gamma) \) are 1-equivalent, i.e., have the same orbits. For example, if \( G \) is a regular permutation group we come to the problem of finding the automorphism group of the S-ring over \( G \) generated by \( \Gamma \) (as to S-rings, see [11,5]).

References

[1] A. Astie, Vertex-symmetric tournaments of order \( n \) with the minimum number of arc orbits, in: M. Fiedler (Ed.) Recent Advances Graph Theory, Academia, Prague, 1975, pp. 17–30.
[12] H. Wielandt, Permutation groups through invariant relations and invariant functions, Lecture Notes, Department of Mathematics, Ohio State University, Columbus, 1969.