Isomorphism problem for finite combinatorial objects via coherent configurations

Ilia Ponomarenko
Petersburg Department of V.A.Steklov
Institute of Mathematics
Fontanka 27, St. Petersburg 191023, Russia

The Graph Isomorphism Problem is to recognize whether two finite graphs are isomorphic by means of an efficient algorithm.

The naive algorithm for n-vertex graphs takes $O(n!)$ steps.

At present **the best general isomorphism test** makes at least $n^{O(\sqrt{n/\log n})}$ steps in the worst case (Babai-Kantor-Luks, 1983).

The corresponding isomorphism problems for directed graphs, multigraphs, hypergraphs, vertex-colored graphs, edge-colored graphs, ... are **polynomial-time equivalent**.

Proposition 1. *The following three problems are polynomial-time equivalent:*

(1) *the Graph Isomorphism Problem,*

(2) *given a graph* Γ *find a generator set of* $\mathrm{Aut}(\Gamma)$*,*

(3) *given a graph* Γ *find the orbits of* $\mathrm{Aut}(\Gamma)$*.*

The Weisfeiler-Leman approach

Let Γ be a graph with the vertex set V and the edge set E.

The **coherent configuration** or briefly the **scheme** of Γ is defined to be the smallest scheme $\mathcal{C}(\Gamma)$ on V for which E is a union of some basis relations of it:

$$\mathcal{C}(\Gamma) = [E]$$

or equivalently,

$$W(\mathcal{C}(\Gamma)) = [A(\Gamma)]$$

where $W(\mathcal{C}(\Gamma))$ is the adjacency algebra of the scheme $\mathcal{C}(\Gamma)$ and $A(\Gamma)$ is the adjacency matrix of Γ.

Proposition 2. *Let $\mathcal{C} = \mathcal{C}(\Gamma)$. Then*

(1) $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\Gamma)$*; if $\mathcal{C}$ is Schurian, then the orbits of* $\mathrm{Aut}(\Gamma)$ *are the fibers of $\mathcal{C}$,*

(2) *the scheme $\mathcal{C}$ can be constructed in time $O(n^3 \log n)$ where $n = |V|$.*

Thus if all the schemes were Schurian, then the Graph Isomorphism Problem would solve by means of **the Weisfeiler-Leman algorithm**.

Circulant graphs

A finite graph Γ (resp. a scheme $\mathcal{C}$) is called **circulant** if the group $\mathrm{Aut}(\Gamma)$ (resp. $\mathrm{Aut}(\mathcal{C})$) contains a full cycle:

$$(1, 2, \ldots, n) \in \mathrm{Aut}(\Gamma) \qquad ((1, 2, \ldots, n) \in \mathrm{Aut}(\mathcal{C}))$$

where n is the number of vertices of Γ.

Theorem 3. (EP, (2001)). *There exists an infinite family of non-Schurian circulant schemes.*

For circulant graphs the isomorphism problem is polynomial-time reducible to the recognition problem:

$$\forall \Gamma_1, \Gamma_2 \in \mathcal{K}_n : \quad \Gamma_1 \cong \Gamma_2 \Leftrightarrow \Gamma_1 \cup \Gamma_2 \in \mathcal{K}_{2n}$$

where $\mathcal{K}_n$ is the class of circulant graphs with n vertices and $\Gamma_{\cup}\Gamma_2$ is the disjoint union Γ_1 and Γ_2.

Muzychuk, (2004) found an efficient algorithm to test isomorphism for circulant graphs with *explicitly given* cyclic automorphism group.

The recognition problem for circulant graphs and circulant schemes are **polynomial-time equivalent**.

Theorem 4. (EP, (2003)). *Given a scheme* $\mathcal{C}$ *on a set* V *one can find in polynomial time in* $|V|$ *a set of* $k \leq |V|$ *of binary relations* $R_1, \ldots, R_k \subset V \times V$ *such that the scheme*

$$\mathcal{C}' = [\mathcal{C}, R_1, \ldots, R_k]$$

is circulant iff so is $\mathcal{C}$*. Moreover, the group* $\mathrm{Aut}(\mathcal{C}')$ *is solvable.*

By means of computational group theory technique one can prove that circulant schemes with solvable automorphism groups are polynomial-time recognizable.

A **Cayley representation** of a graph Γ over a group G is a Cayley graph over G isomorphic to Γ; two such representations are called **equivalent** if some isomorphism of the corresponding Cayley graphs belong to $\mathrm{Aut}(G)$.

Theorem 5. (EP, (2003)) *Given a graph* Γ *with* n *vertices, one can find in time* $n^{O(1)}$ *a full system of pairwise nonequivalent Cayley representations of* Γ *over a cyclic group of order* n*.*

Similarities

Two schemes $\mathcal{C} = (V, \mathcal{R})$ and $\mathcal{C}' = (V', \mathcal{R}')$ are called **similar**, if

$$p_{R,S}^{T} = p_{R^\varphi,S^\varphi}^{T^\varphi}, \qquad R, S, T \in \mathcal{R},$$

for some bijection $R \mapsto R^\varphi$ from $\mathcal{R}$ to $\mathcal{R}'$, called a **similarity** (or an **algebraic isomorphism**).

Properties of the similarity φ:

(1) $|V| = |V'|$,

(2) $(R^T)^\varphi = (R^\varphi)^T$ for all $R \in \mathcal{R}$,

(3) $W(\mathcal{C}) \rightarrow W(\mathcal{C}'), A(R) \mapsto A(R^\varphi),\ R \in \mathcal{R}$ is a matrix algebra isomorphism,

Any isomorphism $f \in \mathrm{Iso}(\mathcal{C}, \mathcal{C}')$ induces a similarity $\varphi_f : \mathcal{C} \rightarrow \mathcal{C}'$ such that

$$R^{\varphi_f} = R^f, \qquad R \in \mathcal{R}.$$

However, there exist similar schemes which are not isomorphic. In the class of circulant schemes the smallest known example has 4225 points (EP, (2001)).

Given graphs Γ and Γ' set $\mathcal{C} = \mathcal{C}(\Gamma)$ and $\mathcal{C}' = \mathcal{C}(\Gamma')$. Then

$$\mathrm{Iso}(\Gamma, \Gamma') \subset \mathrm{Iso}(\mathcal{C}, \mathcal{C}')$$

and

$$E^{\varphi_f} = E', \qquad f \in \mathrm{Iso}(\Gamma, \Gamma')$$

where E and E' are the edge sets of Γ and Γ' respectively.

Proposition 6. (Weisfeiler-Leman) *Let $\mathcal{C} = [E]$ and $\mathcal{C}' = [E']$ where $E, E' \subset V \times V$. Then in polynomial time one can test whether there exists a similarity $\varphi : \mathcal{C} \to \mathcal{C}'$ such that $E^{\varphi} = E'$ and find it if it does exist.*

Proposition 6 gives a constructive necessary condition for isomorphism of graphs Γ and Γ'.

Algebraic forests

A graph Γ is called an **algebraic forest** if there exists a forest T such that

$$\mathcal{C}(\Gamma) = \mathcal{C}(T)_L$$

where L is the set of leaves of T and $\mathcal{C}(T)_L$ is the restriction of the scheme $\mathcal{C}(T)$ to the set L. (One can prove that L is a union of some fibers of $\mathcal{C}(T)$).

Examples.

1. Any **tree** is an algebraic forest.

2. Any **interval graph** is an algebraic forest. (An interval graph has a set of line segments as the set of vertices and two vertices are adjacent if the corresponding segments have nonempty intersection.)

3. Any **cograph** is an algebraic forest. (A cograph is a graph that contain no induced path on four vertices.)

For all the above classes of graphs there exist polynomial-time algorithms to test isomorphism. However, the corresponding algorithms are different.

Set $\mathcal{F}$ to be the class of all schemes of algebraic forests. One can prove that $\mathcal{F}$ is closed with respect to the **direct sums** and **wreath products**:

The direct sum of schemes $\mathcal{C}_1$ on V_1 and $\mathcal{C}_2$ on V_2 where V_1 and V_2 are disjoint sets, is defined to be

$$\mathcal{C}_1 \boxplus \mathcal{C}_2 = [\mathcal{C}_1, \mathcal{C}_2].$$

The group $\mathrm{Aut}(\mathcal{C}_1 \boxplus \mathcal{C}_2)$ is induced by the natural action of $\mathrm{Aut}(\mathcal{C}_1) \times \mathrm{Aut}(\mathcal{C}_2)$ on $V_1 \cup V_2$.

Let $\mathcal{C}_1 = (V_1, \{R_0, \ldots, R_{m-1}\})$ be a scheme. **The wreath product** of the scheme $\mathcal{C}_1$ and a scheme $\mathcal{C}_2$ on V_2 of rank 2 is defined to be

$$\mathcal{C}_1 \wr \mathcal{C}_2 = [R'_0, \ldots, R'_{m-1}].$$

where R'_i is the disjoint union of $|V_2|$ copies of R_i. The group $\mathrm{Aut}(\mathcal{C}_1 \wr \mathcal{C}_2)$ is induced by the natural action of $\mathrm{Aut}(\mathcal{C}_1) \wr \mathrm{Sym}(V_2)$ on $V_1 \times V_2$.

Theorem 7. **(EPT, (2000))** *Given a scheme* $\mathcal{C} \in \mathcal{F}$ *one of the following three statements holds:*

(1) $\mathrm{rk}(\mathcal{C}) \le 2$,

(2) $\mathcal{C} = \mathcal{C}_1 \boxplus \mathcal{C}_2$ *for some schemes* $\mathcal{C}_1, \mathcal{C}_2 \in \mathcal{F}$,

(3) $\mathcal{C} = \mathcal{C}_1 \wr \mathcal{C}_2$ *for some scheme* $\mathcal{C}_1 \in \mathcal{F}$, *and a scheme* $\mathcal{C}_2$ *of rank 2.*

(The direct sum in (2) and the wreath product in (3) are nontrivial.)

From Theorem 7 one can deduce the following statement showing that the Weisfeiler-Leman algorithm solves the isomorphism problem in the class of algebraic forests.

Theorem 8. **(EPT, (2000))** *Let* $\mathcal{C}, \mathcal{C}' \in \mathcal{F}$. *Then for each similarity* $\varphi : \mathcal{C} \to \mathcal{C}'$ *there exists an isomorphism* $f \in \mathrm{Iso}(\mathcal{C}, \mathcal{C}')$ *such that* $\varphi = \varphi_f$.