Two-closure of odd permutation group in polynomial time

Sergei Evdokimov [*] **Ilia Ponomarenko** [†]

October, 1996

Abstract

We present a polynomial-time algorithm which constructs the 2-closure of a permutation group of odd order.

[*]St.Petersburg Institute for Informatics and Automation of the Academy of Sciences of Russia, 199178 St.Petersburg and University of Bonn, 53117 Bonn. E-mail: evdokim@pdmi.ras.ru. Research supported by the Volkswagen-Stiftung Program on Computational Complexity.

[†]St.Petersburg Department of Mathematical Institute of the Academy of Sciences of Russia, 191011 St.Petersburg and University of Bonn, 53117 Bonn. E-mail: ponom-ko@pdmi.ras.ru. Research supported by the Volkswagen-Stiftung Program on Computational Complexity.

1 Introduction

The method of invariant relations in permutation group theory was firstly applied by H. Wielandt in [11]. In [12] 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 for each positive integer k a Galois correspondence between permutation groups on a finite set V and all partitions of V^k (see [4]). Namely, to each permutation group $\mathcal{G}$ on V we associate a partition $\mathrm{Orb}_k(\mathcal{G})$ which is the partition of V^k into k-orbits of $\mathcal{G}$, i.e. the orbits of the induced action of $\mathcal{G}$ on V^k. On the other hand, to each partition P of V^k we associate its automorphism group $\mathrm{Aut}(P)$ consisting by definition of all permutations of V preserving the partition P. Denoting by $\geq$ the natural partial orders on the sets of all permutation groups on V and partitions of V^k we have

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

which expresses the correspondence.

In the context of computational complexity theory the above correspondence leads to two natural problems: given a partition P find $\mathrm{Orb}_k(\mathrm{Aut}(P))$ and given a permutation group $\mathcal{G}$ find $\mathrm{Aut}(\mathrm{Orb}(\mathcal{G}))$. It is well-known that for $k = 2$ the first of them is equivalent to the Graph Isomorphism Problem (a modern knowledge of it can be found in [2]). In this paper we are interested in the other problem.

According to [11] we define the k-closure $\mathcal{G}^{(k)}$ of a permutation group $\mathcal{G}$ to be $\mathrm{Aut}(\mathrm{Orb}(\mathcal{G}))$ and say that $\mathcal{G}$ is k-closed if $\mathcal{G} = \mathcal{G}^{(k)}$. It is easy to see that $\mathcal{G}^{(k)}$ coincides with the intersection of all k-closed permutation groups on V containing $\mathcal{G}$.

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

The case $k = 1$ is trivial because the 1-closure of a permutation group $\mathcal{G}$ is the direct product of symmetric groups acting on the orbits of $\mathcal{G}$. 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 subexponential algorithm from [3] constructing the automorphism group of a tournament (and so solving the 2-closure problem for odd order groups) 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 $\mathcal{G}^{(k)} \leq \mathcal{G}^{(2)}$ for $k \geq 2$ provide a $n^{O(k)}$ reduction of the k-closure problem to the 2-closure problem in the case when the group $\mathcal{G}^{(2)}$ is solvable.

The setting of the 2-closure problem appeared in [7] 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 extend the result to solvable groups is the observation that the 2-closure of a solvable group is not necessary solvable: there are 2-transitive solvable groups. It was remarked in [7] that the next interesting case is that of groups of odd order. This class is closed under 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 *Let $\mathcal{G}$ be a permutation group of odd order on V. Then the generators of $\mathcal{G}^{(2)}$ can be found in polynomial time in the cardinality of V.*

It was proved in [8] 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 *Let $\mathcal{G}$ be a primitive permutation group of odd order on V. Then for $k \geq 1$ the generators of $\mathcal{G}^{(k)}$ can be found in polynomial time in the cardinality of V.*

Let us discuss the basic ideas of the proof. Firstly, using the standard permutation group technique 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 preserves the property "to be 2-closed".

To manage with primitive permutation groups of odd order we make use of Suprunenko's theory [9]. In this case a one point stabilizer $\mathcal{G}_v$, $v \in V$ can be viewed as an irreducible linear group over a prime field $\mathrm{GF}(p)$ for $p > 2$. Using the algorithm BLOCK (see section 5) we proceed depending on the imprimitivity or primitivity of this group. If it is imprimitive we construct an imbedding of $\mathcal{G}$ to the wreath product in primitive action of two smaller permutation groups of odd order (see subsection 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 $\mathcal{G}_v$ is a primitive linear group then there are two possibilities: either $\mathcal{G} = \mathcal{G}^{(2)}$ or $\mathcal{G}$ is permutation equivalent to a subgroup of odd order of the group $\mathrm{AGL}(1, p^d)$ consisting of all semilinear affine transformations of $\mathrm{GF}(p^d)$. In the first case we are done. In the second one the algorithm IMBED (see section 5) constructs the required imbedding and we find $\mathcal{G}^{(2)}$ using the 2-closeness of the odd part of $\mathrm{AGL}(1, p^d)$.

The paper consists of 7 sections. In the second one we give some definitions concerning permutation and linear groups. The wreath product and its actions compose the subject of section 3. Here we prove Proposition 3.1 in which the invariance of 2-closure with respect to these actions is stated. In section 4 we apply Suprunenko's theory to 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 concentrating around the k-closure problem is presented in section 7.

Notation. As usual $\mathrm{GF}(p^d)$ 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 $\mathrm{Sym}(V)$. The unity of $\mathrm{Sym}(V)$ is denoted by id_V. In all our algorithms a permutation group on V will be given by a set of at most n^2 generators (for this fact and the standard permutation group algorithms see [5]).

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

2 Permutation and linear groups

All undefined below notions concerning permutation and linear groups can be found in [10] and [9] respectively.

2.1. Under a *permutation group* $\mathcal{G} = (G, V)$ on a set V we mean a group G with a faithful action $v \mapsto v^g$ of G on V. We write $\mathbf{1}_V$ instead of (id_V, V). If $\mathcal{H} = (H, V)$ is another permutation group on V, then we write $\mathcal{H} \le \mathcal{G}$ if H is a subgroup of G and the action of H is induced by that of G. In particular, $\mathcal{G} \le \mathbf{Sym}(V)$ where $\mathbf{Sym}(V) = (\mathrm{Sym}(V), V)$. Let $\varphi : V \to V'$ be a bijection. We say that φ produces an imbedding $\mathcal{G} \hookrightarrow_\varphi \mathcal{G}'$ of $\mathcal{G}$ in $\mathcal{G}'$, if $\mathcal{G}^\varphi \le \mathcal{G}'$. Here $\mathcal{G}^\varphi = (G^\varphi, V')$ where G^φ it the image of G with respect to the isomorphism from $\mathrm{Sym}(V)$ on $\mathrm{Sym}(V')$ induced by φ.

For two permutation groups $\mathcal{G}_1 = (G_1, V_1)$ and $\mathcal{G}_2 = (G_2, V_2)$ we define their direct sum and direct product by

$$\mathcal{G}_1 + \mathcal{G}_2 = (G_1 \times G_2, V_1 + V_2), \quad \mathcal{G}_1 \times \mathcal{G}_2 = (G_1 \times G_2, V_1 \times V_2),$$

where $V_1 + V_2$ is the disjoint union of V_1 and V_2 and the actions are defined in a natural way.

Let k be a positive integer. For a permutation group $\mathcal{G}$ denote by $\mathrm{Orb}_k(\mathcal{G})$ the set of all orbits of the componentwise action of G on V^k. Set $\mathcal{G}^{(k)} = (G^{(k)}, V)$ where

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

This group is called the *k-closure* of $\mathcal{G}$ (see [11]). It is known that

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

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

Let U be a subset of V. Denote by

$$\mathcal{G}_U = (G_U, V), \qquad \mathcal{G}^U = (G^U, U)$$

the setwise stabilizer of U in $\mathcal{G}$ and the restriction of $\mathcal{G}_U$ to U respectively. If $U = \{v\}$, then we write $\mathcal{G}_v$ instead of $\mathcal{G}_{\{v\}}$ and G_v instead of $G_{\{v\}}$.

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

To each $\mathcal{G}$-block U we associate a $\mathcal{G}$-invariant equivalence $E = E(U)$ on V with $V/E = \{U^g : \ g \in G\}$. Denote by

$$\mathcal{G}^E = (G^E, V/E)$$

the image of $\mathcal{G}$ with respect to the natural surjection $V \to V/E$.

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

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

$$V = \sum_{U^g,\ g \in \Gamma} U^g \tag{1}$$

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

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

3 Wreath product and its properties

3.1. Let G be a group and $\mathcal{K} = (K, X)$ be a permutation group. Set

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

Then the multiplication given by

$$(\{g_x\}, k)(\{g'_x\}, k') = (\{g_x g'_{x^k}\}, kk')$$

turns the set $G \wr \mathcal{K}$ into a group called the *wreath product* of G and $\mathcal{K}$. 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 $G \wr \mathcal{K}$ on X with kernel G^X.

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

The *imprimitive action* is given by

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

and defines a permutation group $(G \wr \mathcal{K}, V \times X)$ denoted by $\mathcal{G} \downarrow \mathcal{K}$. The name "imprimitive" is explained by the fact that if $\mathcal{G}$ is a transitive group, E is a $\mathcal{G}$-invariant equivalence on V and $U \in V/E$, then there exists an imbedding $\mathcal{G} \hookrightarrow_\varphi \mathcal{G}^U \downarrow \mathcal{G}^E$ for a suitable bijection $\varphi = \varphi_U$ from V on $U \times V/E$. This bijection φ_U can be efficiently constructed but is not uniquely determined.

The *primitive action* is given by

$$\{v_x\}^{(\{g_x\}, k)} = \{v_{x^{k^{-1}}}^{g_{x^{k^{-1}}}}\}, \qquad v \in V,\ x \in X$$

and defines a permutation group $(G \wr \mathcal{K}, V^X)$ denoted by $\mathcal{G} \uparrow \mathcal{K}$. If $\mathcal{G}$ is primitive, noncyclic and $\mathcal{K}$ is transitive, then $\mathcal{G} \uparrow \mathcal{K}$ is primitive (see [4]), which explains the name "primitive".

3.3. Let V be a linear space and $\Gamma \leq \mathrm{GL}(V)$ be a group. Then the group $\Gamma \wr \mathcal{K}$ can be viewed as a subgroup of $\mathrm{GL}(V^X)$ where $V^X = \oplus_{x \in X} V$. If Γ is an irreducible linear group, U is a Γ-block and $\mathcal{E} = \mathcal{E}(U)$ is the decomposition (1), then there exists an imbedding $\Gamma \hookrightarrow_\varphi \Gamma^U \wr \Gamma^{\mathcal{E}}$ for a suitable linear isomorphism $\varphi = \varphi_U$ from V on $U^{V/\mathcal{E}}$.

This isomorphism φ_U can be efficiently constructed but is not uniquely determined. It is worth noting that to each linear group $\Gamma \le \mathrm{GL}(V)$ one can associate a permutation group (Γ, V) defined by a natural injection of $\mathrm{GL}(V)$ in $\mathrm{Sym}(V)$, so that

$$(\Gamma \wr \mathcal{K}, V^X) = (\Gamma, V) \uparrow \mathcal{K}. \tag{2}$$

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 $\mathcal{G}_1$, $\mathcal{G}_2$, $\mathcal{G} = (G, V)$ and $\mathcal{K} = (K, X)$ the following statements hold:*

(1) $(\mathcal{G}_1 + \mathcal{G}_2)^{(2)} = \mathcal{G}_1^{(2)} + \mathcal{G}_2^{(2)}$;

(2) $(\mathcal{G}_1 \times \mathcal{G}_2)^{(2)} = \mathcal{G}_1^{(2)} \times \mathcal{G}_2^{(2)}$;

(3) $(\mathcal{G} \downarrow \mathcal{K})^{(2)} = \mathcal{G}^{(2)} \downarrow \mathcal{K}^{(2)}$;

(4) $(\mathcal{G} \uparrow \mathcal{K})^{(2)} \le \mathcal{G}^{(2)} \uparrow \mathcal{K}^{(2)}$ *if* $\mathcal{G}^{(2)} \ne \mathbf{Sym}(V)$.

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 2-orbits of the groups in the both sides of (3) coincide. So $\mathcal{G}^{(2)} \downarrow \mathcal{K}^{(2)} \le (\mathcal{G} \downarrow \mathcal{K})^{(2)}$. On the other hand,

$$(\mathcal{G} \downarrow \mathcal{K})^{(2)} \le \mathbf{Sym}(V) \downarrow \mathbf{Sym}(X).$$

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

$$\Delta(x_1, x_2) = \{(\{v_x\}, \{v'_x\}) : \ (v_{x_1}, v'_{x_1}) \in R_1, \ (v_{x_2}, v'_{x_2}) \in R_2, \ v_x = v'_x \text{ for } x \notin \{x_1, x_2\}\}$$

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

$$\Delta(x_1, x_2)^{(\{g_x\}, k)} = \Delta(x_1^k, x_2^k), \quad k \in \mathrm{Sym}(X). \tag{3}$$

Besides,

$$\Delta(x_1, x_2) \cap \Delta(x'_1, x'_2) = \emptyset, \quad \text{if } (x_1, x_2) \ne (x'_1, x'_2). \tag{4}$$

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

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

It follows from (3) that $\Delta(S)$ is a union of 2-orbits of $\mathcal{G} \uparrow \mathcal{K}$ 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 (4).

Now we prove the fourth statement. Since $\mathcal{G} \uparrow \mathcal{K} \le \mathbf{Sym}(V) \uparrow \mathbf{Sym}(X)$ and the last permutation group is 2-closed by [4], we have $(\mathcal{G} \uparrow \mathcal{K})^{(2)} \le \mathbf{Sym}(V) \uparrow \mathbf{Sym}(X)$. Let $(\{g_x\}, k)$ stabilize each 2-orbit of $\mathcal{G} \uparrow \mathcal{K}$ where $g_x \in \mathrm{Sym}(V)$, $k \in \mathrm{Sym}(X)$. Then

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

for all $S \in \mathrm{Orb}_2(\mathcal{K})$ (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 $\mathcal{G} \uparrow \mathcal{K}$ for all $R \in \mathrm{Orb}_2(\mathcal{G})$, 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 (4) is not always true. A counterexample is given by $\mathcal{G} = \mathbf{1}_V$ and an arbitrary $\mathcal{K}$ with $\mathcal{K} \neq \mathcal{K}^{(2)}$ and $\#X$ not more than n.*

Corollary 3.3 *If the permutation groups $\mathcal{G}_1$, $\mathcal{G}_2$, $\mathcal{G}$, $\mathcal{K}$ are 2-closed, then so are $\mathcal{G}_1+\mathcal{G}_2$, $\mathcal{G}_1 \times \mathcal{G}_2$, $\mathcal{G} \downarrow \mathcal{K}$ and for $\mathcal{G} \neq \mathbf{Sym}(V)$ so is also $\mathcal{G} \uparrow \mathcal{K}$.*■

3.5. Below we mainly deal with groups of odd order called for brevity odd groups. By the Feit-Thompson theorem they are solvable. The class of odd permutation groups is closed with respect to taking direct sums and direct and wreath products. It was proved in [11] that the k-closure of an odd permutation group is also odd for $k \geq 2$. Thus the condition of statement (4) of Proposition 3.1 is satisfied for such a group.

4 Odd primitive permutation groups

4.1. All facts cited in this subsection can be found for instance in [9]. Let $\mathcal{G} = (G, V)$ 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. The permutation group $\mathcal{H} = (H, V)$ is regular, i.e., transitive with $\mathcal{H}_v = \mathbf{1}_V$. 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 $\mathrm{GF}(p)$ with zero v so that G_v can be viewed as an irreducible linear group on V. Moreover,

$$G = G_v H \leq \mathrm{AGL}(V), \qquad H = T(V). \tag{5}$$

Below we study $\mathcal{G}$ depending on the primitivity or imprimitivity of G_v as a linear group.

4.2. Let $\Gamma \leq \mathrm{GL}(V)$ be an irreducible linear group and U be a Γ-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' on U. Collecting all φ' we obtain a linear isomorphism $\varphi_U : V \to U^X$ such that $\Gamma \hookrightarrow_\varphi \Gamma^U \wr \Gamma^{\mathcal{E}}$ (see [9]).

Proposition 4.1 *Let $\mathcal{G} = (G, V)$ be a solvable primitive permutation group and U be a G_v-block, $v \in V$. Then the bijection $\varphi = \varphi_U$ produces an imbedding $\mathcal{G} \hookrightarrow_\varphi \mathcal{G}^U \uparrow \mathcal{K}$ with $\mathcal{K} = G_v^{\mathcal{E}}$ where φ_U and $\mathcal{E}$ are as above for $\Gamma = G_v$.*

Proof. Since $\varphi(v) = (v, \ldots, v)$, we have by (2)

$$(\mathcal{G}^U \uparrow \mathcal{K})_{\varphi(v)} = (\mathcal{G}^U)_v \uparrow \mathcal{K} = (\mathcal{G}_v)^U \uparrow \mathcal{K} = ((\mathcal{G}_v)^U \wr \mathcal{K}, U^X).$$

By the definition of φ this gives the imbedding $G_v \hookrightarrow_\varphi (\mathcal{G}^U \uparrow \mathcal{K})_{\varphi(v)}$. On the other hand, $T(V)^\varphi = T(U^X) = T(U)^X$. Thus the required statement follows from (5).■

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

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

This group is solvable and has a uniquely determined maximal subgroup of odd order, $G_{odd}(p,d)$. The corresponding permutation groups are denoted by $\mathcal{G}(p,d)$ and $\mathcal{G}_{odd}(p,d)$. The group $\mathcal{G}(p,d)$ is clearly 2-transitive whereas $\mathcal{G}_{odd}(p,d)$ is a maximal by inclusion odd subgroup of $\mathbf{Sym}(F)$ (see [1]) and so 2-closed by 3.5. We say that a permutation group $\mathcal{G} \le \mathbf{Sym}(V)$ is *cyclotomic* if $\mathcal{G} \hookrightarrow_{\varphi} \mathcal{G}(p,d)$ for some bijection $\varphi : V \to F$.

4.4. Here we consider primitive groups with primitive one point stabilizer.

Proposition 4.2 *Let $\mathcal{G} = (G,V)$ be a primitive odd permutation group with primitive $G_v \le \mathrm{GL}(V)$, $v \in V$. Then $\mathcal{G} = \mathcal{G}^{(2)}$, unless $\mathcal{G}$ is cyclotomic.*

Proof. Set $\overline{\mathcal{G}} = \mathcal{G}^{(2)}$. Since $\overline{\mathcal{G}} \ge \mathcal{G}$, $\overline{\mathcal{G}}$ is a primitive permutation group and $\overline{G}_v$ is a primitive linear group. On the other hand, if $\mathcal{G}$ is not cyclotomic, then $\overline{G}_v$ cannot be imbedded in $G(p,d)_0$ $(= \Gamma(1,p^d)$ in notation of [8]). Then by [8, Th. 2.12] there exists $U \in \mathrm{Orb}_1(\overline{\mathcal{G}}_v)$ for which the permutation group $(\overline{G}_v, U)$ is regular. Since $\mathrm{Orb}_1(\mathcal{G}_v) = \mathrm{Orb}_1(\overline{\mathcal{G}}_v)$ and $\mathcal{G}_v \le \overline{\mathcal{G}}_v$, it follows that $\#\overline{G}_v = \#G_v = \#U$. Thus $\overline{\mathcal{G}} = \mathcal{G}$.■

Note that if $\mathcal{G}$ is a cyclotomic group satisfying the hypothesis of the proposition, then G_v has a uniquely determined maximal normal Abelian subgroup A. Moreover, it is cyclic and its linear span $[A]$ in $\mathrm{End}_{\mathrm{GF}(p)}(V)$ 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 $\mathcal{G}$ be a primitive odd permutation group. Then at least one of the following statements holds:*

1. *$\mathcal{G} \hookrightarrow \mathcal{H} \uparrow \mathcal{K}$ for some odd permutation groups $\mathcal{H}, \mathcal{K}$ with $\mathcal{H} \ne \mathcal{G}$;*
2. *$\mathcal{G}$ is cyclotomic;*
3. *$\mathcal{G}$ is 2-closed.*

5 Algorithmic tools

5.1. Let $\mathcal{G} = (G,V)$ be a primitive solvable permutation group. Below we show how to find the minimal G_v-block $U = U(S)$ containing a nonempty set $S \subset V$ different from $\{v\}$ in polynomial time in n. Note that G_v is an imprimitive linear group iff $U(\{w\}) \ne V$ for some $w \in V \setminus \{v\}$. Moreover, within the same time one can find the set $V/\mathcal{E}$ where $\mathcal{E} = \mathcal{E}(U)$ is the decomposition (1) and the permutation group $(G_v)^{\mathcal{E}}$. According to [6] we have $\#G \le n^4$, so the permutation group $\mathcal{G}^U$ can be found within the same time by exaustive search.

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

BLOCK

Step 1. If $L^M = V$, then output L.

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

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

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

IMBED

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

Output: "$\mathcal{G}$ is not cyclotomic" or a bijection $\varphi : V \to \mathrm{GF}(p^d)$ giving an imbedding $\mathcal{G} \hookrightarrow_\varphi \mathcal{G}(p, d)$.

Step 1. By exaustive search find a maximal by inclusion normal cyclic subgroup A of G_v. If it is not uniquely determined or $\#K \neq n$ where $K = [A] \subset \mathrm{End}_{\mathrm{GF}(p)}(V)$ is the span of A, then output "$\mathcal{G}$ is not cyclotomic".

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

Claim. The algorithm IMBED is correctly defined and runs in time polynomial in n.

Proof. The time upper bound is clear from $\#G \leq n^4$ (see [6]). If the group $\mathcal{G}$ appears as an input of Step 2, then it is cyclotomic by [9, §19.1 Cor. 2] and so φ is the required bijection. This proves the correctness of the algorithm for a non-cyclotomic $\mathcal{G}$ and after taking into account the end of 4.4 also for a cyclotomic one.∎

Remark. If $\mathcal{G}$ is an odd cyclotomic group, then the bijection φ produces the imbedding $\mathcal{G} \hookrightarrow_\varphi \mathcal{G}_{odd}(p, d)$.

5.3. The following construction is the basic auxiliary tool of the main algorithm. Let $\mathcal{G} = (G, V)$ and $\mathcal{G}' = (G', V')$ are permutation groups and $\varphi : V \to V'$ is a bijection. Set

$$\mathrm{CLOSURE}(\mathcal{G}, \mathcal{G}', \varphi) = ((\mathcal{G}^\varphi)^{(2)} \cap \mathcal{G}')^{\varphi^{-1}}.$$

Claim. If G' is solvable, then the group CLOSURE$(\mathcal{G}, \mathcal{G}', \varphi)$ can be found in time polynomial in n.

Proof. It suffices to assume that $V = V'$ and $\varphi = \mathrm{id}_V$. Denote by Γ the edge colored graph with V as a vertex set, $V \times V$ as an edge set and $\mathrm{Orb}_2(\mathcal{G})$ as the set of colored classes. Then clearly $\mathcal{G}^{(2)} = \mathrm{Aut}(\Gamma)$. Since the group G' is solvable, the claim follows from [3, Cor. 3.6].∎

6 Proof of Theorem 1.1

We start with describing the algorithm.

MAIN ALGORITHM

Input: an odd permutation group $\mathcal{G} = (G, V)$.

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

Step 1. If $\mathcal{G}$ is intransitive and $U \in \mathrm{Orb}_1(\mathcal{G})$, then output

$$\mathrm{CLOSURE}(\mathcal{G}, (\mathcal{G}^U)^{(2)} + (\mathcal{G}^{V\setminus U})^{(2)}, \varphi)$$

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

Step 2. If $\mathcal{G}$ is imprimitive and U is a nontrivial $\mathcal{G}$-block, then output

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

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

Step 3. If $\mathcal{G}$ is primitive, $G_v \leq \mathrm{GL}(V)$ is imprimitive and U is a nontrivial G_v-block (see 5.1), then output

$$\mathrm{CLOSURE}(\mathcal{G}, (\mathcal{G}^U)^{(2)} \uparrow (G_v^{\mathcal{E}})^{(2)}, \varphi_U)$$

where $(\mathcal{G}^U)^{(2)}$ and $(G_v^{\mathcal{E}})^{(2)}$ are found recursively, $\mathcal{E} = \mathcal{E}(U)$ is the decomposition (1) (see 2.2) and $\varphi_U : V \to U^{V/\mathcal{E}}$ is the bijection from 4.2.

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

$$\mathrm{CLOSURE}(\mathcal{G}, \mathcal{G}_{odd}(p, d), \varphi).$$

Step 5. Output $\mathcal{G}$.∎

To prove the correctness of the algorithm it suffices to check that the output of each its step coincides with $\mathcal{G}^{(2)}$. For Step 5 it follows from Proposition 4.2. For Steps 1-4 the statement is easily deduced from the fact that the second argument of CLOSURE is a 2-closed group containing $\mathcal{G}^{\varphi}$. The last is the consequence of Corollary 3.3 (Steps 1-3) and subsection 4.3 (Step 4).

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 Claim of 5.3. Finally, the bijections φ_U and φ at Steps 2-4 can be found in time $n^{O(1)}$ (see 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. *Given a colored graph* Γ *and a permutation group* $\mathcal{G} \leq \mathrm{Aut}(\Gamma)$ *find the generators of* $\mathrm{Aut}(\Gamma)$.

If $\mathcal{G}$ is the identity group, the problem is equivalent to the Graph Isomorphism Problem. If $\mathcal{G}$ and $\mathrm{Aut}(\Gamma)$ 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 odd $\mathcal{G}$. It would be interesting to extend this result to the case when $\mathcal{G}$ and $\mathrm{Aut}(\Gamma)$ are 1-equivalent, i.e. have the same orbits. For example, if $\mathcal{G}$ is a regular permutation group we come to the problem of finding the automorphism group of the S-ring over $\mathcal{G}$ generated by Γ (as to S-rings see [10] and [4]).

References

[1] A. Astie, *Vertex-symmetric tournaments of order n with the minimum number of arc orbits*, in: "Recent Advances Graph Theory", Academia, Praha, 1975, 17-30.

[2] L. Babai, *Automorphism Groups, Isomorphism, reconstruction*, in: R.L. Graham, M. Grötschel, L.Lovász (eds): Handbook of combinatorics, vol. 2, Amsterdam (etc.), Elsevier (etc.), 1995, 1447-1540.

[3] L. Babai, and E.M. Luks, *Canonical labeling of graphs*, Proc. 15th ACM STOC, (1983), 1-15.

[4] I.A. Faradžev, M.H. Klin, and M.E. Muzichuk, *Cellular rings and groups of automorphisms of graphs*, in: I.A. Faradžev et al. (eds): Investigations in algebraic theory of combinatorial objects, Kluwer Acad. Publ., Dordrecht, 1994, 1-152.

[5] W.M. Kantor, and E.M. Luks, *Computing in quotient groups*, Proc. 22nd ACM STOC, (1990), 524-534.

[6] P.P. Palfy, *A polynomial bound for the orders of primitive solvable groups*, J. Algebra, 77 (1982), 127-137.

[7] I. Ponomarenko, *Graph Isomorphism Problem and 2-closed Permutation groups*, Applicable Algebra in Engineering, Communication and Computing, 5 (1994), 9-22.

[8] A. Seress, *The minimal base size of primitive solvable permutation groups*, appear in J. London Math. Soc.

[9] D.A. Suprunenko, *Matrix Groups*, AMS, Providence, 1976.

[10] H. Wielandt, *Finite permutation groups*, Academic press, New York - London, 1964.

[11] H. Wielandt, *Permutation groups through invariant relations and invariant functions*, Lect. Notes Dept. Math. Ohio St. Univ., Columbus, 1969.

[12] H. Wielandt, *Permutation representations*, Illinois J. Math., 13 (1969), 91-94.