PRIMITIVE GROUPS ACTIONS AND GROUPS DESCRIPTIONS

GUSTAVO DE PAULA
SUPERVISED BY ANDRÉ NIES

Abstract. We say a group action is primitive if it does not preserve a partition on its action domain. We show that any group action can be decomposed in primitive group actions. We are also going to prove a better version of the reachability theorem presented by Babai and Szemerédi in [4].

1. Introduction

It is already known that some groups can be described in first-order language [1], in other worlds, there is a first-order sentence ϕ such that G is a model of ϕ up to isomorphism. In finite cases ϕ can be a description of the group table, it is easy to do but it is very inefficient because that way $|\phi| = O(|G|^2)$.

In [2] and [3] it was shown how to make shorter group description, usually of polylogarithmical size, i.e., of size $O(log^n(|G|))$. There are two possible ways to develop the subject, we can make the group descriptions even shorter or we can find a way to describe other structures related to group theory in first-order logic. We are going to show results for both situations.

We are going to show a better version of the reachability theorem that was first proved in [4] and used in [2]. It creates a more efficient set of generators for a group. We are also going to prove a way to decompose a group action into primitive group actions, we believe it can be used to describe group actions in first-order logic.

2. Reachability Theorem

Definition 2.1. Let G be a group generated by a subset S, a straight-line program is a sequence $L = (g_1, g_2, g_3, ..., g_n)$ where for $i \leq n$:

(1) $g_i \in S$ or
(2) $g_i = g_m \cdot g_n$ for $m, n < i$ or
(3) $g_i = {g_m}^{-1}$ for $m < i$.

We say that g_i is generated by L and we define the straight-line cost of some $g \in G$ to be length of the shortest straight-line program containing g.

Reachability Theorem 2.2. Given a group G of order n and a set S of generators, the straight-line cost of any element of G is $\leq log(n)^2 + log(n)$.

The proof of this theorem is due by creating a subset $Z(s)$ of G such that any $g \in G$ can be generated from it in at most $2i$ steps. This set is not mentioned in the statement of the theorem but it was used by Nies and Tent in [2] to create a existential first-order formula stating that $g \in < s_1, s_2, \cdots, s_r >$, $s_i \in G$.

Proof. We shall define recursively a set $Z(s) = \{z_1, z_2, z_3, \cdots, z_s\} \subset G$.

Let $Z(i) = \{z_j : j \leq i\}$, $K(i) = \{z_1^{\alpha_1}.z_2^{\alpha_2} \cdots z_i^{\alpha_i} : \alpha_j \in \{0,1\}\}$ and let $c(i)$ be the length of the shortest straight-line program that contains $Z(i)$.

We consider $K(0) = \{1\}$ and $c(0) = 0$.

- If $K(i)^{-1}K(i) = G$ we define $s = i$ and stop.
- Else we choose $z_i+1 \in G - K(i)^{-1}K(i)$ that minimizes $c(i+1)-c(i)$.

Claim 1. *If $i < s$ then $|K(i+1)| = 2|K(i)|$.*

Proof. Clearly $|K(i+1)| \leq 2|K(i)|$.

Suppose $|K(i+1)| < 2|K(i)|$, then by the pigeonwhole principle there are $k_1, k_2 \in K(i+1)$ with $k_1 = k_2$.

$k_1 = z_1^{\alpha_1}.z_2^{\alpha_2} \cdots z_{i+1}^{\alpha_{i+1}} = z_1^{\beta_1}.z_2^{\beta_2} \cdots z_{i+1}^{\beta_{i+1}} = k_2$ with $\alpha_j, \beta_j \in \{0,1\}$.

Let k be the biggest integer such $\alpha_k \neq \beta_k$, assuming that $\alpha_k = 1$. We have $z_k = z_{k-1}^{-\alpha_{k-1}} \cdots z_2^{-\alpha_2}.z_1^{-\alpha_1}.z_1^{\beta_1}.z_2^{\beta_2} \cdots z_{k-1}^{\beta_{k-1}}$, then $z_k \in K(k-1)^{-1}K(k-1)$ which is a contradiction, therefore $|K(i+1)| \geq 2|K(i)|$ and $|K(i+1)| = 2|K(i)|$. □

Corollary 2.3. *$s \leq log(|G|)$.* □

Claim 2. *$c(i+1) - c(i) \leq 2i$.*

Proof. Since the Cayley graph of G is connected and $K(i)^{-1}K(i) \neq G$ for $i < s$, there is an element of the form $q.r \in G - K(i)^{-1}K(i)$, $q \in K(i)^{-1}K(i)$, $r \in S$. Let us define $z_{i+1} = q.r$.

For any $k \in K(i)$, at most i steps are needed to generate k from the straight-line program that generated z_i because k is the product of at most i elements of the straight-line program.

It takes at most $2i$ steps to generate $q \in K(i)^{-1}K(i)$. There is no point in generating the element of maximum length because it is the identity, $2i-1$ steps are enough. To generate $q.r \in G - K(i)^{-1}K(i)$ $2i$ steps are sufficient. □

Corollary 2.4. *$c(i) \leq i^2 - i$.*

Since $K(s)^{-1}K(s) = G$, any $g \in G$ can be written in the form $g = k_1^{-1}k_2$, $k_1, k_2 \in K(s)$. We need $s^2 - s$ steps to generate $Z(s)$ and another $2s-1$ steps to generate g from $Z(s)$.

For any $g \in G$, $c(g) \leq s^2 + s - 1 \leq log(n)^2 + log(n)$.

This version of the reachability theorem has a better upper bound than the original version from Babai and Szemerdi. The original upper bound was $(1 + log(|G|))^2$. This change is due to the claim 2, where we had $c(i+1) - c(i) \leq 2i$ while Babai and Szemerdi had $2i+1$. This upper bound improvement raised the question if it is possible to improve it even more.

During our work we had two ideas about how to improve the upper bound:

The first idea is a detail on the first corollary, which states that $s \leq log(|G|)$ because $|K(s)| = |G|$, therefore $K(s) = G$ and then $K(s)^{-1}K(s) = G$.It can be understood as $|K(i)| = 2^i$ being used as a lower bound to the size of

$K(i)^{-1}K(i)$, if some lower bound for the size of $K(s)^{-1}K(s)$ bigger than $|K(s)|$ is provable, we could use it to reduce the value of s and then reduce the upper bound of the theorem.

The second idea is to create reachability theorems for specific cases. For example, in the abelian case with independent set of generators it is possible to prove a version of the theorem with $3.log(|G|)$ as the new the upper bound, but we did not find a way to prove it for broader cases.

2.1. Gradual Reachability theorem.

Let's consider a case where you not only need a efficient generator set for the group G but you need efficient generators sets for a sequence of subsets of G, each one included in the next.

Let $cost(A|T)$ be the length of the shortest straight line program computing A from T.

Theorem 2.5. *Let G be a group, S a set of generators of G and $T_1 \subset T_2 \subset \cdots \subset T_k \subset G$. There are $Z_1 \subset Z_2 \subset \cdots Z_k \subset G$ such $cost(Z_i|S) \leq log(|T_i|)^2$ and $t \in T_i$ can be generated from Z_i in at most $2.log(|T_i|)$ steps.*

Proof. The proof is similar to the usual reachability theorem:

The definition of $K(i), c(i)$ are the same as in the usual reachability theorem. We only change the recursion that defines $Z(s)$.

We consider $K_0(0) = \{1\}$, $c(0) = 0$ and initially $j = 1$.

- While $T_j \subset K(i)^{-1}K(i)$ we define $Z_j = Z(i)$ and $j = j + 1$.
- If $K(i)^{-1}K(i) = G$ we define $s = i$ and stop.
- If there is $g \in T_{j+1} - K(i)^{-1}K(i)$ such the cost to compute g from $Z(i)$ is less than $2i$, define $z_{i+1} = g$.
- Else we choose $z_{i+1} \in G - K(i)^{-1}K(i)$ that minimizes $c(i+1) - c(i)$.

□

There are no major difference in its proof when compared with the usual theorem. It is important to notice that it is possible to have $Z_i = Z_{i+1}$ for $i < k$. That is the reason for us to have a *while* loop instead of another if.

3. Reachability algorithm

The algorithm 1 uses the group table and S as inputs to build the set Z(s) as stated in the theorem 2.2. It is interesting to change the computational context from straight line programs to the usual computational structure. This algorithm is largely based on Dijkstra algorithm for graphs and it runs in polynomial time.

4. Primitive actions

The main theorem of this section shows that it is possible to decompose a finite group action $X \curvearrowleft G$ into primitive actions over partitions of X. Our initial inspirations was to build a group action decomposition similar to the composition series of groups, but instead of simple groups there are primitive actions as factors.

The motivation was to make possible to describe a primitive action using first-order logic. We found out that given a group action, the action decompositions are possible but not always unique.

```
[Reachability algorithm]
Data: Group table and S
Result: The set of generators Z(s);
cost[$e$]=0
add e to Q //Q=$K(i)^{-1}K(i)$
for $g \in G$ do
    if $g \neq e$ then
        cost[$g$] = $|G|$// cost[g] is the straight-line cost of g
        add $g$ to $J$// J=$G - K(i)^{-1}K(i)$
    end
end
for $s \in S$ do
    cost[$s$] = 1
end
while $J \neq \emptyset$ do
    $h$ = element in $J$ with min $cost[h]$
    add $h$ to $Z$
    for $q \in Q$ do
        if $kh \in J$ then
            remove $kh$ from $J$
            add $kh$ to $Q'$
        end
        if $h^{-1}k \in J$ then
            remove $h^{-1}k$ from $J$
            add $h^{-1}khtoQ'$
        end
        if $h^{-1}kh \in J$ then
            remove $h^{-1}kh$ from $J$
            add $h^{-1}kh$ to $Q'$
        end
    end
    for $q \in Q'$ do
        add $q$ to $Q$
        remove $q$ to $Q'$
    end
    for $q \in Q$ do
        for $s \in S$ do
            if $cost[qs] < cost[q] + 1$ then
                $cost[qs] = cost[q] + 1$
            end
            if $cost[sq] < cost[q] + 1$ then
                $cost[sq] = cost[q] + 1$
            end
        end
    end
end
return Z
```

Algorithm 1: How to generate Z(s) from the group table and the set of generators

Before introducing the concept of primitive group actions, it is necessary to define what is a group action.

Definition 4.1. Let G be a group and $\mathcal{M}$ be a set, named as action domain, we say that G acts on M iff for $m \in \mathcal{M}$, $g_1, g_2 \in G$, we have that $mg_1, mg_2 \in \mathcal{M}$, $(mg_1)g_2 = m(g_1 \cdot g_2)$ and $me = m$.

The concept of group actions can look complicated at first sight, but examples of it are presented to algebra students when they are first introduced to the concept of groups without naming it as actions.

Our initial examples of groups are the symmetries of polygons and permutations over finite sets. The connection of the symmetry group and the set of vertices of the polygon can be described as a group action. In the same way the connection between the permutation group and the set it is permuting can be described a a group action.

Three definitions that we are going to use:

Definition 4.2. A group action $X \curvearrowleft G$ is called transitive iff for any $x, y \in X$, there is $\pi \in G$ such $x = y\pi$.

Definition 4.3. Let G be a group acting on a set X. The stabilizer of $x \in X$ is $G_x = \{g \in G | xg = x\}$.

Definition 4.4. Let G be a transitive permutation group over X, we say $Y \subset X$ is a domain of imprimitivity iff $1 < |Y| < |X|$ and $\forall g \in G$, $Yg = Y$ or $Yg \cap Y = \emptyset$.

Theorem 4.5. *Let G be a transitive permutation group over X and Y be an domain of imprimitivity of X.*

(1) *$E = \{Yg : g \in G\}$ is a partition of X.*
(2) *$[x]_E g = [xg]_E$ for $x \in X$ and $g \in G$.*
(3) *The elements of E have size $|Y|$.*

Proof. (1) Since G is transitive over X then $\bigcup_{E_i \in E} E_i = X$.

Let $H = \{g | Yg = Y, g \in G\}$, since G is transitive and Y is a domain of imprimitivity, $yH = Y$ for $y \in Y$.

Suppose $x \in Yg_1 \cap Yg_2$, for $g_1, g_2 \in G$. There are $y_1, y_2 \in Y$ such $y_1 g_1 = x = y_2 g_2$, then $y_1 = y_2 g_2 g_1^{-1}$ therefore $g_2 g_1^{-1} \in H$ and $g_2 \in Hg_1$. That way, we have that $Yg_1 = y_1 H g_1 = y_1 H g_2 = Yg_2$ and therefore E is a partition of X.

(2)Clearly $[y]_E g = [yg]_E$ for $y \in Y$.

Let $x \in X$, then there is $\pi \in G$ such $y\pi = x$ for $y \in G$. Then $[x]_E g = [y\pi]_E g = ([y]_E \pi) g = [y]_E (\pi g) = [y\pi g]_E$

(3)It follows directly from the fact that G is a permutation group over X and, therefore, a bijection. □

Using the previous theorem and definition it is possible to understand a domain of imprimitivity as a element of a partition of X that is G-invariant.

When you have a group acting on itself by right multiplication, you can understand a sub-group and its co-sets as domains of imprimitivity. We will show more examples later on.

It is possible to notice that (3) let us make a connection between the size of the action domain and the domains of imprimitivity. A straightforward consequence of that any action over a action domain with prime size has no domain of imprimitivity and, as stated in the following definition, the action is primitive.

Definition 4.6. A transitive group action of a group G over a finite set X is primitive iff G has no domain of imprimitivity.

The definition of primitive action is adequate, but it can be hard to prove it directly, so we have a theorem that helps us do it.

Theorem 4.7. *A transitive group action of a group G over a finite set X is primitive iff G_a is maximal for every $a \in X$.*

Proof. Suppose G_a is not maximal, so there is H with $G_a < H < G$.

We claim $Y = aH$ is a domain of imprimitivity. Since $G_a < H$, $|aH| \geq 2$.

Since G is transitive, for any $x \in X$ $x = ag$ for some $g \in G$. Suppose $Y = X$, then for any $g \in G$ there is $h \in H$ such $ag = ah$, therefore $a = ahg^{-1}$ and then $hg^{-1} \in G_a$. So we have $H = G$, which is a contradiction.

Let $y \in Y \cap Yg$, then there are $h_1, h_2 \in H$ such $y = ah_1 = ah_2g$ then $a = ah_2gh_1^{-1}$ and therefore $g \in H$ and finally $Y = Yg$.

Conversely, suppose G has a domain of imprimitivity Y.

Let $H = \{r : Yr = Y\}$. We may suppose $a \in Y$, so $G_a \leq H$. Y is a domain of imprimitivity, then $|Y| > 1$ so there is $b \in Y$ with $b \neq a$. G is transitive then there is $\pi \in G$ such $a\pi = b$. Since Y is a domain of imprimitivity, $Y\pi = Y$ then $\pi \in H - G_a$ and $G_a < H$.

Since $|Y| < |X|$ and G is transitive, there is $\pi \in G$ such $a\pi \notin Y$. Therefore $\pi \notin H$, $H < G$.

That way, there is H such $G_a < H < G$. □

Corollary 4.8. *Let G be a permutation group over a finite set X and H such $G_a < H < G$ with $a \in X$ then $aH = \{ah : h \in H\}$ is a domain of imprimitivity.*

Another equivalent definition of primitive action that is commonly used is:

Theorem 4.9. *Let G be a transitive permutation group over a finite X. G is primitive iff any non-diagonal orbit of $X^2 \curvearrowleft G$ describe a connected graph on X.*

Proof. Suppose there is an non-diagonal orbit $\{x, y\}G$ of $(x, y) \in X^2$ that describes a not connected graph. We want to prove that the connected component $C_x \subset X$ containing x is a domain of imprimitivity.

Since $\{x, y\}G$ is not connected, $C_x \neq X$. We claim that C_xg is connected and C_x is a domain of imprimitivity.

Take $c_1g, c_2g \in C_xg$, there is a path λ connecting c_1 to c_2, that way λg connects c_1g to c_2g and therefore C_xg is connected.

Let $z \in C_x \cap C_xg$, since C_xg is connected, any element of C_xg is connected to z and z is connected to x. We have that $C_xg = C_x$ and C_x is a domain of imprimitivity.

Suppose there is some domain of imprimitivity $Y \subset X$ and let $x, y \in Y$, $x \neq y$. Let ω be the graph described by $\{x, y\}G$.

We claim that there is some $z \in X$ that is not connected to x by ω. Take $z \in X - Y$, suppose there is a path

$$\{x,y\} = \{x,y\}g_0, \{x,y\}g_1, ..., \{x,y\}g_n = \{xg_n, z\}$$

of ω connecting x to z. We are going to prove by induction that $z \in Y$:

By hypothesis, $\{x,y\} \subset Y$, since $\{x,y\} \cap \{x,y\}g_1 \neq \emptyset$ and Y is a domain of imprimitivity, then $\{x,y\}g_1 \subset Y$.

Similarly, $\{x,y\}g_i \subset Y$ implies $\{x,y\}g_{i+1} \subset Y$. Therefore $\{xg_n, z\} \subset Y$ and $z \in Y$ which is a contradiction.

That way, ω is not connected. □

Iwasawa's Lemma is an important criterion to show that a finite group is simple, in [5] it was used to prove that $SL_n(q)$, $F_4(q)$, $E_6(q)$ and others groups are simple.

The version of the lemma we state here does not mention the group being simple, the version that does has the hypothesis of G being perfect,i.e., equals to the commutator subgroup.

Iwasawa's Lemma 4.10. Let G be a primitive permutation group over X. Suppose that for some $a \in X$, G_a contains a abelian subgroup A such $A \lhd G_a$ whose conjugates in G generate all of G. Then any nontrivial subgroup $N \lhd G$ contains the commutator subgroup of G.

Proof. Suppose N is a nontrivial normal subgroup of G then there is $a \in X$ such $N \not\subset G_a$. Suppose there isn't such a, then $N \subset G_x, \forall x \in X$ which is a contradiction since G acts faithfully on X.

By 4.7 G_a is maximal, then $NG_a = G$. Let A be a normal subgroup of G_a as stated in Iwasawa's Lemma. For any $g \in G$, $g = n.k$, $n \in N$,$k \in G_a$. Then

$$gAg^{-1} = nkAk^{-1}n^{-1} = nAn^{-1} \subset NAN = NA$$

Since the conjugates of A generate all G, $NA = G$.

By the second isomorphism theorem $G/N \cong NA/N \cong A/(N \cap A)$

Since $A/(N \cap A)$ is abelian, $N \cap A$ contains the commutator subgroup and therefore N also contains it. □

4.1. **Primitive decomposition.**

Definition 4.11. Two group actions $U_i^x = S_1 \curvearrowleft G_1$ and $U_i^y = S_2 \curvearrowleft G_2$ are equivalent iff there is a bijection $\theta : S_1 \to S_2$ and a group isomorphism $\phi : G_1 \to G_2$ such $\forall s \in S_1$, $\forall g \in G_1$, $\theta(s \cdot g) = \theta(s).\phi(g)$.

Theorem 4.12. *Let G be a group transitivily acting on a set X. Let*

$$G_a = H_0 < H_1 < \cdots < H_n = G$$

be a sequence of subgroups of G such that H_{i-1} is maximal on H_i for $i > 0$. Then

1. $[x]_{E_i \big/ E_{i-1}} \curvearrowleft H_i$ *is a primitive action and*
2. $[a]_{E_i \big/ E_{i-1}} \curvearrowleft H_i$ *is equivalent to* $[b]_{E_i \big/ E_{i-1}} \curvearrowleft H_i^p$,

where $E_i := \{aH_ig : g \in G\}$, $b = ap$ with $a, b \in X$ and $p \in G$.

Proof. (1) By definition: $[x]_{E_i} = \{aH_ig : x = ag, g \in H_i\}$ and

$$[x]_{E_i \big/ E_{i-1}} = \{aH_{i-1}h : h \in H_i\}.$$

H_{i-1} is the stabilizer of the action and since it is maximal in H_i the action is primitive.

(2) We have that $y = xp, p \in G$. Let $\theta : X \to X$ and $\phi : G \to G$ behaving like in the diagram:

$$\begin{tikzcd}
{[a]}_{E_i/E_{i-1}} \arrow[d, "\theta : x \mapsto xp"'] & H_i \arrow[l, bend right] \arrow[d, "\phi : g \mapsto g^p"] \\
{[b]}_{E_i/E_{i-1}} & H_i^p \arrow[l, bend right]
\end{tikzcd}$$

Remark 4.13. $[x]_{E_i/E_{i-1}} = \{aH_{i-1}h : h \in H_i\}$

By 4.8 we have that aH_j with $1 < j < n$ is a domain of imprimitivity. By 4.5 E_j is a partition with $[x]_{E_j}g = [xg]_{E_j}$

Let $\alpha = aH_{i-1}k \in [a]_{E_i/E_{i-1}}$ and $g \in G$. Then:

$$\begin{aligned}
\theta(\alpha) &= aH_{i-1}hp \\
&= aH_{i-1}pp^{-1}hp \\
&= aH_{i-1}p\phi(h) \\
&= [a]_{E_{i-1}}p\phi(h) \\
&= [ap]_{E_{i-1}}\phi(h) \\
&= [b]_{E_{i-1}}\phi(h)
\end{aligned} \tag{1}$$

$$\begin{aligned}
\theta(\alpha g) &= aH_{i-1}hgp \\
&= aH_{i-1}pp^{-1}hpp^{-1}gp \\
&= aH_{i-1}p\phi(h)\phi(g) \\
&= [a]_{E_{i-1}}p\phi(h)\phi(g) \\
&= [ap]_{E_{i-1}}p\phi(h)\phi(g) \\
&= [b]_{E_{i-1}}\phi(h)\phi(g) = \theta(\alpha)\phi(g)
\end{aligned} \tag{2}$$

□

4.2. **Examples of decompositions.** We intend to show three examples of primitive decomposition using the alternating group A_4.

Example 4.14. *The simplest example is A_4 permuting a set X with 4 elements as induced by S_4. In this case, the stabilizer of any element is a isomorphic copy of Z_3 and maximal, so the action is primitive. In this case, our decomposition is trivial.*

Example 4.15. *Let $H < S_6$,$H =< (34)(56), (12)(56), (135)(246) >$ acting on $X = \{1, 2, 3, 4, 5, 6\}$.*

Clearly $J =< (34)(56), (12)(56) >\cong Z_2^2$. Take $\alpha = (135)(246)$ since J is small, it is not hard to calculate and see that $\alpha^{-1}J\alpha = J$ and therefore $J \lhd$

$H.J$, $J\alpha$ and $J\alpha^2$ are the only coset, therefore $|H| = 12$. Taking $(34)(56) = \beta$, $(12)(56) = \alpha^2\beta\alpha$, we can now compute that H satisfy the presentation of A_4: $< \alpha, \beta | \alpha^3, \beta^2, (\alpha\beta)^3 >$, therefore $A_4 \cong H$.

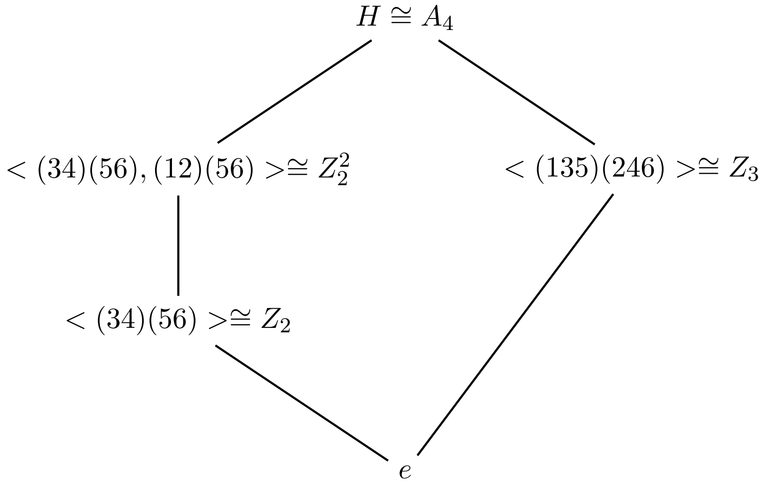

$H \cong A_4$
$< (34)(56), (12)(56) >\cong Z_2^2$
$< (135)(246) >\cong Z_3$
$< (34)(56) >\cong Z_2$
e

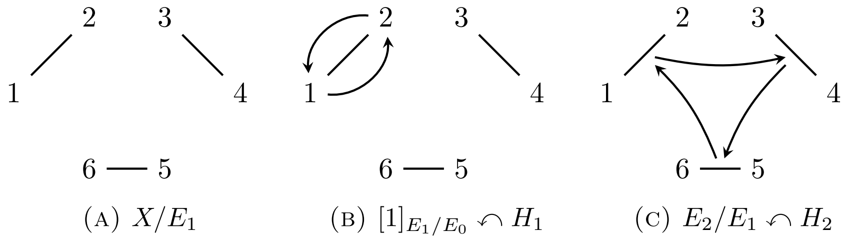
FIGURE 1. Subgroup Lattice of $A_4 < S_6$

Not all subgroups of H are represented in the lattice, but any other subgroup is isomorphic to those represented.

It is clear that $< (34)(56) >\cong Z_2$ is the stabilizer of $1 \in X$, since it is not maximal H does not act primitivily on X.

Using 4.12 we have that $Z_2 < Z_2^2 < H$ is a chain of submaximal subgroups as described by 4.12, X/E_0 and $X/E2$ are trivial partitions.

The other partition and the group actions that arise from the theorem can be represented like this:



(A) X/E_1 (B) $[1]_{E_1/E_0} \curvearrowleft H_1$ (C) $E_2/E_1 \curvearrowleft H_2$

FIGURE 2. Primitive decomposition of $A_4 < S_6$

Example 4.16. *Let A_4 acting on itself by right multiplication.*

Clearly $\{e\}$ is the stabilizer of any $a \in A_4$. Looking at figure 1 we see that it is possible to choose two different chains of submaximal subgroups:

$$G_a = H_0 < Z_2 < Z_2^2 < A_4 = H_3 \text{ and}$$
$$G_a = K_0 < Z_3 < A_4 = K_2$$

Since they have different lengths they give us two different decompositions, one decompose the action into 3 primitive actions while the other decompose it into 2 primitive actions.

We can represent the two different action decomposition as follows:

$[x]_{E_1/E_0} \curvearrowleft H_1$ is a permutation between the two elements of $[x]_{E_1/E_0}$, represented as edges in Figure 3:

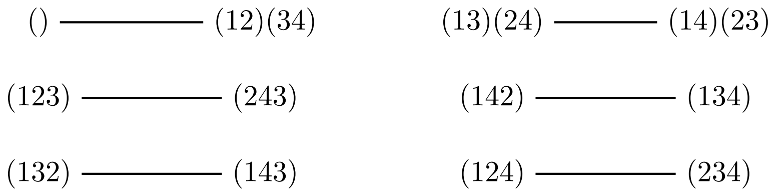


Figure 3. X/E_1

$[x]_{E_2/E_1} \curvearrowleft H_2$ is a permutation between the two elements of $[x]_{E_2/E_1}$, represented as ellipses in Figure 4:

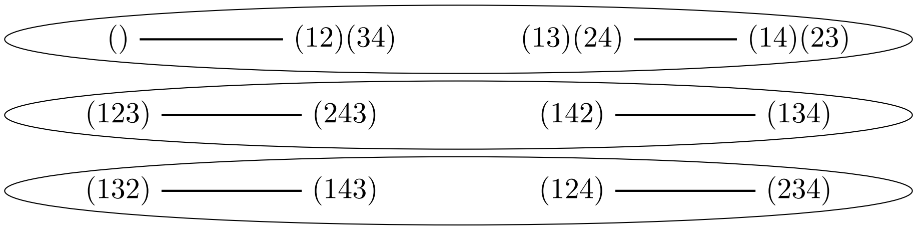


Figure 4. X/E_2

$[x]_{E_3/E_2} \curvearrowleft H_3$ is equivalent to Z_3 acting on itself by right multiplication, that is also equivalent to action described in 4.15.

Let F_i be the partition generated by K_i as described by 4.12. X/F_1 can be represented as:

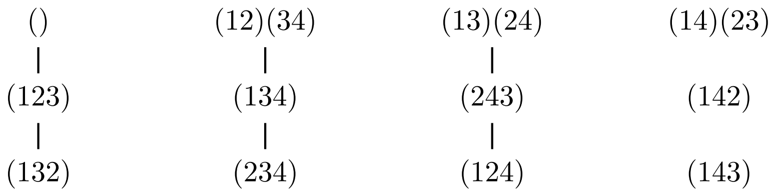


Figure 5. X/F_1

$[x]_{F_1/F_0} \curvearrowleft K_1$ is equivalent to Z_3 acting on itself by right multiplication.

$[x]_{F_2/F_1} \curvearrowleft K_2$ is equivalent to Z_2^2 acting on itself by right multiplication.

To study the relation between different decompositions of a same action or the conditions for uniqueness of the decomposition might be a good way to understand better group actions and their decompositions.

References

[1] André Nies. Describing Groups. *Bull. Symb. Logic. 13 no 3 (2007), 305-339.* 1

[2] André Nies and Katrin Tent. Describing finite groups by short first-order sentences. *To be published* 1, 2

[3] Yuki Maehara. Describing groups using first-order language. *arXiv:1305.0080 [math.GR]* 1

[4] László Babai and Endre Szemerédi. On the complexity of matrix group problems I.*Proceedings of 25th Annual Symposium on Foundations of Computer Science* 1

[5] Robert A. Wilson. The Finite Simple Groups. *Springer Science & Business Media, 2009* 4