A FASTER ISOMORPHISM TEST FOR GRAPHS OF SMALL DEGREE[*]

MARTIN GROHE[†], DANIEL NEUEN[†], AND PASCAL SCHWEITZER[‡]

Abstract. In a recent breakthrough, Babai [*Proceedings of STOC*, ACM, New York, 2016, pp. 684–697] gave a quasipolynomial-time graph isomorphism test. In this work, we give an improved isomorphism test for graphs of small degree: our algorithm runs in time $n^{\mathcal{O}((\log d)^c)}$, where n is the number of vertices of the input graphs, d is the maximum degree of the input graphs, and c is an absolute constant. The best previous isomorphism test for graphs of maximum degree d due to Babai, Kantor, and Luks [*Proceedings of FOCS*, IEEE, New York, 1983, pp. 162–171] runs in time $n^{\mathcal{O}(d/\log d)}$.

Key words. graph isomorphism, bounded degree graphs, permutation groups, groups with restricted composition factors

AMS subject classifications. 68Q25, 68R10, 68W05, 20B40, 20B15

DOI. 10.1137/19M1245293

1. Introduction. Luks's polynomial-time isomorphism test [24] for graphs of bounded degree is one of the cornerstones of the algorithmic theory of graph isomorphism. With a slight improvement given later [5], it tests in time $n^{\mathcal{O}(d/\log d)}$ whether two n-vertex graphs of maximum degree d are isomorphic. Over the past few decades Luks's algorithm and its algorithmic framework have been used as a building block for many isomorphism algorithms (see, e.g., [5, 6, 14, 18, 25, 29, 31]). More importantly, it also forms the basis for Babai's recent isomorphism test for general graphs [1, 2] which runs in quasipolynomial time (i.e., the running time is bounded by $n^{\mathrm{polylog}(n)}$). Indeed, Babai's algorithm follows Luks's algorithm but attacks the obstacle cases for which the recursion performed by Luks's framework does not lead to the desired running time. Graphs whose maximum degree d is at most polylogarithmic in the number n of vertices are not a critical case for Babai's algorithm, because for such graphs no large alternating or symmetric groups appear as factors of the automorphism group, and therefore the running time of Babai's algorithm on the class of all these graphs is still quasipolynomial. Hence graphs of polylogarithmic maximum degree form one of the obstacle cases toward improving Babai's algorithm. This alone is a strong motivation for trying to improve Luks's algorithm. In view of Babai's quasipolynomial-time algorithm, it is natural to ask whether there is an $n^{\mathrm{polylog}(d)}$-isomorphism test for graphs of maximum degree d. In this paper we answer this question affirmatively.

THEOREM 1.1. *The graph isomorphism problem for graphs of maximum degree d can be solved in time $n^{\mathcal{O}((\log d)^c)}$ for an absolute constant c.*

To prove the result we follow the standard route of considering the *string isomorphism problem*, which is an abstraction of the graph isomorphism problem that was introduced by Luks in order to facilitate a recursive isomorphism test based on

the structure of the permutation groups involved [6, 24]. Here a *string* is simply a mapping $\mathfrak{x} : \Omega \to \Sigma$, where the *domain* Ω and *alphabet* Σ are just finite sets. Given two strings $\mathfrak{x}, \mathfrak{y} : \Omega \to \Sigma$ and a permutation group $G \leq \mathrm{Sym}(\Omega)$, the objective of the string isomorphism problem is to compute the set $\mathrm{Iso}_G(\mathfrak{x}, \mathfrak{y})$ of all *G-isomorphisms* from $\mathfrak{x}$ to $\mathfrak{y}$, that is, all permutations $g \in G$ mapping $\mathfrak{x}$ to $\mathfrak{y}$. We study the string isomorphism problem for groups G in the class $\widehat{\Gamma}_d$ of groups all of whose composition factors are isomorphic to subgroups of S_d, the symmetric group acting on d points. Luks introduced this class because he observed that, after fixing a single vertex, the automorphism group of a connected graph of maximum degree d is in $\widehat{\Gamma}_d$.[1] Our main technical result, Theorem 7.4, states that we can solve the string isomorphism problem for groups $G \in \widehat{\Gamma}_d$ in time $n^{\mathrm{polylog}(d)}$, where $n = |\Omega|$ is the length of the input strings. This implies Theorem 1.1 (as outlined in section 8).

To prove this result, we introduce the new concept of an *almost d-ary sequence* of invariant partitions. More precisely, we exploit for the group G a sequence $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$ of G-invariant partitions $\mathfrak{B}_i$ of Ω, where $\mathfrak{B}_{i-1} \succ \mathfrak{B}_i$ means that $\mathfrak{B}_i$ refines $\mathfrak{B}_{i-1}$. For this sequence we require that for all i the induced group of permutations of the subclasses in $\mathfrak{B}_i$ of a given class in $\mathfrak{B}_{i-1}$ is permutationally equivalent to a subgroup of the symmetric group S_d or semiregular (i.e., only the identity has fixed points). Our algorithm that exploits such a sequence is heavily based on techniques introduced by Babai for his quasipolynomial-time isomorphism test. We even use Babai's algorithm as a black box in one case. One of our technical contributions is an adaptation of Babai's unaffected stabilizers theorem [2, Theorem 6] to groups constrained by an almost d-ary sequence of invariant partitions. In [2], the unaffected stabilizers theorem lays the groundwork for the group theoretic algorithms (the local certificates routine), and it plays a similar role here. However, we need a more refined running time analysis. Based on this we can then adapt the local certificates routine to our setting.

However, not every group in $\widehat{\Gamma}_d$ has such an almost d-ary sequence required by our technique. We remedy this by changing the operation of the group while preserving string isomorphisms. The structural and algorithmic results enabling such a change of operation form the second technical contribution of our work. For this we employ some heavy group theoretic results. First, applying the classification of finite simple groups via the O'Nan–Scott theorem and several other group theoretic characterizations, we obtain a structure theorem for primitive permutation groups in $\widehat{\Gamma}_d$ showing that they either are small (of size at most $n^{\mathrm{polylog}(d)}$) or have a specific structure. More precisely, large primitive groups in $\widehat{\Gamma}_d$ are composed, in a well-defined manner, of Johnson groups (i.e., symmetric/alternating groups with an induced action on t-element subsets of the standard domain). Second, to construct the almost d-ary sequence of partitions, we exploit the existence of these Johnson schemes and introduce subset lattices which are unfolded yielding the desired group operation.

With Luks's framework being used as a subroutine in various other algorithms, one can ask for the impact of the improved running time in such contexts. As a first, simple application we obtain an improved isomorphism test for relational structures (Theorem 8.3) and hypergraphs (Corollary 8.4). A deeper application is an improved fixed-parameter tractable algorithm for graph isomorphism of graphs parameterized by tree width [15], which substantially improves the algorithm from [23].

---

[1] In [24], the class $\widehat{\Gamma}_d$ is denoted by Γ_d. However, in the more recent literature Γ_d typically refers to a larger class of groups [3] (see subsection 2.2.3).

Outline. Section 3 is concerned with the structure of primitive $\widehat{\Gamma}_d$ groups; it culminates in Theorem 3.13 with a structural description. In section 4 we describe how to algorithmically change the operation of a group in $\widehat{\Gamma}_d$ to force the existence of an almost d-ary sequence of invariant partitions $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$ without changing string isomorphisms. In sections 5 and 6 we extend Babai's structural group theoretic results to our situation. Finally, in section 7 we prove our main algorithmic results, Theorems 7.3 and 7.4. Applications of these results, among them Theorem 1.1, are presented in section 8.

2. Preliminaries.

2.1. Graphs and other structures. A *graph* is a pair $\Gamma = (V, E)$ with vertex set $V = V(\Gamma)$ and edge relation $E = E(\Gamma)$. In this paper all graphs are finite and simple, i.e., there are no loops or multiple edges. The *neighborhood* of $v \in V(\Gamma)$ is denoted $N(v)$. A *path* of length k is a sequence $v_0, \ldots, v_k$ of distinct vertices such that $(v_{i-1}, v_i) \in E(\Gamma)$ for all $i \in [k]$ (where $[k] := \{1, \ldots, k\}$). The *distance* between two vertices $v, w \in V(\Gamma)$, denoted by $\mathrm{dist}(v, w)$, is the length of the shortest path from v to w.

An *isomorphism* from a graph Γ_1 to another graph Γ_2 is a bijective mapping $\varphi \colon V(\Gamma_1) \to V(\Gamma_2)$ which preserves the edge relation, that is, $(v, w) \in E(\Gamma_1)$ if and only if $(\varphi(v), \varphi(w)) \in E(\Gamma_2)$ for all $v, w \in V(\Gamma_1)$. Two graphs Γ_1 and Γ_2 are *isomorphic* ($\Gamma_1 \cong \Gamma_2$) if there is an isomorphism from Γ_1 to Γ_2. An *automorphism* of a graph Γ is an isomorphism from Γ to itself. By $\mathrm{Aut}(\Gamma)$ we denote the group of automorphisms of Γ. The *graph isomorphism problem* asks, given two (undirected) graphs Γ_1 and Γ_2, whether they are isomorphic.

A *t-ary relational structure* is a tuple $\mathfrak{A} = (D, R_1, \ldots, R_k)$ with domain D and t-ary relations $R_i \subseteq D^t$ for $i \in [k]$. An *isomorphism* from a structure $\mathfrak{A}_1 = (D_1, R_1, \ldots, R_k)$ to another structure $\mathfrak{A}_2 = (D_2, S_1, \ldots, S_k)$ is a bijective mapping $\varphi \colon D_1 \to D_2$ such that $(v_1, \ldots, v_t) \in R_i$ if and only if $(\varphi(v_1), \ldots, \varphi(v_t)) \in S_i$ for all $v_1, \ldots, v_t \in D_1$ and $i \in [k]$. As before, $\mathrm{Aut}(\mathfrak{A})$ denotes the automorphism group of $\mathfrak{A}$.

Let $\mathfrak{B}_1, \mathfrak{B}_2$ be two partitions of the same set Ω. We say $\mathfrak{B}_1$ *refines* $\mathfrak{B}_2$, denoted by $\mathfrak{B}_1 \preceq \mathfrak{B}_2$, if for every $B_1 \in \mathfrak{B}_1$ there is some $B_2 \in \mathfrak{B}_2$ such that $B_1 \subseteq B_2$. If additionally $\mathfrak{B}_1$ and $\mathfrak{B}_2$ are distinct we say $\mathfrak{B}_1$ *strictly refines* $\mathfrak{B}_2$ ($\mathfrak{B}_1 \prec \mathfrak{B}_2$). The *index* of $\mathfrak{B}_1$ in $\mathfrak{B}_2$ is $|\mathfrak{B}_2 : \mathfrak{B}_1| := \max_{B_2 \in \mathfrak{B}_2} |\{B_1 \in \mathfrak{B}_1 \mid B_1 \subseteq B_2\}|$. A partition $\mathfrak{B}$ (of the set Ω) is an *equipartition* if all elements $B \in \mathfrak{B}$ have the same size. For $S \subseteq \Omega$ we define the *induced partition* $\mathfrak{B}[S] = \{B \cap S \mid B \in \mathfrak{B} \text{ such that } B \cap S \neq \emptyset\}$. Note that $\mathfrak{B}[S]$ forms a partition of the set S.

For a set M and a natural number $t \leq |M|$ we denote by $\binom{M}{t}$ the set of all t-element subsets of M, that is, $\binom{M}{t} = \{X \subseteq M \mid |X| = t\}$. Note that the number of elements in $\binom{M}{t}$ is exactly $\binom{|M|}{t}$. Moreover, $\binom{M}{\leq t}$ denotes the set of all subsets of M of cardinality at most t.

2.2. Group theory. In this section we introduce the group theoretic notions required in this work. For a general background on group theory we refer to [30], whereas background on permutation groups can be found in [12].

2.2.1. Permutation groups. A *permutation group* acting on a set Ω is a subgroup $G \leq \mathrm{Sym}(\Omega)$ of the symmetric group. The size of the permutation domain Ω is called the *degree* of G and, throughout this work, is denoted by $n = |\Omega|$. If $\Omega = [n]$, then we also write S_n instead of $\mathrm{Sym}(\Omega)$. For $g \in G$ and $\alpha \in \Omega$ we denote by α^g the

image of α under the permutation g. The set $\alpha^G = \{\alpha^g \mid g \in G\}$ is the *orbit* of α. The group G is *transitive* if $\alpha^G = \Omega$ for some (and therefore every) $\alpha \in \Omega$.

For $\alpha \in \Omega$ the group $G_\alpha = \{g \in G \mid \alpha^g = \alpha\} \leq G$ is the *stabilizer* of α in G. The group G is *semiregular* if $G_\alpha = \{1\}$ for all $\alpha \in \Omega$. If additionally G is transitive, then the group G is called *regular*. For $\Delta \subseteq \Omega$ and $g \in G$ let $\Delta^g = \{\alpha^g \mid \alpha \in \Delta\}$. The *pointwise stabilizer* of Δ is the subgroup $G_{(\Delta)} = \{g \in G \mid \forall \alpha \in \Delta \colon \alpha^g = \alpha\}$. The *setwise stabilizer* of Δ is the subgroup $G_\Delta = \{g \in G \mid \Delta^g = \Delta\}$. Observe that $G_{(\Delta)} \leq G_\Delta$.

Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive group. A *block* of G is a nonempty subset $B \subseteq \Omega$ such that $B^g = B$ or $B^g \cap B = \emptyset$ for all $g \in G$. The trivial blocks are Ω and the singletons $\{\alpha\}$ for $\alpha \in \Omega$. The group G is said to be *primitive* if there are no nontrivial blocks. If G is not primitive it is called *imprimitive*. If $B \subseteq \Omega$ is a block of G, then $\mathfrak{B} = \{B^g \mid g \in G\}$ forms a *block system* of G. Note that $\mathfrak{B}$ is an equipartition of Ω. The group $G_{(\mathfrak{B})} = \{g \in G \mid \forall B \in \mathfrak{B} \colon B^g = B\}$ denotes the subgroup stabilizing each block $B \in \mathfrak{B}$ setwise. Observe that $G_{(\mathfrak{B})}$ is a normal subgroup of G. We denote by $G^{\mathfrak{B}} \leq \mathrm{Sym}(\mathfrak{B})$ the natural action of G on the block system $\mathfrak{B}$. More generally, if A is a set of objects on which G acts naturally, we denote by $G^A \leq \mathrm{Sym}(A)$ the action of G on the set A. A block system $\mathfrak{B}$ is *minimal* if there is no nontrivial block system $\mathfrak{B}'$ such that $\mathfrak{B} \prec \mathfrak{B}'$. Note that a block system $\mathfrak{B}$ is minimal if and only if $G^{\mathfrak{B}}$ is primitive.

A class of primitive groups that plays an important role in this work is the class of *Johnson groups*, alternating and symmetric groups with their actions on t-element subsets of the standard domain. For $m \in \mathbb{N}$ we denote by A_m the alternating group acting on the set $[m]$. For $t \leq \frac{m}{2}$ let $A_m^{(t)}$ be the action of A_m on the set of t-element subsets of $[m]$. Similarly, $S_m^{(t)}$ denotes the action of S_m on the set of t-element subsets of $[m]$.

Let $G \leq \mathrm{Sym}(\Omega)$ and $G' \leq \mathrm{Sym}(\Omega')$. A *homomorphism* is a mapping $\varphi \colon G \to G'$ such that $\varphi(g)\varphi(h) = \varphi(gh)$ for all $g, h \in G$. For $g \in G$ we denote by g^φ the φ-image of g. Similarly, for $H \leq G$ we denote by H^φ the φ-image of H (note that H^φ is a subgroup of G').

A *permutational isomorphism* from G to G' is a bijective mapping $f : \Omega \to \Omega'$ such that $G' = \{f^{-1}gf \mid g \in G\}$, where $f^{-1}gf \colon \Omega' \to \Omega'$ is the unique map mapping $f(\alpha)$ to $f(\alpha^g)$ for all $\alpha \in \Omega'$. If there is a permutational isomorphism from G to G', we call G and G' *permutationally equivalent*. A *permutational automorphism* of G is a permutational isomorphism from G to itself.

2.2.2. Algorithms for permutation groups. We review some basic facts about algorithms for permutation groups. For detailed information we refer to [31].

In order to perform computational tasks for permutation groups efficiently the groups are represented by generating sets of small size. Indeed, most algorithms are based on so-called strong generating sets, which can be chosen of size quadratic in the size of the permutation domain of the group and can be computed in polynomial time given an arbitrary generating set.

THEOREM 2.1 (cf. [31]).   *Let $G \leq \mathrm{Sym}(\Omega)$ and let S be a generating set for G. Then the following tasks can be performed in time polynomial in n and $|S|$:*
1. *compute the order of G,*
2. *given $g \in \mathrm{Sym}(\Omega)$, test whether $g \in G$,*
3. *compute the orbits of G,*
4. *given $\Delta \subseteq \Omega$, compute a generating set for $G_{(\Delta)}$, and*
5. *compute a minimal block system for G.*

For a second group $G' \leq \mathrm{Sym}(\Omega')$ with domain size $n' = |\Omega'|$, the following tasks can be solved in time polynomial in n, n' and $|S|$:

6. *given a homomorphism $\varphi \colon G \to G'$ (given as a list of images for $g \in S$),*
   (a) *compute a generating set for $\ker(\varphi) = \{g \in G \mid \varphi(g) = 1\}$, and*
   (b) *given $g' \in G'$, compute an element $g \in G$ such that $\varphi(g) = g'$ (if it exists).*

2.2.3. Groups with restricted composition factors. In this work we shall be interested in a particular subclass of permutation groups, namely groups with restricted composition factors. Let G be a group. A *subnormal series* is a sequence of subgroups $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_k = \{1\}$. The length of the series is k and the groups G_{i-1}/G_i are the factor groups of the series, $i \in [k]$. A *composition series* is a strictly decreasing subnormal series of maximal length. For every finite group G all composition series have the same family of factor groups considered as a multiset (cf. [30]). A *composition factor* of a finite group G is a factor group of a composition series of G.

LEMMA 2.2 (see [3, Lemma 2.2]). *Suppose $d \geq 6$. Let G be a permutation group of degree n such that G has no composition factor isomorphic to an alternating group A_k of degree $k > d$. Then $|G| \leq d^{n-1}$.*

DEFINITION 2.3. *For $d \geq 2$ let $\widehat{\Gamma}_d$ denote the class of all groups G for which every composition factor of G is isomorphic to a subgroup of S_d.*

We want to stress the fact that there are two similar classes of groups that have been used in the literature, both typically denoted by Γ_d. One of these is the class we define as $\widehat{\Gamma}_d$ introduced by Luks [24], while the other one used in [3] in particular allows composition factors that are simple groups of Lie type of bounded dimension.

LEMMA 2.4 (see Luks [24]). *Let $G \in \widehat{\Gamma}_d$. Then*
1. *$H \in \widehat{\Gamma}_d$ for every subgroup $H \leq G$, and*
2. *$G^\varphi \in \widehat{\Gamma}_d$ for every homomorphism $\varphi \colon G \to H$.*

2.2.4. String isomorphism and Luks's algorithm. In the following we give an outline of Luks's algorithm [24]. Our description of the algorithm as well as the notation mainly follow [2].

Let $\mathfrak{x}, \mathfrak{y} \colon \Omega \to \Sigma$ be two strings over a finite alphabet Σ and let $G \leq \mathrm{Sym}(\Omega)$ be a group. For $\sigma \in \mathrm{Sym}(\Omega)$ the string $\mathfrak{x}^\sigma$ is defined by

$$\mathfrak{x}^\sigma(\alpha) = \mathfrak{x}(\alpha^{\sigma^{-1}})$$

for all $\alpha \in \Omega$. A permutation $\sigma \in \mathrm{Sym}(\Omega)$ is a *G-isomorphism* from $\mathfrak{x}$ to $\mathfrak{y}$ if $\sigma \in G$ and $\mathfrak{x}^\sigma = \mathfrak{y}$. The *string isomorphism problem* asks, given $\mathfrak{x}, \mathfrak{y} \colon \Omega \to \Sigma$ and a group $G \leq \mathrm{Sym}(\Omega)$ given as a set of generators, whether there is a G-isomorphism from $\mathfrak{x}$ to $\mathfrak{y}$. The set of G-isomorphisms is denoted by $\mathrm{Iso}_G(\mathfrak{x}, \mathfrak{y}) := \{g \in G \mid \mathfrak{x}^g = \mathfrak{y}\}$.

More generally, for $K \subseteq \mathrm{Sym}(\Omega)$ and $W \subseteq \Omega$ we define

$$(2.1) \qquad \mathrm{Iso}_K^W(\mathfrak{x}, \mathfrak{y}) = \{g \in K \mid \forall \alpha \in W \colon \mathfrak{x}(\alpha) = \mathfrak{y}(\alpha^g)\}.$$

In this work $K = Gg$ will always be a coset where $G \leq \mathrm{Sym}(\Omega)$ and $g \in \mathrm{Sym}(\Omega)$ and the set W will be G-invariant. In this case $\mathrm{Iso}_K^W(\mathfrak{x}, \mathfrak{y})$ is either empty or a coset of the group $\mathrm{Aut}_G^W(\mathfrak{x}) := \mathrm{Iso}_G^W(\mathfrak{x}, \mathfrak{x})$, that is, $\mathrm{Iso}_K^W(\mathfrak{x}, \mathfrak{y}) = \mathrm{Aut}_G^W(\mathfrak{x})\sigma$, where $\sigma \in \mathrm{Iso}_K^W(\mathfrak{x}, \mathfrak{y})$ is arbitrary. Hence, the set $\mathrm{Iso}_K^W(\mathfrak{x}, \mathfrak{y})$ can be represented by a generating set for $\mathrm{Aut}_G^W(\mathfrak{x})$ and an element σ. Moreover, using the identity

Algorithm 1. Orbit-by-orbit processing.

1: $K := G$
2: **for** $i = 1, \ldots, s$ **do**
3:     $K := \mathrm{Iso}_K^{\Omega_i}(\mathfrak{x}, \mathfrak{y})$
4: **end for**
5: **return** K

$$(2.2) \qquad \mathrm{Iso}_{Gg}^W(\mathfrak{x}, \mathfrak{y}) = \mathrm{Iso}_G^W(\mathfrak{x}, \mathfrak{y}^{g^{-1}})g,$$

it is actually possible to restrict ourselves to the case where K is a group.

We now describe the two main recursive steps used in Luks's algorithm [24]. First suppose $G \leq \mathrm{Sym}(\Omega)$ is not transitive and let $\Omega_1, \ldots, \Omega_s$ be the orbits of G. Then the strings are processed orbit by orbit as described in Algorithm 1.

Note that the set $\mathrm{Iso}_K^{\Omega_i}(\mathfrak{x}, \mathfrak{y})$ can be computed making one call to string isomorphism over domain size $n_i = |\Omega_i|$. Indeed, using (2.2), it can be assumed that $K \leq \mathrm{Sym}(\Omega)$ is a group and Ω_i is K-invariant. Then

$$\mathrm{Iso}_K^{\Omega_i}(\mathfrak{x}, \mathfrak{y}) = \left\{ k \in K \mid k^{\Omega_i} \in \mathrm{Iso}_{K^{\Omega_i}}(\mathfrak{x}^{\Omega_i}, \mathfrak{y}^{\Omega_i}) \right\}.$$

Here, $\mathfrak{x}^{\Omega_i}$ (respectively, $\mathfrak{y}^{\Omega_i}$) denotes the restriction of the string $\mathfrak{x}$ (respectively, $\mathfrak{y}$) to the set Ω_i. Having computed the set $\mathrm{Iso}_{K^{\Omega_i}}(\mathfrak{x}^{\Omega_i}, \mathfrak{y}^{\Omega_i})$ making one recursive call to string isomorphism over domain size $n_i = |\Omega_i|$, the set $\mathrm{Iso}_K^{\Omega_i}(\mathfrak{x}, \mathfrak{y})$ can be computed in polynomial time by Theorem 2.1. So overall the algorithm needs to make s recursive calls to string isomorphism over domain sizes $n_1, \ldots, n_s$.

For the second type of recursion let $H \leq G$ be a subgroup and let $T = \{g_1, \ldots, g_t\}$ be a transversal for H. Then

$$(2.3) \qquad \mathrm{Iso}_G(\mathfrak{x}, \mathfrak{y}) = \bigcup_{i \in [t]} \mathrm{Iso}_{Hg_i}(\mathfrak{x}, \mathfrak{y}).$$

In Luks's algorithm this type of recursion is applied when G is a transitive group, $\mathfrak{B}$ is a minimal block system, and $H = G_{(\mathfrak{B})}$. Observe that $G^{\mathfrak{B}}$ is a primitive group and $t = |G^{\mathfrak{B}}|$. Also note that H is not transitive. Indeed, each orbit of H has size n/b where $b = |\mathfrak{B}|$. Hence, combining both types of recursion the computation of $\mathrm{Iso}_G(\mathfrak{x}, \mathfrak{y})$ is reduced to $t \cdot b$ instances of string isomorphism over domain size n/b. We refer to this as the *standard Luks reduction*.

Now suppose $G \in \widehat{\Gamma}_d$. The crucial step to analyze Luks's algorithm is to determine the size of primitive groups occurring in the recursion.

THEOREM 2.5 (see [3]). *There exists a function f such that every primitive $\widehat{\Gamma}_d$-group $G \leq \mathrm{Sym}(\Omega)$ has order $|G| \leq n^{f(d)}$.*

Indeed, the function f can be chosen to be linear in d (cf. [20]). As a result, Luks's algorithm runs in time $n^{\mathcal{O}(d)}$ for all groups $G \in \widehat{\Gamma}_d$.

2.3. Recursion. For the purpose of later analyzing our recursion, we record some bounds.

LEMMA 2.6. *Let $k, n \in \mathbb{N}$ and suppose $n_1, \ldots, n_\ell \leq n/2$ such that $\sum_{i=1}^\ell n_i \leq 2^k n$. Then $\sum_{i=1}^\ell \left(\frac{n_i}{n} \right)^{k+1} \leq 1$.*

Proof. For $i \in [\ell]$ define $\alpha_i = \frac{n_i}{n}$. Observe that $\alpha_i \leq \frac{1}{2}$ and $\sum_{i=1}^\ell \alpha_i \leq 2^k$. Now suppose toward a contradiction that there are $\ell \in \mathbb{N}$ and nonnegative reals

$\alpha_1, \ldots, \alpha_\ell \in \mathbb{R}$ meeting these assumptions such that $\sum_{i=1}^{\ell} \alpha_i^{k+1} > 1$. Pick $\ell \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_\ell \in \mathbb{R}$ such that

(i) $\alpha_i \leq \frac{1}{2}$ for all $i \in [\ell]$ and $\sum_{i=1}^{\ell} \alpha_i \leq 2^k$,

(ii) $\sum_{i=1}^{\ell} \alpha_i^{k+1} > 1$,

(iii) ℓ is minimal subject to conditions (i) and (ii),

(iv) $|\{i \in [\ell] \mid \alpha_i = \frac{1}{2}\}|$ is maximal subject to conditions (i)–(iii).

Then $\alpha_i + \alpha_j > \frac{1}{2}$ for all $i, j \in [\ell]$. Let $A = \{i \in [\ell] \mid \alpha_i \neq \frac{1}{2}\}$ and suppose $|A| \geq 2$. Let $i, j \in A$ be distinct. Then

$$\alpha_i^{k+1} + \alpha_j^{k+1} \leq \left(\frac{1}{2}\right)^{k+1} + \left(\alpha_i + \alpha_j - \frac{1}{2}\right)^{k+1},$$

which contradicts condition (iv). Condition (iii) implies $\alpha_i > 0$ for all i. Hence, $(\ell-1)\frac{1}{2} < \sum_{i=1}^{\ell} \alpha_i \leq 2^k$, which implies $\ell \leq 2^{k+1}$. Therefore, $\sum_{i=1}^{\ell} \alpha_i^{k+1} \leq \ell \left(\frac{1}{2}\right)^{k+1} \leq 1$, contradicting condition (ii). $\square$

LEMMA 2.7. *Let $k \in \mathbb{N}$ and $t \colon \mathbb{N} \to \mathbb{N}$ such that*

1. *$t(1) = 1$ and*

2. *for every $n \geq 2$ there are natural numbers $\ell \in \mathbb{N}$ and $n_1, \ldots, n_\ell \leq n/2$ such that $t(n) \leq \sum_{i=1}^{\ell} t(n_i)$ and $\sum_{i=1}^{\ell} n_i \leq 2^k n$.*

Then $t(n) \leq n^{k+1}$ for all $n \in \mathbb{N}$.

Proof. The statement is proved by induction on $n \in \mathbb{N}$. For $n > 1$ it holds that

$$t(n) \leq \sum_{i=1}^{\ell} t(n_i) \leq \sum_{i=1}^{\ell} n_i^{k+1} = n^{k+1} \sum_{i=1}^{\ell} \left(\frac{n_i}{n}\right)^{k+1} \leq n^{k+1}$$

by Lemma 2.6. $\square$

LEMMA 2.8. *Let $k \in \mathbb{N}$ and $t \colon \mathbb{N} \to \mathbb{N}$ be a function such that $t(1) = 1$. Suppose that for every $n \in \mathbb{N}$ there are natural numbers $n_1, \ldots, n_\ell$ for which one of the following holds:*

1. *$t(n) \leq \sum_{i=1}^{\ell} t(n_i)$ where $\sum_{i=1}^{\ell} n_i \leq 2^k n$ and $n_i \leq n/2$ for all $i \in [\ell]$, or*

2. *$t(n) \leq \sum_{i=1}^{\ell} t(n_i)$ where $\sum_{i=1}^{\ell} n_i \leq n$ and $\ell \geq 2$.*

Then $t(n) \leq n^{k+1}$.

Proof. The statement is proved by induction on $n \in \mathbb{N}$. For the first option it holds that

$$t(n) \leq \sum_{i=1}^{\ell} t(n_i) \stackrel{\text{I.H.}}{\leq} \sum_{i=1}^{\ell} n_i^{k+1} = n^{k+1} \sum_{i=1}^{\ell} \left(\frac{n_i}{n}\right)^{k+1} \leq n^{k+1}$$

by Lemma 2.6. For the second case we have

$$t(n) \leq \sum_{i=1}^{\ell} t(n_i) \stackrel{\text{I.H.}}{\leq} \sum_{i=1}^{\ell} n_i^{k+1} \leq \left(\sum_{i=1}^{\ell} n_i\right)^{k+1} \leq n^{k+1}. \qquad \square$$

LEMMA 2.9. *Let $m, k \geq 1$ and suppose $k \leq \frac{m}{2}$. Then*

$$(2.4) \qquad \qquad \binom{m}{k}^{\log m} \geq m^k.$$

Proof. It holds that

$$\binom{m}{k}^{\log m} \geq \left(\frac{m}{k}\right)^{k \log m} \geq 2^{k \log m} = m^k. \qquad \square$$

3. The structure of primitive groups in $\widehat{\Gamma}_d$. Recall that we denote by $\widehat{\Gamma}_d$ the class of groups whose composition factors are all isomorphic to subgroups of S_d. In this section we will prove several properties concerning the structure of primitive permutation groups in $\widehat{\Gamma}_d$ with a focus on their size in relation to their degree and d. More precisely, the goal of this section is to find a precise description of large primitive groups in $\widehat{\Gamma}_d$. For the purpose of this work, a primitive permutation group $G \in \widehat{\Gamma}_d$ is large if the order of G exceeds the term $n^{\mathcal{O}(\log d)}$. We shall prove that large primitive permutation groups in $\widehat{\Gamma}_d$ are composed of Johnson groups in a well-defined manner, meaning that Johnson groups form the only obstacles to efficient Luks reduction. For the proof we perform a case-by-case analysis following the well-known O'Nan–Scott theorem that classifies primitive permutation groups into five types.

3.1. The O'Nan–Scott theorem. Let G be a primitive permutation group acting on a set Ω of size n. By the well-known O'Nan–Scott theorem (see, for example, [12]) the group G has to be one of the following types. The *socle* of G, denoted by $\mathrm{Soc}(G)$, is the subgroup generated by all minimal normal subgroups of G.

I. *Affine groups.* In this case there is a vector space V over a field of prime order p such that G is isomorphic to a group H that satisfies $V^+ \leq H \leq \mathrm{AGL}(V)$, where V^+ is the additive group of the vector space V. The socle N of the group is a transitive abelian group (i.e., $\mathbb{Z}_p^k$ for the prime p and an integer k) and can be identified with V^+. Furthermore, the stabilizer G_0 of the 0-vector is an irreducible linear group (i.e., it does not have an invariant subspace).

II. *Almost simple groups.* In this case $\mathrm{Soc}(G) = T$ is a non-abelian simple group and $T \leq G \leq \mathrm{Aut}(T)$.

III. *Simple diagonal action.* In this case $\mathrm{Soc}(G) \cong T_1 \times \cdots \times T_k$, where all T_i are isomorphic to some non-abelian simple group T. Additionally, $n = |T|^{k-1}$, and the stabilizer of some point $\alpha \in \Omega$ is a diagonal subgroup $D \leq T_1 \times \cdots \times T_k$.

IV. *Product action.* In this case the set Ω can be identified with the k-tuples of some set M. In particular $n = |M|^k$. Furthermore there is some primitive group $P \leq \mathrm{Sym}(M)$ of Type II or III and a transitive group $K \leq S_k$ such that $G \leq P \wr K$. The group G acts in the natural product action of the wreath product. The socle of G is $\mathrm{Soc}(G) = T^k$ where $T = \mathrm{Soc}(P)$.

V. *Twisted wreath product action.* In this case there is a transitive permutation group $P \leq S_k$ and a non-abelian simple group T such that $G = B \rtimes P$, where B is isomorphic to T^k. Furthermore $|\Omega| = |T|^k$ and B acts regularly on Ω.

We analyze the structure of primitive $\widehat{\Gamma}_d$-groups according to the distinction into these five types. For each of them we will be interested in either a structural description or a bound on the size. To obtain such a bound we use the existence of small bases.

DEFINITION 3.1. *Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group. A subset $B \subseteq \Omega$ is a base for G if $G_{(B)} = \{1\}$. We define the minimum base size as $b(G) = \min\{|B| \mid B \subseteq \Omega \colon G_{(B)} = \{1\}\}$.*

The base size is related to the order of the group by the equation $2^{b(G)} \leq |G| \leq n^{b(G)}$.

3.2. Affine type. In the affine case we have a group $V^+ \leq G \leq \mathrm{AGL}(V)$, where $V = \mathbb{F}_p^k$ and $V^+ \cong \mathbb{Z}_p^k$ is the additive group of V, such that the point stabilizer G_0 is irreducible. We say that a group $G_0 \leq \mathrm{GL}(k, p)$ *acts primitively as a linear group* if it does not preserve any direct sum decomposition $V = V_1 \oplus \cdots \oplus V_\ell$, $\ell \geq 2$, of the underlying vector space $V = \mathbb{F}_p^k$. For primitive affine groups in $\widehat{\Gamma}_d$ we will

draw conclusions using a characterization of [21, 22]. The characterization involves quasisimple classical groups $\mathrm{SL}_r(q')$, $\mathrm{SU}_r(q')$, $\mathrm{Sp}_r(q')$, or $\Omega_r(q')$. Recall that a group is quasisimple if it is equal to its own commutator subgroup (i.e., perfect) and it is simple modulo its center. With finitely many exceptions, the mentioned groups are indeed quasisimple [8, Proposition 1.10.3].

THEOREM 3.2 (consequence of [21], [22]). *There are constants $c_1, c_2, c_3 \in \mathbb{N}$ such that the following holds. Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive group of Type* I *such that G_0 acts primitively as a linear group. Then*

1. *$b(G) \leq c_1$, or*
2. *G contains a quasisimple classical group of rank k, more precisely $\mathrm{SL}_k(q')$, $\mathrm{SU}_k(q')$, $\mathrm{Sp}_k(q')$, or $\Omega_k(q')$, and $b(G) \leq c_2 k + c_3$, or*
3. *G contains an alternating group A_k and $b(G) \leq c_2 \log k + c_3$.*

Proof. Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive group of Type I such that G_0 acts primitively as a linear group.

Theorem 1 in [22] (which applies to G; see the comment after that theorem) states that either $b(G) \leq C$ or $F^*(G_0) \leq G$ contains $\prod_{i=1}^{s} \mathrm{Alt}(m_i) \cdot \prod_{i=1}^{t} \mathrm{Cl}_{d_i}(q_i)^{(\infty)}$ for some integers $m_1, \ldots, m_s, q_1, \ldots q_t$ (the group G_0 is denoted by H^0 in [22]). Here $\mathrm{Cl}_{(d_i)}(q_i)$ is the normalizer of a quasisimple classical group, namely $\mathrm{SL}_{d_i}(q')$, $\mathrm{SU}_{d_i}(q')$, $\mathrm{Sp}_{d_i}(q')$, or $\Omega_{d_i}(q')$. Furthermore $\mathrm{Cl}_{(d_i)}(q_i)^{(\infty)}$ is the last group of the derived series of $\mathrm{Cl}_{(d_i)}(q_i)$. Only finitely many of the groups $\mathrm{SL}_{d_i}(q')$, $\mathrm{SU}_{d_i}(q')$, $\mathrm{Sp}_{d_i}(q')$, or $\Omega_{d_i}(q')$ are not perfect. Thus, by referring to case 1 for the finitely many exceptions, we can assume that $\mathrm{Cl}_{(d_i)}(q_i)^{(\infty)}$ contains $\mathrm{SL}_{d_i}(q')$, $\mathrm{SU}_{d_i}(q')$, $\mathrm{Sp}_{d_i}(q')$, or $\Omega_{d_i}(q')$.

Proposition 2 in [22] states further that either $b^*(G_0) \leq 9d_i + 22$ for some $i \in [s]$ or $b^*(G_0) \leq 3 \log_p m_i + 22$ for some $i \in [t]$. Also $b(G) \leq b(G_0) + 1 \leq b^*(G_0) + 1$.   □

LEMMA 3.3 (see [11], [17]). *Let $G \in \widehat{\Gamma}_d$ be a simple group of Lie type of rank k or one of the quasisimple classical groups $\mathrm{SL}_k(q')$, $\mathrm{SU}_k(q')$, $\mathrm{Sp}_k(q')$, or $\Omega_k(q')$. Then $k = \mathcal{O}(\log d)$.*

Proof. Note that by our definition of $\widehat{\Gamma}_d$, a simple group is in $\widehat{\Gamma}_d$ if and only if it is a subgroup of S_d. To prove the lemma it thus suffices to show that the smallest $d(k)$ for which $S_{d(k)}$ contains a simple group of Lie type of rank k is exponential in k.

Cooperstein [11] lists the minimum degree of a permutation representation of the mentioned quasisimple classical groups. They are all exponential in the rank k. In [17] the minimum degree of a permutation representation is listed for all simple groups of Lie type. Likewise they are exponential in k.   □

THEOREM 3.4. *Let $G \in \widehat{\Gamma}_d$ be a primitive permutation group of degree n of Type* I. *Then $b(G) = \mathcal{O}(\log d)$ and therefore $|G| = n^{\mathcal{O}(\log d)}$.*

Proof. Let $G \in \widehat{\Gamma}_d$ be a primitive permutation group of Type I. This implies that the point stabilizer $G_0 \leq \mathrm{GL}(k, p)$, where $p^k = n$, is an irreducible linear group. It suffices to show that $b(G_0) \in \mathcal{O}(\log d)$ since $b(G) = b(G_0) + 1$.

If G_0 is primitive as a linear group this follows by assembling Theorem 3.2 and Lemma 3.3: indeed, if G_0 is in case 1 of Theorem 3.2 the claim is obvious. For case 2 we see that $b(G) \leq c_2 k + c_3 \in \mathcal{O}(\log d)$ by the lemma and for the last case we know that $b(G) \leq c_2 \log k + c_3 \in \mathcal{O}(\log d)$.

Now suppose that G_0 is irreducible but imprimitive. Then G_0 can be written as $P \wr H$ for some primitive linear group $P \leq \mathrm{GL}(k/\ell, p)$ and transitive group H that permutes ℓ subspaces $V_1, \ldots, V_\ell$ of V^k. By [13, Lemma 4.2(a)] there is a set B_1 of $\mathcal{O}(\log d)$ points in V^k such that for the pointwise stabilizer we have $(G_0)_{(B_1)} \leq P^\ell$.

We now follow the techniques from section 6 of [13]. Since P is a primitive linear group, by the first part of the proof there is a base $\{x_1 \ldots, x_t\}$ of P of size $t = \mathcal{O}(\log d)$. Let b_i be the point $(x_i, x_i, \ldots, x_i)$ in $V_1 \times V_2 \times \cdots \times V_\ell$. Then $B_2 = \{b_1, \ldots, b_t\}$ is a base of P^ℓ. If follows that $B_1 \cup B_2$ is a base for G_0 of size at most $\mathcal{O}(\log d)$. □

3.3. Nonaffine type. For a group G we denote by $\mathrm{Out}(G)$ the outer automorphism group of G. It is well known that $|\mathrm{Out}(S_m)| = 1$ and $|\mathrm{Out}(A_m)| = 2$ for all $m > 6$.

LEMMA 3.5. *Let G be a non-abelian simple group. Then $|\mathrm{Out}(G)| \leq \mathcal{O}(\log |G|)$.*

Proof. For finite simple groups of Lie type, this follows by inspecting Tables 5 and 6 in the *Atlas of Finite Groups* [10]. In Table 5 the size of the outer automorphism group is given as the product $d \cdot f \cdot g$ which, according to Table 6, is logarithmic in the size of the group for each simple group of Lie type. For alternating simple groups the statement is obvious. The values for the sporadic groups disappear in the $\mathcal{O}$-notation. □

Recall that for $t \leq \frac{m}{2}$ we denote by $A_m^{(t)}$ be the action of the alternating group A_m on the set of t-element subsets of $[m]$.

THEOREM 3.6 (see Liebeck [19]). *Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive group and suppose $N = \mathrm{Soc}(G)$ is simple. Then one of the following holds:*
1. *N is permutationally equivalent to $A_m^{(t)}$ for some $m \in \mathbb{N}$ and $t \leq \frac{m}{2}$,*
2. *N is permutationally equivalent to A_m acting on the set of partitions of $[m]$ into subsets of size b (for some $b \leq m$),*
3. *N is a classical simple group acting on an orbit of subspaces of the natural module or pairs of subspaces of complementary dimension, or*
4. *$|G| \leq n^9$.*

We will not exploit the structure of the action of N in case 3 of the theorem and rather only use that N is a simple group of Lie type.

LEMMA 3.7. *Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive $\widehat{\Gamma}_d$-group of Type II. Let $N = \mathrm{Soc}(G)$. Then one of the following holds:*
1. *N is permutationally equivalent to $A_m^{(t)}$ for some $m \leq d$ and $t \leq \frac{m}{2}$ and $|G : N| \leq 2$, or*
2. *$|G| = n^{\mathcal{O}(\log d)}$.*

Proof. The proof is based on Theorem 3.6. First suppose N is permutationally equivalent to $A_m^{(t)}$ for some $m \in \mathbb{N}$ and $t \leq \frac{m}{2}$. Note that $m \leq d$ since $N \in \widehat{\Gamma}_d$ by Lemma 2.4. Furthermore $|G : N| \leq |\mathrm{Out}(N)| \leq 2$ since N is an alternating group (in case $m \leq 6$ the second option is satisfied).

Next consider the case that N is permutationally equivalent to A_m acting on partitions of $[m]$ into subsets of size b. Again, $m \leq d$ and $|G : N| \in \mathcal{O}(1)$. In this case $n = \frac{m!}{(b!)^a a!}$, where $a \cdot b = m$. Using Stirling's approximation it can be calculated that $n = 2^{\Omega(m)}$. Hence, $|N| \leq m^m = n^{\mathcal{O}(\log m)} = n^{\mathcal{O}(\log d)}$ and consequently $|G| = n^{\mathcal{O}(\log d)}$.

It remains to analyze the third case. It suffices to show that $|N| \in n^{\mathcal{O}(\log d)}$ since then $|G| \leq |N||G : N| \leq |N||\mathrm{Out}(N)| \leq |N|\mathcal{O}(\log(|N|)) \in n^{\mathcal{O}(\log d)}$. For this let $\varphi : N \to S_{d'}$ be a permutation representation of N with d' as small as possible. Then $d' \leq d$ and $d' \leq n$. Moreover, being minimal, the action is faithful and primitive

since N is simple. Not being an alternating group, the group N is not a Cameron group[2] and we conclude $|N| \leq (d')^{1+\log(d')} \in n^{\mathcal{O}(\log d)}$ [9, 26].   □

LEMMA 3.8 (see [13]).   *Let $G \in \widehat{\Gamma}_d$ be a primitive group of Type* III. *Then $b(G) \leq 2\ell + 1$ and thus $|G| \leq n^{2\ell+1} \in n^{\mathcal{O}(\log d)}$, where $\ell := \max\{5, \lceil \log d \rceil\}$.*

Remark on the proof. While not explicitly stated in [13], the lemma is implicit from [13, Lemma 4.2(c)] and the comment in section 6 on Type III(a) in [13]. (We advise that the types in that paper do not agree with ours.)   □

LEMMA 3.9. *Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive $\widehat{\Gamma}_d$-group of Type* IV. *Let $N = \mathrm{Soc}(G)$. Then one of the following holds:*
1. *$G \leq P \wr K$ is a wreath product in the product action of a transitive group $K \leq S_k$ in $\widehat{\Gamma}_d$ and a group P of Type* II *with a socle T permutationally equivalent to $A_m^{(t)}$ for some $m \leq d$ and $t \leq \frac{m}{2}$, and N is isomorphic to T^k with $|G : N| \leq n^{1+\log d}$, or*
2. *$|G| = n^{\mathcal{O}(\log d)}$.*

Proof. If $G \in \widehat{\Gamma}_d$ is of Type IV, then $G \leq P \wr K$ for some primitive group $P \leq \mathrm{Sym}(M)$ and a transitive group $K \leq S_k$. Observe that both $P \in \widehat{\Gamma}_d$ and $K \in \widehat{\Gamma}_d$. Let $H = P^k$. Then $|G : H| = |K| \leq d^{k-1} \leq 2^{k \cdot \log d} \leq n^{\log d}$ by Lemma 2.2. Moreover $|G| \leq n^{\log d} \cdot |P|^k$.

In case $|P| = |M|^{\mathcal{O}(\log d)}$ we thereby conclude $|G| \leq n^{\log d} \cdot (|M|^{\mathcal{O}(\log d)})^k = n^{\mathcal{O}(\log d)}$. Thus, by Lemmata 3.8 and 3.7, it suffices to consider the case where P is a primitive group of Type II which satisfies part 1 of Lemma 3.7. That is, the socle $T = \mathrm{Soc}(P)$ of P is permutationally equivalent to $A_m^{(t)}$ for some $m \leq d$ and $t \leq \frac{m}{2}$ and $|P : T| \leq 2$. Note that $N = T^k \leq P^k = H$. Thus, $|G : N| = |G : H| \cdot |P : T|^k \leq n^{\log d} \cdot 2^k \leq n^{1+\log d}$.   □

LEMMA 3.10. *Let $G \in \widehat{\Gamma}_d$ be a primitive group of Type* V. *Then $|G| \leq n^{1+\log d}$.*

Proof. For a primitive group G of Type V, a primitive twisted wreath product, there is a transitive group $P \leq S_k$ and a non-abelian simple group T such that $G \cong T^k \rtimes P$. Moreover, $n = |\Omega| = |T|^k$ and thus $k \leq \log(n)$. Note that $P \in \widehat{\Gamma}_d$ since $\widehat{\Gamma}_d$ is closed under subgroups and thus $|P| \leq d^{k-1}$ by Lemma 2.2. We conclude that $|G| = |T^k| \cdot |P| = n \cdot |P| \leq n \cdot d^{k-1} \leq n \cdot d^{\log n} = n^{1+\log d}$.   □

3.4. Structure theorem for primitive groups in $\widehat{\Gamma}_d$. Having analyzed the structure of large $\widehat{\Gamma}_d$-groups for all five types of primitive groups we now combine those statements into a structure theorem. For this, we need two auxiliary lemmata.

LEMMA 3.11. *Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive group and $\alpha \in \Omega$. Then*

$$B_\alpha = \{\beta \in \Omega \mid \beta^{G_\alpha} = \{\beta\}\}$$

forms a block of G.

Proof. Let $R = \{(\alpha, \beta) \in \Omega^2 \mid \beta^{G_\alpha} = \{\beta\}\}$. Clearly the relation R is reflexive and transitive. Suppose that $(\alpha, \beta) \in R$. Then $G_\alpha \leq G_\beta$. Moreover, $|G_\alpha| = |G|/|\alpha^G| = |G|/|\beta^G| = |G_\beta|$ since G is transitive. It follows that $G_\alpha = G_\beta$ and thus, $(\beta, \alpha) \in R$. So R is also symmetric and hence R is an equivalence relation.

---

[2]Cameron groups form a collection of primitive permutation groups that exactly characterize primitive permutation groups of size greater than $n^{1+\log n}$ (for n sufficiently large) [9, 26]. We shall not formally define Cameron groups in this work and rather only remark that the only simple Cameron groups are alternating groups (not necessarily in their standard action).

Now let $(\alpha, \beta) \in R$ and $g \in G$. Then $(\alpha^g, \beta^g) \in R$ because $G_{\alpha^g} = g^{-1} G_\alpha g$. Thus, R is invariant under G and the partition into equivalence classes forms a block system for G. □

LEMMA 3.12. *Let $P \leq \mathrm{Sym}(\Omega)$ be a nonregular primitive group and $k \geq 2$. Let $\mathfrak{B}$ be a block system of P^k with its natural action on Ω^k. Then there is some $I \subseteq [k]$ such that*

$$\mathfrak{B} = \{\{(\alpha_1, \ldots, \alpha_k) \in \Omega^k \mid \forall i \in I \colon \alpha_i = \beta_i\} \mid (\beta_i)_{i \in I} \in \Omega^{|I|}\}.$$

Proof. Let $B \in \mathfrak{B}$ be a block and let $I = \{i \in [k] \mid |\pi_i(B)| = 1\}$, where $\pi_i(B) = \{\alpha_i \mid (\alpha_1, \ldots, \alpha_k) \in B\}$. For every $i \in I$ suppose $\pi_i(B) = \{\beta_i\}$. It suffices to show that $B = \{(\alpha_1, \ldots, \alpha_k) \in \Omega^k \mid \forall i \in I \colon \alpha_i = \beta_i\}$. Let $j \in [k] \setminus I$ and let $(\alpha_1, \ldots, \alpha_k), (\alpha'_1, \ldots, \alpha'_k) \in B$ such that $\alpha_j \neq \alpha'_j$. Since G is nonregular and primitive there is some $g \in G_{\alpha_j}$ such that $(a'_j)^g \neq \alpha'_j$ (see Lemma 3.11). Note that $(\alpha'_1, \ldots, \alpha'_{j-1}, (a'_j)^g, \alpha'_{j+1}, \alpha'_k) \in B$. Let $\Delta = \{\alpha \in \Omega \mid (\alpha'_1, \ldots, \alpha'_{j-1}, \alpha, \alpha'_{j+1}, \alpha'_k) \in B\}$. Since Δ forms a block of P and $|\Delta| \geq 2$ we get that $\Delta = \Omega$. This implies that $B = \{(\alpha_1, \ldots, \alpha_k) \in \Omega^k \mid \forall i \in I \colon \alpha_i = \beta_i\}$. □

Let $G \leq \mathrm{Sym}(\Omega)$ and let $\mathfrak{B}, \mathfrak{B}'$ be two G-invariant partitions such that $\mathfrak{B} \prec \mathfrak{B}'$. Consistent with our previous notation we denote by $G_B^{\mathfrak{B}[B]}$ the natural induced action of G_B on the set $\mathfrak{B}[B]$ for all $B \in \mathfrak{B}'$.

THEOREM 3.13. *Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive $\widehat{\Gamma}_d$-group. Then one of the following holds:*

1. *$|G| \leq n^{c_1 \log d + c_2}$ for some absolute constants c_1, c_2, or*
2. *for the normal subgroup $N = \mathrm{Soc}(G) \leq G$ there is a sequence of partitions $\{\Omega\} = \mathfrak{B}_1 \succ \cdots \succ \mathfrak{B}_k = \{\{\alpha\} \mid \alpha \in \Omega\}$ such that the following holds:*
   (a) *$|G : N| \leq n^{1 + \log d}$,*
   (b) *$\mathfrak{B}_i$ is N-invariant for every $i \in [k]$, and*
   (c) *there are $m \leq d$ and $t \leq \frac{m}{2}$ with $m > 4 \log s$ where $s = \binom{m}{t}$ such that for all $i \in [k-1]$ and $B \in \mathfrak{B}_i$ the group $N_B^{\mathfrak{B}_{i+1}[B]}$ is permutationally equivalent to $A_m^{(t)}$.*

Moreover, there is a polynomial-time algorithm that determines one of the options that is satisfied and in case of the second option computes N and the partitions $\mathfrak{B}_1, \ldots, \mathfrak{B}_k$.

Proof. First suppose G is a primitive group of Type I, III, or V. Then 1 holds; the claimed bound on the group size follows from Corollary 3.4 and Lemmata 3.8 and 3.10, respectively. So it remains to consider primitive groups of Types II and IV.

Let $N = \mathrm{Soc}(G)$ be the socle of G. Suppose G is a primitive group of Type II. Then by Lemma 3.7 we conclude $|G| = n^{\mathcal{O}(\log d)}$ or N is permutationally equivalent to $A_m^{(t)}$ for some $m \leq d$ and $t \leq \frac{m}{2}$ and $|G : N| \leq 2$. In case $m \leq 4 \log \binom{m}{t} = 4 \log n$, it holds that $|N| \leq m^m \leq n^{4 \log m} \leq n^{4 \log d}$ and thus $|G| = n^{\mathcal{O}(\log d)}$. In case $m > 4 \log \binom{m}{t}$ we set $\mathfrak{B}_1 = \{\Omega\}$ and $\mathfrak{B}_2 = \{\{\alpha\} \mid \alpha \in \Omega\}$.

Next assume G is of Type IV. By Lemma 3.9, $G \leq P \wr K$ is a wreath product in the product action for a transitive group $K \leq S_k$ in $\widehat{\Gamma}_d$ and a group $P \leq \mathrm{Sym}(M)$ of Type II with a socle T permutationally equivalent to $A_m^{(t)}$ for some $m \leq d$ and $t \leq \frac{m}{2}$, and N is isomorphic to T^k with $|G : N| \leq n^{1 + \log d}$. Moreover, in case $m \leq 4 \log |M|$ we have $|T| \leq m! \leq |M|^{4 \log m}$ and hence $|N| \leq n^{4 \log d}$. This implies that $|G| = n^{\mathcal{O}(\log d)}$, so we can assume $m > 4 \log |M| = 4 \log \binom{m}{t}$.

Observe that, since the wreath product is in the product action, an element $h = (p_1, \ldots, p_k) \in P^k$ acts on an element $(m_1, \ldots, m_k) \in M^k = \Omega$ via $(m_1, \ldots, m_k)^h = (m_1^{p_1}, \ldots, m_k^{p_k})$. For $i \in [k+1]$ define

$$\mathfrak{B}_i = \{\{(m_1, \ldots, m_k) \in M^k \mid \forall j < i \colon m_j = m_j^*\} \mid m_1^*, \ldots, m_{i-1}^* \in M\}.$$

Clearly, $\mathfrak{B}_i$ is an N-invariant partition for all $i \in [k+1]$. Observe that $N_B^{\mathfrak{B}_{i+1}[B]}$ is permutationally equivalent to T for all $i \in [k]$, which itself is permutationally equivalent to $A_m^{(t)}$.

We describe a polynomial-time algorithm as required by the theorem. Note first that $|G|$ can be computed in polynomial time, so option 1 can be detected. Also note that the socle of a group is a normal subgroup and can be computed in polynomial time (see [16]).

The algorithm now sets $\mathfrak{B}_1 = \{\Omega\}$. To compute $\mathfrak{B}_{i+1}$ from $\mathfrak{B}_i$ we choose an arbitrary block $B \in \mathfrak{B}_i$ and compute a maximal block B' within B, that is a block that is inclusionwise maximal with the property that $B' \subsetneq B$. We set $\mathfrak{B}_{i+1} = (B')^N$.

Note that, up to permuting the coordinates, by Lemma 3.12 the block systems described above are the only block systems of N. Hence every sequence of block systems $\{\Omega\} = \mathfrak{B}_1 \succ \cdots \succ \mathfrak{B}_k = \{\{\alpha\} \mid \alpha \in \Omega\}$ that cannot be extended has the desired properties.

Finally note that the algorithm is also correct for groups of Type II, since then N is primitive and we get the sequence $\mathfrak{B}_1 = \{\Omega\}$ and $\mathfrak{B}_2 = \{\{\alpha\} \mid \alpha \in \Omega\}$. $\qquad\square$

Remark 3.14. Let Γ_d denote the family of groups G with the property that G has no alternating composition factors of degree greater than d and no classical composition factors of rank greater than d. (There is no restriction on the cyclic, exceptional, and sporadic composition factors of G.) While the class $\widehat{\Gamma}_d$ considered in this paper follows the original definition of Luks [24], most of the recent literature is concerned with the more general class of groups Γ_d [3, 13]. The reason is that many results that can be proved for the class $\widehat{\Gamma}_d$ indeed carry over to the more general class of groups Γ_d. We want to stress the fact that this is not the case for the results presented in this section. Indeed, consider the affine general linear group $G = \mathrm{AGL}(d, p)$ of dimension d (with its natural action on the corresponding vector space). Then G is a primitive group of affine type and $|G| = n^{\Omega(d)}$, where $n = p^d$ is the size of the vector space. For this group Theorem 3.13 does not hold. The group G is contained in the class Γ_d, but it is not contained in $\widehat{\Gamma}_d$.

4. Almost d-ary block system sequences. In the previous section we essentially proved that the only obstacles to efficient Luks reduction are Johnson groups, which is very similar to Babai's quasipolynomial-time algorithm. Hence, the natural approach to tackle the obstacle cases seems to be an adaption of the techniques introduced by Babai [1, 2]. However, there is an intrinsic problem. The group-theoretic methods forming the basis for Babai's algorithm rest on a group-theoretic statement, the unaffected stabilizers theorem, for which the natural adaption to our setting does not hold (cf. [1, Remark 8.2.5]). To remedy this problem we introduce a preprocessing step that reduces the string isomorphism problem for $\widehat{\Gamma}_d$-groups to a more restricted version of this problem. In this restricted version, the group is equipped with a sequence of block systems satisfying a particular property defined as follows. (Recall that a permutation group $G \leq \mathrm{Sym}(\Omega)$ is semiregular if $G_\alpha = \{1\}$ for every $\alpha \in \Omega$. Also remember that, for G-invariant partitions $\mathfrak{B} \prec \mathfrak{B}'$ and $B \in \mathfrak{B}'$, we denote by $G_B^{\mathfrak{B}[B]}$ the natural induced action of G_B on the set $\mathfrak{B}[B]$.)

DEFINITION 4.1. *Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group. A G-invariant sequence of partitions $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_k = \{\{\alpha\} \mid \alpha \in \Omega\}$ is called* almost d-ary *if for every $i \in [k]$ and $B \in \mathfrak{B}_{i-1}$ it holds that*

    1. *$G_B^{\mathfrak{B}_i[B]}$ is semiregular, or*

    2. *$|\mathfrak{B}_i[B]| \leq d$.*

The sequence is called d-ary if the second property is satisfied for every $i \in [k]$ and $B \in \mathfrak{B}_{i-1}$.

A simple but crucial observation is that such sequences are inherited by subgroups and restrictions to invariant subsets.

Observation 4.2. Let $G \le \mathrm{Sym}(\Omega)$ be a group, and let $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$ be an (almost) d-ary sequence of G-invariant partitions. Moreover, let $H \le G$. Then $\mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m$ also forms an (almost) d-ary sequence of H-invariant partitions. Additionally, for an H-invariant subset $\Delta \subseteq \Omega$ it holds that $\mathfrak{B}_0[\Delta] \succeq \cdots \succeq \mathfrak{B}_m[\Delta]$ forms an (almost) d-ary sequence of H^Δ-invariant partitions.

For groups equipped with an almost d-ary sequence of partitions it is possible to give a natural variant of the unaffected stabilizers theorem which, in turn, allows for an adaption of Babai's algorithmic techniques to give an efficient algorithm deciding string isomorphism for this type of group.

The goal of this section is to describe a reduction that, given an instance of string isomorphism for $\widehat{\Gamma}_d$-groups, computes a new equivalent instance, in which the permutation group is equipped with an almost d-ary G-invariant sequence of partitions. This reduction runs in time $n^{\mathrm{polylog}(d)}$ and builds on the classification of large primitive groups obtained in the previous section. We shall then see in subsequent sections that the string isomorphism problem for groups equipped with such a sequence can be solved in time $n^{\mathrm{polylog}(d)}$.

4.1. The high-level idea. The central idea for the reduction is to change the action of the permutation group G. More precisely, we shall construct a new permutation domain Ω^* and consider an action of the group G on the set Ω^*. Indeed, the set Ω^* will be larger than the original permutation domain Ω. Note that this is acceptable for our purposes as long as $|\Omega^*| \le |\Omega|^{\mathrm{polylog}(d)}$.

Let us first illustrate this on a high level for the special case that G is a primitive group. Using the characterization of primitive $\widehat{\Gamma}_d$-groups given in the previous section we have to distinguish two cases. First suppose that $|G| \le n^{c_1 \log d + c_2}$ for some appropriate absolute constants c_1, c_2. Now define $\Omega^* = G \times \Omega$. Then $g \in G$ acts on Ω^* via

$$(h, \alpha)^g = (hg, \alpha^g).$$

Let $G^* \le \mathrm{Sym}(\Omega^*)$ be the permutation group obtained from the action of G on the set Ω^*. It is easy to check that G^* is semiregular. Also note that $|\Omega^*| \le n^{\mathcal{O}(\log d)}$. Of course we also need to transform the strings. For a string $\mathfrak{x} \colon \Omega \to \Sigma$ define $\mathfrak{x}^* \colon \Omega^* \to \Sigma \colon (h, \alpha) \mapsto \mathfrak{x}(\alpha)$. Note that no information is lost in this transformation. Indeed, it can be verified that two strings $\mathfrak{x}, \mathfrak{y}$ are G-isomorphic if and only if $\mathfrak{x}^*$ is G^*-isomorphic to $\mathfrak{y}^*$. So this gives us the desired reduction.

Next, let us consider the more interesting case that G satisfies property 2 of Theorem 3.13. Let $N = \mathrm{Soc}(G)$. Then, in a first step, we consider the set $\Omega^* = G/N \times \Omega$. An element $g \in G$ acts on Ω^* via

$$(Nh, \alpha)^g = (Nhg, \alpha^g).$$

Let $G^* = G^{\Omega^*} \le \mathrm{Sym}(\Omega^*)$ denote the permutation group corresponding to the action of G on Ω^*. Now the crucial observation is that $\mathfrak{B} = \{\{(Nh, \alpha) \mid \alpha \in \Omega\} \mid h \in G\}$ is a G^*-invariant partition. For every $B \in \mathfrak{B}$, it holds that $(G^*)_B^B$ is permutationally equivalent to N, and the group $(G^*)^\mathfrak{B}$ is regular. Note that again $|\Omega^*| \le n^{\mathcal{O}(\log d)}$. Also, the strings can be transformed in the same way as before. Hence, it remains to consider only the group N.

Finally, for an intuition on how the group N is transformed suppose for simplicity that $N = A_m^{(t)}$. The group A_m has another action closely related to the action $A_m^{(t)}$ on the t-element subsets of $[m]$, namely the action on the set $[m]^{\langle t \rangle}$ of all t-tuples with distinct entries. A crucial difference between these actions is that the action on the tuples is not primitive. Indeed, fixing more and more coordinates, we get the following sequence of partitions. For $i = 0, \ldots, t$ let

$$\mathfrak{B}_i^* = \{\{(a_1, \ldots, a_t) \in [m]^{\langle t \rangle} \mid \forall j \leq i \colon a_j = b_j\} \mid (b_1, \ldots, b_i) \in [m]^{\langle i \rangle}\}.$$

Let N^* be the action of N on the set of ordered t-tuples with distinct entries. For every $i \in [t]$ the partition $\mathfrak{B}_i^*$ is N^*-invariant and for every $B \in \mathfrak{B}_{i-1}^*$ it holds that $|\mathfrak{B}_i^*[B]| \leq m \leq d$. Moreover, with every element $\bar{a} \in [m]^{\langle t \rangle}$ we can associate the underlying unordered set of elements. This way, we can also transform the strings in a way similar to before. Also note that the set $[m]^{\langle t \rangle}$ is only slightly larger than $\binom{m}{t}$ (cf. Lemma 2.9).

In the following we describe this reduction for general groups. Analogous to this high-level description we proceed in two steps.

4.2. First step.

THEOREM 4.3. *Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive $\widehat{\Gamma}_d$-group and let $\mathfrak{x}, \mathfrak{y} \colon \Omega \to \Sigma$ be two strings. Then there is a set Ω^*, a $\widehat{\Gamma}_d$-group $G^* \leq \mathrm{Sym}(\Omega^*)$, two strings $\mathfrak{x}^*, \mathfrak{y}^* \colon \Omega^* \to \Sigma$, and a sequence of partitions $\{\Omega^*\} = \mathfrak{B}_0^* \succ \cdots \succ \mathfrak{B}_k^* = \{\{\alpha^*\} \mid \alpha^* \in \Omega^*\}$ of the set Ω^* such that the following holds:*
1. $|\Omega^*| \leq n^{c_1 \log d + c_2 + 1}$ *for some absolute constants c_1, c_2 where $n = |\Omega|$,*
2. G^* *is transitive,*
3. $\mathfrak{B}_i^*$ *is G^*-invariant for all $i \in [k]$,*
4. $\mathfrak{x} \cong_G \mathfrak{y}$ *if and only if $\mathfrak{x}^* \cong_{G^*} \mathfrak{y}^*$, and*
5. *for every $i \in [k]$ and $B \in \mathfrak{B}_{i-1}^*$ it holds that*
    (a) $(G^*)_B^{\mathfrak{B}_i^*[B]}$ *is semiregular, or*
    (b) $(G^*)_B^{\mathfrak{B}_i^*[B]}$ *is permutationally equivalent to $A_m^{(t)}$ for some $m \leq d$ and $t \leq \frac{m}{2}$, where $m > 4 \log s$ for $s = \binom{m}{t}$.*
Moreover, one can compute all objects in time polynomial in the size of Ω^*.

We remark that the constants required for property 1 are precisely the constants from Theorem 3.13, option 1.

Proof. Inductively, by changing the action of G, we transform a sequence $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_\ell$ for which the last partition is not discrete into a sequence $\{\Omega^*\} = \mathfrak{B}_0^* \succ \cdots \succ \mathfrak{B}_k^*$ such that the blocks in $\mathfrak{B}_k^*$ are smaller than the blocks in $\mathfrak{B}_\ell$.

More precisely, let $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_\ell$ be a sequence of G-invariant partitions such that property 5 holds for all $i \leq \ell$ with respect to the group G, i.e., for all $i \in [\ell]$ and $B \in \mathfrak{B}_{i-1}$ it holds that
(A) $G_B^{\mathfrak{B}_i[B]}$ is semiregular, or
(B) $G_B^{\mathfrak{B}_i[B]}$ is permutationally equivalent to $A_m^{(t)}$ for some $m \leq d$ and $t \leq \frac{m}{2}$, where $m > 4 \log s$ for $s = \binom{m}{t}$.

Let $q = |B|$ for some (and therefore every) $B \in \mathfrak{B}_\ell$ and suppose $q > 1$. We show that there is a set Ω^*, a $\widehat{\Gamma}_d$-group $G^* \leq \mathrm{Sym}(\Omega^*)$, two strings $\mathfrak{x}^*, \mathfrak{y}^* \colon \Omega^* \to \Sigma$, and a sequence of partitions $\{\Omega^*\} = \mathfrak{B}_0^* \succ \cdots \succ \mathfrak{B}_k^*$ of the set Ω^* and natural numbers b, p with $b > 1$ and $b \cdot p = q$ such that the following holds:
(i) $|\Omega^*| \leq n \cdot b^{c_1 \log d + c_2}$,
(ii) G^* is transitive,

(iii) $\mathfrak{B}_i^*$ is G^*-invariant for all $i \in [k]$,

(iv) $|B| \leq p$ for all $B \in \mathfrak{B}_k^*$,

(v) $\mathfrak{x} \cong_G \mathfrak{y}$ if and only if $\mathfrak{x}^* \cong_{G^*} \mathfrak{y}^*$, and

(vi) for every $i \in [k]$ and $B \in \mathfrak{B}_{i-1}^*$ it holds that

  (a) $(G^*)_B^{\mathfrak{B}_i^*[B]}$ is semiregular, or

  (b) $(G^*)_B^{\mathfrak{B}_i^*[B]}$ is permutationally equivalent to $A_m^{(t)}$ for some $m \leq d$ and $t \leq \frac{m}{2}$, where $m > 4 \log s$ for $s = \binom{m}{t}$.

Moreover, one can compute all objects in time polynomial in the size of Ω^*. Then the statement of the theorem follows by a simple induction.

 Let $\mathfrak{B}_{\ell+1} \prec \mathfrak{B}_\ell$ be a G-invariant partition such that $G_B^{\mathfrak{B}_{\ell+1}[B]}$ is primitive for every $B \in \mathfrak{B}_\ell$. Note that such a partition can be computed in polynomial time by computing a maximal block B' of the group G_B^B (where $B \in \mathfrak{B}_\ell$ is arbitrary) and setting $\mathfrak{B}_{\ell+1} = \{(B')^g \mid g \in G\}$. Let $b = |\mathfrak{B}_{\ell+1}[B]|$ for some $B \in \mathfrak{B}_\ell$ and $p = q/b = |B'|$ for $B' \in \mathfrak{B}_{\ell+1}$. For $B \in \mathfrak{B}_\ell$ let $G^B = G_B^{\mathfrak{B}_{\ell+1}[B]}$ and let

$$(4.1) \qquad N^B = \begin{cases} \mathrm{Soc}\left(G^B\right) & \text{if } \left|G^B\right| > b^{c_1 \log d + c_2}, \text{ and} \\ \{1\} & \text{otherwise.} \end{cases}$$

Note that $N^B \trianglelefteq G^B$. By Theorem 3.13 it holds that $|G^B : N^B| \leq b^{c_1 \log d + c_2}$. As described above the main idea is now to act on the set of cosets of N^B in G^B. The main difficulty in defining this action is that there are multiple blocks each equipped with a set of cosets on which the action needs to be defined in a consistent manner. Let

$$\Omega^* = \bigcup_{B \in \mathfrak{B}_\ell} \left(\{N^B h \mid h \in G^B\} \times B\right).$$

Note that $|\Omega^*| \leq n \cdot b^{c_1 \log d + c_2}$ and hence property (i) holds. In order to define the action of G on the set Ω^* we first fix a set of elements mapping the blocks in $\mathfrak{B}_\ell$ onto each other. Suppose $\mathfrak{B}_\ell = \{B_1, \dots, B_s\}$. For $i = 2, \dots, s$ let $\sigma_{1 \to i} \in G$ such that $B_1^{\sigma_{1 \to i}} = B_i$ and let $\sigma_{1 \to 1} = 1$ (the identity element). Since the groups G^B are defined on the domain $\mathfrak{B}_{\ell+1}[B]$ it is actually convenient to define group elements $\overline{\sigma_{1 \to i}}$ over the same domain. Let

$$\overline{\sigma_{1 \to i}} := \left((\sigma_{1 \to i})^{\mathfrak{B}_{\ell+1}}\right)|_{\mathfrak{B}_{\ell+1}[B_1]}$$

(that is, we consider the natural action of $\sigma_{1 \to i}$ on $\mathfrak{B}_{\ell+1}$ and restrict the domain to the set $\mathfrak{B}_{\ell+1}[B_1]$). Note that the image of $\overline{\sigma_{1 \to i}}$ is precisely $\mathfrak{B}_{\ell+1}[B_i]$. Moreover, for $i, j \in [k]$ let

$$\overline{\sigma_{i \to j}} := \overline{\sigma_{1 \to i}}^{-1} \overline{\sigma_{1 \to j}}.$$

Note that $\overline{\sigma_{i \to j}}^{-1} = \overline{\sigma_{j \to i}}$ and $\overline{\sigma_{i \to j}}\, \overline{\sigma_{j \to r}} = \overline{\sigma_{i \to r}}$. Additionally, for every element $g \in G$ we introduce a similar notation defining

$$\overline{g_{(i)}} = \left(g^{\mathfrak{B}_{\ell+1}}\right)|_{\mathfrak{B}_{\ell+1}[B_i]}.$$

Now the group G acts on the set Ω^* via

$$(N^{B_i} h, \alpha)^g := ((N^{B_i} h)^g, \alpha^g),$$

where $\alpha \in B_i$ and, choosing j such that $B_j = B_i^g$,

$$(N^{B_i} h)^g := \overline{\sigma_{i \to j}}^{-1} (N^{B_i} h) \overline{g_{(i)}}.$$

To argue that this is well-defined we need to argue that $(N^{B_i}h, \alpha)^g \in \Omega^*$. For this first note that

$$\overline{\sigma_{i \to j}}^{-1}(N^{B_i}h)\overline{g_{(i)}} = \overline{\sigma_{i \to j}}^{-1}N^{B_i}\overline{\sigma_{i \to j}}\,\overline{\sigma_{i \to j}}^{-1}h\overline{g_{(i)}}$$
$$= N^{B_j}\overline{\sigma_{i \to j}}^{-1}h\overline{g_{(i)}}.$$

Observe that $\overline{\sigma_{i \to j}}^{-1}h\overline{g_{(i)}} \in G^{B_j}$ and $\alpha^g \in B_j$. It follows that $(N^{B_i}h, \alpha)^g \in \Omega^*$.

We also need to argue that we really defined an action of G on Ω^*. For this let $g, g' \in G$ and $\alpha \in B_i$. Pick $j, r \in [s]$ such that $B_i^g = B_j$ and $B_j^{g'} = B_r$. Note that $B_r = B_i^{(gg')}$. Then

$$
\begin{aligned}
\left(N^{B_i}h, \alpha\right)^{(gg')} &= \left(\overline{\sigma_{i \to r}}^{-1}\left(N^{B_i}h\right)\overline{(gg')_{(i)}}, \alpha^{(gg')}\right) \\
&= \left(\overline{\sigma_{j \to r}}^{-1}\overline{\sigma_{i \to j}}^{-1}\left(N^{B_i}h\right)\overline{g_{(i)}}\,\overline{g'_{(j)}}, (\alpha^g)^{g'}\right) \\
&= \left(\overline{\sigma_{i \to j}}^{-1}\left(N^{B_i}h\right)\overline{g_{(i)}}, \alpha^g\right)^{g'} \\
&= \left(\left(N^{B_i}h, \alpha\right)^g\right)^{g'}.
\end{aligned}
$$

Now let $G^* = G^{\Omega^*}$ be the induced action of G on Ω^* (at this point G^* may not be transitive; this is fixed later). Also, for $g \in G$, let $g^* = g^{\Omega^*}$. For a string $\mathfrak{x} \colon \Omega \to \Sigma$ we define the string $\mathfrak{x}^* \colon \Omega^* \to \Sigma \colon (N^B h, \alpha) \mapsto \mathfrak{x}(\alpha)$.

CLAIM 4.4. *For every $g \in G$ it holds that $\mathfrak{x}^g = \mathfrak{y}$ if and only if $(\mathfrak{x}^*)^{g^*} = \mathfrak{y}^*$.*

Proof. Let $g \in G$. For the forward direction, suppose that $\mathfrak{x}^g = \mathfrak{y}$, that is, $\mathfrak{x}(\alpha) = \mathfrak{y}(\alpha^g)$ for all $\alpha \in \Omega$. Then $\mathfrak{x}^*(N^B h, \alpha) = \mathfrak{x}(\alpha) = \mathfrak{y}(\alpha^g) = \mathfrak{y}^*((N^B h)^g, \alpha^g) = \mathfrak{y}^*((N^B h, \alpha)^{g^*})$ and hence $(\mathfrak{x}^*)^{g^*} = \mathfrak{y}^*$.

For the backward direction, suppose that $(\mathfrak{x}^*)^{g^*} = \mathfrak{y}^*$. Let $\alpha \in \Omega$ and let $B \in \mathfrak{B}_\ell$ such that $\alpha \in B$ and let $h \in G^B$. Then $\mathfrak{x}(\alpha) = \mathfrak{x}^*(N^B h, \alpha) = \mathfrak{y}^*((N^B h, \alpha)^{g^*}) = \mathfrak{y}^*((N^B h)^g, \alpha^g) = \mathfrak{y}(\alpha^g)$. So $\mathfrak{x}^g = \mathfrak{y}$. □

Next, we define the desired sequence of partitions. For $i \in [\ell]$ let

$$\mathfrak{B}_i^* = \left\{ \bigcup_{B \in \mathfrak{B}_\ell \colon B \subseteq B'} \left\{N^B h \mid h \in G^B\right\} \times B \;\middle|\; B' \in \mathfrak{B}_i \right\}.$$

It is easy to check that $\mathfrak{B}_i^*$ is G^*-invariant for all $i \in [\ell]$. Moreover, $G^{\mathfrak{B}_\ell}$ is permutationally equivalent to $(G^*)^{\mathfrak{B}_\ell^*}$ via the permutational isomorphism $f \colon \mathfrak{B}_\ell \to \mathfrak{B}_\ell^*$ where

$$f(B) = \{N^B h \mid h \in G^B\} \times B$$

for all $B \in \mathfrak{B}_\ell$. As a result $G^{\mathfrak{B}_i}$ is permutationally equivalent to $(G^*)^{\mathfrak{B}_i^*}$ for all $i \in [\ell]$. In particular, property (vi) holds for all $i \in [\ell]$.

Now we distinguish two cases. First suppose $\left|G^B\right| \leq b^{c_1 \log d + c_2}$ where $b = |\mathfrak{B}_{\ell+1}[B]|$ for some (and therefore every) $B \in \mathfrak{B}_\ell$. Recall that $N^B = \{1\}$ in this case. Let

$$\mathfrak{B}_{\ell+1}^* = \left\{\{N^B h\} \times B' \mid h \in G^B, B \in \mathfrak{B}_\ell, B' \in \mathfrak{B}_{\ell+1} \text{ with } B' \subseteq B\right\}$$

and set $k = \ell + 1$. Clearly, $\mathfrak{B}_{\ell+1}^*$ is G^*-invariant and $|B^*| \leq p$ for all $B^* \in \mathfrak{B}_{\ell+1}^*$. Now consider the group

$$(G^*)^{B^*} = (G^*)_{B^*}^{\mathfrak{B}_{\ell+1}^*[B^*]}$$

for $B^* \in \mathfrak{B}_\ell^*$. It is easy to check that $(G^*)^{B^*}$ is permutationally equivalent to $G^B = G_B^{\mathfrak{B}_{\ell+1}[B]}$ with its natural action on the set $G^B \times \mathfrak{B}_{\ell+1}[B]$ (acting regularly on the first component) where $B^* = \{N^B h \mid h \in G^B\} \times B$ and $B \in \mathfrak{B}_\ell$. Hence, $(G^*)^{B^*}$ is semiregular. So it only remains to argue that (ii) holds. Indeed, the group G^* is not necessarily transitive. Let $A^* \subseteq \Omega^*$ be an orbit of G^*. Then, by restricting all partitions and the two strings to A^* the group $(G^*)^{A^*}$ satisfies all required properties. This is trivial for all properties but (v). For property (v) note that G is transitive. So for every $\alpha \in \Omega$ there is some element $a \in A^*$ whose second component is α. This is all we need to prove a variant of Claim 4.4 where we restrict the strings and the group to the set A^*.

In the other case $|G^B| > b^{c_1 \log d + c_2}$ and $N^B = \mathrm{Soc}(G^B)$. We consider the block $B_1 \in \mathfrak{B}_\ell$ (recall that in the beginning of the proof we fixed a numbering of the blocks in $\mathfrak{B}_\ell$ and elements $\sigma_{1 \to i}$ mapping the first block to the ith block). By Theorem 3.13 there is a sequence of partitions $\{\mathfrak{B}_{\ell+1}[B_1]\} = \mathcal{P}_0 \succ \cdots \succ \mathcal{P}_t = \{\{B'\} \mid B' \in \mathfrak{B}_{\ell+1}[B_1]\}$ such that

   (I) $\mathcal{P}_i$ is N^{B_1}-invariant for every $i \in [t]$, and

   (II) there are $m \le d$ and $t \le \frac{m}{2}$ with $m > 4 \log s$ where $s = \binom{m}{t}$ such that for all $i \in [t]$ and $P \in \mathcal{P}_{i-1}$ the group $(N^{B_1})_P^{\mathcal{P}_i[P]}$ is permutationally equivalent to $A_m^{(t)}$.

Let
$$\mathfrak{B}_{\ell+1}^* = \left\{\{N^B h\} \times B \mid h \in G^B, B \in \mathfrak{B}_\ell\right\}$$

and for $i \in [t]$ let

$$\mathfrak{B}_{\ell+1+i}^* = \left\{\{N^{B_j} h\} \times \left(\bigcup_{B' \in P} (B')^{\sigma_{1 \to j}}\right) \middle| h \in G^{B_j}, j \in [s], P \in \mathcal{P}_i\right\}.$$

We set $k = \ell + 1 + t$. First note that $|B^*| \le p$ for every $B^* \in \mathfrak{B}_k^*$. We argue that $\mathfrak{B}_{\ell+1+i}^*$ is a G^*-invariant partition for $i \in [t]$. Let $B^* \in \mathfrak{B}_{\ell+1+i}^*$ and $g^* \in G^*$ such that $(B^*)^{g^*} \cap B^* \ne \emptyset$. Let $g \in G$ be the element corresponding to g^* and suppose

$$B^* = \{N^{B_j} h\} \times \left(\bigcup_{B' \in P} (B')^{\sigma_{1 \to j}}\right),$$

and let $B = B_j$. Due to the action on the first component (i.e., the action on $N^B h$) we conclude that $g \in G_B$ and $g^{\mathfrak{B}_{\ell+1}[B]} \in N^B$. Since $\mathcal{P}_i$ is N^{B_1}-invariant we conclude that $(B^*)^{g^*} = B^*$. Hence, $\mathfrak{B}_{\ell+1+i}^*$ is a G^*-invariant partition.

Moreover, $(G^*)_{B^*}^{\mathfrak{B}_{\ell+1}^*[B^*]}$ is semiregular for every $B^* \in \mathfrak{B}_\ell^*$ and, for every $i \in [t]$ and every $B^* \in \mathfrak{B}_{\ell+i}^*$, the group $(G^*)_{B^*}^{\mathfrak{B}_{\ell+1+i}^*[B^*]}$ is permutationally equivalent to $(N^{B_1})_P^{\mathcal{P}_i[P]}$. To see this first observe that $\mathfrak{B}_{\ell+1+t}^* = \{\{N^B h\} \times B' \mid B \in \mathfrak{B}_\ell, B' \in \mathfrak{B}_{\ell+1}, B' \subseteq B, h \in G^B\}$. Let $B^* \in \mathfrak{B}_{\ell+1}^*$ and suppose $B^* = \{N^B h\} \times B$, where $B \in \mathfrak{B}_\ell$. For every $g^* \in (G^*)_{B^*}$ it holds that $(N^B h)^g = N^B h$, where g is the element corresponding to g^* and thus $g^{\mathfrak{B}_{\ell+1}[B]} \in N^B$. Hence, $(G^*)_{B^*}^{\mathfrak{B}_{\ell+1+t}^*[B^*]}$ is permutationally equivalent to N^B. Translating the sequence of partitions $\mathcal{P}_1, \ldots, \mathcal{P}_t$ for N^B back then gives the sequence of partitions described above.

Finally, as in the previous case, if the group G^* is not transitive we restrict the group (along with strings $\mathfrak{x}^*$ and $\mathfrak{y}^*$) to one of its orbits. $\qquad\square$

4.3. Second step. For the second step we require the following auxiliary lemmata. The first one is implicitly given in [7, section 4].

LEMMA 4.5 (see [7]). *Let $G \leq \mathrm{Sym}(\Omega)$ and suppose G is permutationally equivalent to $A_m^{(t)}$ or $S_m^{(t)}$ for $m > 4 \log n$ and $t \leq \frac{m}{2}$. Then a permutational isomorphism $\rho \colon \Omega \to \binom{[m]}{t}$ can be computed in polynomial time.*

LEMMA 4.6. *Let $m \geq 7$ and suppose $\gamma \in \mathrm{Sym}(\binom{[m]}{t})$ is a permutational automorphism of $A_m^{(t)}$. Then γ is induced by a unique permutation $\sigma \in S_m$, that is, $X^\gamma = X^\sigma = \{x^\sigma \mid x \in X\}$ for every $X \in \binom{[m]}{t}$.*

Proof. Every nontrivial permutational automorphism of $A_m^{(t)}$ gives a unique nontrivial automorphism of A_m (as an abstract group) and every element $\sigma \in S_m$ induces a permutational automorphism of $A_m^{(t)}$. Since $\mathrm{Aut}(A_m) \cong S_m$ (for $m \geq 7$) the statement follows. $\square$

THEOREM 4.7. *Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive $\widehat{\Gamma}_d$-group and let $\mathfrak{x}, \mathfrak{y} \colon \Omega \to \Sigma$ be two strings. Then there is a set Ω^*, a $\widehat{\Gamma}_d$-group $G^* \leq \mathrm{Sym}(\Omega^*)$, two strings $\mathfrak{x}^*, \mathfrak{y}^* \colon \Omega^* \to \Sigma$, and a G^*-invariant almost d-ary sequence of partitions $\{\Omega^*\} = \mathfrak{B}_0^* \succ \cdots \succ \mathfrak{B}_k^* = \{\{\alpha^*\} \mid \alpha^* \in \Omega^*\}$ of the set Ω^* such that the following holds:*
  1. $|\Omega^*| \leq n^{(c_1 \log d + c_2 + 1) \log d}$, *and*
  2. $\mathfrak{x} \cong_G \mathfrak{y}$ *if and only if* $\mathfrak{x}^* \cong_{G^*} \mathfrak{y}^*$.
Moreover, one can compute all objects in time polynomial in the size of Ω^*.

Proof. By Theorem 4.3 we can assume that there is a sequence of G-invariant partitions $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_\ell = \{\{\alpha\} \mid \alpha \in \Omega\}$ such that for every $i \in [\ell]$ and $B \in \mathfrak{B}_{i-1}$ it holds that
  (A) $G_B^{\mathfrak{B}_i[B]}$ is semiregular, or
  (B) $G_B^{\mathfrak{B}_i[B]}$ is permutationally equivalent to $A_m^{(t)}$ for some $m \leq d$ and $t \leq \frac{m}{2}$, where $m > 4 \log s$ for $s = \binom{m}{t}$.
Actually, using Theorem 4.3, the above condition can be achieved only by increasing the size of the set Ω as described in Theorem 4.3, property 1. We argue that under the above assumption the set Ω^* constructed in this proof has size at most $n^{\log d}$ which in combination with Theorem 4.3 results in the desired bound given in 1.

In order to get almost d-arity, we need to worry about those blocks that satisfy item (B). Let

$$I = \left\{ i \in [\ell] \mid \exists B \in \mathfrak{B}_{i-1} \colon G_B^{\mathfrak{B}_i[B]} \text{ is permutationally equivalent to } A_{m_i}^{(t_i)} \right\}.$$

Note that for $B, B' \in \mathfrak{B}_{i-1}$ the groups $G_B^{\mathfrak{B}_i[B]}$ and $G_{B'}^{\mathfrak{B}_i[B']}$ are permutationally equivalent. So the existential quantifier in the definition of the set I can also be replaced by a universal quantifier.

For $i \in I$ and $B \in \mathfrak{B}_{i-1}$ let $\rho_{i,B} \colon \mathfrak{B}_i[B] \to \binom{[m_i]}{t_i}$ be a permutational isomorphism from $G_B^{\mathfrak{B}_i[B]}$ to $A_{m_i}^{(t_i)}$. Note that such a $\rho_{i,B}$ can be computed in polynomial time by Lemma 4.5. Let $\Gamma = (V(\Gamma), E(\Gamma))$ be the directed graph with

$$V(\Gamma) = \bigcup_{i \in \{0, \ldots, \ell\}} \mathfrak{B}_i \cup \left\{ (i, B, X) \mid i \in I, B \in \mathfrak{B}_{i-1}, X \in \binom{[m_i]}{\leq t_i} \right\}$$
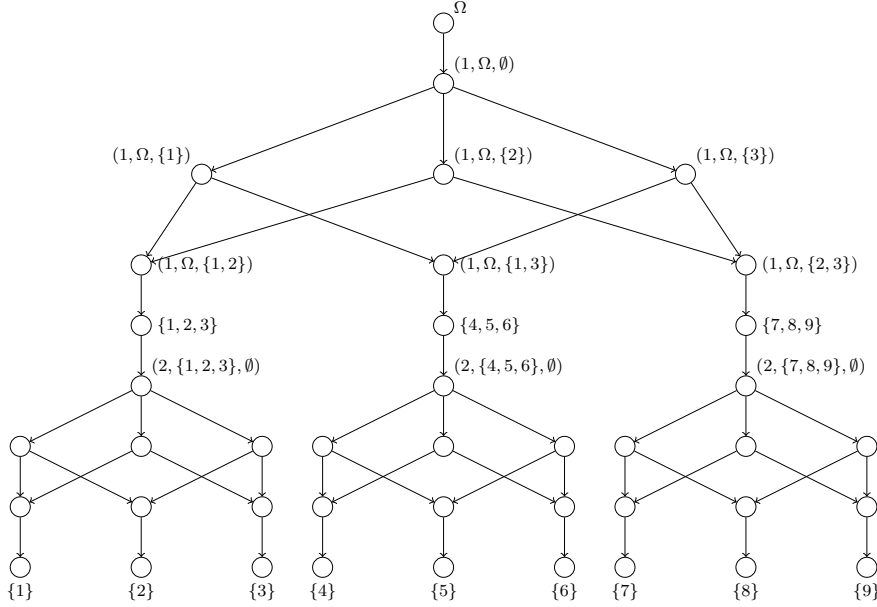
FIG. 1. *A visualization of* Γ. *Here* $\Omega = [9]$, $k = 3$, *and* $\mathfrak{B}_0 = \{\Omega\}$, $\mathfrak{B}_1 = \{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}\}$, $\mathfrak{B}_3 = \{\{1\}, \ldots, \{9\}\}$. *Furthermore,* $I = \{1, 2\}$, $m_i = 3$, *and* $t_i = 2$; *we ignore the condition* $t_i \leq m_i/2$ *for illustration purposes.*

and

$$\begin{aligned}
((i, B, X), (i', B', X')) \in E(\Gamma) \quad &:\Leftrightarrow \quad i = i' \wedge B = B' \wedge X \subseteq X' \wedge |X' \setminus X| = 1, \\
(B, (i, B', X)) \in E(\Gamma) \quad &:\Leftrightarrow \quad B = B' \wedge X = \emptyset, \\
((i, B, X), B') \in E(\Gamma) \quad &:\Leftrightarrow \quad |X| = t_i \wedge B' \in \mathfrak{B}_i \wedge B' \subseteq B \wedge \rho_{i,B}(B') = X, \\
(B, B') \in E(\Gamma) \quad &:\Leftrightarrow \quad \exists i \in [\ell] \setminus I \colon B \in \mathfrak{B}_{i-1} \wedge B' \in \mathfrak{B}_i \wedge B' \subseteq B.
\end{aligned}$$

We regard $v_0 \coloneqq \Omega \in \mathfrak{B}_0$ as the "root" of Γ (v_0 is the unique vertex with in-degree 0 in Γ). An illustration of the graph Γ is given in Figure 1.

A *branch of* (Γ, v_0) is a path $(v_0, v_1, \ldots, v_p)$ such that $\operatorname{dist}(v_0, v_i) = i$ for all $i \in [p]$. A *maximal branch of* (Γ, v_0) is a branch of maximal length. Observe that for every maximal branch $(v_0, v_1, \ldots, v_p)$ it holds that $v_p = \{\alpha\}$ for some $\alpha \in \Omega$. Let M be the set of maximal branches of (Γ, v_0).

CLAIM 4.8. $|M| \leq n^{\log d}$.

Proof. We can view the sequence of partitions $\mathfrak{B}_i$ as a tree of height ℓ. Each leaf of this tree corresponds to an element $\alpha \in \Omega$.

The graph Γ is obtained from the partition tree by squeezing subset lattices of the ($\leq t_i$)-element subsets of $[m_i]$ between some internal node of the tree and its $\binom{m_i}{t_i}$ children. Counting the number of branches in Γ amounts to counting the number of leaves in the tree unfolding of Γ. To obtain the tree unfolding, we replace each of the subset lattices of size $\binom{m_i}{t_i}$ by a tree of size $m_i^{t_i}$. For a fixed subset lattice every element $X \subseteq [m_i]$ of size t_i corresponds to $m_i^{t_i}/\binom{m_i}{t_i}$ many tuples in the tree unfolding. Hence,

$$|M| \leq n \cdot \prod_{i \in I} \left(m_i^{t_i} / \binom{m_i}{t_i} \right)$$

$$\leq n \cdot \prod_{i \in I} \binom{m_i}{t_i}^{\log d - 1} \qquad \text{by Lemma 2.9}$$

$$\leq n \cdot \left(\prod_{i \in I} \binom{m_i}{t_i} \right)^{\log d - 1}$$

$$\leq n \cdot \left(\prod_{i \in I} |\mathfrak{B}_{i-1} : \mathfrak{B}_i| \right)^{\log d - 1}$$

$$\leq n^{\log d}. \qquad\qquad \square$$

For every branch $\bar{v} = (v_0, \dots, v_p) \in M$ define $\sigma(\bar{v}) = \alpha$ for the unique $\alpha \in \Omega$ such that $v_p = \{\alpha\}$. Now let $\Omega^* = \{(\alpha, \bar{v}) \mid \alpha \in \Omega, \bar{v} \in M, \alpha = \sigma(\bar{v})\}$. Clearly, $|\Omega^*| = |M| \leq n^{\log d}$ by Claim 4.8. Let $\mathfrak{x}^* \colon \Omega^* \to \Sigma \colon (\alpha, \bar{v}) \mapsto \mathfrak{x}(\alpha)$ and $\mathfrak{y}^* \colon \Omega^* \to \Sigma \colon (\alpha, \bar{v}) \mapsto \mathfrak{y}(\alpha)$.

For $g \in G$ define $g^\Gamma \in \mathrm{Sym}(V(\Gamma))$ to be the permutation defined by

$$B^{(g^\Gamma)} = B^g$$

and

$$(i, B, X)^{(g^\Gamma)} = (i, B^g, X'),$$

where X' is defined as follows. Let $g^{\mathfrak{B}_i[B]} \colon \mathfrak{B}_i[B] \to \mathfrak{B}_i[B^g] \colon B' \mapsto (B')^g$ and define

$$f \colon \binom{[m_i]}{t_i} \to \binom{[m_i]}{t_i} \colon Y \mapsto Y^{\rho_{i,B}^{-1} \cdot g^{\mathfrak{B}_i[B]} \cdot \rho_{i,B^g}}.$$

The bijection $f \in \mathrm{Sym}(\binom{[m_i]}{t_i})$ is induced by a unique permutation $\pi \in S_{m_i}$ (see Lemma 4.6). Now define $X' = X^\pi$.

CLAIM 4.9. *For every $g \in G$ we have $g^\Gamma \in \mathrm{Aut}(\Gamma, v_0)$.*

Proof. Clearly, the root of the graph Γ is mapped to the root. For the edge relation we consider the four types of edges one by one. First suppose $(B, B') \in E(\Gamma)$ for some $B \in \mathfrak{B}_{i-1}$, $B' \in \mathfrak{B}_i$ such that $B' \subseteq B$ and $i \notin I$. Then $(B, B')^{(g^\Gamma)} = (B^g, (B')^g)$, where $B^g \in \mathfrak{B}_{i-1}$, $(B')^g \in \mathfrak{B}_i$, and $(B')^g \subseteq B^g$. Hence, $(B, B')^{(g^\Gamma)} \in E(\Gamma)$.

Next suppose $((i, B, X), (i', B', X')) \in E(\Gamma)$. Then $i = i'$, $B = B'$, $X \subseteq X'$, and $|X' \setminus X| = 1$. Let $\pi, \pi' \in S_{m_i}$ such that $(i, B, X)^{(g^\Gamma)} = (i, B^g, X^\pi)$ and $(i', B', X')^{(g^\Gamma)} = (i', (B')^g, (X')^{\pi'})$. From $B = B'$ it follows that $\pi = \pi'$. Hence, $X^\pi \subseteq (X')^{\pi'}$ and $|(X')^{\pi'} \setminus X^\pi| = 1$. So $((i, B, X)^{(g^\Gamma)}, (i', B', X')^{(g^\Gamma)}) \in E(\Gamma)$.

So assume that $(B, (i, B', X)) \in E(\Gamma)$. Then $B = B'$ and $X = \emptyset$. Let $\pi \in S_{m_i}$ such that $(i, B', X)^{(g^\Gamma)} = (i, (B')^g, X^\pi)$. But $X^\pi = \emptyset^\pi = \emptyset$ and $B^g = (B')^g$. This implies that $(B^{(g^\Gamma)}, (i, B', X)^{(g^\Gamma)}) \in E(\Gamma)$.

Finally suppose $((i, B, X), B') \in E(\Gamma)$. We have $|X| = t_i$, $B' \in \mathfrak{B}_i$, $B' \subseteq B$, and $\rho_{i,B}(B') = X$. Let $\pi \in S_{m_i}$ such that $(i, B, X)^{(g^\Gamma)} = (i, (B)^g, X^\pi)$. It suffices to show that $\rho_{i,B^g}((B')^g) = X^\pi$. But this follows directly from the definition of the permutation g^Γ. $\square$

For $g \in G$ define $g^* \in \mathrm{Sym}(\Omega^*)$ via

$$(\alpha, (v_0, \ldots, v_p))^{g^*} = \left(\alpha^g, \left(v_0^{(g^\Gamma)}, \ldots, v_p^{(g^\Gamma)}\right)\right)$$

and let $G^* = \{g^* \mid g \in G\}$.

CLAIM 4.10. *For every $g, h \in G$ it holds that $(gh)^* = g^* h^*$.*

Proof. Looking at the definition it is not difficult to see that $g^\Gamma h^\Gamma = (gh)^\Gamma$ for all $g, h \in G$. From this we immediately get that $(gh)^* = g^* h^*$. □

Hence, G^* forms a group and the mapping $\varphi \colon G \to G^* \colon g \mapsto g^*$ is a group isomorphism. So $G^* \in \widehat{\Gamma}_d$ by Lemma 2.4.

CLAIM 4.11. *For every $g \in G$ it holds that $\mathfrak{x}^g = \mathfrak{y}$ if and only if $(\mathfrak{x}^*)^{g^*} = \mathfrak{y}^*$.*

Proof. First suppose there is some $g \in G$ such that $\mathfrak{x}^g = \mathfrak{y}$, that is, $\mathfrak{x}(\alpha) = \mathfrak{y}(\alpha^g)$ for all $\alpha \in \Omega$. Then $\mathfrak{x}^*(\alpha, \bar{v}) = \mathfrak{x}(\alpha) = \mathfrak{y}(\alpha^g) = \mathfrak{y}^*(\alpha^g, \bar{v}^{(g^\Gamma)}) = \mathfrak{y}^*((\alpha, \bar{v})^{g^*})$ and hence $(\mathfrak{x}^*)^{g^*} = \mathfrak{y}^*$.

For the backward direction assume there is some $g^* \in G^*$ such that $(\mathfrak{x}^*)^{g^*} = \mathfrak{y}^*$. Let $\alpha \in \Omega$ and let $\bar{v} \in M$ be a maximal branch such that $\alpha = \sigma(\bar{v})$. Then $\mathfrak{x}(\alpha) = \mathfrak{x}^*(\alpha, \bar{v}) = \mathfrak{y}^*((\alpha, \bar{v})^{g^*}) = \mathfrak{y}^*(\alpha^g, \bar{v}^{(g^\Gamma)}) = \mathfrak{y}(\alpha^g)$. So $\mathfrak{x}^g = \mathfrak{y}$. □

It remains to define the sequence of block systems. Let $k = \max_{v \in V(\Gamma)} \mathrm{dist}(v_0, v)$. Note that k is the length of every maximal branch $\bar{v} \in M$. For $i \in \{0, \ldots, k\}$ define

$$\mathfrak{B}_i^* = \{\{(\alpha, (v_0, \ldots, v_k)) \in \Omega^* \mid \forall j \le i \colon v_j = w_j\} \mid (w_0, \ldots, w_i) \text{ is a branch of } (\Gamma, v_0)\}.$$

Clearly, $\mathfrak{B}_i^*$ is invariant under G^* and $\mathfrak{B}_{i-1}^* \succeq \mathfrak{B}_i^*$ for all $i \in [k]$. So it only remains to check that the sequence $\mathfrak{B}_0^*, \ldots, \mathfrak{B}_k^*$ is almost d-ary. For every $B^* \in \mathfrak{B}_{i-1}^*$, $i \in [k]$, it holds that

$$|\mathfrak{B}_i^*[B^*]| \le \max_{v \in V(\Gamma) \colon \mathrm{dist}(v_0, v) = i-1} |N^+(v)|,$$

where $N^+(v) = \{w \in N(v) \mid \mathrm{dist}(v_0, w) > \mathrm{dist}(v_0, v)\}$. Let $i \in [k]$ and $B^* \in \mathfrak{B}_{i-1}^*$. Suppose that $|\mathfrak{B}_i^*[B^*]| > d$. Let $(w_0, \ldots, w_{i-1})$ be the branch of (Γ, v_0) that corresponds to the block B^*. Then $|N^+(w_{i-1})| > d$ and thus, $w_{i-1} = B$ for some $B \in \mathfrak{B}_{j-1}$ and $j \in [\ell]$, where $j \notin I$. Moreover, $G_B^{\mathfrak{B}_j[B]}$ is semiregular since property (A) holds for all $B \in \mathfrak{B}_{j-1}$ and $j \in [\ell]$, where $j \notin I$. But in this case $(G^*)_{B^*}^{\mathfrak{B}_j^*[B^*]}$ is permutationally equivalent to a subgroup of $G_B^{\mathfrak{B}_j[B]}$ and hence the group $(G^*)_{B^*}^{\mathfrak{B}_j^*[B^*]}$ is also semiregular. □

The previous theorem states that there is an $n^{\mathrm{polylog}(d)}$-reduction from the string isomorphism problem for $\widehat{\Gamma}_d$-groups to the string isomorphism problem for groups where we are additionally given an almost d-ary sequence of invariant partitions. Hence, in the remainder of this work, we shall be concerned with solving the latter problem. The basic approach to do this is to adapt the local certificates routine developed by Babai for his quasipolynomial-time isomorphism test [2].

5. Affected orbits. The basis of Babai's local certificates algorithm is a group theoretic statement, the unaffected stabilizers theorem (see [2, Theorem 6]). In the following we generalize this theorem to our setting. For the proof we roughly follow the argumentation from [1]. However, on the technical level, several details need to be changed to allow for the treatment of the semiregular operations allowed in our setting.

LEMMA 5.1 (cf. [1, 27]). *Let $G \leq K_1 \times \cdots \times K_\ell$ be a subdirect product and let $\varphi \colon G \to S$ be an epimorphism where S is a non-abelian simple group. Furthermore let $\pi_i \colon G \to K_i$ be the projection to the ith component and $M_i = \ker(\pi_i)$. Then there is some $i^* \in [\ell]$ such that $M_{i^*} \leq \ker(\varphi)$.*

LEMMA 5.2. *Let G be a group, $H, K \trianglelefteq G$ and suppose $\varphi \colon G \to S$ is an epimorphism where S is a non-abelian simple group. Furthermore suppose that $H^\varphi = K^\varphi = S$. Then $(H \cap K)^\varphi = S$.*

Proof. Let $N = \ker(\varphi)$. Suppose that $(H \cap K)^\varphi \neq S$. Since $H \cap K \trianglelefteq G$ and S is a simple group we conclude that $(H \cap K)^\varphi = \{1\}$, that is, $H \cap K \leq N$.

Now let $s_1, s_2 \in S$ be two arbitrary elements. Then there are $h \in H$, $k \in K$ such that $\varphi(h) = s_1$ and $\varphi(k) = s_2$. Moreover, $n := h^{-1}k^{-1}hk \in H \cap K \leq N$ since $H \trianglelefteq G$ and $K \trianglelefteq G$. Note that $hk = khn$. But then

$$s_1 s_2 = \varphi(h)\varphi(k) = \varphi(hk) = \varphi(khn) = \varphi(k)\varphi(h)\varphi(n) = s_2 s_1.$$

Since $s_1, s_2 \in S$ were chosen arbitrarily it follows that S is abelian. $\qquad\square$

LEMMA 5.3 (see [1, Lemma 8.3.1]). *Let $G \leq S_d$ be a transitive group and $\varphi \colon G \to A_k$ an epimorphism where $k > \max\{8, 2 + \log_2 d\}$. Then $G_\alpha^\varphi \neq A_k$ for all $\alpha \in [d]$.*

LEMMA 5.4. *Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive group and suppose there is an almost d-ary sequence of invariant partitions $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$. Furthermore let $k > \max\{8, 2 + \log_2 d\}$, and let $\varphi \colon G \to A_k$ be an epimorphism. Then $G_\alpha^\varphi \neq A_k$ for all $\alpha \in \Omega$.*

Proof. We prove the statement by induction on the cardinality of G. Let $K = G_{(\mathfrak{B}_1)}$ be the normal subgroup stabilizing the block system $\mathfrak{B}_1$ and $N = \ker(\varphi)$. Observe that N is a maximal normal subgroup of G ($N \trianglelefteq G$ is a maximal normal subgroup of G if and only if the quotient group G/N is simple; here G/N is isomorphic to $G^\varphi = A_k$). Hence, it holds that $K \leq N$ or $\langle K, N \rangle = KN = G$.

First suppose $K \leq N$. Then φ factors across $G \to G^{\mathfrak{B}_1} \overset{\psi}{\to} A_k$. Observe that ψ is an epimorphism since φ is an epimorphism. Suppose $|\mathfrak{B}_1| \leq d$. Then, by Lemma 5.3, for every $B \in \mathfrak{B}_1$ it holds that $(G^{\mathfrak{B}_1})_B^\psi \neq A_k$. Hence, $G_\alpha^\varphi \leq G_B^\varphi \neq A_k$, where $B \in \mathfrak{B}_1$ is the unique set such that $\alpha \in B$. Otherwise $G^{\mathfrak{B}_1}$ is semiregular and hence $(G^{\mathfrak{B}_1})_B^\psi = \{1\} \neq A_k$ for all $B \in \mathfrak{B}_1$. Again, $G_\alpha^\varphi \leq G_B^\varphi \neq A_k$, where $B \in \mathfrak{B}_1$ is the unique set such that $\alpha \in B$.

So consider the case that $KN = G$, that is, $K^\varphi = A_k$. Suppose toward a contradiction that there is some $\alpha \in \Omega$ such that $G_\alpha^\varphi = A_k$. Pick $B \in \mathfrak{B}_1$ such that $\alpha \in B$. In particular, $G_B^\varphi = A_k$.

CLAIM 5.5. $G_{(B)}^\varphi \neq A_k$.

Proof. Assume toward a contradiction that $G_{(B)}^\varphi = A_k$. Then, by Lemma 5.2, $K_{(B)}^\varphi = (G_{(B)} \cap K)^\varphi = A_k$ since $G_{(B)} \trianglelefteq G_B$, $K \trianglelefteq G_B$ and $K^\varphi = A_k$.

On the other hand, let $\Omega_1, \ldots, \Omega_\ell$ be the orbits of K. Let $\pi_i \colon K \to \mathrm{Sym}(\Omega_i)$ be the restriction of K to Ω_i, $K_i = \mathrm{im}(\pi_i)$, and $M_i = \ker(\pi_i)$. By Lemma 5.1 there is some $i \in [\ell]$ such that $M_i \leq N$. Since G acts transitively on the blocks $\{\Omega_1, \ldots, \Omega_\ell\}$ the groups M_i, $i \in [\ell]$, are conjugate subgroups in G and therefore $M_i \leq N$ for all $i \in [\ell]$. Pick $i^* \in [\ell]$ such that $\alpha \in \Omega_{i^*}$. Since $M_{i^*} \leq N$ the epimorphism $\varphi|_K \colon K \to A_k$ factors across K_{i^*} as $K \overset{\pi_{i^*}}{\to} K_{i^*} \overset{\psi}{\to} A_k$. Hence, $K_{i^*}^\psi = A_k$. Moreover, $\mathfrak{B}_1[\Omega_{i^*}] \succ \cdots \succ \mathfrak{B}_m[\Omega_{i^*}]$ is an almost d-ary sequence of partitions for K_{i^*}. By the

induction hypothesis it follows that $(K_{i^*})^\psi_\alpha \neq A_k$ and thus $K^\varphi_\alpha \neq A_k$. But this is a contradiction since $K^\varphi_{(B)} \leq K^\varphi_\alpha$. □

Since $G^\varphi_{(B)} \trianglelefteq G^\varphi_B$ it follows $G^\varphi_{(B)} = \{1\}$. So $\varphi|_{G_B}$ factors across $G_B \to G^B_B \xrightarrow{\psi} A_k$.

Moreover, $\varphi|_{G_\alpha}$ factors across $G_\alpha \to G^B_\alpha \xrightarrow{\psi'} A_k$, where $\psi' = \psi|_{G^B_\alpha}$. Overall this means $(G^B_B)^\psi = A_k$ and $(G^B_B)^\psi_\alpha = (G^B_\alpha)^{\psi'} = A_k$. But this contradicts the induction hypothesis since $\mathfrak{B}_1[B] \succ \cdots \succ \mathfrak{B}_m[B]$ is an almost d-ary sequence of G^B_B-invariant partitions and G^B_B is transitive. □

The following lemma shows that we can drop the assumption of G being transitive in Lemma 5.4 if we are only looking for some element $\alpha \in \Omega$ such that $G^\varphi_\alpha \neq A_k$.

LEMMA 5.6. *Let* $G \leq \mathrm{Sym}(\Omega)$ *be a group and suppose there is an almost d-ary sequence of G-invariant partitions* $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$. *Furthermore let* $k > \max\{8, 2 + \log_2 d\}$, *and let* $\varphi\colon G \to A_k$ *be an epimorphism. Then* $G^\varphi_\alpha \neq A_k$ *for some* $\alpha \in \Omega$.

Proof. Let $\Omega_1, \ldots, \Omega_\ell$ be the orbits of G and let $\pi_i\colon G \to \mathrm{Sym}(\Omega_i)$ be the restriction of G to Ω_i. Let $G_i = \mathrm{im}(\pi_i)$ and $M_i = \ker(\pi_i)$. By Lemma 5.1 there is some $i \in [\ell]$ such that $M_i \leq \ker(\varphi)$. So φ factors across G_i as $G \xrightarrow{\pi_i} G_i \xrightarrow{\psi} A_k$. It follows that $G^\psi_i = A_k$. Now let $\alpha \in \Omega_i$. Note that $\mathfrak{B}_0[\Omega_i] \succeq \cdots \succeq \mathfrak{B}_m[\Omega_i]$ forms an almost d-ary sequence of G_i-invariant partitions. Thus by Lemma 5.4 it follows that $(G_i)^\psi_\alpha \neq A_k$ and thus $G^\varphi_\alpha \neq A_k$. □

For a set Δ we denote by $\mathrm{Alt}(\Delta)$ the alternating group acting with its standard action on the set Δ. Moreover, we refer to the groups $\mathrm{Alt}(\Delta)$ and $\mathrm{Sym}(\Delta)$ as the *giants* where Δ is an arbitrary finite set.

DEFINITION 5.7 (Babai [2]). *Let* $G \leq \mathrm{Sym}(\Omega)$. *A homomorphism* $\varphi\colon G \to S_k$ *is a* giant representation *if* $G^\varphi \geq A_k$. *In this case an element* $\alpha \in \Omega$ *is* affected *by* φ *if* $G^\varphi_\alpha \not\geq A_k$.

Remark 5.8. Let $\varphi\colon G \to S_k$ be a giant representation and suppose $\alpha \in \Omega$ is affected by φ. Then every element in the orbit α^G is affected by φ. We call α^G an *affected orbit* (with respect to φ).

With this definition we can now state the generalization of the unaffected stabilizers theorem (see [2, Theorem 6]).

THEOREM 5.9. *Let* $G \leq \mathrm{Sym}(\Omega)$ *be a permutation group and suppose there is an almost d-ary sequence of G-invariant partitions* $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$. *Furthermore let* $k > \max\{8, 2 + \log_2 d\}$ *and* $\varphi\colon G \to S_k$ *be a giant representation. Let* $D \subseteq \Omega$ *be the set of elements not affected by* φ. *Then* $G^\varphi_{(D)} \geq A_k$.

Proof. First suppose that $G^\varphi = A_k$. The set D is G-invariant (cf. Remark 5.8). Let $\psi\colon G \to \mathrm{Sym}(D)$ be the restriction of G to D. Observe that $\ker(\psi) = G_{(D)}$. So $G_{(D)} \trianglelefteq G$ and hence, $G^\varphi_{(D)} \trianglelefteq G^\varphi = A_k$. Assume toward a contradiction that $G^\varphi_{(D)} \neq A_k$. Then $G^\varphi_{(D)} = 1$, that is, $G_{(D)} \leq \ker(\varphi)$. So φ factors across $H := G^\psi \leq \mathrm{Sym}(D)$ as $G \xrightarrow{\psi} H \xrightarrow{\rho} A_k$. Note that $\mathfrak{B}_0[D] \succeq \cdots \succeq \mathfrak{B}_m[D]$ forms an almost d-ary sequence of H-invariant partitions. It follows that $H^\rho = A_k$ and hence $H^\rho_\alpha \neq A_k$ for some $\alpha \in D$ by Lemma 5.6. But $G^\varphi_\alpha = H^\rho_\alpha = A_k$ since $\alpha \in D$ is not affected, which is a contradiction.

So consider the case that $G^\varphi = S_k$ and let $G' = \varphi^{-1}(A_k)$. Let $\varphi' = \varphi|_{G'}$. Let D' be the set of points not affected by φ'. We argue that $D' = D$. We have $D' \subseteq D$

because $G_\alpha^\varphi \geq (G_\alpha')^\varphi$ for all $\alpha \in \Omega$. Now suppose there is some $\alpha \in D \setminus D'$. Then $G_\alpha^\varphi \geq A_k$, $(G_\alpha')^\varphi < A_k$ and $|G_\alpha^\varphi : (G_\alpha')^\varphi| \leq 2$. Overall, this gives us a subgroup of A_k of index 2. But such a subgroup would be a normal subgroup contradicting the fact that A_k is simple. So $D' = D$. Then, by the previous case, $G_{(D)}^\varphi \geq (G')_{(D)}^{\varphi'} = (G')_{(D')}^{\varphi'} \geq A_k$. $\qquad\square$

We also use Babai's affected orbit lemma, which does not need to be adapted to our setting.

THEOREM 5.10 (see [2, Theorem 6(b)]).   *Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group and suppose $\varphi\colon G \to S_k$ is a giant representation for $k \geq 5$. Suppose $\Delta \subseteq \Omega$ is an affected orbit of G (with respect to φ). Then every orbit of $\ker(\varphi)$ in Δ has length at most $|\Delta|/k$.*

6. Local certificates. In this section we adapt the local certificates technique developed in [2] to our setting using the generalization to the unaffected stabilizers theorem presented in the previous section (Theorem 5.9). As before the basic argumentation and also the notation follows [1]. Besides an adaptation to our setting, the main difference is a more precise analysis of the running time which is required for our overall analysis.

6.1. Algorithm. Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group and let $\mathfrak{x}\colon \Omega \to \Sigma$ be a string. Furthermore let $\varphi\colon G \to S_k$ be a giant representation. For a set $T \subseteq [k]$ let $G_T = \varphi^{-1}((G^\varphi)_T)$ and $G_{(T)} = \varphi^{-1}((G^\varphi)_{(T)})$.

Since our notation may be getting hard to trace here, as an example, let us disassemble it for one of the groups appearing in the next definition: $((\mathrm{Aut}_{G_T}(\mathfrak{x}))^\varphi)^T$. We start from the group $G \leq \mathrm{Sym}(\Omega)$. With the homomorphism φ we map it to $G^\varphi \leq S_k$ acting on the set $[k]$. Then we take the setwise stabilizer of the set $T \subseteq [k]$ and obtain the subgroup $G_T^\varphi \leq S_k$. We pull back to Ω via φ^{-1} and obtain the subgroup $G_T := \varphi^{-1}(G_T^\varphi) \leq \mathrm{Sym}(\Omega)$. We move on to the subgroup $\mathrm{Aut}_{G_T}(\mathfrak{x})$ and, once more, transfer it back to $[k]$ via φ to obtain $(\mathrm{Aut}_{G_T}(\mathfrak{x}))^\varphi \leq S_k$. The set T is invariant with respect to this group, so the group also acts on T. This, finally, gives us $((\mathrm{Aut}_{G_T}(\mathfrak{x}))^\varphi)^T \leq \mathrm{Sym}(T)$. What makes this complicated is the going back and forth between Ω and $[k]$. But this interplay between the two sets, or rather the groups acting on these sets, is crucial for the overall reasoning.

DEFINITION 6.1. *A set $T \subseteq [k]$ is full if $((\mathrm{Aut}_{G_T}(\mathfrak{x}))^\varphi)^T \geq \mathrm{Alt}(T)$. A certificate of fullness is a subgroup $K \leq \mathrm{Aut}_{G_T}(\mathfrak{x})$ such that $(K^\varphi)^T \geq \mathrm{Alt}(T)$. A certificate of nonfullness is a nongiant $M \leq \mathrm{Sym}(T)$ such that $((\mathrm{Aut}_{G_T}(\mathfrak{x}))^\varphi)^T \leq M$.*

Let $W \subseteq \Omega$ be G-invariant and let $\mathfrak{y}\colon \Omega \to \Sigma$ be a second string. Recall that $\mathrm{Iso}_G^W(\mathfrak{x}, \mathfrak{y}) = \{g \in G \mid \forall \alpha \in W\colon \mathfrak{x}(\alpha) = \mathfrak{y}(\alpha^g)\}$ and $\mathrm{Aut}_G^W(\mathfrak{x}) = \mathrm{Iso}_G^W(\mathfrak{x}, \mathfrak{x})$.

For $H \leq G$ we define $\mathrm{Aff}(H, \varphi) = \{\alpha \in \Omega \mid H_\alpha^\varphi \not\geq A_k\}$. Note that for $H_1 \leq H_2 \leq G$ it holds that $\mathrm{Aff}(H_1, \varphi) \supseteq \mathrm{Aff}(H_2, \varphi)$.

Finally, recall that n always denotes the size of the permutation domain Ω.

LEMMA 6.2. *Let $\mathfrak{x}\colon \Omega \to \Sigma$ be a string, let $G \leq \mathrm{Sym}(\Omega)$ be a group, and suppose there is an almost d-ary sequence of G-invariant partitions $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$. Furthermore suppose there is a giant representation $\varphi\colon G \to S_k$ and let $T \subseteq [k]$ be a set of size $|T| = t > \max\{8, 2 + \log_2 d\}$.*

Then there are natural numbers $n_1, \ldots, n_\ell \leq n/2$ such that $\sum_{i=1}^\ell n_i \leq n$ and, for each $i \in [\ell]$ using at most $t!$ recursive calls to string isomorphism over domain size n_i and $\mathcal{O}(t! \cdot n^c)$ additional computation, one can decide whether T is full or not and generate a corresponding certificate.

Algorithm 2. The LocalCertificates algorithm.

Input: $G \leq \mathrm{Sym}(\Omega)$, $\mathfrak{x} \colon \Omega \to \Sigma$, and $\varphi \colon G \to S_k$ with $k > \max\{8, 2 + \log_2 d\}$. There exists an almost d-ary sequence of G-invariant partitions $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$.

Output: nongiant $M \leq S_k$ with $(\mathrm{Aut}_G(\mathfrak{x}))^\varphi \leq M$ or $K \leq \mathrm{Aut}_G(\mathfrak{x})$ with $K^\varphi \geq A_k$.

1: $G_0 := G$
2: $W_0 := \emptyset$
3: $i := 0$
4: **while** $G_i^\varphi \geq A_k$ and $W_i \neq \mathrm{Aff}(G_i, \varphi)$ **do**
5:      $W_{i+1} := \mathrm{Aff}(G_i, \varphi)$
6:      $W_{i+1}^* := W_{i+1} \setminus W_i$
7:      **if** $|W_{i+1}^*| \leq \frac{1}{2}|\Omega|$ **then**
8:          $G_{i+1} := \mathrm{Aut}_{G_i}^{W_{i+1}^*}(\mathfrak{x})$
9:      **else**
10:          $G_{i+1} := \emptyset$
11:          $N := \ker(\varphi|_{G_i})$
12:          **for** $g \in G_i^\varphi$ **do**
13:              compute $\bar{g} \in \varphi^{-1}(g)$
14:              $G_{i+1} := G_{i+1} \cup \mathrm{Aut}_{N\bar{g}}^{W_{i+1}^*}(\mathfrak{x})$
15:          **end for**
16:      **end if**
17:      $i := i + 1$
18: **end while**
19: **if** $G_i^\varphi \not\geq A_k$ **then**
20:      **return** G_i^φ
21: **else**
22:      **return** $(G_i)_{(\Omega \setminus W_i)}$
23: **end if**

Proof. Without loss of generality assume $T = [k]$. Otherwise, we can compute the group G_T and restrict the image of φ to the set T.

Consider Algorithm 2. The algorithm computes, for increasing windows $W_0 \subseteq W_1 \subseteq W_2 \subseteq \ldots$, the group G_i of permutations that respect the input string $\mathfrak{x}$ on the window W_i, that is, $G_i = \mathrm{Aut}_G^{W_i}(\mathfrak{x}) = \mathrm{Aut}_{G_{i-1}}^{W_i^*}(\mathfrak{x})$, where $W_i^* = W_i \setminus W_{i-1}$. Note that $G_i \leq G_{i-1}$ and $W_{i+1} \supseteq W_i$ for $i \geq 1$ (initially $W_1 \neq \emptyset$ since by Lemma 5.6 at least one point has to be affected). The algorithm stops when the current group G_i^φ is not a giant or the window stops growing.

Let i^* be the value of the variable i at the end of while-loop. Furthermore let $W = W_{i^*}$. Note that $\{W_j^* \mid 1 \leq j \leq i^*\}$ forms a partition of the set W.

We first show the correctness of the algorithm. For every $0 \leq j \leq i^*$ it holds that $\mathrm{Aut}_G(\mathfrak{x}) \leq G_j \leq G$. We distinguish two cases. First suppose that $G_{i^*}^\varphi \not\geq A_k$. Then $G_{i^*}^\varphi$ forms a certificate of nonfullness. Otherwise $G_{i^*}^\varphi \geq A_k$ and $W = \mathrm{Aff}(G_{i^*}, \varphi)$. Note that $\mathfrak{B}_0, \ldots, \mathfrak{B}_m$ forms an almost d-ary sequence of invariant partitions for the group G_{i^*} (cf. Observation 4.2). So $((G_{i^*})_{(\Omega \setminus W)})^\varphi \geq A_k$ by Theorem 5.9. Furthermore, it is easy to check that G_{i^*} respects the string $\mathfrak{x}$ on all positions in W_j for all $0 \leq j \leq i^*$. Hence, $(G_{i^*})_{(\Omega \setminus W)} \leq \mathrm{Aut}_G(\mathfrak{x})$ because it respects all positions within W and fixes all other positions.

It remains to analyze the running time of the algorithm. Again we distinguish two cases. First suppose $|W_j^*| \leq n/2$ for all $j \in [i^*]$. Then, for each $j \in [i^*]$, the algorithm

makes one recursive call to string isomorphism over domain size $|W_i^*| \leq n/2$ (line 8) and $\sum_{j \in [i^*]} |W_j^*| \leq |W| \leq n$. Otherwise there is a unique $j^* \in \{0, \ldots, i^* - 1\}$ such that $|W_{j^*+1}^*| > n/2$. Let $N = \ker(\varphi|_{G_{j^*}})$. Since all elements in $W_{j^*+1}^*$ are affected by φ with respect to G_{j^*} it holds that every orbit of N in $W_{j^*+1}^*$ has size at most $|W_{j^*+1}^*|/k$ by Theorem 5.10. Since $G_{j^*+1}^\varphi \leq S_k$, for each orbit the algorithm makes at most $k!$ calls to string isomorphism where the domain is restricted to exactly this orbit (line 14). (Recall the assumption $T = [k]$, which implies $t! = k!$.) Additionally, for every $j \in [i^*], j \neq j^* + 1$ there is one recursive call to string isomorphism over domain size $|W_j^*|$. □

6.2. Comparing local certificates.

LEMMA 6.3. *Let $\mathfrak{x}_1, \mathfrak{x}_2 \colon \Omega \to \Sigma$ be two strings, let $G \leq \mathrm{Sym}(\Omega)$ be a group, and suppose there is an almost d-ary sequence of G-invariant partitions $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$. Furthermore suppose there is a giant representation $\varphi \colon G \to S_k$. Let $T_1, T_2 \subseteq [k]$ be sets of equal size $t = |T_1| = |T_2| > \max\{8, 2 + \log_2 d\}$ and suppose T_1 is not full.*

Then there are natural numbers $n_1, \ldots, n_\ell \leq n/2$ such that $\sum_{i=1}^\ell n_i \leq n$ and, for each $i \in [\ell]$ using $t!$ recursive calls to string isomorphism over domain size n_i and $\mathcal{O}(t! n^c)$ additional computation, one can compute a nongiant group $M \leq \mathrm{Sym}(T_1)$ and a bijection $\sigma \colon T_1 \to T_2$ such that

$$\text{(6.1)} \qquad \left\{ g^\varphi|_{T_1} \ \middle| \ g \in \mathrm{Iso}_G(\mathfrak{x}_1, \mathfrak{x}_2) \wedge T_1^{(g^\varphi)} = T_2 \right\} \subseteq M\sigma.$$

Moreover, the set of bijections $M\sigma$ is canonical for the two test sets (w.r.t. $\mathfrak{x}_1, \mathfrak{x}_2, G$ and the giant representation φ).

Here, canonical means that given additional test sets $T_1', T_2' \subseteq [k]$ such that $T_i' = T_i^g$ for some $g \in \mathrm{Aut}_G(\mathfrak{x}_i)$ for both $i \in \{1, 2\}$, the algorithm computes a set $M'\sigma'$ such that $(M\sigma)^g = M'\sigma'$.

Proof. Consider Algorithm 3. First suppose toward a contradiction there is some i such that $W_{i+1} = W_i$. Then $((G_i)_{(\Omega \setminus W_i)})^\psi \geq \mathrm{Alt}(T_1)$ by Theorem 5.9. Furthermore $(G_i)_{(\Omega \setminus W_i)} \leq \mathrm{Aut}_G(\mathfrak{x})$. Together this implies that $(\mathrm{Aut}_{G_{T_1}}(\mathfrak{x}))^\psi \geq \mathrm{Alt}(T_1)$ contradicting the fact that T_1 is not full.

So the algorithm terminates and returns a nongiant group $M \leq \mathrm{Sym}(T_1)$ and a bijection $\sigma \colon T_1 \to T_2$ with the desired properties. The complexity analysis is completely analogous to Lemma 6.2.

Finally, the canonicity of the set of bijections $M\sigma$ follows from the fact that in each iteration the set of affected points is canonically defined. □

6.3. Aggregating local certificates. Let $G \leq \mathrm{Sym}(\Omega)$ be a group. The *symmetry defect* of G is the minimal $t \in [n]$ such that there is a set $\Delta \subseteq \Omega$ of size $|\Delta| = n - t$ such that $\mathrm{Alt}(\Delta) \leq G$ (the group $\mathrm{Alt}(\Delta)$ fixes all elements of $\Omega \setminus \Delta$). In this case the *relative symmetry defect* is t/n.

For any relational structure $\mathfrak{A}$ we define the *(relative) symmetry defect* of $\mathfrak{A}$ to be the (relative) symmetry defect of its automorphism group $\mathrm{Aut}(\mathfrak{A})$.

THEOREM 6.4 (cf. [12, Theorem 5.2 A,B]). *Let $A_n \leq S \leq S_n$ and suppose $n > 9$. Let $G \leq S$ and $r < n/2$. Suppose that $|S : G| < \binom{n}{r}$. Then the symmetry defect of G is strictly less than r.*

Using the inequality $\binom{n}{\lfloor n/4 \rfloor} \geq (\frac{n}{\lfloor n/4 \rfloor})^{\lfloor n/4 \rfloor} \geq \frac{1}{4} \cdot \sqrt{2}^n$ we get the following corollary.

Algorithm 3. The CompareLocalCertificates algorithm.

Input: $G \leq \mathrm{Sym}(\Omega)$, $\mathfrak{x}_1, \mathfrak{x}_2 \colon \Omega \to \Sigma$, $\varphi \colon G \to S_k$, and $T_1, T_2 \subseteq [k]$ of size $t > \max\{8, 2 + \log_2 d\}$. There exists an almost d-ary sequence of invariant partitions $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$ and T_1 is not full.

Output: non-giant group $M \leq \mathrm{Sym}(T_1)$ and bijection $\sigma \colon T_1 \to T_2$ such that

$$\left\{ g^\varphi|_{T_1} \;\middle|\; g \in \mathrm{Iso}_G(\mathfrak{x}_1, \mathfrak{x}_2) \wedge T_1^{(g^\varphi)} = T_2 \right\} \subseteq M\sigma.$$

1: compute $\sigma_0 \in G$ such that $T_1^{(\sigma_0^\varphi)} = T_2$
2: $G_0 := G_{T_1}$
3: $W_0 := \emptyset$
4: $i := 0$
5: $\psi \colon G_0 \to \mathrm{Sym}(T_1)$ homomorphism obtained from φ by restricting the image to T_1
6: **while** $G_i^\psi \geq \mathrm{Alt}(T_1)$ **do**
7: $\quad W_{i+1} := \mathrm{Aff}(G_i, \psi)$
8: $\quad W_{i+1}^* := W_{i+1} \setminus W_i$
9: $\quad$ **if** $|W_{i+1}^*| \leq \frac{1}{2}|\Omega|$ **then**
10: $\quad\quad G_{i+1}\sigma_{i+1} := \mathrm{Iso}_{G_i\sigma_i}^{W_{i+1}^*}(\mathfrak{x}, \mathfrak{y})$
11: $\quad$ **else**
12: $\quad\quad G_{i+1} := \emptyset$
13: $\quad\quad N := \ker(\psi|_{G_i})$
14: $\quad\quad \ell := 0$
15: $\quad\quad$ **for** $g \in G_i^\psi$ **do**
16: $\quad\quad\quad$ compute $\bar{g} \in \psi^{-1}(g)$
17: $\quad\quad\quad H_\ell h_\ell := \mathrm{Iso}_{N\bar{g}\sigma_i}^{W_{i+1}^*}(\mathfrak{x}, \mathfrak{y})$
18: $\quad\quad\quad \ell := \ell + 1$
19: $\quad\quad$ **end for**
20: $\quad\quad G_{i+1}\sigma_{i+1} := \bigcup_{j \leq \ell} H_j h_j$
21: $\quad$ **end if**
22: $\quad i := i + 1$
23: **end while**
24: **return** $(G_i^\psi, (\sigma_i^\varphi)|_{T_1})$

COROLLARY 6.5. *Let $A_n \leq S \leq S_n$ and suppose $n \geq 24$. Let $G \leq S$ and suppose the relative symmetry defect of G is at least $1/4$. Then $|S : G| \geq (4/3)^n$.*

LEMMA 6.6. *Let $\mathfrak{x}_1, \mathfrak{x}_2 \colon \Omega \to \Sigma$ be two strings, $G \leq \mathrm{Sym}(\Omega)$ be a group and suppose there is an almost d-ary sequence of G-invariant partitions $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$. Furthermore suppose there is a giant representation $\varphi \colon G \to S_k$. Let $\max\{8, 2 + \log_2 d\} < t < k/10$.*

Then there are natural numbers $\ell \in \mathbb{N}$ and $n_1, \ldots, n_\ell \leq n/2$ such that $\sum_{i=1}^\ell n_i \leq k^{\mathcal{O}(t)} n$ and, for each $i \in [\ell]$ using a recursive call to string isomorphism over domain size n_i, and $k^{\mathcal{O}(t)} n^c$ additional computation, one obtains for $i = 1, 2$ one of the following:

1. *a family of $r \leq k^6$ many t-ary relational structures $\mathfrak{A}_{i,j}$, for $j \in [r]$, associated with $\mathfrak{x}_i$, each with domain $D_{i,j} \subseteq [k]$ of size $|D_{i,j}| \geq \frac{3}{4}k$ and with relative symmetry defect at least $\frac{1}{4}$ such that*

$$\{\mathfrak{A}_{1,1}, \ldots, \mathfrak{A}_{1,r}\}^{\varphi(g)} = \{\mathfrak{A}_{2,1}, \ldots, \mathfrak{A}_{2,r}\} \ \text{for every } g \in \mathrm{Iso}_G(\mathfrak{x}_1, \mathfrak{x}_2),$$

or

2. *a subset* $\Delta_i \subseteq [k]$ *associated with* $\mathfrak{x}_i$ *of size* $|\Delta_i| \geq \frac{3}{4}k$ *and* $K_i \leq \mathrm{Aut}_{G_{\Delta_i}}(\mathfrak{x}_i)$ *such that* $(K_i^{\varphi})^{\Delta_i} \geq \mathrm{Alt}(\Delta_i)$ *and*

$$\Delta_1^{\varphi(g)} = \Delta_2 \ \text{for every } g \in \mathrm{Iso}_G(\mathfrak{x}_1, \mathfrak{x}_2).$$

The proof is completely analogous to the proof of [2, Theorem 24], replacing the methods to compute the local certificates. Note that colorings and equipartitions of a subset of $[k]$ can be viewed as relational structures. For the sake of completeness a full proof of the lemma is given in Appendix A.

Next we describe how we use the two possible outcomes of the previous lemma to make progress.

LEMMA 6.7. *Suppose option* 1 *of Lemma* 6.6 *is satisfied, yielding a number* $r \leq k^6$ *and relational structures* $\mathfrak{A}_{i,j}$ *for* $i \in [2], j \in [r]$. *Then there are subgroups* $H_j \leq G$ *and elements* $h_j \in \mathrm{Sym}(\Omega)$ *for* $j \in [r]$ *such that*
    1. $|G^{\varphi} : H_j^{\varphi}| \geq (4/3)^k$ *for all* $j \in [r]$, *and*
    2. $\mathfrak{x}_1 \cong_G \mathfrak{x}_2$ *if and only if* $\mathfrak{x}_1 \cong_{H_j h_j} \mathfrak{x}_2$ *for some* $j \in [r]$, *and given representations for the sets* $\mathrm{Iso}_{H_j h_j}(\mathfrak{x}_1, \mathfrak{x}_2)$ *for all* $j \in [r]$ *one can compute in polynomial time a representation for* $\mathrm{Iso}_G(\mathfrak{x}_1, \mathfrak{x}_2)$.
Moreover, given the relational structures $\mathfrak{A}_{i,j}$ *for all* $i \in [2]$ *and* $j \in [r]$, *the groups* H_j *and elements* h_j *can be computed in time* $k^{\mathcal{O}(t^c(\log k)^c)}n^c$ *for some constant* c.

Proof. Let $D_{i,j} \subseteq [k]$ be the domain of $\mathfrak{A}_{i,j}$ for all $i \in [2]$ and $j \in [r]$. Let $\mathfrak{A}_1 = \mathfrak{A}_{1,1}$ and $D_1 = D_{1,1}$. Now define

$$H_j h_j = \{g \in G \mid (D_1)^{(g^{\varphi})} = D_{2,j} \wedge (g^{\varphi})|_{D_1} \in \mathrm{Iso}(\mathfrak{A}_1, \mathfrak{A}_{2,j})\}.$$

Using the quasipolynomial-time isomorphism test from [2] the set $\mathrm{Iso}(\mathfrak{A}_1, \mathfrak{A}_{2,j})$ can be computed in time $k^{\mathcal{O}(t^c(\log k)^c)}$ for some constant c (first translate the relational structures into two graphs of size $k^{\mathcal{O}(t)}$ (see, e.g., [28]) and then apply the isomorphism test from [2] to the resulting graphs). Hence, the groups $H_j \leq G$ and elements $h_j \in \mathrm{Sym}(\Omega)$ can be computed within the desired time bound. Moreover

$$\mathrm{Iso}_G(\mathfrak{x}_1, \mathfrak{x}_2) = \bigcup_{j \in [r]} \mathrm{Iso}_{H_j h_j}(\mathfrak{x}_1, \mathfrak{x}_2).$$

Finally observe that the symmetry defect of H_j^{φ} is at least $\frac{1}{4}$. So $|G^{\varphi} : H_j^{\varphi}| \geq (4/3)^k$ by Corollary 6.5. $\qquad\square$

Remark 6.8. The proof of the previous lemma is the only place where we use Babai's quasipolynomial-time isomorphism test [2] as a black box.

LEMMA 6.9. *Suppose option* 2 *of Lemma* 6.6 *is satisfied. Then there is a number* $r \in \{1, 2\}$, *a subgroup* $H \leq G$, *and elements* $h_j \in \mathrm{Sym}(\Omega)$ *for* $j \in [r]$ *such that*
    1. $|G^{\varphi} : H^{\varphi}| \geq (4/3)^k$, *and*
    2. $\mathfrak{x}_1 \cong_G \mathfrak{x}_2$ *if and only if* $\mathfrak{x}_1 \cong_{H h_j} \mathfrak{x}_2$ *for some* $j \in [r]$, *and given representations for the sets* $\mathrm{Iso}_{H h_j}(\mathfrak{x}_1, \mathfrak{x}_2)$ *for all* $j \in [r]$ *and a generating set for* K_1 *one can compute in polynomial time a representation for* $\mathrm{Iso}_G(\mathfrak{x}_1, \mathfrak{x}_2)$.
Moreover, given the sets Δ_i *for all* $i \in [2]$, *the group* H *and the elements* h_i *can be computed in polynomial time.*

Proof. Let $H = G_{(\Delta_1)}$ (recall that $G_{(T)} = \varphi^{-1}((G^\varphi)_{(T)})$ for $T \subseteq [k]$). Let $g \in G$ such that $\Delta_1^{g^\varphi} = \Delta_2$ and $\tau \in G_{\Delta_1}$ such that $(\tau^\varphi)^{\Delta_1}$ is a transposition. Now define $h_1 = g$ and $h_2 = \tau g$. Then $\mathfrak{x}_1 \cong_G \mathfrak{x}_2$ if and only if $\mathfrak{x}_1 \cong_{Hh_j} \mathfrak{x}_2$ since $(K_1^\varphi)^{\Delta_1} \geq \mathrm{Alt}(\Delta_1)$. Moreover, if $G_j g_j = \mathrm{Iso}_{Hh_j}(\mathfrak{x}_1, \mathfrak{x}_2)$, then $\mathrm{Iso}_G(\mathfrak{x}_1, \mathfrak{x}_2) = \bigcup_{j=1,2} \langle K_1, G_j \rangle g_j$. Finally, $|G^\varphi : H^\varphi| \geq |\mathrm{Alt}(\Delta_1)| \geq (4/3)^k$. $\qquad\square$

7. String isomorphism. We are now ready to formalize our algorithm. We shall need the following result characterizing the obstacle cases for efficient Luks reduction.

LEMMA 7.1 (cf. [1, Theorem 3.2.1]). *Let $G \leq S_d$ be a primitive group of order $|G| \geq d^{1+\log d}$ where d is greater than some absolute constant. Then there is a polynomial time algorithm computing a normal subgroup $N \leq G$ of index $|G : N| \leq d$, an N-invariant equipartition $\mathfrak{B}$, and a giant representation $\varphi \colon N \to S_k$, where $k \geq \log d$ and $\ker(\varphi) = N_{(\mathfrak{B})}$.*

LEMMA 7.2. *Let $G \leq \mathrm{Sym}(\Omega)$ be transitive and let $\mathfrak{x}, \mathfrak{y} \colon \Omega \to \Sigma$ be two strings. Moreover, suppose there is an almost d-ary sequence of G-invariant partitions $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$ such that $|\mathfrak{B}_1| \leq d$. Then there are natural numbers $\ell \in \mathbb{N}$ and $n_1, \ldots, n_\ell \leq n/2$ such that $\sum_{i=1}^{\ell} n_i \leq 2^{\mathcal{O}((\log d)^3)} n$ and, using a recursive call to string isomorphism over domain size at most n_i for each $i \in [\ell]$ and $d^{\mathcal{O}((\log d)^c)} n^c$ additional computation, one can compute $\mathrm{Iso}_G(\mathfrak{x}, \mathfrak{y})$.*

Proof. Let $\mathfrak{B} = \mathfrak{B}_1$ and let $P = G^{\mathfrak{B}}$ be the induced action of G on the partition $\mathfrak{B}$. Without loss of generality suppose P is primitive (otherwise replace $\mathfrak{B}$ with a block system of smaller size). First suppose $|P| \leq d^{1+\log d}$. Then the statement immediately follows by standard Luks reduction. Otherwise let $N \leq P$ be the normal subgroup computed by Lemma 7.1 and let $\mathfrak{C}$ be the corresponding partition and $\psi \colon N \to S_k$ the giant representation. Observe that $k \leq d$ since $N \leq P \leq \mathrm{Sym}(\mathfrak{B})$ and $|\mathfrak{B}| \leq d$. Let $G' = \{g \in G \mid g^{\mathfrak{B}} \in N\}$. Also let $\mathfrak{C}' = \{\{\alpha \in \Omega \mid \exists B \in C \colon \alpha \in B\} \mid C \in \mathfrak{C}\}$. Note that $\mathfrak{C}'$ is G'-invariant. Since $|G : G'| \leq d$ it suffices to prove the statement for the group G'. Let $\varphi \colon G' \to S_k \colon g \mapsto (g^{\mathfrak{B}})^\psi$. Note that φ is a giant representation and $(G')_{(\mathfrak{C}')} = \ker(\varphi)$. Let $t = \max\{9, 3 + \log d\}$. In case $k \leq 10t$ the statement follows again by standard Luks reduction (in this case $|G' : (G')_{(\mathfrak{C}')}| = |G' : \ker(\varphi)| \leq k! \leq 2^{\mathcal{O}((\log d)^2)}$). So suppose $\max\{8, 2 + \log d\} < t < k/10$. In this case the requirements of Lemma 6.6 are satisfied.

Using Lemma 6.6, 6.7, and 6.9 we can reduce the problem (using additional recursive calls to string isomorphism over domain size at most $n/2$) to at most k^6 instances of H-isomorphism over the same strings $\mathfrak{x}, \mathfrak{y}$ for groups $H \leq G'$ with $|(G')^\varphi : H^\varphi| \geq (4/3)^k$. Applying the same argument to these instances of H-isomorphism and repeating the process until we can afford to perform standard Luks reduction gives our desired algorithm. It remains to analyze its running time, that is, we have to analyze the number of times this process has to be repeated until we reach a group that is sufficiently small to perform standard Luks reduction. Toward this end, we analyze the parameter k of the giant representation and show that it has to be reduced in each round by a certain amount. Recall that our algorithm performs standard Luks reduction as soon as $k \leq 10t$.

Consider the recursion tree of the algorithm (ignoring the additional recursive calls to string isomorphism over domain size at most $n/2$ for the moment). Recall that $\mathfrak{C}'$ is G'-invariant and thus it is also H-invariant. In case H is not transitive it is processed orbit by orbit. Note that there is at most one orbit of size greater than $n/2$ that has to

be considered in the current recursion (for the other orbits additional recursive calls to string isomorphism over domain size at most $n/2$ suffice and these recursive calls are ignored for the moment). Let $\varphi' \colon H' \to S_{k'}$ be the giant representation computed on the next level of the recursion where H' is the projection of H'' to an invariant subset of the domain for some $H'' \leq H$ (if no giant representation is computed, then the algorithm performs standard Luks reduction and the node on the next level is a leaf). Observe that $|(H')^{\mathfrak{C}'}| \geq \frac{(k')!}{2}$ because $(H')^{\varphi'} \geq A_{k'}$ and $H'_{(\mathfrak{C}')} \leq \ker(\varphi')$. Also note that $|H^{\mathfrak{C}'}| \leq \frac{k!}{(4/3)^k}$ since $\ker(\varphi) = G'_{(\mathfrak{C}')}$ by Lemma 7.1. So

$$\frac{(k')!}{2} \leq \frac{k!}{(4/3)^k}.$$

Hence,

$$(4/3)^k \leq 2 \cdot 2^{(k-k')\log k} \leq (4/3)^{3(k-k')\log k}$$

since k is sufficiently large. So

$$k' \leq k - \frac{k}{3\log k}.$$

It follows that the height of the recursion tree is $\mathcal{O}((\log d)^2)$. Thus, the number of nodes of the recursion tree is bounded by $d^{\mathcal{O}((\log d)^2)} = 2^{\mathcal{O}((\log d)^3)}$. By Lemmata 6.6, 6.7, and 6.9 each node of the recursion tree makes recursive calls to string isomorphism over domain sizes $n_i \leq n/2$ where $\sum_i n_i \leq 2^{\mathcal{O}((\log d)^2)} n$ and uses additional computation $d^{\mathcal{O}((\log d)^c)} n^c$ for some constant c. Putting this together, the desired bound follows. □

THEOREM 7.3. *Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group and let $\mathfrak{x}, \mathfrak{y} \colon \Omega \to \Sigma$ be two strings. Moreover, suppose there is an almost d-ary sequence of G-invariant partitions $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$. Then one can compute $\mathrm{Iso}_G(\mathfrak{x}, \mathfrak{y})$ in time $n^{\mathcal{O}((\log d)^c)}$ for an absolute constant c.*

Proof. Consider Algorithm 4. The algorithm essentially distinguishes between two cases. If the input group G is not transitive or the action of G on the block system $\mathfrak{B}_1$ is semiregular, the algorithm follows Luks algorithm recursively computing the set $\mathrm{Iso}_G(\mathfrak{x}, \mathfrak{y})$. In the other case G is transitive and $|\mathfrak{B}_1| \leq d$ and hence we can apply Lemma 7.2 to recursively compute $\mathrm{Iso}_G(\mathfrak{x}, \mathfrak{y})$.

Clearly, it computes the desired set of isomorphisms. The bound on the running follows from Lemma 2.8. Note that the bottleneck is the type of recursion used in Lemma 7.2. Also observe that every group H, for which the algorithm performs a recursive call, is the projection of a subgroup of G to an invariant subset of the domain. Hence, by restricting the partitions $\mathfrak{B}_0, \ldots, \mathfrak{B}_m$ to the domain of H one obtains a sequence of partitions for the group H with the desired properties (cf. Observation 4.2). □

Combining Theorems 4.7 and 7.3 we obtain the main technical result of this work.

THEOREM 7.4. *Let $G \leq \mathrm{Sym}(\Omega)$ be a $\widehat{\Gamma}_d$-group and let $\mathfrak{x}, \mathfrak{y} \colon \Omega \to \Sigma$ be two strings. Then there is an algorithm deciding whether $\mathfrak{x} \cong_G \mathfrak{y}$ in time $n^{\mathcal{O}((\log d)^c)}$ for an absolute constant c.*

Proof. Using orbit-by-orbit processing we can assume that the group G is transitive. For a transitive group the statement follows by first applying Theorem 4.7 and then Theorem 7.3. □

Algorithm 4. String isomorphism algorithm.

Input: $G \leq \mathrm{Sym}(\Omega)$ a $\widehat{\Gamma}_d$-group, $\mathfrak{x}, \mathfrak{y} \colon \Omega \to \Sigma$ two strings and an almost d-ary sequence of G-invariant partitions $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$.
Output: $\mathrm{Iso}_G(\mathfrak{x}, \mathfrak{y})$.
 1: **if** G is not transitive **then**
 2:      compute orbits $\Omega_1, \ldots, \Omega_s$
 3:      recursively process group orbit by orbit $\triangleright$ restrict partitions to orbits
 4:      **return** $\mathrm{Iso}_G(\mathfrak{x}, \mathfrak{y})$
 5: **else**
 6:      **if** $G^{\mathfrak{B}_1}$ is semiregular **then**
 7:          apply standard Luks reduction $\triangleright$ restrict partitions to orbits of $G_{(\mathfrak{B}_1)}$
 8:          **return** $\mathrm{Iso}_G(\mathfrak{x}, \mathfrak{y})$
 9:      **else** $\triangleright$ assumptions of Lemma 7.2 are satisfied
10:          apply Lemma 7.2
11:          **return** $\mathrm{Iso}_G(\mathfrak{x}, \mathfrak{y})$
12:      **end if**
13: **end if**

---

8. Applications.

8.1. Isomorphism for graphs of bounded degree. Using the improved algorithm for string isomorphism we can now prove the main result of this work using the following well-known reduction.

THEOREM 8.1 (see [24, 6]). *There is a polynomial-time Turing reduction from the graph isomorphism problem for graphs of maximum degree d to the string isomorphism problem for $\widehat{\Gamma}_d$-groups (the running time of the reduction does not depend on d).*

The reduction follows [24] using an additional trick presented in [6, section 4.2] to remove the dependence of the running time on d.

Combining this reduction with the improved algorithm for string isomorphism, we get the desired algorithm for isomorphism tests of bounded degree graphs.

THEOREM 8.2 (Theorem 1.1 restated). *The isomorphism problem for graphs of maximum degree d can be solved in time $n^{\mathcal{O}((\log d)^c)}$ for an absolute constant c.*

Proof. This follows from Theorems 7.4 and 8.1.   □

8.2. Isomorphism for relational structures and hypergraphs. For the second application of Theorem 7.4 consider the isomorphism problem for relational structures.

THEOREM 8.3. *Let $\mathfrak{A} = (D, R)$, $\mathfrak{A}' = (D, R')$ be relational structures where $R, R' \subseteq D^t$ are t-ary relations. Then one can decide whether $\mathfrak{A}$ is isomorphic to $\mathfrak{A}'$ in time $n^{\mathcal{O}(t \cdot (\log n)^c)}$, where $n = |D|$.*

Proof. Let $\mathfrak{x} \colon D^t \to \{0, 1\}$ be the string with $\mathfrak{x}(a_1, \ldots, a_t) = 1$ if and only if $(a_1, \ldots, a_t) \in R$. Similarly define the string $\mathfrak{x}' \colon D^t \to \{0, 1\}$ for the relation R'. Now let $G = \mathrm{Sym}(D)^{(D^t)}$ be the symmetric group over the set D with its natural action on t-tuples. Then $\mathfrak{A}$ is isomorphic to $\mathfrak{A}'$ if and only if $\mathfrak{x}$ is G-isomorphic to $\mathfrak{x}'$. Moreover, $G \in \widehat{\Gamma}_n$. Hence, by Theorem 7.4, one can decide in time $n^{\mathcal{O}(t \cdot (\log n)^c)}$ whether $\mathfrak{x}$ is G-isomorphic to $\mathfrak{x}'$.   □

In many cases this leads to a better running time than first translating the struc-

ture into a graph and then applying Babai's algorithm to test whether the two resulting graphs are isomorphic. In particular, in case the arity t is large and also the size of the relation is large our method gives a much better worst-case complexity than the other approach.

Also note that as a special case the same running time can be obtained for hypergraphs if t is the maximal hyperedge size. This also improves on previous results (see, e.g., [4]).

COROLLARY 8.4. *Let $\mathcal{H} = (V, \mathcal{E})$, $\mathcal{H}' = (V, \mathcal{E}')$ be two hypergraphs such that every hyperedge $E \in \mathcal{E} \cup \mathcal{E}'$ has size $|E| \leq t$. Then one can decide whether $\mathcal{H}$ is isomorphic to $\mathcal{H}'$ in time $n^{\mathcal{O}(t \cdot (\log n)^c)}$, where $n = |V|$.*

9. Concluding remarks. We have obtained a new graph isomorphism test with a running time bounded by a polynomial of degree polylogarithmic in the maximum degree of the input graphs. Technically, this result relies on some heavy group theory, new combinatorial tricks that allow us to reduce the string isomorphism problem for $\widehat{\Gamma}_d$ groups to a setting where we have an "almost d-ary" sequence of invariant partitions controlling the operation of the groups, and a refinement of the techniques introduced by Babai [2] for his quasipolynomial-time isomorphism test.

We hope that the machinery we have developed here will have further applications and ultimately even lead to an improvement of Babai's isomorphism test. More immediate applications may be obtained for the isomorphism problem under restrictions of other parameters than the maximum degree. For example, we conjecture that there also is an isomorphism test running in time $n^{\mathcal{O}((\log k)^c)}$, where k is the tree width of the input graphs. We remark that the results established in this work have already been used in [15] to obtain an improved fixed-parameter tractable algorithm for isomorphism testing parameterized by tree width.

Another related problem that we leave open is whether the graph isomorphism problem parameterized by the maximum degree of the input graphs is fixed-parameter tractable.

Appendix A. Aggregating local certificates. We give a proof for Lemma 6.6.

DEFINITION A.1. *A group $G \leq \mathrm{Sym}(\Omega)$ is t-transitive if its natural induced action on the set of $n(n-1)\ldots(n-t+1)$ ordered t-tuples of distinct elements is transitive. The* degree of transitivity $d(G)$ *is the largest t such that G is t-transitive.*

THEOREM A.2 (classification of finite simple groups). *Let $G \leq \mathrm{Sym}(\Omega)$ be a nongiant group. Then $d(G) \leq 5$.*

A slightly weaker statement, namely $d(G) \leq 7$ for all nongiants permutation groups, can be shown using only Schreier's hypothesis (see [12, Theorem 7.3A]).

LEMMA A.3 (cf. [1, Corollary 2.4.13]). *Let Γ be a nontrivial regular graph. Then the relative symmetry defect of Γ is at least $1/2$.*

LEMMA A.4 (Lemma 6.6 restated). *Let $\mathfrak{x}_1, \mathfrak{x}_2 \colon \Omega \to \Sigma$ be two strings, let $G \leq \mathrm{Sym}(\Omega)$ be a group, and suppose there is an almost d-ary sequence of G-invariant partitions $\{\Omega\} = \mathfrak{B}_0 \succ \cdots \succ \mathfrak{B}_m = \{\{\alpha\} \mid \alpha \in \Omega\}$. Furthermore suppose there is a giant representation $\varphi \colon G \to S_k$. Let $\max\{8, 2 + \log_2 d\} < t < k/10$.*

Then there are natural numbers $\ell \in \mathbb{N}$ and $n_1, \ldots, n_\ell \leq n/2$ such that $\sum_{i=1}^{\ell} n_i \leq k^{\mathcal{O}(t)}n$ and, for each $i \in [\ell]$ using a recursive call to string isomorphism over domain size n_i, and $k^{\mathcal{O}(t)}n^c$ additional computation, one obtains for $i = 1, 2$ one of the following:

1. *a family of $r \leq k^6$ many t-ary relational structures $\mathfrak{A}_{i,j}$, for $j \in [r]$, associated with $\mathfrak{x}_i$, each with domain $D_{i,j} \subseteq [k]$ of size $|D_{i,j}| \geq \frac{3}{4}k$ and with relative symmetry defect at least $\frac{1}{4}$ such that*

$$\{\mathfrak{A}_{1,1}, \ldots, \mathfrak{A}_{1,r}\}^{\varphi(g)} = \{\mathfrak{A}_{2,1}, \ldots, \mathfrak{A}_{2,r}\} \ \text{for every } g \in \mathrm{Iso}_G(\mathfrak{x}_1, \mathfrak{x}_2),$$

   or

2. *a subset $\Delta_i \subseteq [k]$ associated with $\mathfrak{x}_i$ of size $|\Delta_i| \geq \frac{3}{4}k$ and $K_i \leq \mathrm{Aut}_{G_{\Delta_i}}(\mathfrak{x}_i)$ such that $(K_i^\varphi)^{\Delta_i} \geq \mathrm{Alt}(\Delta_i)$ and*

$$\Delta_1^{\varphi(g)} = \Delta_2 \ \text{for every } g \in \mathrm{Iso}_G(\mathfrak{x}_1, \mathfrak{x}_2).$$

Proof. For every t-element subset $T \subseteq [k]$ determine whether T is full (with respect to $\mathfrak{x}_i$) and compute a corresponding certificate using Lemma 6.2. Let $F_i \leq \mathrm{Sym}(\Omega)$ be the group generated by the fullness certificates for all full subsets $T \subseteq [k]$ with respect to string $\mathfrak{x}_i$. Note that the group F_i is canonical. Let $S_i \subseteq [k]$ be the support of F_i^φ (the set of elements not fixed by F_i^φ).

First suppose $\frac{1}{4}k \leq |S_i| \leq \frac{3}{4}k$. Then one obtains a canonical structure $\mathfrak{A}_i$ with domain $[k]$ and relative symmetry defect at least $\frac{1}{4}$ by coloring each element $\alpha \in [k]$ depending on whether $\alpha \in S_i$.

Next suppose $|S_i| > \frac{3}{4}k$. We distinguish between three subcases. First assume there is no orbit of F_i^φ of size at least $\frac{3}{4}k$. Then the partition into the orbits of F_i^φ gives a canonical structure $\mathfrak{A}_i$ with domain $[k]$ and relative symmetry defect at least $\frac{1}{4}$. So assume there is a (unique) orbit $C \subseteq [k]$ of size $C \geq \frac{3}{4}k$. If $(F_i^\varphi)^C \geq \mathrm{Alt}(C)$, then the second option of the lemma is satisfied. Hence suppose $(F_i^\varphi)^C$ is not a giant. By Theorem A.2 the degree of transitivity satisfies $d((F_i^\varphi)^C) \leq 5$. Let $I \subseteq C$ be an arbitrary set of size $d((F_i^\varphi)^C) - 1$ and individualize the elements of I. Then $(F_i^\varphi)_{(I)}^{C'}$ is transitive, but not 2-transitive, where $C' = C \setminus I$. Note that the number of possible choices for the set I is at most k^4. Now let $\mathfrak{X}_i = (C', R_1, \ldots, R_r)$ be the *orbital configuration* of $(F_i^\varphi)_{(I)}$ on the set C', that is, the relations R_i are the orbits of $(F_i^\varphi)_{(I)}$ in its natural action on $C' \times C'$. Note that $r \geq 3$ since $(F_i^\varphi)_{(I)}^{C'}$ is not 2-transitive. Also observe that the numbering of the R_i is not canonical (isomorphisms may permute the R_i). Without loss of generality suppose that R_1 is the diagonal. Now individualize one of the R_i for $i \geq 2$ at a multiplicative cost of $r - 1 \leq k - 1$. If R_i is undirected (i.e., $R_i = R_i^{-1}$), then it defines a nontrivial regular graph. Since the symmetry defect of this graph is at least $1/2$ (see Lemma A.3) this gives us the desired structure. Otherwise R_i is directed. If the out-degree of a vertex is strictly less $(|C'| - 1)/2$, then the undirected graph $\Gamma = (C', R_i \cup R_i^{-1})$ is again a nontrivial regular graph. Otherwise, by individualizing one vertex (at a multiplicative cost of $|C'| \leq k$), one obtains a coloring of symmetry defect at least $1/2$ by coloring vertices depending on whether they are an in- or an out-neighbor of the individualized vertex.

Finally suppose $|S_i| < \frac{1}{4}k$. Let $D_i = [k] \setminus S_i$. Indeed it can be assumed that $|D_1| = |D_2| \geq \frac{3}{4}k$. Observe that every $T \subseteq D_i$ is not full with respect to the string $\mathfrak{x}_i$. Let $D_i' = D_i \times \{i\}$ (to make the sets disjoint).

Consider the following category $\mathcal{L}$. The objects are the pairs (T, i), where $T \subseteq D_i$ is a t-element subset. The morphisms $(T, i) \rightarrow (T', i')$ are the bijections computed in Lemma 6.3 for the test sets T and T' along with the corresponding strings. The morphisms define an equivalence relation on the set $(D_1')^{\langle t \rangle} \cup (D_2')^{\langle t \rangle}$, where $(D_i')^{\langle t \rangle}$ denotes the set of all ordered t-tuples with distinct elements over the set D_i'. Let $R_1, \ldots, R_r$ be the equivalence classes and define $R_j(i) = R_j \cap (D_i')^{\langle t \rangle}$. Then

$\mathfrak{A}_i = (D'_i, R_1(i), \ldots, R_r(i))$ is a canonical t-ary relational structure. Moreover, the symmetry defect of $\mathfrak{A}_i$ is at least $|D_i| - t + 1 \geq |D_i|/4$. ⯀

REFERENCES

[1] L. Babai, *Graph Isomorphism in Quasipolynomial Time*, CoRR, http://arxiv.org/abs/1512.03547, 2015.

[2] L. Babai, *Graph isomorphism in quasipolynomial time [extended abstract]*, in Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, Cambridge, MA, D. Wichs and Y. Mansour, eds., ACM, 2016, pp. 684–697, https://doi.org/10.1145/2897518.2897542.

[3] L. Babai, P. J. Cameron, and P. P. Pálfy, *On the orders of primitive groups with restricted nonabelian composition factors*, J. Algebra, 79 (1982), pp. 161–168, https://doi.org/10.1016/0021-8693(82)90323-4.

[4] L. Babai and P. Codenotti, *Isomorhism of hypergraphs of low rank in moderately exponential time*, in Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science, Philadelphia, IEEE Computer Society, 2008, pp. 667–676, https://doi.org/10.1109/FOCS.2008.80.

[5] L. Babai, W. M. Kantor, and E. M. Luks, *Computational complexity and the classification of finite simple groups*, in Proceedings of the 24th Annual Symposium on Foundations of Computer Science, Tucson, AZ, IEEE Computer Society, 1983, pp. 162–171, https://doi.org/10.1109/SFCS.1983.10.

[6] L. Babai and E. M. Luks, *Canonical labeling of graphs*, in Proceedings of the 15th Annual ACM Symposium on Theory of Computing, Boston, D. S. Johnson, R. Fagin, M. L. Fredman, D. Harel, R. M. Karp, N. A. Lynch, C. H. Papadimitriou, R. L. Rivest, W. L. Ruzzo, and J. I. Seiferas, eds., ACM, 1983, pp. 171–183, https://doi.org/10.1145/800061.808746.

[7] L. Babai, E. M. Luks, and Á. Seress, *Permutation groups in NC*, in Proceedings of the 19th Annual ACM Symposium on Theory of Computing, New York, A. V. Aho, ed., ACM, 1987, pp. 409–420, https://doi.org/10.1145/28395.28439.

[8] J. N. Bray, D. F. Holt, and C. M. Roney-Dougal, *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*, London Math. Soc. Lecture Note Ser. 407, Cambridge University Press, Cambridge, UK, 2013, https://doi.org/10.1017/CBO9781139192576.

[9] P. J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc., 13 (1981), pp. 1–22, https://doi.org/10.1112/blms/13.1.1.

[10] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*, Oxford University Press, Eynsham, UK, 1985.

[11] B. N. Cooperstein, *Minimal degree for a permutation representation of a classical group*, Israel J. Math., 30 (1978), pp. 213–235, https://doi.org/10.1007/BF02761072.

[12] J. D. Dixon and B. Mortimer, *Permutation Groups*, Grad. Texts in Math. 163, Springer-Verlag, New York, 1996, https://doi.org/10.1007/978-1-4612-0731-3.

[13] D. Gluck, A. Seress, and A. Shalev, *Bases for primitive permutation groups and a conjecture of Babai*, J. Algebra, 199 (1998), pp. 367–378, https://doi.org/10.1006/jabr.1997.7149.

[14] M. Grohe and D. Marx, *Structure theorem and isomorphism test for graphs with excluded topological subgraphs*, SIAM J. Comput., 44 (2015), pp. 114–159, https://doi.org/10.1137/120892234.

[15] M. Grohe, D. Neuen, P. Schweitzer, and D. Wiebking, *An improved isomorphism test for bounded-tree-width graphs*, in Proceedings of the 45th International Colloquium on Automata, Languages, and Programming, Prague, I. Chatzigiannakis, C. Kaklamanis, D. Marx, and D. Sannella, eds., LIPIcs Leibniz Int. Proc. Inform. 107, Schloss Dagstuhl Leibniz-Zentrum fuer Informatik, 2018, pp. 67:1–67:14, https://doi.org/10.4230/LIPIcs.ICALP.2018.67.

[16] W. M. Kantor and E. M. Luks, *Computing in quotient groups*, in Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, Baltimore, H. Ortiz, ed., ACM, 1990, pp. 524–534, https://doi.org/10.1145/100216.100290.

[17] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Ser. 129, Cambridge University Press, Cambridge, UK, 1990, https://doi.org/10.1017/CBO9780511629235.

[18] S. Kratsch and P. Schweitzer, *Graph isomorphism for graph classes characterized by two forbidden induced subgraphs*, Discrete Appl. Math., 216 (2017), pp. 240–253, https://doi.org/10.1016/j.dam.2014.10.026.

[19] M. W. LIEBECK, *On minimal degrees and base sizes of primitive permutation groups*, Arch. Math. (Basel), 43 (1984), pp. 11–15, https://doi.org/10.1007/BF01193603.

[20] M. W. LIEBECK AND A. SHALEV, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc., 12 (1999), pp. 497–520, https://doi.org/10.1090/S0894-0347-99-00288-X.

[21] M. W. LIEBECK AND A. SHALEV, *Bases of primitive linear groups*, J. Algebra, 252 (2002), pp. 95–113, https://doi.org/10.1016/S0021-8693(02)00001-7.

[22] M. W. LIEBECK AND A. SHALEV, *Bases of primitive linear groups* II, J. Algebra, 403 (2014), pp. 223–228, https://doi.org/10.1016/j.jalgebra.2014.01.011.

[23] D. LOKSHTANOV, M. PILIPCZUK, M. PILIPCZUK, AND S. SAURABH, *Fixed-parameter tractable canonization and isomorphism test for graphs of bounded treewidth*, in Proceedings of the 55th IEEE Annual Symposium on Foundations of Computer Science, Philadelphia, IEEE Computer Society, 2014, pp. 186–195, https://doi.org/10.1109/FOCS.2014.28.

[24] E. M. LUKS, *Isomorphism of graphs of bounded valence can be tested in polynomial time*, J. Comput. System Sci., 25 (1982), pp. 42–65, https://doi.org/10.1016/0022-0000(82)90009-5.

[25] E. M. LUKS, *Permutation groups and polynomial-time computation*, in Groups and Computation, Proceedings of a DIMACS Workshop, New Brunswick, NJ, L. Finkelstein and W. M. Kantor, eds., DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 11, DIMACS/AMS, 1991, pp. 139–175, https://doi.org/10.1090/dimacs/011/11.

[26] A. MARÓTI, *On the orders of primitive groups*, J. Algebra, 258 (2002), pp. 631–640, https://doi.org/10.1016/S0021-8693(02)00646-4.

[27] U. MEIERFRANKENFELD, *Non-finitary locally finite simple groups*, in Finite and Locally Finite Groups (Istanbul, 1994), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. 471, Kluwer, Dordrecht, 1995, pp. 189–212, https://doi.org/10.1007/978-94-011-0329-9_7.

[28] G. L. MILLER, *Graph isomorphism, general remarks*, J. Comput. System Sci., 18 (1979), pp. 128–142, https://doi.org/10.1016/0022-0000(79)90043-6.

[29] I. N. PONOMARENKO, *The isomorphism problem for classes of graphs closed under contraction*, J. Soviet Math., 55 (1991), pp. 1621–1643, https://doi.org/10.1007/BF01098279.

[30] J. J. ROTMAN, *An Introduction to the Theory of Groups*, 4th ed., Grad. Texts in Math. 148, Springer-Verlag, New York, 1995, https://doi.org/10.1007/978-1-4612-4176-8.

[31] A. SERESS, *Permutation Group Algorithms*, Cambridge Tracts in Math. 152, Cambridge University Press, Cambridge, UK, 2003, https://doi.org/10.1017/CBO9780511546549.