数理解析研究所講究録
第 1964 巻 2015 年 180-182

A proposal of an index to the graph isomorphism based on the structural square of a graph

Shuji JIMBO (jimbo-s@okayama-u.ac.jp) and Yuki NAKAGAWA
Graduate School of Natural Science and Technology,
Okayama University, Japan

31 May 2015

1 Introduction

It has not yet been known whether the graph isomorphism problem is NP-complete or not. However, there is enough evidence that the graph isomorphism problem is not NP-complete[3][6]. A polynomial time graph isomorphism algorithms is, therefore, hoped to be developed. We consider the possibility of positions of board games like Pentago or Five in a Row to be expressed as a labeled graphs. A polynomial time graph isomorphism algorithm might be useful in that case.

We proposed several notions in graph theory in the RIMS workshop held on 18 February 2015. Those are the *Ultimate refinement* of a labeled graph using structural square and removal of a vertex with *apportionment* from a labeled graph. However, it was indicated that the procedure to obtain the ultimate refinement of a graph is similar to the Weisfeiler-Lehman algorithm very much at a workshop held in March 2015[5]. We examined the indication and decided that it is applicable. We will therefore write a very short note about the status of our research concerning the graph isomorphism problem.

In the next section, similarity and difference between previous research and ours will be briefly stated. In the third section, targets of our research based on current original idea will be shown.

2 Similarity and Difference

The definition of the Graph Isomorphism problem (GI) is as follows:

> Inputs: two graphs G and H, where those are simple undirected graphs, that is, there are neither multiple edges nor loops
>
> Question: Is there a permutation (one-to-one and onto mapping) $\sigma : V(G) \to V(H)$ such that for any $v \in V(G)$ and $w \in V(G)$, $vw \in E(G) \Leftrightarrow \sigma(v)\sigma(w) \in E(H)$ holds?

The definition can be describe with matrices as follows:

Question: Is there a permutation matrix P such that $P^{-1}A(G)P = A(H)$ holds?

Here $A(G)$ and $A(H)$ are the adjacency matrices of G and H, respectively

We defined a procedure on a symmetric matrix called structural square, and the ultimate refinement of a symmetric matrix obtained by repeating structural square. However, those notions can be replaced with a coherent configuration and the Weisfeiler-Lehman algorithm.

A coherent configuration can be defined as a square matrix $M = (a(u,v))$[1]. Let V denote the coordinate set of M, For any $u, v \in V$, $a(u,v)$ denote the component of M at coordinate (u,v). Let $\Delta(V)$ denote $\{(v,v) \mid v \in V\}$. Let $\mathcal{R}_M$ denote the set of all components of M. For any $r \in \mathcal{R}_M$, let $M(r) \subseteq V \times V$ denote the set of all coordinates such that the corresponding component equals r. For $R \subseteq V \times V$, let R^{T} denote the set $\{(u,v) \in V \times V \mid (v,u) \in R\}$, and $\mathcal{R}_M(R)$ the set of all components of M at a coordinate in R. Square matrix $M = a(u,v)$ is a coherent configuration if the following three conditions hold:

1. $\mathcal{R}_M(\Delta(V)) \cap \mathcal{R}_M(V \times V - \Delta(V)) = \varnothing$.

2. For any $r \in \mathcal{R}_M$, there is an $s \in \mathcal{R}_M$ such that $M(r) = M(s)^{\mathrm{T}}$.

3. For any $r, s, t \in \mathcal{R}_M$, let $c_{r,s}(u,v) : V \times V \to \mathbb{Z}$ denote the number of vertices $w \in V$ such that $a(u,w) = r$ and $a(w,v) = s$. Then, $c_{r,s}(u,v)$ is constant over $(u,v) \in M(t)$.

Matrix $M' = (b(u,v))$ with the same coordinate set V as M. M' is a refinement of M if $\mathcal{R}_M \subseteq \mathcal{R}_{M'}$ and, for any $r \in \mathcal{R}_{M'}$, there is an $s \in \mathcal{R}_M$ such that $M'(r) \subseteq M(s)$. We say M' is greater than M if M' is a refinement of M, and $M' \neq M$. The Weisfeiler-Lehman algorithm can be regarded as a procedure to calculate the least refinement of an adjacency matrix of a given undirected graph[2].

Let $M = (a(u,v))$ is a coherent configuration whose components are all nonnegative integers, and V denote the coordinate set of M. For any $v \in V$, square matrix $M' = (b(x,y))$ with the coordinate set $V - \{v\}$ is defined as follows.

1. For any $x, y \in V - \{v\}$ with $x \neq y$, $b(x,y) = (a(x,y), a(x,y), a(x,y))$.

2. For any $x \in V - \{v\}$, $b(x,x) = (b(x,y), a(x,v), a(v,x))$.

Then, $r(M,v) = (c(x,y))$ is obtained by renumbering the components of M'. Let $(b_0, b_1, b_2, \ldots, b_k)$ denote the sequence consisting of all the components of M' lined in lexicographic order. Then, $c(x,y) = i$ if and only if $b(x,y) = b_i$ for any $i \in \{0, 1, \ldots, k\}$.

For any square matrix M, let $C(M)$ denote the coherent configuration of M. We conjectured that an efficient graph isomorphism algorithm can be designed according to the following principles:

1. Coherent configurations $M = (a(u,v))$ and $M'(b(u,v))$ are isomorphic, if and only if $\mathcal{R}_M = \mathcal{R}_{M'}$, and there are $u, v \in V$ such that $a(u,u) = b(v,v)$ and $C(r(M,u))$ and $C(r(M',v))$ are isomorphic.

2. The determinant of a square matrix does not change by applying any permutation. In other words, for any square matrix M and any permutation matrix P, $\det(M) = \det(P^{-1}MP)$ holds.

As far as I know, any similar notion to removal of a vertex with apportionment has not been directly used in previous research yet. However, there are sentences suggesting that a similar idea was used in old literature[7].

3 Future targets

Completion of the design and theoretical analysis of the algorithm suggested in the last part of the previous section seem to be interesting challenges. Furthermore, we have another present target. A graph is called *circulant*, if the cyclic permutation $(0, 1, 2, \ldots, n)$ is an automorphism of the graph. There is a polynomial-time graph isomorphism algorithm for the class of circulant graphs[4]. We expect that a more efficient graph isomorphism algorithm for circulant graphs can be developed using the notions in the previous section. We notice that the determinant of the adjacency matrix of a circulant graph has a closed expression when each component is regarded as a variable.

Acknowledgment

We would like to thank Dr. Yota Otachi at Japan Advanced Institute of Science and Technology to provide valuable advices.

References

[1] Amir Rahnamai Barghi and Ilya Ponomarenko. Non-isomorphic graphs with cospectral symmetric powers. *the electronic journal of combinatorics*, 16(R120):1, 2009.

[2] Brendan L Douglas. The weisfeiler-lehman method and graph isomorphism testing. *arXiv preprint arXiv:1101.5211*, 2011.

[3] Rudolf Mathon. A note on the graph isomorphism counting problem. *Information Processing Letters*, 8(3):131–136, 1979.

[4] Mikhail Muzychuk. A solution of the isomorphism problem for circulant graphs. *Proceedings of the London Mathematical Society*, 88(01):1–41, 2004.

[5] Yuki Nakagawa and Shuji Jimbo. A proposal of a randomized algorithm for the graph isomorphism based on the structural square of a graph. *IPSJ SIG Technical Report*, 2015-AL-152(7):1–7, March 2015.

[6] Uwe Schöning. Graph isomorphism is in the low hierarchy. *Journal of Computer and System Sciences*, 37(3):312–323, 1988.

[7] Boris Weisfeiler. On construction and identification of graphs. In *Lecture Notes in Mathematics*. Citeseer, 1976.