ISSN 1342-2812

Research Reports on
Mathematical and
Computing Sciences

# Yet Another Reduction from Graph to Ring Isomorphism Problems

Tomoyuki Hayasaka

Nov. 2009, C–264

Department of
Mathematical and
Computing Sciences
Tokyo Institute of Technology

SERIES C: Computer Science

# Yet Another Reduction from Graph to Ring Isomorphism Problems

Tomoyuki Hayasaka
Department of Mathematical and Computing Sciences
Tokyo Institute of Technology, Tokyo, Japan
hayasak6@is.titech.ac.jp

**Abstract**

It has been known that the graph isomorphism problem is polynomial-time many-one reducible to the ring isomorphism problem. In fact, two different reductions have already been proposed. For those reductions, rings of certain types have been used to represent a given graph. In this paper, we give yet another reduction, which is based on a simpler and more natural construction of a ring from a graph. By the existing reductions, one of the original graph isomorphisms can be found in each ring isomorphism obtained for the reduced ring isomorphism problem instance. On the other hand, in our new reduction, it is not clear how to get a graph isomorphism between two graphs from an obtained ring isomorphism between rings constructed from the graphs. However, we show that we can compute a graph isomorphism from an obtained ring isomorphism in polynomial time. In fact, one ring isomorphism may correspond to many graph isomorphisms in our reduction. Our proof essentially shows a way to obtain all graph isomorphisms corresponding to one ring isomorphism.

## 1 Introduction

A ring is an algebraic structure consisting of a set together with addition (+) and multiplication ( $\cdot$ ), and it plays an important role in mathematics, especially in algebra and number theory.

Rings are also important in computer science, since many problems in computer science can be regarded as problems of rings. For example, the deterministic primality test proposed by Agrawal *et al.* [1] can be seen as checking some automorphisms of a ring $\mathbb{Z}_n[X]/\langle X^r - 1\rangle$. Similarly, the integer factorization problem is reducible to problems related to rings, such as counting isomorphisms or computing an isomorphism between certain rings [2].

It has also been known that the graph isomorphism problem is polynomial-time many-one reducible to the ring isomorphism problem. In fact, two different reductions have already been proposed [2, 3]. In this paper, we give yet another reduction, which is simpler and more natural than previous reductions.

The organization of this paper is as follows. We start with the definitions of ring isomorphism problem and graph isomorphism problem in section 2. In Section 3, we overview the existing reductions from the graph isomorphism problem to the ring isomorphism problem. In Section 4, we propose a new and simple way of constructing a ring from a graph, and prove that our new way of construction can be used for the reduction. In Section 5, we discuss how to compute an original graph isomorphism from a ring isomorphism between rings constructed by our new reduction. The last section concludes the paper and lists some open problems.

## 2 Preliminaries

In this section, we give the definitions of ring isomorphism problem and graph isomorphism problem.

A *ring* is a set $\mathbf{R}$ equipped with two binary operations, addition(+) and multiplication( $\cdot$ ), which satisfy following conditions:

- $\mathbf{R}$ is an abelian group under addition with identity element 0;
- $\mathbf{R}$ is a monoid under multiplication with identity element 1;
- Multiplication distributes over addition.

For two rings $\mathbf{R}_1$ and $\mathbf{R}_2$, a bijection $\phi\colon \mathbf{R}_1 \to \mathbf{R}_2$ is called a *ring isomorphism* if and only if it satisfies these two conditions below:

- for all $a, b \in \mathbf{R}_1$, $\phi(a) + \phi(b) = \phi(a + b)$;
- for all $a, b \in \mathbf{R}_1$, $\phi(a) \cdot \phi(b) = \phi(a \cdot b)$.

We say the two rings are *isomorphic* if and only if there exists a ring isomorphism between two rings. The *ring isomorphism problem* is to decide whether two given rings are isomorphic. The corresponding language can be defined as:

$$\text{RING ISOMORPHISM} = \{(\mathbf{R}_1, \mathbf{R}_2) \mid \text{ Rings } \mathbf{R}_1 \text{ and } \mathbf{R}_2 \text{ are isomorphic}\}.$$

To represent rings, we use basis representation of rings described in [2].

A *graph* $G$ of $n$ vertices is a pair $(V, E)$, where $V = \{1, \ldots, n\}$ is a set of vertices and $E$ is a set of edges, which are pairs of vertices. In this paper, we focus on simple graphs, that is, edges are undirected and neither parallel edges nor loops are allowed. A *clique* $C$ of a graph $G = (V, E)$ is a subset of the vertex set $V$, such that for every pair of vertices in $C$, there exists an edge connecting them. A clique $C$ is called a *maximal clique* if and only if $C$ is not a proper subset of any larger clique.

For two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, a bijection $\pi\colon V_1 \to V_2$ is called a *graph isomorphism* if and only if $\{(\pi(u), \pi(v)) \mid (u, v) \in E_1\} = E_2$. We say that the two graphs are *isomorphic* if and only if there exists a graph isomorphism between two graphs. The *graph isomorphism problem* is to decide whether two graphs are isomorphic. The corresponding language can be defined as:

$$\text{GRAPH ISOMORPHISM} = \{(G_1, G_2) \mid \text{ Graphs } G_1 \text{ and } G_2 \text{ are isomorphic}\}.$$

## 3 Known Reductions

To reduce from the graph isomorphism problem to ring isomorphism problem, we use rings of certain types to represent the structure of given graphs.

Kayal *et al.* [2] proposed the following construction of a ring from a graph.

Construction 1 ([2])

Given a simple graph $G = (V, E)$ with $n$ vertices, define the following ring $\mathbf{R}_G$:

$$\mathbf{R}_G := \mathbb{Z}_{p^3}[V_1, \dots, V_n, A_{(1,2)}, \dots, A_{(n-1,n)}]/I,$$

where $p$ is an odd prime number and the ideal $I$ has the following relations:

- for all $1 \leq i \leq n$ , $V_i^2 = 0$;
- for all $1 \leq i < j \leq n$ , $V_iV_j = V_jV_i = A_{(i,j)}$;
- for all $1 \leq i \leq n$ and $e, e' \in \{(k,l) \mid 1 \leq k < l \leq n\}$, $A_eV_i = A_iV_e = 0, A_eA_{e'} = 0$;
- for all $e \in E$ , the order of $A_e$ is $p$;
- for all $e \notin E$ , the order of $A_e$ is $p^2$.

In this construction of a ring, the variables $V_1, \dots, V_n$ represent vertices and $A_{(1,2)}, \dots, A_{(n-1,n)}$ represent pairs of vertices. The structure of edges is embedded in a ring by setting orders of variables differently according to whether the corresponding pair has an edge or not.

Suppose we are given two graphs $G_1$ and $G_2$, and let $\mathbf{R}_{G_1}$ and $\mathbf{R}_{G_2}$ be the rings constructed from $G_1$ and $G_2$ using construction 1, respectively. Kayal *et al.* [2] proved that two graphs $G_1$, $G_2$ are isomorphic if and only if $\mathbf{R}_{G_1}$ and $\mathbf{R}_{G_2}$ are isomorphic. This shows that the graph isomorphism problem can be reduced to the ring isomorphism problem.

Their proof is based on a observation that one can compute a graph isomorphism from a ring isomorphism between $\mathbf{R}_{G_1}$ and $\mathbf{R}_{G_2}$. Suppose that $\mathbf{R}_{G_1}$ and $\mathbf{R}_{G_2}$ are isomorphic and we are given an isomorphism $\phi\colon \mathbf{R}_{G_1} \to \mathbf{R}_{G_2}$. Let

$$\phi(V_i) = \alpha_i + \sum_{1 \leq j \leq n} \beta_{i,j} V_j' n + \sum_{1 \leq j < k \leq n} \gamma_{i,j,k} A'_{(j,k)}.$$

Here, we use variables $V_1', \dots, V_n', A'_{(1,2)}, \dots, A'_{(n-1,n)}$ for $\mathbf{R}_{G_2}$ instead of $V_1, \dots, V_n, A_{(1,2)}, \dots, A_{(n-1,n)}$. It can be proved that exactly one of $\beta_{i,1}, \dots, \beta_{i,n}$ is a unit of $\mathbb{Z}_{p^3}$. Let $\pi$ be the mapping satisfying the following condition:

$$\pi(i) = j \Leftrightarrow \ \beta_{i,j} \text{ is a unit.}$$

Then, it can be proved that $\pi$ is indeed an isomorphism from $G_1$ to $G_2$.

Agrawal *et al.* [3] proposed another construction of a ring as stated below. Here, $\langle S \rangle$ denotes the ideal generated by $S$.

Construction 2 ([3])

Given a simple graph $G = (V, E)$ with $n$ vertices, define the following ring $\mathbf{R}_G$:

$$\mathbf{R}_G := \mathbb{F}_q[X_1, \dots, X_n]/\langle \{p_G(X_1, \dots, X_n)\} \cup \bigcup_{1 \leq i \leq n} \{X_i^2\} \cup \bigcup_{1 \leq i,j,k \leq n} \{X_iX_jX_k\} \rangle,$$

where $\mathbb{F}_q$ is a finite field of odd characteristic and $p_G \in \mathbb{F}_q[X_1, \dots, X_n]$ is a polynomial defined as follows:

$$p_G(X_1, \dots, X_n) := \sum_{(i,j) \in E} X_iX_j.$$

In this construction, the variables $X_1, \ldots, X_n$ represent vertices, and the products of two variables $X_1X_2$, $\ldots$ , $X_{n-1}X_n$ represent pairs of vertices. To embed the structure of edges of a graph, a ring satisfies the condition that the sum of all $X_iX_j$ that correspond to the edges is zero in a ring.

Suppose we are given two graphs $G_1$ and $G_2$ of $n$ vertices, and let $\mathbf{R}_{G_1}$ and $\mathbf{R}_{G_2}$ be the rings constructed from $G_1$ and $G_2$ using construction 2. Then, Agrawal *et al.* [3] proved that two graphs $G_1$, $G_2$ are isomorphic if and only if either $\mathbf{R}_{G_1}$ and $\mathbf{R}_{G_2}$ are isomorphic or $G_1 \cong G_2 \cong K_{n-k} \cup D_k$ for some $k$ (here, $K_{n-k}$ is the complete graph of $n-k$ vertices and $D_k$ is a collection of $k$ isolated vertices).

They proved that by showing every ring isomorphism from $\mathbf{R}_{G_1}$ to $\mathbf{R}_{G_2}$ contains a graph isomorphism from $G_1$ to $G_2$. Suppose $\mathbf{R}_{G_1}$ and $\mathbf{R}_{G_2}$ are isomorphic and we are given an isomorphism $\phi\colon \mathbf{R}_{G_1} \to \mathbf{R}_{G_2}$, and let

$$\phi(X_i) = \alpha_i + \sum_{1 \le j \le n} \beta_{i,j} Y_j + \sum_{1 \le j < k \le n} \gamma_{i,j,k} Y_j Y_k.$$

Here, we use $Y_1, \ldots, Y_n$ for $\mathbf{R}_{G_2}$ instead of $X_1, \ldots, X_n$. Then, it can be shown that exactly one of $\beta_{i,1}, \ldots, \beta_{i,n}$ is nonzero. Let $\pi$ be the mapping satisfying the following condition:

$$\pi(i) = j \Leftrightarrow \beta_{i,j} \neq 0.$$

Then, it can be proved that $\pi$ is an isomorphism from $G_1$ to $G_2$.

# 4 New Reduction

Construction 1 has a relatively complex structure. Construction 2 is simple but has some special case (namely, when a graph can be written as a union of a complete graph and isolated vertices), and the condition that "the sum of all edges is zero" is some what unnatural.

Hence, we propose the following "simpler" and "more natural" construction of a ring.

Construction 3

Given a simple graph $G = (V, E)$ with $n$ vertices, define the following ring $\mathbf{R}_G$:

$$\mathbf{R}_G := \mathbb{F}_q[X_1, \ldots, X_n] / \langle \bigcup_{(i,j) \in E} \{X_iX_j\} \cup \bigcup_{1 \le i \le n} \{X_i^2\} \cup \bigcup_{1 \le i,j,k \le n} \{X_iX_jX_k\})\rangle,$$

where $\mathbb{F}_q$ is a finite field with odd characteristic.

This construction of a ring from a graph is very similar to construction 2, but the condition is changed from "the sum of all edges is zero" to "every edge is zero." In this way, the structure of a ring is much simpler than construction 1, and the way of embedding the information of edges is more natural than construction 2.

However, it is not clear whether this construction can be used for the reduction. To see this, suppose we get an isomorphism $\phi\colon \mathbf{R}_{G_1} \to \mathbf{R}_{G_2}$, where $\mathbf{R}_{G_1}$ and $\mathbf{R}_{G_2}$ are the rings constructed from $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ using construction 3, and let

$$\phi(X_i) = \phi(X_i) = \alpha_i + \sum_{1 \le j \le n} \beta_{i,j} Y_j + \sum_{(j,k) \notin E_2} \gamma_{i,j,k} Y_j Y_k.$$

Then, there may be more than one of $\beta_{i,1}, \ldots, \beta_{i,n}$ which are nonzero, and every nonzero $\beta_{i,j}$ is a unit. Therefore, we cannot get a graph isomorphism from a ring isomorphism using the same way as we did in construction 1 or 2. Hence, there might be some cases in which rings are isomorphic even if graphs are not isomorphic.

Nevertheless, we prove the following.

**Theorem 4.1.** Let $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$ be simple graphs and $\mathbf{R}_{G_1}, \mathbf{R}_{G_2}$ be the rings constructed from $G_1$ and $G_2$ using construction 3. Then, $G_1$ and $G_2$ are isomorphic if and only if $\mathbf{R}_{G_1}$ and $\mathbf{R}_{G_2}$ are isomorphic.

**Proof** For simplicity of notation, we will use $\mathbf{R}_1$ and $\mathbf{R}_2$ instead of $\mathbf{R}_{G_1}$ and $\mathbf{R}_{G_2}$, respectively.

If $G_1$ and $G_2$ are isomorphic, any graph isomorphism between graphs induces a natural isomorphism between $\mathbf{R}_1$ and $\mathbf{R}_2$. So we only have to prove the other direction.

Suppose that there is an isomorphism $\phi$ from $\mathbf{R}_1$ to $\mathbf{R}_2$. We will prove that $G_1$ and $G_2$ are indeed isomorphic.

First of all, we can assume that the number of vertices of $G_1$ and that of $G_2$ are equal, since the rings cannot be isomorphic if two graphs have different numbers of vertices. Let $n$ be the number of vertices of $G_1$ and $G_2$. We will use $X_1, \dots, X_n$ for the variables of $\mathbf{R}_1$ and $Y_1, \dots, Y_n$ for those of $\mathbf{R}_2$ instead, so that we can distinguish an element of $\mathbf{R}_1$ from an element of $\mathbf{R}_2$ easily.

**Remark 4.2.** Note that $\phi$ satisfies the following conditions from the definition of isomorphism.

- $\{\phi(1), \{\phi(X_i)\}_{1 \le i \le n}, \{\phi(X_i X_j)\}_{(i,j) \notin E_1}\}$ forms a basis of $\mathbf{R}_2$, and hence they are linearly independent.
- $\phi(X_i)\phi(X_j) = \phi(X_i X_j)$ holds for all $1 \le i, j \le n$

□

**Claim 4.3.** $\phi\colon \mathbf{R}_1 \to \mathbf{R}_2$ satisfies the following conditions:

$$\begin{aligned} \phi(1) &= 1, \\ \phi(X_i) &= \sum_{1 \le j \le n} \beta_{i,j} Y_j + \sum_{(j,k) \notin E_2} \gamma_{i,j,k} Y_j Y_k \qquad \text{for all } 1 \le i \le n, \\ \phi(X_i X_j) &= \sum_{(k,l) \notin E_2} \delta_{i,j,k,l} Y_k Y_l \qquad \text{for all } (i,j) \notin E_1. \end{aligned}$$

**Proof**

Let

$$\phi(X_i) = \alpha_i + \sum_{1 \le j \le n} \beta_{i,j} Y_j + \sum_{(j,k) \notin E_2} \gamma_{i,j,k} Y_j Y_k.$$

Since $X_i^2 = 0$ in the ring $\mathbf{R}_1$,

$$0 = \phi(X_i^2) = \phi(X_i)^2 = \alpha_i^2 + (\text{higher degree terms}).$$

This gives $\alpha_i = 0$. Therefore, $\phi(X_i)$ can be written as

$$\phi(X_i) = \sum_{1 \le j \le n} \beta_{i,j} Y_j + \sum_{(j,k) \notin E_2} \gamma_{i,j,k} Y_j Y_k.$$

For all $(i,j) \notin E_1$, $\phi(X_i X_j) = \phi(X_i)\phi(X_j)$ holds and neither $\phi(X_i)$ nor $\phi(X_j)$ has a constant term. Hence, $\phi(X_i X_j)$ has quadratic terms only and can be written as

$$\phi(X_i X_j) = \sum_{(k,l) \notin E_2} \delta_{i,j,k,l} Y_k Y_l.$$

□

**Corollary 4.4.** $\phi^{-1}\colon \mathbf{R}_2 \to \mathbf{R}_1$ satisfies the following conditions:

$$\begin{aligned}
\phi^{-1}(1) &= 1, \\
\phi^{-1}(Y_i) &= \sum_{1\le j\le n} \beta'_{i,j} X_j + \sum_{(j,k)\notin E_1} \gamma'_{i,j,k} X_j X_k \qquad \text{for all } 1 \le i \le n, \\
\phi^{-1}(Y_i Y_j) &= \sum_{(k,l)\notin E_1} \delta'_{i,j,k,l} X_k X_l \qquad \text{for all } (i,j) \notin E_2.
\end{aligned}$$

□

**Claim 4.5.** For all $(i,j) \notin E_2$, $Y_iY_j$ can be written as a linear combination of $\{\phi(X_kX_l) \mid (k,l) \notin E_1\}$.

**Proof** From Corollary 4.4, $\phi^{-1}(Y_iY_j)$ can be written as

$$\phi^{-1}(Y_iY_j) = \sum_{(k,l)\notin E_1} \delta'_{i,j,k,l} X_k X_l.$$

By mapping both sides by $\phi$, we get

$$Y_iY_j = \sum_{(k,l)\notin E_1} \delta'_{i,j,k,l} \phi(X_k X_l).$$

□

Now, we define a new mapping $\phi' : \mathbf{R}_1 \to \mathbf{R}_2$ as follows:

$$\begin{aligned}
\phi'(1) &= 1, \\
\phi'(X_i) &= \sum_{1\le j\le n} \beta_{i,j} Y_j \qquad \text{for all } 1 \le i \le n, \\
\phi'(X_iX_j) &= \sum_{(k,l)\notin E_2} \delta_{i,j,k,l} Y_k Y_l \quad \text{for all } (i,j) \notin E_1.
\end{aligned}$$

The mappings $\phi'$ and $\phi$ are almost the same, but $\phi'(X_i)$'s are a little bit different from $\phi(X_i)$'s since quadratic terms are removed from $\phi(X_i)$.

**Claim 4.6.** $\phi'$ is also an isomorphism from $\mathbf{R}_1$ to $\mathbf{R}_2$.

**Proof** It suffices to show that $\phi'$ satisfies the conditions described in Remark 4.2.

First, we will check if $\{\phi'(1), \{\phi'(X_i)\}_{1\le i\le n}, \{\phi'(X_iX_j)\}_{(i,j)\notin E_1}\}$ are linearly independent. Notice that $\phi'(1)$ and $\phi'(X_iX_j)$'s are equal to $\phi(1)$ and $\phi(X_iX_j)$'s, and $\phi'(X_i)$'s are "changed" from $\phi(X_i)$'s by removing quadratic terms. From Claim 4.5, $Y_kY_l$'s can be written as a linear combination of $\{\phi(X_iX_j)\}$, so the difference between $\phi'(X_i)$ and $\phi(X_i)$ is a linear combination of $\{\phi(X_kX_l)\}$. Therefore, they are still linearly independent.

Second, $\phi'(X_i)\phi'(X_j) = \phi'(X_iX_j)$ holds since

$$\phi'(X_iX_j) = \phi(X_iX_j) = \phi(X_i)\phi(X_j) = \sum_{1\le k\le n}\sum_{1\le l\le n} \beta_{i,k}\beta_{j,l} Y_k Y_l = \phi'(X_i)\phi'(X_j).$$

Therefore, $\phi'$ is indeed an isomorphism. □

**Remark 4.7.** Note that $\phi'^{-1} \colon \mathbf{R}_2 \to \mathbf{R}_1$ satisfies the following conditions:

$$\begin{aligned}
\phi^{-1}(1) &= 1, \\
\phi^{-1}(Y_i) &= \sum_{1 \le j \le n} \beta'_{i,j} X_j && \text{for all } 1 \le i \le n, \\
\phi^{-1}(Y_i Y_j) &= \sum_{(k,l) \notin E_1} \delta'_{i,j,k,l} X_k X_l && \text{for all } (i,j) \notin E_2.
\end{aligned}$$

□

From here, we assume that $\phi(X_i)$'s have no quadratic term, since, even if $\phi(X_i)$'s have quadratic terms, we can construct a new isomorphism (namely, $\phi'$) by removing quadratic terms from $\phi(X_i)$.

We define a mapping $f_\phi \colon 2^{V_1} \to 2^{V_2}$ as

$$f_\phi(S) := \{j \mid i \in S, \beta_{i,j} \neq 0\}.$$

A mapping $f_{\phi^{-1}} : 2^{V_2} \to 2^{V_1}$ is defined similarly:

$$f_{\phi^{-1}}(S') := \{j \mid i \in S', \beta'_{i,j} \neq 0\}.$$

**Claim 4.8.** Let $C \subset V_1$ be a clique in $G_1$. Then, $f_\phi(C)$ is a clique in $G_2$. Similarly, let $C' \subset V_2$ be a clique in $G_2$. Then, $f_{\phi^{-1}}(C')$ is a clique in $G_1$.

**Proof** We will prove the former statement. The latter one can be proved similarly.

It suffices to show that $(i,j) \in E_2$ (i.e. $Y_iY_j = 0$) for any $i, j \in \phi(C)$ , $i \neq j$. There are two cases to consider.

1. There exists $k \in C$ such that $\beta_{k,i} \neq 0$ and $\beta_{k,j} \neq 0$.
2. There exists no such $k \in C$.

In case 1, $\phi(X_k^2)$ can be written as:

$$\phi(X_k^2) = 2\beta_{k,i}\beta_{k,j}Y_iY_j + (\text{other terms}).$$

Since $\phi(X_k^2) = 0$ and $2\beta_{k,i}\beta_{k,j}$ is nonzero by the choice of $k$, $Y_iY_j$ must be zero.

In case 2, we can choose $k, l \in C$ such that $\beta_{k,i} \neq 0$ and $\beta_{l,j} \neq 0$. Then, $\phi(X_kX_l)$ can be written as:

$$\phi(X_kX_l) = \beta_{k,i}\beta_{l,j}Y_iY_j + (\text{other terms}).$$

Since $C$ is a clique, $\phi(X_kX_l) = 0$. By the choice of $k$ and $l$, $\beta_{k,i}\beta_{k,j}$ is nonzero. This gives $Y_iY_j = 0$. □

**Claim 4.9.** For all $S \subset V_1$ and $S' \subset V_2$,

$$|S| \le |f_\phi(S)|,$$

$$|S'| \le |f_{\phi^{-1}}(S')|.$$

**Proof** We will prove the former one. Each of $\{\phi(X_i) \mid i \in S\}$ is a linear combination of $\{Y_j \mid j \in \phi(S)\}$, and they are linearly independent. Therefore, $|\phi(S)|$ must be at least $|S|$. □

**Claim 4.10.** For all $S \subset V_1$ and $S' \subset V_2$,

$$f_{\phi^{-1}}(f_\phi(S))) \supseteq S,$$

$$f_\phi(f_{\phi^{-1}}(S'))) \supseteq S'.$$

**Proof** We will prove the former one. For $i \in S$, let

$$\phi(X_i) = \sum_{k \in f_\phi(S)} \beta_{i,k} Y_k.$$

By mapping both sides by $\phi$,

$$X_i = \sum_{k \in f_\phi(S)} \beta_{i,k} \phi^{-1}(Y_k).$$

Hence, there exists $k \in f_\phi(S)$ such that $\beta'_{k,i}$ is nonzero (that is, $X_i$ appears in $\phi^{-1}(Y_k)$). This shows $i \in f_{\phi^{-1}}(f_\phi(S))$. □

**Corollary 4.11.** Let $C$ be a maximal clique in $G_1$, and $C'$ be a maximal clique in $G_2$. Then,

$$f_{\phi^{-1}}(f_\phi(C))) = C,$$

$$f_\phi(f_{\phi^{-1}}(C'))) = C'.$$

**Proof** Immediate from Claim 4.8 and Claim 4.9. □

**Claim 4.12.** Let $C$ be a maximal clique in $G_1$. Then, $f_\phi(C)$ is a maximal clique in $G_2$ and $|C| = |f_\phi(C)|$ holds. Similarly, Let $C'$ be a maximal clique in $G_2$. Then, $f_{\phi^{-1}}(C')$ is a maximal clique in $G_1$ and $|C'| = |f_{\phi^{-1}}(C)|$ holds.

**Proof** We will prove the former statement Let $C^*$ be a clique in $G_2$ which contains $f_\phi(C)$. We are going to show that $|C| = |f_\phi(C)|$ and $|f_\phi(C)| = |C^*|$.

Since $C$ is a maximal clique, $f_{\phi^{-1}}(f_\phi(C))) = C$ holds from Corollary 4.11. By the choice of $C^*$, $f_{\phi^{-1}}(C^*) \supseteq f_{\phi^{-1}}(f_\phi(C)) = C$ holds. This means $f_{\phi^{-1}}(C^*)$ is a clique which contains $C$. Since $C$ is maximal, $f_{\phi^{-1}}(C^*)$ must be equal to $C$.

On the other hand, from Claim 4.9, we get

$$|C| \leq |f_\phi(C)| \leq |C^*| \leq |f_{\phi^{-1}}(C^*)|.$$

Since we already know that $f_{\phi^{-1}}(C^*) = C$, the equalities hold throughout the inequalities above. This gives $|C| = |f_\phi(C)|$ and $|f_\phi(C)| = |C^*|$. □

**Claim 4.13.** Let $\mathcal{M}$ be the set of maximal cliques of $G_1$, and $\mathcal{M}'$ be the set of maximal cliques of $G_2$. The mapping

$$\mathcal{M} \to \mathcal{M}' : C \mapsto f_\phi(C)$$

yields one-to-one correspondence between $\mathcal{M}$ and $\mathcal{M}'$.

**Proof** The mapping is injective since $f_\phi(C)$ is a maximal clique in $G_2$ from Claim 4.12. It is also surjective because, for any $C' \in \mathcal{M}'$, $f_{\phi^{-1}}(C')$ is a maximal clique in $G_1$ and $f_\phi(f_{\phi^{-1}}(C')) = C'$ from Corollary 4.11. □

From the claim above, $G_1$ and $G_2$ have the same number of maximal cliques. Let $l$ be the number of maximal cliques in $G_1$ and $G_2$. Let $C_1, C_2, C_3, \ldots, C_l$ be maximal cliques in $G_1$, and $C'_1, C'_2, C'_3, \ldots, C'_l$ be maximal cliques in $G_2$. Here, we assume that $f_\phi(C_i) = C'_i$ holds for all $i$.

**Claim 4.14.** For all $1 \leq m \leq n$ and $1 \leq j_1 < \cdots < j_m \leq n$, the following equality holds:

$$|\bigcup_{i=1}^{m} C_{j_i}| = |\bigcup_{i=1}^{m} C'_{j_i}|.$$

**Proof** From Claim 4.12, the statement holds when $m = 1$.

Let us consider the case when $m = 2$. Since $\phi(X_i)$ , $i \in C_{j_1} \cup C_{j_2}$ , are linearly independent,

$$|C_{j_1} \cup C_{j_2}| \leq |C'_{j_1} \cup C'_{j_2}|.$$

Applying the above argument to the other direction, we also get

$$|C_{j_1} \cup C_{j_2}| \geq |C'_{j_1} \cup C'_{j_2}|.$$

Combining these two inequalities, we get

$$|C_{j_1} \cup C_{j_2}| = |C'_{j_1} \cup C'_{j_2}|.$$

We can prove the statement similarly when $m > 2$. □

The above claim shows that the structure of maximal cliques of $G_1$ and that of $G_2$ is exactly the same. Therefore, $G_1$ and $G_2$ are isomorphic. Thus, we finish the whole proof of Theorem 4.1. □

## 5 Computing a Graph Isomorphism from a Ring Isomorphism

In this section, we discuss how to compute a graph isomorphism from a ring isomorphism between rings constructed from graphs using our new reduction.

As discussed above, in known reductions, one of the original graph isomorphisms can be found easily in each ring isomorphism obtained for the reduced ring isomorphism problem instance. On the other hand, it is not clear how to get a graph isomorphism from a ring isomorphism in our reduction.

However, we can show a way to obtain one as stated below.

**Theorem 5.1.** Let $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ be simple graphs and $\mathbf{R}_{G_1}, \mathbf{R}_{G_2}$ be rings constructed from $G_1$ and $G_2$ using construction 3. Given an isomorphism $\phi : \mathbf{R}_{G_1} \to \mathbf{R}_{G_2}$, we can compute a graph isomorphism from $G_1$ to $G_2$ in polynomial time.

**Proof** Throughout the proof, we use the same notation as in the proof of Theorem 4.1.

We define $P_S$ and $Q_S$ for $S \subseteq \{1, \ldots, l\}$ as follows.

$$\begin{aligned} P_S &= \{\bigcap_{i \in S} C_i\} \cap \{\bigcap_{i \notin S} \overline{C_i}\}, \\ Q_S &= \bigcap_{i \in S} C_i. \end{aligned}$$

We define $P'_S$ and $Q'_S$ similarly. For example, when $l = 4$, $P_{\{1,4\}} = C_1 \cap \overline{C_2} \cap \overline{C_3} \cap C_4$ and $Q_{\{1,4\}} = C_1 \cap C_4$. We can see that the following equality holds from the definition:

$$Q_S = \bigcup_{T \supseteq S} P_S.$$

The similar equality between $P'_S$ and $Q'_S$ also holds. Now, $G_1$ and $G_2$ are isomorphic since $\mathbf{R}_1$ and $\mathbf{R}_2$ are isomorphic. Thus, the following equalities hold for every $S \subseteq \{1, \dots, l\}$:

$$\begin{aligned} |P_S| &= |P'_S|, \\ |Q_S| &= |Q'_S|. \end{aligned}$$

**Claim 5.2.** A bijection $\pi\colon V_1 \to V_2$ is a graph isomorphism if it satisfies the condition below:

$$i \in P_S \Rightarrow \pi(i) \in P'_S.$$

**Proof** We will prove that for any $i \in P_S$ and $j \in P_T$, $(\pi(i), \pi(j)) \in E_2$ if and only if $(i, j) \in E_1$.

Suppose that $(i, j) \in E_1$. Then, $S \cap T$ is not empty, since there is at least one maximal clique in $G_1$ that contains both $i$ and $j$. From the condition, $\pi(i) \in P'_S$ and $\pi(j) \in P'_T$ hold. Thus, there is at least one maximal clique in $G_2$ that contains both $\pi(i)$ and $\pi(j)$. Therefore, $(\pi(i), \pi(j)) \in E_2$.

On the other hand, suppose that $(i, j) \notin E_1$. Then, $S \cap T$ must be empty. Hence, there is no maximal clique in $G_2$ that contains both $\pi(i) \in P'_S$ and $\pi(j) \in P'_T$. This means $(\pi(i), \pi(j)) \notin E_2$. □

**Claim 5.3.** For any $S \subseteq \{1, \dots, l\}$ and $i \in P_S$, $f_\phi(\{i\}) \subseteq Q'_S$.

**Proof** For all $k \in S$, $f_\phi(\{i\}) \subseteq f_\phi(C_k) = C'_k$ holds since $\{i\} \subseteq C_k$. Therefore, we get

$$f_\phi(\{i\}) \subseteq \bigcap_{k \in S} C'_k = Q'_S.$$

□

**Claim 5.4.** Given $\phi\colon \mathbf{R}_1 \to \mathbf{R}_2$, let $\pi\colon V_1 \to V_2$ be a bijection such that $\pi(i) \in f_\phi(\{i\})$ holds for all $i \in V_1$. Then, $\pi$ is a graph isomorphism between $G_1$ and $G_2$.

**Proof** From Claim 5.2, it suffices to show that $\pi(i) \in P'_S$ for all $S \subseteq \{1, \dots l\}$ and $i \in P_S$. We will prove it by induction on $S$. Note that from the condition and Claim 5.3, $\pi(i) \in Q'_S$ holds since $\pi(i) \in f_\phi(\{i\}) \subset Q'_S$.

When $S = \{1, \dots, l\}$, the statement clearly holds since $\pi(i) \in Q'_S = P'_S$.

Assume that the above statement holds for all $T \supsetneq S$. For all $i \in P_S$,

$$\pi(i) \in Q'_S = \bigcup_{T \supseteq S} P'_T.$$

This means that bijection $\pi$ maps $i$ to a vertex in $P'_T$ such that $T \supseteq S$. From the induction hypothesis, for all $T \supsetneq S$, all vertices in $P_T$ are already mapped to vertices in $P'_T$. Combining the condition that $|P_T| = |P'_T|$ and that $\pi$ is a bijection, $i$ cannot be mapped to vertices in $P'_T$ such that $T \supseteq S$. Thus, $i$ must be mapped to vertices in $P'_S$, so $\pi(i) \in P'_S$ holds. This completes the induction. □

The problem of finding a bijection $\pi : V_1 \to V_2$ such that $\pi(i) \in f_\phi(\{i\})$ for all $i \in V_1$ can be regarded as a problem of finding a perfect matching of the bipartite graph $G'$ defined below:

$$\begin{aligned} G' &:= (V', E'), \\ V' &:= V_1 \cup V_2, \\ E' &:= \{(i, j) \mid j \in f_\phi(\{i\})\}. \end{aligned}$$

Claim 5.4 shows that any perfect matching of $G'$ forms a graph isomorphism. It is well-known that a maximum matching in a bipartite graph can be found in polynomial time [4]. From Claim 4.9, $|S| \leq |f_\phi(S)|$ holds for all $S \subset V_1$. Combining Hall's theorem [5], we can see that there is at least one perfect matching in $G'$.

Therefore, we can compute a graph isomorphism $\pi : V_1 \to V_2$ from a ring isomorphism $\phi : \mathbf{R}_1 \to \mathbf{R}_2$ in polynomial time.

□

**Remark 5.5.** In the existing reductions, one ring isomorphism corresponds to one graph isomorphism. On the other hand, the proof of Theorem 5.1 essentially shows that one ring isomorphism in our reduction may correspond to many graph isomorphisms, since there may be more than one solutions for perfect matching of $G'$, and each matching corresponds to a different graph isomorphism.

## 6 Conclusion and Open Problems

In this paper, we proposed a new reduction from the graph isomorphism problems to the ring isomorphism problem, which is based on a simpler and more natural construction of a ring from a graph than the existing reductions. We also show that one ring isomorphism in our reduction may correspond to many graph isomorphisms, and we can compute one in polynomial time.

We pose a few open problems which we expect answers.

- Can we reduce the ring isomorphism problem to the graph isomorphism problem, or the hypergraph isomorphism problem?
- Is there a polynomial-time quantum algorithm for the ring isomorphism problem? Using specific structure of rings, we might be able to solve it efficiently using quantum computers.

## References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in P. *Annals of Mathematics*, Vol. 160, No. 2, pp. 781–793, 2004.

[2] Neeraj Kayal and Nitin Saxena. Complexity of ring morphism problems. *Comput. Complex.*, Vol. 15, No. 4, pp. 342–390, 2006.

[3] Manindra Agrawal and Nitin Saxena. Automorphisms of finite rings and applications to complexity of problems. In *STACS'05, Springer LNCS 3404*, pp. 1–17. Springer Verlag, 2005.

[4] John E. Hopcroft and Richard M. Karp. An $\mathrm{n}^{5/2}$ algorithm for maximum matchings in bipartite graphs. *SIAM J. Comput.*, Vol. 2, No. 4, pp. 225–231, 1973.

[5] P. Hall. On representatives of subsets. *J. London Math. Soc.*, Vol. 10, No. 37, pp. 26–30, 1935.