数理解析研究所講究録
第1649巻 2009年 189-194

グラフ同型問題から環同型問題への新たな帰着

早坂智行 (Tomoyuki Hayasaka)
東京工業大学 理学部 情報科学科
Dept. of Information Science, School of Science,
Tokyo Institute of Technology

概要

グラフ同型問題は環同型問題に帰着することができることが知られている．また，帰着の際にグラフからどのような環を作るかについて2通りの構成法が既に知られている．本論文では，既知の2つの構成法よりも自然でシンプルな第3の構成法を考案し，この構成法においてもグラフの同型性と環の同型性が同値であることを示した．また，既知の2つの構成法において，環の同型写像はある一つのグラフ同型写像を直接含んでいる．これに対し，今回の新しい構成法における環の同型写像からも，多項式時間でグラフの同型写像を計算することができるだけでなく，複数のグラフ同型写像の情報を含んでいる可能性があることも示した．

1 はじめに

環とは，加法（+）と乗法（$\cdot$）の二つの二項演算を備えた代数系のことであり，数学の研究，特に数論や代数学の研究において欠かせないものである．

また，計算機科学の世界においても，様々な問題が環の問題としてとらえることができることが知られている．たとえば，[1] の決定的多項式時間の素数判定テストは，環 $\mathbb{Z}_n[X]/\langle X^r-1\rangle$ なる環の自己同型写像を調べていると見なすことができる [2]．同様に素因数分解問題も，ある環の同型写像の数を計算する，あるいは同型写像を一つ求める，といった環の同型写像の問題に帰着される [3]．

またそれに類する結果として，グラフ同型問題を環同型問題へ多項式時間多対一還元を行うことができる，ということが知られている [3, 2]．本論文では，これに対し別証を与える．

第2章ではグラフ同型問題を環同型問題へ帰着を行うための既知の構成法を紹介する．第3章ではより自然でシンプルな新しい構成法を紹介し，それにより帰着を行うことができることを証明する．第4章では新しい構成法における環の同型写像から，グラフの同型写像を計算する方法を与える．第5章ではまとめと今後の課題について述べる．

2 既知の帰着法

グラフ同型問題から環同型問題への帰着では，与えられたグラフから「グラフの構造を表現する環」を構成する，という事を行う．

[3] においては，以下のような帰着法が紹介された．

構成法 1([3])

n 頂点のグラフ $G=(V,E)$ に対応して，$V_1,\ldots,V_n$, $A_{(1,2)},\ldots,A_{(n-1,n)}$ を変数とする次のような多項式環 $\mathbf{R}_G$ を作る．

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

ただし，p は奇素数であり，イデアル I は，この環が以下のような関係式を満たすように決める．

- $V_i^2=0$
- $V_iV_j=V_jV_i=A_{(i,j)}$
- $A_eV_i=A_iV_e=0, A_eA_{e'}=0$
- $e\in E$ において，A_e の位数は p
- $e\notin E$ において，A_e の位数は p^2

このとき，グラフ G_1，G_2 が同型のとき，かつその時に限り，構成法1により作られた環 $\mathbf{R}_{G_1}$，$\mathbf{R}_{G_2}$ が同型となる．これにより，グラフ同型問題を環同型問題に帰着させる事ができる．

この構成法においては、変数 $V_1,\ldots,V_n$ が各頂点を表しており，$A_{(1,2)},\ldots,A_{(n-1,n)}$ が頂点のペアを表している，と見ることができる．また，辺がある点のペアにおいてはその位数を p に，辺がない点のペアにおいてはその位数を p^2 にすることで，グラフの辺の情報を表現している．

$\mathbf{R}_{G_1}\cong\mathbf{R}_{G_2}$ であるとき，同型写像 $\phi:\mathbf{R}_{G_1}\to\mathbf{R}_{G_2}$ において，各 V_i について $\phi(V_i)$ は次のように書ける．

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

ただし，$\mathbf{R}_{G_2}$ における $V_1,\ldots,V_n,A_{(1,2)},\ldots,A_{(n-1,n)}$ を区別のために $V_1',\ldots,V_n',A'_{(1,2)},\cdots,A'_{(n-1,n)}$ と表記している．このとき，ただ一つの j において，$\beta_{i,j}$ が $\mathbb{Z}_{p^3}$ において逆元を持つ．このような j を $\pi(i)$ と書くことにすると，$\pi(i)$ は G_1 から G_2 への同型写像を与えることが知られている．

[2] においては，以下のような帰着法が紹介された．ここで，$\langle S\rangle$ は集合 S から生成されるイデアルを表すものとする．

構成法 2([2])

n 頂点のグラフ $G=(V,E)$ に対応して，$X_1,\ldots,X_n$ を変数とする次のような多項式環 $\mathbf{R}_G$ を作る．

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

ただし，$\mathbb{F}_q$ は奇数位数の有限体であり，多項式 $p_G\in\mathbb{F}_q[X_1,\ldots,X_n]$ は次のような多項式である．

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

このとき，グラフ G_1，G_2 が，孤立点を除くと完全グラフになるようなグラフでないとき，G_1，G_2 が同型のとき，かつその時に限り，構成法 2 により作られた環 $\mathbf{R}_{G_1}$，$\mathbf{R}_{G_2}$ が同型となる．

この構成法においては，一次の項 $X_1,\ldots,X_n$ が各頂点を表しており，二次の項 $X_1X_2,\ldots,X_{n-1}X_n$ が頂点のペアを表している，とみることができる．また，辺がある点のペアを全て足すと 0 になる，という条件を環が満たすようにすることで，グラフの辺の情報を保存している．

2 の場合，同型写像 $\phi:\mathbf{R}_{G_1}\to\mathbf{R}_{G_2}$ において，$\phi(X_i)$ は次のように書ける．

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

ただし，$\mathbf{R}_{G_2}$ における $X_1,\ldots,X_n$ を区別のため $Y_1,\ldots,Y_n$ と表記している．このとき，ただ一つの j において，$\beta_{i,j}\neq0$ となる．このような j を $\pi(i)$ と書くことにすると，$\pi(i)$ は G_1 から G_2 への同型写像を与えることが知られている．

3 新しい帰着法

一つ目の帰着法は，比較的複雑な構造をしている．また，二つ目の帰着法は，シンプルではあるが，条件付きであることと，「辺のあるところを足すと 0 になる」という構造となっていることが若干不自然である．

そこで，次のようなよりシンプルにグラフの構造を表現している環も，グラフ同型性問題から環同型性問題への帰着に利用できないか，と考えるのはごく自然なことである．

構成法 3

n 頂点のグラフ $G=(V,E)$ に対応して，次のような環 $\mathbf{R}_G$ を作る．

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

ただし、$\mathbb{F}_q$ は奇数位数の有限体である．

この構成法 3 は，構成法 2 における「辺のあるところをすべて足すと 0 になる」という部分を変更し，「辺は 0 である」としたものである．この構成は構成法 1 より簡潔であり，かつ構成法 2 よりも辺の情報の埋め込みかたが自然である．

しかし，この構成法 3 において，グラフが同型であることと構成された環が同型であることが同値であるかどうかは明らかではない．なぜなら，環の同型写像は直接的にはグラフの同型写像を表さない場合があるからである．実際，ある環の同型写像 $\phi:\mathbf{R}_{G_1}\to\mathbf{R}_{G_2}$ が与えられ，

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

と書いたとき，$\beta_{i,j}\neq0$ となるような j は複数ある場合があり，またそのような $\beta_{i,j}$ は有限体の要素であるから逆元を必ず持つ．そのため，構成法 1 や構成法 2 の際と

同様の方法ではグラフの同型写像を得られない．したがって，環が同型のときグラフも同型であるかどうかは自明ではない．

しかしながら，この構成法について次の結果を得た．

定理 3.1. グラフ G_1，G_2 が同型のとき，かつその時に限り，構成法 3 により作られた環 $\mathbf{R}_{G_1}$，$\mathbf{R}_{G_2}$ が同型である．

証明. 以下，$G_1=(V_1,E_1), G_2=(V_2,E_2)$ から構成法 3 により作られた環を $\mathbf{R}_1, \mathbf{R}_2$ と書く．

グラフ G_1 と G_2 が同型であるとき，グラフの同型写像が自然に導く環の同型写像により $\mathbf{R}_1$ と $\mathbf{R}_2$ が同型となるのは明らかである．

逆に，$\mathbf{R}_1$ から $\mathbf{R}_2$ への同型写像 ϕ が存在すると仮定する．このとき，G_1 と G_2 が同型であることを示す．

まず，一般性を失わずに G_1 と G_2 の頂点数は等しいとして良い．なぜなら，G_1 と G_2 の頂点数が等しくない場合は，$\mathbf{R}_1$ と $\mathbf{R}_2$ が同型にはならないことが簡単に分かるからである．G_1 と G_2 の頂点数を n とおく．$\mathbf{R}_2$ における変数 $X_1,\ldots,X_n$ を区別のため $Y_1,\ldots,Y_n$ と表記する．

注 3.2. 同型写像の定義より，ϕ は次の条件を満たすことに注意する．

- $\{\phi(1),\{\phi(X_i)\}_{1\le i\le n},\{\phi(X_iX_j)\}_{(i,j)\notin E_1}\}$ が $\mathbf{R}_2$ において基底をなしている．したがって，これらは線形独立である．
- $\phi(X_i)\phi(X_j)=\phi(X_iX_j)$ が成立している．

主張 3.3. 同型写像 $\phi:\mathbf{R}_1\to\mathbf{R}_2$ は以下のような形をしている．

$$\begin{aligned}
\phi(1)&=1\\
\phi(X_i)&=\sum_{1\le j\le n}\beta_{i,j}Y_j+\sum_{(j,k)\notin E_2}\gamma_{i,j,k}Y_jY_k \quad (1\le i\le n)\\
\phi(X_iX_j)&=\sum_{(k,l)\notin E_2}\delta_{i,j,k,l}Y_kY_l \qquad ((i,j)\notin E_1)
\end{aligned}$$

証明. 任意の X_i について，$\phi(X_i)$ は，

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

という形で書けるはずである．$\mathbf{R}_1$ 上で $X_i^2=0$ であることを利用すると，

$$0=\phi(X_i^2)=\phi(X_i)^2=\alpha_i^2+(\text{一次以上の項})$$

より $\alpha_i=0$ である．したがって，$\phi(X_i)$ は次のように書ける．

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

また，$\phi(X_iX_j)$(ただし $(i,j)\notin E_1$) について，$\phi(X_iX_j)=\phi(X_i)\phi(X_j)$ であり，$\phi(X_i),\phi(X_j)$ が定数項を持たず一次以上の項しか持たないことから，$\phi(X_iX_j)$ は二次の項しか持たない．したがって，$\phi(X_iX_j)$ は次のように書ける．

$$\phi(X_iX_j)=\sum_{(k,l)\notin E_2}\delta_{i,j,k,l}Y_kY_l$$

以上により主張は示された． □

系 3.4. ϕ^{-1} は以下のような形をしている．

$$\begin{aligned}
\phi^{-1}(1)&=1\\
\phi^{-1}(Y_i)&=\sum_{1\le j\le n}\beta'_{i,j}X_j+\sum_{(j,k)\notin E_1}\gamma'_{i,j,k}X_jX_k \quad (1\le i\le n)\\
\phi^{-1}(Y_iY_j)&=\sum_{(k,l)\notin E_1}\delta'_{i,j,k,l}X_kX_l \qquad ((i,j)\notin E_2)
\end{aligned}$$

主張 3.5. 任意の $(i,j)\notin E_2$ について，Y_iY_j は $\{\phi(X_kX_l)\mid(k,l)\notin E_1\}$ の線形結合で書ける．

証明. 系 3.4 より，

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

と書けるから，ϕ を両辺に作用させると，

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

□

ϕ を若干変更して次のような写像 $\phi':\mathbf{R}_1\to\mathbf{R}_2$ を作ることができる．

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

X_i の写像先のみ，ϕ と ϕ' は異なっており，$\phi'(X_i)$ は，$\phi(X_i)$ から二次の項 Y_kY_l が省かれている．

主張 3.6. ϕ' も $\mathbf{R}_1$ から $\mathbf{R}_2$ への同型写像である．

証明. ϕ' について，注 3.2 の各性質が満たされているかどうかをチェックすれば良い．

まず，線形独立性について確かめる．$\phi'(X_i)$ は，$\phi(X_i)$ から Y の二次の項 Y_kY_l を除いたものであるが，主張 3.5 より Y_kY_l は $\{\phi(X_iX_j)\}$ の線形結合で書けるから，$\phi'(X_i)$ は $\phi(X_i)$ から $\{\phi(X_kX_l)\}$ の線形結合を除いたものであるといえる．したがって線形独立性は保たれる．

また，$\phi'(X_i)\phi'(X_j)=\phi'(X_iX_j)$ が満たされることは，

$$\phi'(X_iX_j)=\phi(X_iX_j)=\phi(X_i)\phi(X_j)=\phi'(X_i)\phi'(X_j)$$

となることより確かめられる．

以上により ϕ' も $\mathbf{R}_1$ から $\mathbf{R}_2$ への同型写像である． □

注 3.7. ϕ'^{-1} は以下のようになることが容易に分かる．

$$\phi^{-1}(1)=1$$
$$\phi^{-1}(Y_i)=\sum_{1\le j\le n}\beta'_{i,j}X_j$$
$$\phi^{-1}(Y_iY_j)=\sum_{(k,l)\notin E_1}\delta'_{i,j,k,l}X_kX_l \quad ((i,j)\notin E_2)$$

以降は，議論を簡単にするため，ϕ' をあらためて ϕ と置く．

ϕ を用いた，G_1 の点集合から G_2 の点集合への写像 $f_\phi:2^{V_1}\to 2^{V_2}$ を以下のように定義する．

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

これは，G_1 の点集合 S から，「S に含まれる X_i を ϕ で写した先に現れる Y_j」の点集合へ写像するものである．これと同様に $f_{\phi^{-1}}:2^{V_2}\to 2^{V_1}$ を以下のように定義する．

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

主張 3.8. $C\subset V_1$ が G_1 上クリークであるとき，$f_\phi(C)$ は G_2 上クリークである．同様に，$C'\subset V_2$ が G_2 上クリークであるとき，$f_{\phi^{-1}}(C')$ は G_1 上クリークである．

証明. 前者のみ示す．後者も同様にして示される．任意の $i,j\in\phi(C)$(ただし $i\neq j$) について，$(i,j)\in E_2$ であること，すなわち $Y_iY_j=0$ であることを示せばよい．次の 2 つの場合に分けて考える．

1. ある $k\in C$ において $\beta_{k,i}\neq 0$ かつ $\beta_{k,j}\neq 0$ となる場合
2. そうでない場合

1 の場合，$\phi(X_k^2)$ の値は次のように書ける．

$$\phi(X_k^2)=2\beta_{k,i}\beta_{k,j}Y_iY_j+(Y_iY_j\text{を含まない項})$$

$\phi(X_k^2)=0$ であり，$2\beta_{k,i}\beta_{k,j}\neq 0$ であるから，$Y_iY_j=0$ である．

2 の場合，$\beta_{k,i}\neq 0$，$\beta_{l,j}\neq 0$ となる $k,l\in C$ を取ってくると，$\phi(X_kX_l)$ の値は以下のようになる．

$$\phi(X_kX_l)=\beta_{k,i}\beta_{l,j}Y_iY_j+(Y_iY_j\text{を含まない項})$$

C がクリークであるから $\phi(X_kX_l)=0$ であり，$\beta_{k,i}\beta_{k,j}\neq 0$ であるから，$Y_iY_j=0$ である． □

主張 3.9. $S\subset V_1$ と $S'\subset V_2$ について，

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

が成立する．

証明. 前者のみ示す．$\{\phi(X_i)\mid i\in S\}$ はそれぞれが $\{Y_j\mid j\in\phi(S)\}$ の線形結合でかけ，かつ線形独立である．したがって，$|S|\le|\phi(S)|$ でなければならない． □

主張 3.10. $S\subset V_1$ と $S'\subset V_2$ について，

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

が成立する．

証明. 前者のみ示す．$i\in S$ について，

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

と書ける．これより，

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

となる．したがって，ある $k\in f_\phi(S)$ において $\beta'_{k,i}\neq 0$ である（つまり $\phi^{-1}(Y_k)$ の値に X_i が現れる）．したがって，$i\in f_{\phi^{-1}}(f_\phi(S))$ である． □

系 3.11. G_1 上の極大クリーク C と G_2 上の極大クリーク C' について，

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

が成立する．

主張 3.12. G_1 上の極大クリーク C について，$f_\phi(C)$ は G_2 上の極大クリークであり，$|C|=|f_\phi(C)|$ が成立する．同様に，G_2 上の極大クリーク C' について，$f_{\phi^{-1}}(C')$ は G_1 上の極大クリークであり，$|C'|=|f_{\phi^{-1}}(C')|$ が成立する．

証明. 前者のみ示す．C は極大クリークであるから，$f_{\phi^{-1}}(f_\phi(C)))=C$ が成立する．$C^*\supseteq f_\phi(C)$ なる G_2 上の任意のクリーク C^* について，$f_{\phi^{-1}}(C^*)\supseteq f_{\phi^{-1}}(f_\phi(C))=C$ であり，C が極大であることにより $f_{\phi^{-1}}(C^*)=C$ である．ここで 主張 3.9 を用いると，

$$|C|\le|f_\phi(C)|\le|C^*|\le|f_{\phi^{-1}}(C^*)|=|C|$$

となるので，上式中の不等号は実際には全て等号であることが分かる．したがって $|f_\phi(C)|=|C^*|$ より $f_\phi(C)$ は極大クリークであり，$|C|=|f_\phi(C)|$ が成立する． □

系 3.13. G_1 上の極大クリーク C と G_2 上の極大クリーク C' について，

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

が成立する．

これより，$f_\phi(C) = C'$ という G_1 上の極大クリーク C と G_2 上の極大クリーク C' の関係は，一対一の対応関係であることが簡単に分かる．この対応関係から，G_1 の極大クリークの総数と G_2 極大クリークの総数は等しいことになる．

以下，G_1 と G_2 の極大クリークの総数を l とする．また，グラフ G_1 の極大クリークを $C_1, C_2, C_3, \ldots, C_l$ とし，G_2 の極大クリークを $C'_1, C'_2, C'_3, \ldots, C'_l$ とし，$f_\phi(C_i) = C'_i$ が各 i で成立しているとする．

主張 3.14. $1 \leq m \leq n$ なる任意の m で，$1 \leq j_1 < \cdots < j_m \leq n$ において，

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

が成立する．

証明. $m = 1$ の場合は，主張 3.12 において既に示されている．$m = 2$ の場合を考える．$\{\phi(X_i) \mid i \in C_{j_1} \cup C_{j_2}\}$ が線形独立になるためには，

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

でなければならない．同様な議論を逆方向から行えば，

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

でなくてはならないことが分かる．すなわち，

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

である．$m > 2$ の場合も同様にして示される． □

これは，G_1 の極大クリークの構造と，G_2 の極大クリークの構造が完全に一致していることを示している．

したがって，$G_1 \cong G_2$ である． □

4 環の同型写像からのグラフの同型写像の構成

ここで，構成法 3 によりグラフから作られた環の同型写像が与えられたとき，そこからグラフの同型写像を構成できるか，ということを考える．

前述の通り，以前の構成法 1 と構成法 2 において，環の同型写像はグラフの同型写像を直接的に表しているのに対し，今回の構成法 3 における環の同型写像は直接的にはグラフの同型写像を表していない．しかし，構成法 3 から得られた環の同型写像からでも，グラフの同型写像を多項式時間で計算できることが示される．

定理 4.1. グラフ $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$ が同型であるとする．構成法 3 により作られた環 $\mathbf{R}_{G_1}$ と $\mathbf{R}_{G_2}$ の任意の同型写像 $\phi : \mathbf{R}_{G_1} \to \mathbf{R}_{G_2}$ が与えられたとき，多項式時間でグラフの同型写像 $\pi : V_1 \to V_2$ を計算できる．

証明. 定理 3.1 の証明中と同様に $\mathbf{R}_{G_1}$ を $\mathbf{R}_1$，$\mathbf{R}_{G_2}$ を $\mathbf{R}_2$ と略記し，$\beta_{i,j}$，f_ϕ，$C_i (1 \leq i \leq l)$ といった記号も，先と同様のものを指すものとする．

証明の準備として新たな記号の定義を行う．$S \subseteq \{1, \ldots l\}$ に対して P_S, Q_S を次のように定義する．

$$P_S = \{\bigcap_{i \in S} C_i\} \cap \{\bigcap_{i \notin S} \overline{C_i}\}$$
$$Q_S = \bigcap_{i \in S} C_i$$

P'_S, Q'_S も同様に定義する．例えば，$l = 4$ のとき，$P_{\{1,4\}} = C_1 \cap \overline{C_2} \cap \overline{C_3} \cap C_4$ であり，$Q_{\{1,4\}} = C_1 \cap C_4$ である．

今，$G_1 \cong G_2$ であるから，任意の $S \subseteq \{1, \ldots, l\}$ において次が成立する．

$$|P_S| = |P'_S|$$
$$|Q_S| = |Q'_S|$$

また，定義より P_S と Q_S の関係として次の式が成立する．

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

P'_S と Q'_S の間でも同様の関係が成り立つ．

主張 4.2. 全単射写像 $\pi : V_1 \to V_2$ について，$i \in P_S$ ならば $\pi(i) \in P'_S$ となっているとき，π はグラフの同型写像である．

証明. $i \in P_S$ と $j \in P_T$ に対し，$(i, j) \in E_1$ のとき，またそのときに限り $(\pi(i), \pi(j)) \in E_2$ であることを示せばよい．

$(i, j) \in E_1$ であるとき，$S \cap T$ は空集合でない．なぜなら (i, j) という辺を含んだ極大クリークが少なくとも一つ存在するからである．今，$\pi(i) \in P'_S$ かつ $\pi(j) \in P'_T$ であり，さらに $S \cap T$ が空でないのだから $(\pi(i), \pi(j)) \in E_2$ である．

同様に，$(i, j) \notin E_1$ であるとき，$S \cap T$ は空集合であり，$\pi(i) \in P'_S$ かつ $\pi(j) \in P'_T$ であるから，$(\pi(i), \pi(j)) \notin E_2$ である． □

主張 4.3. 任意の $i \in V_1$ について，$i \in P_S$ であるならば，$f_\phi(\{i\}) \subseteq Q'_S$ である．

証明. $k \in S$ となる任意の k について，$\{i\} \subseteq C_k$ であることより $f_\phi(\{i\}) \subseteq \phi(C_k) = C'_k$ となる．したがって，$f_\phi(\{i\}) \subseteq Q'_S$ である． □

主張 4.4. 任意の同型写像 $\phi : \mathbf{R}_1 \to \mathbf{R}_2$ が与えられたとき，任意の i で $\beta_{i,\pi(i)} \neq 0$ である（すなわち $\pi(i) \in f_\phi(\{i\})$ である）ような全単射写像 $\pi : V_1 \to V_2$ は，グラフの同型写像となっている．

証明. $S \subseteq \{1,\ldots,l\}$ において，$i \in P_S$ ならば $\pi(i) \in P'_S$ である，という事象を $(*)$ と略記することにする．主張 4.2 より，任意の $S \subseteq \{1,\ldots l\}$ で $(*)$ が成立することを示せば良い．仮定より，$i \in P_S$ について $\pi(i) \in f_\phi(\{i\})$ であり，主張 4.3 より $f_\phi(\{i\}) \subset Q'_S$ であるから，$\pi(i) \in Q'_S$ が成立している事に注意し，帰納法により証明する．

$S = \{1,\ldots,l\}$ とする．このとき，$Q'_S = P'_S$ であるから，$i \in P_S$ について $\pi(i) \in Q'_S = P'_S$ となり $(*)$ が成立する．

$S \subseteq \{1,\ldots,l\}$ について，$T \supsetneq S$ となるような任意の $Y \supseteq \{1,\ldots,l\}$ で $(*)$ が成立していたと仮定する．$i \in P_S$ について，

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

であるが，帰納法の仮定より $T \supsetneq S$ なる P'_T に含まれる V_2 の各点について，π による V_1 の点との対応付けが既に決まっているから，結局 $\pi(i) \in P'_S$ でなければならない．したがって $(*)$ が成立する． □

任意の i で $\pi(i) \in f_\phi(\{i\})$ となるような全単射写像 $\pi : V_1 \to V_2$ を計算する問題は，2 部グラフ完全マッチングの問題であるとみなすことが出来る．すなわち，$i \in V_1$ と $j \in V_2$ が $j \in f_\phi(\{i\})$ のときに限り辺で繋がれているような，$V_1 \cup V_2$ を頂点集合とする 2 部グラフ上で，完全マッチングを行うのと同値である．ここで，主張 4.4 はその完全マッチングはグラフの同型写像を導くことを示している．また，任意の $S \subset V_1$ について，$|S| \leq |f_\phi(S)|$ であったから（主張 3.9 による），Hall の定理 [4] より，少なくとも一つ完全マッチングが存在することが保証される．また，2 部グラフの完全マッチングは，多項式時間で計算することが出来る [5]．

以上より，環の同型写像 $\phi : \mathbf{R}_1 \to \mathbf{R}_2$ からグラフの同型写像 $\pi : V_1 \to V_2$ を多項式時間で計算することが出来ることが示された． □

注 4.5. 構成法 1，構成法 2 における環の同型写像は唯一つのグラフ同型写像の情報を含んでいた．しかし，今回の構成法 3 の場合，定理 4.1 の証明から明らかなように，同型写像 $\phi : \mathbf{R}_1 \to \mathbf{R}_2$ は複数のグラフの同型写像の情報を含んでいる可能性がある．なぜなら，V_1 から V_2 へのマッチングの解は複数個ある可能性があり，それらは全てグラフの同型写像となっているからである．

5 まとめと今後の課題

本論文では，グラフ同型問題から環同型問題への帰着における，グラフから環の構成方法について，既知の 2 つの構成法 [3, 2] よりも自然でシンプルな第 3 の構成法を考案し，その構成法においても，グラフの同型性と環の同型性が同値であることを示した．また，既知の構成法において，環の同型写像はある一つのグラフ同型写像を直接含んでいるのに対し，今回の新しい構成法においては，環の同型写像から多項式時間でグラフの同型写像を計算することができるだけでなく，複数のグラフ同型写像の情報を含んでいる可能性があることも示した．

今後の課題としては，環同型問題とグラフ同型問題の難しさの関係を解明する上で，環同型問題からグラフ同型問題への逆向きの帰着は可能なのか，ということが未解決の問題として残されている．

また，量子計算機上において，環同型問題を効率的に解くことができるのか，という問題も未解決である．また，一般の環では難しくとも，帰着で利用される環に限った上で環同型性判定を効率的に解くことができるような量子アルゴリズムが存在するならば，グラフ同型問題も量子計算機上で効率よく解けることになる．

参考文献

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

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

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

[4] Reinhard Diestel. *Graph Theory*, Vol. 173 of *Graduate Texts in Mathematics*. Springer-Verlag, Heidelberg, 3rd edition, 2005.

[5] Thomas Cormen, Charles Leiserson, and Ronald Rivest. *Introduction to Algorithms*. The MIT Press, Cambridge, MA, 1989.