GRAPH ISOMORPHISM AND CIRCUIT ISOMORPHISM

Thinh D. Nguyen

(former member of Vietnam Mathematics Institute)

(email: *kosmofarmer@gmail.com*)

Abstract. In this note, we show that graph isomorphism is reducible to circuit isomorphism, in polynomial time.

1. Notation

We denote the well-known graph isomorphism problem by **GraphIso** which is defined as follows:

$$\textbf{GraphIso} = \{<\boldsymbol{G}_1, \boldsymbol{G}_2>, \text{graph } \boldsymbol{G}_1 \text{ is isomorphic to graph } \boldsymbol{G}_2\}$$

By **CircuitIso**, we denote the circuit isomorphism problem:

$$\textbf{CircuitIso} = \{< \boldsymbol{C}_1, \boldsymbol{C}_2>, \text{two } n\text{-input circuit } \boldsymbol{C}_1 \text{ and } \boldsymbol{C}_2 \text{ are isomorphic}\}$$

Two n-input $\boldsymbol{C}_1, \boldsymbol{C}_1$ are isomorphic if there exists a permutation $\pi \in \mathbf{S}_n$ such that $\boldsymbol{C}_1(\boldsymbol{x})$ and $\boldsymbol{C}_2(\pi(\boldsymbol{x}))$ are equivalent.

2. Main result

We will show that **GraphIso** $\leq_p$ **CircuitIso**.

3. Details of the reduction

Given two n-vertex graph $\boldsymbol{G}_1$, $\boldsymbol{G}_2$, we construct two corresponding circuits $\boldsymbol{C}_1$, $\boldsymbol{C}_2$ as follows:

The number of input bits to $\boldsymbol{G}_1$, $\boldsymbol{G}_2$ is equal to n. We will describe the circuit $\boldsymbol{C}_1$, the construction of $\boldsymbol{C}_2$ is similar. To code the structure of $\boldsymbol{G}_1$ into $\boldsymbol{C}_1$, we consider each edge (u, v) of $\boldsymbol{G}_1$. For each such edge, we create a sub-circuit (gadget in poly-time reduction literature) which guarantees that among the n-input bit **only** two bits corresponding to u and v are 1. Then, to complete our construction, we take the **OR** of all the gadgets as output of $\boldsymbol{C}_1$.

Now, it is easy to see that: $\boldsymbol{G}_1$, $\boldsymbol{G}_2$, are isomorphic iff $\boldsymbol{C}_1$, $\boldsymbol{C}_2$ are isomorphic. Because $\boldsymbol{G}_1$, $\boldsymbol{G}_2$ can be seen as edge-tester for their corresponding graphs. If there is a permutation on vertices making $\boldsymbol{G}_1$ into $\boldsymbol{G}_2$, then the same permutation on input bits will make $\boldsymbol{C}_1$ equivalent to $\boldsymbol{C}_2$. The reverse is also not difficult.

ACKNOWLEDGMENT

My sincere thanks to all my (former) colleagues at Vietnam Institute of Mathematics, Vietnam National University.

REFERENCES

Norman L. Biggs, **Discrete Mathematics**, 2nd edition, Oxord University Press, 2003.