Advanced Algorithms (IV)

Yijia Chen
Fudan University
Luks’ Group-Theoretic Algorithm
The basic idea

Assume $G_1$ and $G_2$ are both connected. We let $G := G_1 \cup G_2$.

$G_1$ and $G_2$ are isomorphic if and only if there is an automorphism $\sigma$ of $G$ such that $\sigma(G_1) = G_2$.

If such automorphisms exist, then any set of generators of $\text{Aut}(G)$ contains at least one of them. Here $\text{Aut}(G)$ is the set of all automorphisms of $G$. 
A group $K = (K, \cdot, 1)$ satisfies the following conditions.

1. **[associativity]** for all $x, y, z \in K$ we have $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

2. **[identity]** $x \cdot 1 = 1 \cdot x = x$ for all $x \in K$.

3. **[inverse]** For every $x \in K$ there exists a $y \in K$ with $x \cdot y = y \cdot x = 1$, i.e., $y = x^{-1}$.

**Example**
Let $n \in \mathbb{N}$. Then all the permutations on $[n]$ form a group with $\cdot$ being the function composition and $1$ the identity mapping. Denote this group by $S_n$.

Let $\text{Sym}(A)$ be the group of all permutations on the set $A$. 
Let $K$ be a group and $S \subseteq K$. We say that $S$ is a set of generators for $K$ if for every $a \in K$ there are $b_1, \ldots, b_m \in K$ with $m \geq 1$ such that

1. $a = b_1 \cdot b_2 \cdots b_m$, and

2. $b_i \in S$ or $b_i^{-1} \in S$ for all $i \in [m]$.

In notation, $K = \langle S \rangle$. 
Groups of graph automorphisms

Let $G = (V, E)$ be a graph. A mapping $\delta : V \to V$ is an automorphism if $\delta$ is a graph isomorphism from $G$ to itself.

Let $\text{Aut}(G)$ be the group $K = (K, \cdot, 1)$ where:

(A1) $K = \{ \delta \mid \delta$ is an automorphism of $G \}$.

(A2) $\cdot$ is the composition of automorphisms.

(A3) $1$ is the identity automorphism.

Similarly for $e \in E$ the group $\text{Aut}_e(G)$ is the subgroup of $\text{Aut}(G)$ whose elements are

$$\{ \delta \mid \delta$ is an automorphism of $G$ with $\delta(e) = e \}.$$
The Color Automorphism Problem

**Input:** A colored set $A$ and generators for a group $K \subseteq \text{Sym}(A)$.

**Problem:** Output a set of generators for the subgroup of $k$ consisting of the color preserving mappings.

Computing generators of $\text{Aut}(G)$ for a graph $G = (V, E)$ is a special case.

1. $A = \{\{u, v\} \mid u, v \in V \text{ with } u \neq v\}$.
2. $\{u, v\}$ is colored black if $\{u, v\} \in E$, and white otherwise.
3. The group $K$ is

$$\left\{ \{u, v\} \mapsto \{\delta(u), \delta(v)\} \right\}_{u \neq v}$$

$\delta$ is a permutation of $V$.
Theorem
GI on graphs of degree at most 3 can be reduced to the problem of determining generators for $\text{Aut}_e(G)$, where $G$ is a connected graph of degree 3 and $e$ an edge of $G$. 
Let $G_1$ and $G_2$ be two connected graphs of degree 3. Fix an $e_1 \in E(G_1)$ and $e_2 \in E(G_2)$. We can test whether there is an isomorphism from $G_1$ to $G_2$ which maps $e_1$ to $e_2$ as follows.

1. Construct a new graph $G$:
   
   1.1 Take the disjoint union $G_1 \cup G_2$.
   1.2 Insert a new vertex $v_1$ in $e_1$ and $v_2$ in $e_2$.
   1.3 Add the edge $\{v_1, v_2\}$.

2. There is an isomorphism from $G_1$ to $G_2$ mapping $e_1$ to $e_2$ if and only if some element of $\text{Aut}_e(G)$ transposes $v_1$ and $v_2$.

3. If such automorphisms exit, any set of generators of $\text{Aut}_e(G)$ must contain one.
Polynomial-Time Algorithms for Permutation Groups
More group theory

Let $K$ be a group. The order $|K|$ of $K$ is the number of elements in $K$.

A subgroup $H \subseteq K$ is a group whose elements are all in $K$ and have the same $\cdot$ as $K$. We define

$$K/H := \{ a \cdot H \mid a \in K \},$$

i.e., the collection of left cosets of $H$ in $K$. By Lagrange’s Theorem

$$|K| = |K/H| \times |H|,$$

where $|K/H|$ is the index of $H$ in $G$. 

Permutation subgroups

Let $g_1 \ldots, g_k$ be permutations on $[n]$. Then the group

$$K := \langle g_1, \ldots, g_k \rangle$$

is the group of all permutations formed by products of the $g_i$'s. Let $I$ be the unique group generated by the identity permutation.
Permutation subgroups (cont’d)

There is a descending chain of subgroups

\[ K = K_0 \supseteq K_1 \supseteq \cdots \supseteq K_{n-1} = I, \]

where

\[ K_i := \{ \sigma \in K \mid \sigma(j) = j \text{ for all } j \leq i \}. \]
Coset representatives

Let $i \in \mathbb{N}$ with $0 \leq i \leq n - 2$ and then

$$K_i/K_{i+1} = \{a \cdot K_{i+1} \mid a \in K_i\}.$$ 

$C_i \subseteq K_i$ is a set of coset representatives of $K_i/K_{i+1}$ if for every $a \in K_i$ we have

$$|C_i \cap (a \cdot K_{i+1})| = 1.$$

**Lemma**

$K_i = C_i \cdot K_{i-1}$ and $|K_i| = |C_i| \times |K_{i-1}|$. 
Coset representatives (cont’d)

Then

\[ K = K_0 = C_0 \cdot K_1 = \cdots = C_0 \cdot C_1 \cdots C_{n-2} \cdot K_{n-1}. \]

And,

\[ |K| = |C_0| \times |C_1| \times \cdots \times |C_{n-2}|. \]

In other words, every \( a \in K \) can be uniquely written as

\[ a = a_0 \cdot a_1 \cdots a_{n-2} \]

where \( a_i \in C_i \), i.e., its canonical representation.
Theorem

We can compute a set of coset representatives $C_0, \ldots, C_{n-2}$.

in polynomial time, in time $n^{O(1)}$. 

The Filter routine

Let $C_0, \ldots, C_{n-2}$ be (possibly partial) sets of coset representatives, and let $x \in K_0$.

FILTER($x$)

1. for $i = 0$ to $n-2$ do
2. if $y^{-1} \cdot x \in K_{i+1}$ for some $y \in C_i$
3. then $x \leftarrow y^{-1} \cdot x$
4. else $C_i \leftarrow C_i \cup \{x\}$ and return
5. return

Observe that $x \in K_i$ and $y^{-1} \cdot x \in K_i$, thus $y^{-1} \cdot x \in K_{i+1}$ if and only if

$$y^{-1} \cdot x(j + 1) = j + 1.$$
The Filter routine (cont’d)

Lemma

After executing \texttt{FILTER(a)}, we have

1. \(a \in C_0 \cdot C_1 \cdots C_{n-2}, \) and

2. \(C_0, \ldots, C_{n-2} \) are still (possibly partial) sets of coset representatives.
Compute complete $C_0, \ldots, C_{n-2}$

1. for $i = 1$ to $k$ do
2. \hspace{2em} \text{FILTER}(g_i)$
3. \hspace{2em} changed $\leftarrow$ false
4. for all $i \geq j$ do
5. \hspace{4em} for all $a \in C_i \cdot C_j$ do
6. \hspace{6em} \text{FILTER}(a)$
7. \hspace{6em} if some $C_k$ increases then changed $\leftarrow$ true
8. \hspace{2em} if changed $=$ true then goto 3 else return
Proof

First for every generator $g_i$ we have

$$g_i \in C_0 \cdot C_1 \cdots C_{n-2}.$$  

For every $0 \leq i \leq n-2$, let $a_i, a'_i \in C_i$. We need to show

$$\prod_{i=0}^{n-2} a_i \cdot \prod_{i=0}^{n-2} a'_i \in C_1 \cdot C_2 \cdots C_{n-2}.$$  

It is suffices to show that for every $i \geq j$

$$C_i \cdot C_j \subseteq C_j \cdot C_{j+1} \cdots C_i \cdot K_{i+1}.$$
Theorem
There is a polynomial time algorithm that on input a permutation $\sigma$ decides whether $\sigma \in K$.

Proof.
$\sigma \in K$ if and only if $\text{FILTER}(\sigma)$ does not increase any $C_i$. \qed
Theorem
There is a polynomial time algorithm \( \mathcal{A} \) such that for every subgroup \( H \subseteq K \) such that

1. \( |K/H| \) is polynomial in terms of \( n \) and the number of generators of \( K \),
2. the membership of \( H \) is decidable in polynomial time,
\( \mathcal{A} \) computes a set of generators of \( H \).

Proof.
We look at the sequence

\[
I = H_{n-1} \subseteq H_{n-2} \subseteq \cdots \subseteq H_2 \subseteq H_1 \subseteq H \subseteq K.
\]

\qed