A Black Box Recognition Algorithm for Wreath Products

December 22, 2019

We present a one-sided Monte Carlo algorithm which, for a given black box group G, decides whether or not G is isomorphic to a wreath product $A_n \wr H$, where H is a transitive subgroup of the symmetric group on Γ and $n \geq 9$. If the algorithm proves G to be isomorphic to $A_n \wr H$, it will return an explicit isomorphism.

As the methods given in this thesis are mostly probabilistic, we rely on estimates of certain proportions of elements in wreath products $K \wr_\Gamma H$. In particular we show that the proportion of elements $g \in K \wr_\Gamma H$, which power to involutions in the base group, is at least as high as the proportion of elements of order divisible by 2 in K. As this and most other observations in this thesis do not require K to be a specific permutation group, this leaves room for generalizing the methods presented to other types of groups.

1 Introduction

2 Background

2.1 The Problem

2.2 Black Box Groups

The term *black box group* was introduced by Babai and Szemerédi in [1] and it refers to a way of representing a group within a computer where the black box performs the group operations. This is the most general representation of a group. The algorithm presented in this paper constructively recognizes a wreath product $A_n \wr_\Gamma H$ given as a black box group where $H \leq S_\Gamma$ transitive. Such an algorithm then works on $A_n \wr H$ given in any representation e.g. as matrices or permutations.

Definition 1. *A* black box group *is a group G whose elements are encoded as bit-strings of uniform length N. The black box can compute strings for gh and g^{-1} or decide whether $g = h$ for any $g, h \in G$.*

Note that each bit-string represents at most one element of G but an element of G can have multiple representations as bit-strings. Thus $|G| \leq 2^N$.

2.3 Notation

3 Outline of the Algorithm

noch 1:1 aus der MA

We briefly outline the steps of the algorithm described in this thesis. The goal is to constructively recognize a black box group G, given it is isomorphic to a wreath product $A_n \wr_\Gamma H$ with $H \leq S_\Gamma$ transitive.

INPUT: a black-box group $G = \langle X \rangle$ encoded as bit strings of uniform length N and a real number ϵ with $0 < \epsilon < 1$.

OUTPUT: an isomorphism $\varphi\colon G \to A_n \wr_\Gamma H$ if G is isomorphic to $A_n \wr_\Gamma H$ with $H \leq S_\Gamma$ transitive, else failure.

In the following description we assume that G is isomorphic to a wreath product $A_n \wr_\Gamma H$ with $H \leq S_\Gamma$ transitive. If this is not the case, then either one of the steps will fail, or the correctness check in Step 5 will report `false`. Further note that we repeat this sequence of steps multiple times, until we either find an isomorphism or with sufficiently high probability G is not isomorphic to a wreath product $A_n \wr_\Gamma H$ with $H \leq S_\Gamma$ transitive.

1. By taking random elements of G, find an element g such that $g^{\frac{|g|}{2}}$ is an element of the base group. As we are in a black box situation, we can not decide whether or not an element is in the base group. Thus we continue the computation until an error occurs. In that case we try with the next element, unless we have tried sufficiently many times such that we can be sure with probability at least $1 - \epsilon$ that G is not isomorphic to a wreath product $A_n \wr_\Gamma H$ with $H \leq S_\Gamma$ transitive. In Lemma 6 we show that for $n \geq 6$ the proportion of elements g in $A_n \wr_\Gamma H$ such that $g^{\frac{|g|}{2}}$ is an element of the base group is at least $\frac{3}{8}$.

2. With Lemma **??** we show that the only normal subgroups A of the base group $B \cong A_n^\Gamma$ are isomorphic to A_n^s with territory size s for $0 \leq s \leq |\Gamma|$. This also yields that, given H is transitive on Γ, the normal closure of an element of the base group under $A_n \wr_\Gamma H$ is equal to the base group. Having the base group computed, we try to reduce the size of the territory by taking random elements g of the current subgroup $A \cong A_n^s$ and computing the normal closure of $g^{\frac{|g|}{2}}$ under A. Lemma **??** shows that for $n \geq 6$ and $s \geq 2$ the proportion of elements g in A_n^s such that $g^{\frac{|g|}{2}}$ is in A_n^t for $1 \leq t < s$ is at least $\frac{1}{10}\frac{1}{\sqrt{n}}$. Hence we repeat this process until with sufficiently high probability we obtain a subgroup isomorphic S to A_n with singleton territory.

3. In Section **??** we show that the top group $(1_{A_n^\Gamma}, H)$ of $A_n \wr_\Gamma H$ acts on the singleton territories precisely as H acts on Γ. Thus, given a subgroup isomorphic

to A_n with singleton territory, we can determine a G-set $\Gamma' = \{S^{t_1}, \ldots, S^{t_m}\}$ for $t_1, \ldots, t_m \in G$. By the transitivity of H this set is in bijection to Γ. This way we can identify the top element of any $g \in G$.

4. We use the recognition algorithm by Jambor et al. 2013 [3] to check if S is isomorphic to an alternating group of degree $n \geq 9$ and determine n. If this is not the case we start from Step 1 again. As shown in Section **??**, we can use the results of the algorithm by Jambor et al. to construct a map φ from G to $A_n \wr_\Gamma S_\Gamma$. If indeed G is isomorphic to $A_n \wr_\Gamma H$ with $H \leq S_\Gamma$ transitive and $S \cong A_n$ is a single component subgroup, then φ is an isomorphism which we proceed to check in the next step.

5. As a last step we perform a correctness check and for now assume that we are uncertain, whether or not G is isomorphic to a wreath product $A_n \wr_\Gamma H$ with $H \leq S_\Gamma$ transitive. For this check we first compute the centralizer C in G of a "diagonal subgroup" $D^* = \{s^{t_1} \ldots s^{t_m} \mid s \in S\}$, as described in Section **??**. We check whether for all $i \in \{1, \ldots, m\}$ and $c \in C$ there is a $j \in \{1, \ldots, m\}$ such that $(s^{t_i})^c = s^{t_j}$ for all $s \in S$. If that is the case, then C acts on Γ' by Lemma **??** and by Corollary **??** we have $(\langle Y \rangle)\varphi = A_n \wr_{\Gamma'} C^{\Gamma'}$ for $\langle S^{t_1}, \ldots, S^{t_m}, C \rangle = \langle Y \rangle$. Further we compute the centralizer of $\langle S^{t_1}, \ldots, S^{t_m} \rangle$ in C and check if it is trivial, which is precisely the case when C acts faithfully on Γ' by Lemma **??**. In this case φ is an isomorphism from $\langle Y \rangle$ to $A_n \wr_{\Gamma'} C^{\Gamma'}$. Hence we found an isomorphism from G to $A_n \wr_{\Gamma'} C^{\Gamma'}$, precisely if $\langle Y \rangle = G$. Thus, for each generator g of G we compute the image under φ and compute the unique preimage in $\langle Y \rangle$ of $(g)\varphi$ under φ, which we can do efficiently, as shown in Sections **??** and **??**. If all generators of G equal their respective preimage, then Y generates G, which means φ passes the correctness test and we return `true` together with the isomorphism φ. Note that, if G is isomorphic to $A_n \wr_\Gamma H$ with $H \leq S_\Gamma$ transitive and $S \cong A_n$ is a single component subgroup, then φ is an isomorphism and S and φ pass the correctness check.

4 Proportions In Wreath Products

ab hier für Lemma 6

Definition 2. *Let K be a group and $q \in \mathbb{N}$. We define*

$$\mathrm{E}_{\neg q}(K) = \{k \in K \mid q \text{ does not divide } |k|\}$$
$$\text{and } \mathrm{E}_q(K) = \{k \in K \mid q \text{ divides } |k|\}.$$

das Lemma hier muss ohne die umständliche Notation auskommen, verweise auf ORE

Lemma 3. *Let $G = K \wr_\Gamma H$, $H \leq S_m$ and $\tilde{G} = K \wr_\Gamma S_\Gamma$. Then*

$$\frac{|\mathrm{E_B}(G)|}{|G|} \geq \frac{|\mathrm{E}_2(K)|}{|K|}.$$

Proof. For each $\pi \in H$ we construct a subset $\mathrm{E}_B(\pi)$ of $\mathrm{E_B}(G)$ containing only base elements with top element π, which has cardinality $|\mathrm{E}_2(K)||K|^{m-1}$. Then the disjoint union of said subsets has cardinality $|H||\mathrm{E}_2(K)||K|^{m-1}$, which yields the result. First let $1 \neq \pi \in H$ with disjoint cycle representation $\pi_1 \dots \pi_s$ ordered such that $|\pi_1|_2 \geq \dots \geq |\pi_s|_2$. Let

$$\begin{aligned}&\mathrm{E}_B(\pi)\\ =&\{c \in \mathrm{SC}_{\tilde{G}}(\pi_1) \mid (c)\,\mathrm{Det} \in \mathrm{E}_2(K^\Gamma)\} \times \mathrm{SC}_{\tilde{G}}(\pi_2) \times \dots \times \mathrm{SC}_{\tilde{G}}(\pi_s) \times B_{\neg\,\mathrm{supp}(\pi)}(G).\end{aligned}$$

First we show that $\mathrm{E}_B(\pi)$ is a subset of $\mathrm{E_B}(G)$. For $g \in \mathrm{E}_B(\pi)$ we can write g as product of disjoint strongly caged elements such that $c_i = (f_i, \pi_i)$ where $\pi_i = 1_H$ for $s+1 \leq i \leq \ell$. By Lemma **??** and the way we ordered the cycles we have

$$\begin{aligned}2\,\mathrm{LCM}(|\pi_1|, \dots, |\pi_s|) &= \mathrm{LCM}(2|\pi_1|, \dots, |\pi_s|)\\ \text{divides } \mathrm{LCM}(|(c_1)\,\mathrm{Det}||\pi_1|, \dots, |(c_\ell)\,\mathrm{Det}||\pi_\ell|) &= |g|.\end{aligned}$$

Hence $c_i^{\frac{|g|}{2}} \in B$ by Lemma **??** and thus $g \in \mathrm{E}_B$.

To show $\mathrm{E}_B(\pi)$ has the desired cardinality we fix a $\gamma \in \mathrm{supp}(\pi_1)$. By Corollary **??** we have $|(c_1)\,\mathrm{Det}| = |(c_1)\,\mathrm{Det}_\gamma|$ and thus $\{c \in \mathrm{SC}_{\tilde{G}}(\pi_1) \mid (c)\,\mathrm{Det} \in \mathrm{E}_2(K^\Gamma)\} = \{c \in \mathrm{SC}_{\tilde{G}}(\pi_1) \mid (c)\,\mathrm{Det}_\gamma \in E_2(K)\}$. Hence by Lemma **??** we have $|\mathrm{E}_B(\pi)| = |\mathrm{E}_2(K)||K|^{m-1}$.

Otherwise, for $\pi = 1_H$ let

$$\mathrm{E}_B(1_H) = \{c \in \mathrm{SC}_{\tilde{G}}(1_H) \mid (c)\,\mathrm{Det}_1 \in \mathrm{E}_2(K)\} \times B_{\neg\{1\}}(G).$$

We have $|\{c \in \mathrm{SC}_{\tilde{G}}(1_H) \mid (c)\,\mathrm{Det}_1 \in \mathrm{E}_2(K)\}| = |\mathrm{E}_2(K)|$ and thus $|\mathrm{E}_B(1_H)| = |\mathrm{E}_2(K)||K|^{m-1}$. Further $\mathrm{E}_B(1_H) \subseteq \mathrm{E}_\mathrm{B}(G)$ as $\mathrm{E}_B(1_H) \subseteq B$ and 2 divides any element of $\mathrm{E}_B(1_H)$. Finally, for $\pi, \sigma \in H$ with $\pi \neq \sigma$ we have $\mathrm{E}_B(\pi) \cap \mathrm{E}_B(\sigma) = \emptyset$ as $\mathrm{E}_B(\pi)$ and $\mathrm{E}_B(\sigma)$ contain exclusively elements with top element π and σ respectively.

Together this yields

$$|\mathrm{E}_\mathrm{B}(G)| \geq \sum_{\pi \in H} |\mathrm{E}_{B_\pi}| = \sum_{\pi \in H} |\mathrm{E}_2(K)||K|^{m-1} = |H||\mathrm{E}_2(K)||K|^{m-1}$$

and thus

$$\frac{|\mathrm{E}_\mathrm{B}(G)|}{|G|} = \frac{|\mathrm{E}_\mathrm{B}(G)|}{|G|} \geq \frac{|H||\mathrm{E}_2(K)||K|^{m-1}}{|H||K|^m} = \frac{|\mathrm{E}_2(K)|}{|K|} = \frac{|\mathrm{E}_2(K)|}{|K|}.$$

□

Theorem 4. *Let $q \geq 2$ and $n \geq 1$*
$\frac{|\mathrm{E}_{\neg q}(S_n)|}{|S_n|} = \prod_{\ell=1}^{\lfloor \frac{n}{q} \rfloor}(1 - \frac{1}{\ell q})$.

Proof. See [2, Theorem 2.3 (a),p.4]. □

The proportion of elements not divisible by 2 within A_n is precisely double the corresponding proportion in S_n as the following Corollary shows.

Corollary 5. *Let $n = 2m + r \geq 2$, where $0 \leq r \leq 1$. Then*

$$\frac{|\mathrm{E}_{\neg 2}(A_n)|}{|A_n|} = 2\frac{|\mathrm{E}_{\neg 2}(S_n)|}{|S_n|}.$$

Proof. By [2, Theorem 3.3 (a), p.8] we have

$$\begin{aligned}\frac{|\mathrm{E}_{\neg 2}(A_n)|}{|A_n|} &= \frac{|\mathrm{E}_{\neg 2}(S_n)|}{|S_n|} + (-1)^{2\lfloor \frac{n}{2} \rfloor} \prod_{\ell=1}^{\lfloor \frac{n}{2} \rfloor}(1 - \frac{1}{2\ell}) \\ &= \frac{|\mathrm{E}_{\neg 2}(S_n)|}{|S_n|} + \prod_{\ell=1}^{\lfloor \frac{n}{2} \rfloor}(1 - \frac{1}{2\ell}) = 2\frac{|\mathrm{E}_{\neg 2}(S_n)|}{|S_n|}.\end{aligned}$$

□

Lemma 6. *Let $n \geq 6$, $G = A_n \wr_\Gamma H$ and $H \leq S_m$. Then $\frac{|\mathrm{E}_\mathrm{B}(G)|}{|G|} \geq \frac{3}{8}$.*

Proof. As $\mathrm{E}_2(A_n) = A_n \setminus \mathrm{E}_{\neg 2}(A_n)$ we have with Lemmata 3, 4 and 5 that

$$\begin{aligned}\frac{|\mathrm{E}_{\mathrm{B}}(G)|}{|G|} &\geq \frac{|\mathrm{E}_2(A_n)|}{|A_n|} = 1 - \frac{|\mathrm{E}_{\neg 2}(A_n)|}{|A_n|} = 1 - 2\frac{|\mathrm{E}_{\neg 2}(S_n)|}{|S_n|} \\ &= 1 - 2\prod_{\ell=1}^{\lfloor \frac{n}{2} \rfloor}(1 - \frac{1}{2\ell}) \geq 1 - 2\prod_{\ell=1}^{\lfloor \frac{6}{2} \rfloor}(1 - \frac{1}{2\ell}) \\ &= 1 - 2(1 - \frac{1}{2})(1 - \frac{1}{4})(1 - \frac{1}{6}) = 1 - \frac{10}{16} = \frac{6}{16} = \frac{3}{8}.\end{aligned}$$

□

References

[1] László Babai and Endre Szemerédi. "On the complexity of matrix group problems I". In: *25th Annual Symposium onFoundations of Computer Science, 1984.* IEEE. 1984, pp. 229–240.

[2] Robert Beals et al. "Permutations with restricted cycle structure and an algorithmic application". In: *Combinatorics, Probability and Computing* 11.5 (2002), pp. 447–464.

[3] Sebastian Jambor et al. "Fast recognition of alternating groups of unknown degree". In: *Journal of Algebra* 392 (2013), pp. 315–335.