巡回グラフの同型問題

名古屋工業大学大学院 工学専攻 情報工学系プログラム 情報数理分野
加藤寛樹 (Hiroki KATO)

1 導入

一般にグラフの同型を判定することは NP である. しかし, グラフの範囲を限定すれば同型問題がやさしくなることが期待される. 隣接行列が巡回行列であるようなグラフを巡回グラフという. 巡回グラフは通信ネットワーク, VLSI 設計, 分散計算など多くのアプリケーションで利用されており, 文献上でも広く研究されている [5]. 巡回グラフに対する同型問題の研究は古くから行われており, 1967 年に Ádám [1] は巡回グラフが同型であるための簡単な判定条件を予想した. Ádám 予想に対して, 反例はいくつか発見されているが, 反例構成の組織的な研究はあまり見当たらない. 本講演では, 頂点数 n が 2 のべきの場合に, 次数最小の反例をすべて求めたことを報告する.

2 巡回グラフ

本節では, 一般のグラフの定義をして, 巡回グラフと共役の定義について述べる. 無限グラフは考えない.

定義 2.1 (グラフ)**.** グラフ G は 2 つの有限集合 $V = V(G)$ と $E = E(G)$ から構成される. V の各要素は頂点と呼ばれる. E の各要素は 2 つの相異なる頂点のペアからなり, 辺と呼ばれる (本稿ではループは許容しないものとする). 集合 E を頂点の順序付きペアの集合に置き換えると, 有向グラフが得られる. $a, b \in V$ に対し, a から b に向かう有向辺を (a, b) で表す.

定義 2.2 (連結グラフ)**.**

(i) 無向グラフにおいて, 任意の 2 頂点が有限個の辺を通って結ばれているとき, 連結グラフであるという.
(ii) 有向グラフの場合は, 向きを忘れて自然に得られる無向グラフが連結なときに連結と定める.

本稿ではグラフは有向な連結グラフのみ考える.

定義 2.3 (グラフの同型)**.** グラフ G, H が同型であるとは, 次の条件を満たす全単射写像 $f : V(G) \to V(H)$ が存在することである.

$$(x, y) \in E(G) \Leftrightarrow (f(x), f(y)) \in E(H) \ (\forall x, y \in V(G))$$

グラフの中でも特にケーリーグラフを以下のように定義する.

定義 2.4 (ケーリーグラフ)**.** G を有限群, Δ をその部分集合とする. G を頂点集合とし, G の 2 つの元 g, h に対し, $h = sg$ となる $s \in \Delta$ があるとき, (g, h) が辺であると定義する. このようにして得られるグラフをケーリーグラフといい, $\mathrm{Cay}(G, \Delta)$ と表す.

注 2.5.

1. $\mathrm{Cay}(G, \Delta)$ が連結であるための必要十分条件は Δ が G を生成すること.
2. $\Delta = \Delta^{-1} = \{s^{-1} | s \in \Delta\}$ のとき, $\mathrm{Cay}(G, \Delta)$ は無向グラフとみなせる.

定義 2.6 (巡回グラフ)**.** $\mathrm{Cay}(\mathbb{Z}_n, \Delta)$ を巡回グラフという. ここで $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

名前の由来は巡回置換 $(0, \ldots, n-1)$ が $\mathrm{Cay}(\mathbb{Z}_n, \Delta)$ の自己同型となっているからである. また, 巡回グラフの隣接行列は巡回行列である. $\mathbb{Z}_n$ は加法群なので, 演算を加法的に書く. 特に単位元は 0 である. $\mathrm{Cay}(\mathbb{Z}_n, \Delta)$ はループをもたないと仮定するので, 以下では $0 \notin \Delta$ とする.

例 2.7. $\mathrm{Cay}(\mathbb{Z}_n, \{-1, 1\})$ はサイクルグラフ. また, $\mathrm{Cay}(\mathbb{Z}_n, \mathbb{Z}_n \backslash \{0\})$ は完全グラフ.

補題 2.8. $d = \gcd(s_1, s_2, \ldots, s_r, n)$ のとき, $\mathrm{Cay}(\mathbb{Z}_n, \{s_1, s_2, \ldots, s_r\})$ は d 個の連結成分に分かれ, 各連結成分は $\mathrm{Cay}(\mathbb{Z}_{n/d}, \{s_1/d, s_2/d, \ldots, s_r/d\})$ に同型である.

巡回グラフが同型であるための十分条件である共役という性質を定義する.

定義 2.9. $\Delta, \Delta' \subset \mathbb{Z}_n \setminus \{0\}$ に対し, ある $m \in \mathbb{Z}_n^*$ が存在して $\Delta' = m\Delta$ が成り立つとき, Δ と Δ' は共役であるという.

補題 2.10. Δ, Δ' が共役であるとき, $\mathrm{Cay}(\mathbb{Z}_n, \Delta) \simeq \mathrm{Cay}(\mathbb{Z}_n, \Delta')$ である.

Ádám は逆に巡回グラフが共役ならば同型であると予想した.

予想 2.11 (Ádám 1967 [1])**.** $\Delta, \Delta' \subset \mathbb{Z}_n \backslash \{0\}$ に対し, $\mathrm{Cay}(\mathbb{Z}_n, \Delta) \simeq \mathrm{Cay}(\mathbb{Z}_n, \Delta')$ となる必要十分条件は Δ と Δ' が共役であることである.

Ádám の予想に対し以下のような反例を Elspas-Turner は発見した.

反例 2.12 (Elspas-Turner 1970 [4])**.** $\{1, 5, 2\}, \{1, 5, 6\} \subset \mathbb{Z}_8$ は共役でないが, $\mathrm{Cay}(\mathbb{Z}_8, \{1, 5, 2\}) \simeq \mathrm{Cay}(\mathbb{Z}_8, \{1, 5, 6\})$ である.(図 1, 図 2 参照) 同型を与える写像 f として, 例えば置換 (2 6)(3 7) がある.(例 3.14 参照)

1979 年には Ádám 予想に対して別の反例が見つかった.

反例 2.13 (Alspach-Parsons 1979 [2],Egorov-Markov 1979 [3])**.**

(i) p を奇素数とするとき, 頂点数 $n = p^2$ で反例が存在する.
(ii) 頂点数が n で反例が存在するならば, 頂点数が mn のときも反例が存在する.

上の反例から以下が分かる.

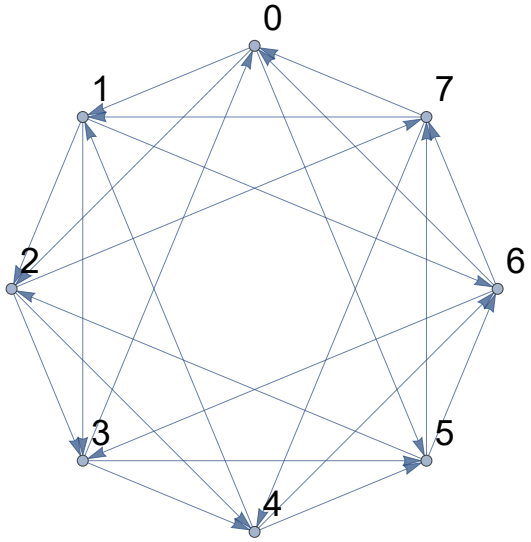

図 1　$\mathrm{Cay}(\mathbb{Z}_8, \{1,5,2\})$

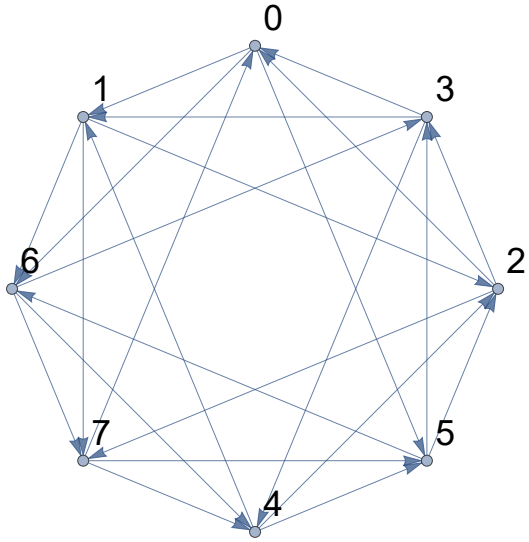

図 2　$\mathrm{Cay}(\mathbb{Z}_8, \{1,5,6\})$

系 2.14. $8|n$ または $p^2|n(\exists p$: 奇素数) のとき Ádám 予想の反例が存在する.

Pálfy [9] は, これ以外の n に対しては反例は存在しないと予想し, この予想は Muzychuk [6][7] によって証明された.

3　キーと解集合

本節では, Muzychuk [8] に従って, 巡回グラフの同型問題を解決するキーという概念を導入する. [8] では一般の頂点数 n に対して巡回グラフの同型問題が解決されているが, 本稿では p を素数, $\alpha \geq 1, n = p^\alpha$ とする.

3.1　キー

定義 3.1. キー空間 K_n は以下の条件を満たす全ての整数ベクトル $(k_1, \ldots, k_\alpha)$ から成る.

$$0 \leq k_i < i \quad (i = 1, \ldots, \alpha), \quad k_{i-1} \leq k_i \quad (i = 2, \ldots, \alpha).$$

キー空間の元をキーという.

キー空間 K_n に以下のような自然な半順序 $\leqslant$ を導入する. $\mathbf{k} = (k_1, \ldots, k_\alpha), \mathbf{m} = (m_1, \ldots, m_\alpha)$ に対し,

$$\mathbf{k} \leqslant \mathbf{m} \Leftrightarrow k_i \leq m_i \quad (\forall i).$$

半順序集合 $(K_n, \leqslant)$ は束であり, 交わり $\mathbf{k} \wedge \mathbf{m}$ と結び $\mathbf{k} \vee \mathbf{m}$ は以下のようになる.

$$(\mathbf{k} \wedge \mathbf{m}) \text{ の } i \text{ 成分} = \min(k_i, m_i),$$
$$(\mathbf{k} \vee \mathbf{m}) \text{ の } i \text{ 成分} = \max(k_i, m_i).$$

例 3.2. キー空間

$$K_8 = \{(0,0,0),(0,0,1),(0,1,1),(0,0,2),(0,1,2)\}$$

のハッセ図は図 3 のようになる.

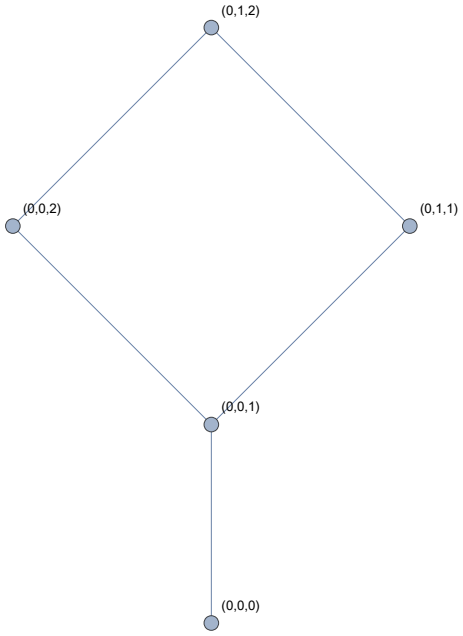

図 3　K_8 のハッセ図

定義 3.3. $\{S_1,\ldots,S_r\}(S_i \subset \mathbb{Z}_n)$ が $\mathbb{Z}_n$ の分割であるとは,

$$S_1 \cup S_2 \cup \cdots \cup S_r = \mathbb{Z}_n,\ S_i \cap S_j = \emptyset (i \neq j)$$

を満たすことである. $\mathrm{Part}(\mathbb{Z}_n)$ を $\mathbb{Z}_n$ のすべての分割から成る集合とする.

定義 3.4. $\Delta, \Sigma \in \mathrm{Part}(\mathbb{Z}_n), \Delta = \{S_1,\ldots,S_r\}, \Sigma = \{T_1,\ldots,T_s\}$ とする. 以下が成り立つとき, Δ は Σ の細分であるといい, $\Sigma \sqsubseteq \Delta$ と表す.

$$\forall S_i, \exists T_j\ s.t.\ S_i \subseteq T_j$$

関係 $\sqsubseteq$ は半順序である. 半順序集合 $(\mathrm{Part}(\mathbb{Z}_n), \sqsubseteq)$ は束であり, Δ と Σ の交わりを $\Delta \wedge \Sigma$, 結びを $\Delta \vee \Sigma$ で表す.

定義 3.5. キー $\mathbf{k} = (k_1,\ldots,k_\alpha) \in K_n$ に対し, $\mathbb{Z}_n$ の分割 $\Sigma(\mathbf{k})$ を以下のように定義する. ここで, $g \in \mathbb{Z}_n$ の位数を $o(g)$ と記し, β は $o(g) = p^\beta$ によって定める.

$$\Sigma(\mathbf{k}) := \{\{0\}\} \cup \{g + \langle p^{\alpha - k_\beta} \rangle | g \in \mathbb{Z}_n \backslash \{0\}\}.$$

例 3.6. K_8 のキー $\mathbf{k}$ と $\Sigma(\mathbf{k})$ は表 1 のようになる.

表 1　K_8 のキー $\mathbf{k}$ と $\Sigma(\mathbf{k})$

$\mathbf{k}$	$\Sigma(\mathbf{k})$
$(0,0,0)$	{{0},{2},{4},{6},{1},{3},{5},{7}}
$(0,0,1)$	{{0},{2},{4},{6},{1,5},{3,7}}
$(0,1,1)$	{{0},{4},{2,6},{1,5},{3,7}}
$(0,0,2)$	{{0},{4},{2},{6},{1,3,5,7}}
$(0,1,2)$	{{0},{4},{2,6},{1,3,5,7}}

命題 3.7. キー $\mathbf{k}$, $\mathbf{m} \in K_n$ に対して以下が成り立つ.

(1) $\mathbf{k} \leqslant \mathbf{m} \Rightarrow \Sigma(\mathbf{m}) \sqsubseteq \Sigma(\mathbf{k})$
(2) $\Sigma(\mathbf{k}) \wedge \Sigma(\mathbf{m}) = \Sigma(\mathbf{k} \vee \mathbf{m})$
(3) $\Sigma(\mathbf{k}) \vee \Sigma(\mathbf{m}) = \Sigma(\mathbf{k} \wedge \mathbf{m})$
(4) $\Sigma(\mathbf{0}) = \{\{g\} | g \in \mathbb{Z}_n\} \quad (\mathbf{0} := (0,0,\ldots,0))$

定義 3.8. $\Delta \subset \mathbb{Z}_n \backslash \{0\}$ に対し,$\{\mathbb{Z}_n \backslash \Delta, \Delta\} \sqsubseteq \Sigma(\mathbf{k})$ を満たす $\mathbf{k} \in K_n$ の中で最大のものを $\mathbf{k}(\Delta)$ と定義する.

例 3.9. $\Delta = \{1,5,2\} \subset \mathbb{Z}_8$ とする. 表 1 より

$$\{\mathbb{Z}_8 \backslash \Delta, \Delta\} \sqsubseteq \Sigma((0,0,1)), \quad \{\mathbb{Z}_8 \backslash \Delta, \Delta\} \not\sqsubseteq \Sigma((0,1,1))$$

が成り立つので $\mathbf{k}(\Delta) = (0,0,1)$ である. 同様に $\Delta' = \{1,5,6\} \subset \mathbb{Z}_8$ に対し, $\mathbf{k}(\Delta') = (0,0,1)$ である.

3.2　解集合

同型な巡回グラフを発見する際に必要となる解集合を定義する. 引き続き $n = p^\alpha$ とする.

定義 3.10.

(*i*) $\mathbb{Z}_n^{**} := \{(m_1,\ldots,m_\alpha) \in \mathbb{N}^\alpha | \forall i, \gcd(m_i, p) = 1\}$
(*ii*) キー $\mathbf{k} \in K_n$ に対し $\mathbb{Z}_n^{**}(\mathbf{k})$ を $m_\delta \equiv m_{\delta-1} \pmod{p^{\delta - k_\delta - 1}}$, $2 \leq \forall\delta \leq \alpha$ をみたす $\mathbf{m} = (m_1,\ldots,m_\alpha) \in \mathbb{Z}_n^{**}$ の全体からなる集合として定義する.
(*iii*) $\mathbb{Z}_n^{**}(\mathbf{k})^o$ を $m_\delta \in \{1,2,\ldots,p^{\delta-k_\delta} - 1\}$, $1 \leq \forall\delta \leq \alpha$ をみたす $\mathbf{m} = (m_1,\ldots,m_\alpha) \in \mathbb{Z}_n^{**}(\mathbf{k})$ の全体からなる集合として定義する.
(*iv*) $\mathbf{m} = (m_1,\ldots,m_\alpha) \in \mathbb{Z}_n^{**}$ に対し, $f_\mathbf{m} : \mathbb{Z}_n \to \mathbb{Z}_n$ を

$$x = \sum_{\beta=0}^{\alpha-1} x_\beta p^\beta, \quad x_\beta \in \{0,\ldots,p-1\}$$

に対して,

$$x^{f_{\mathbf{m}}} = \sum_{\beta=0}^{\alpha-1} m_{\alpha-\beta} x_\beta p^\beta$$

と定義する.

(v) 解集合 $P(\mathbf{k})$ を $P(\mathbf{k}) := \{f_{\mathbf{m}} | \mathbf{m} \in \mathbb{Z}_n^{**}(\mathbf{k})^o\}$ と定義する.

例 3.11. $p = 2, \alpha = 3, \mathbf{k} = (0,0,1)$ とする. このとき,

$$\mathbb{Z}_8^{**}(\mathbf{k})^o = \{(1,1,1),(1,1,3),(1,3,1),(1,3,3)\}, \quad P(\mathbf{k}) = \{f_{(1,1,1)}, f_{(1,1,3)}, f_{(1,3,1)}, f_{(1,3,3)}\}$$

となる. 置換で表すと $f_{(1,1,1)}$ は恒等置換であり,

$$f_{(1,1,3)} = (1\ 3\ 5\ 7), \quad f_{(1,3,1)} = (2\ 6)(3\ 7), \quad f_{(1,3,3)} = (1\ 3)(2\ 6)(5\ 7)$$

となる.

定義 3.12. $\Delta \subset \mathbb{Z}_n \setminus \{0\}$ と $\mathbb{Z}_n$ の置換 f に対し

$$\mathrm{Cay}(\mathbb{Z}_n, \Delta)^f := \mathrm{Cay}(\mathbb{Z}_n, \Delta^f)$$

と定義する.

定理 3.13 (Muzychuk 2004 [8])**.** $\Delta, \Delta' \subset \mathbb{Z}_n \setminus \{0\}$ に対し, 以下が成り立つ.

1. $\mathbf{k}(\Delta) \neq \mathbf{k}(\Delta') \Rightarrow \mathrm{Cay}(\mathbb{Z}_n, \Delta) \not\simeq \mathrm{Cay}(\mathbb{Z}_n, \Delta')$
2. $\mathbf{k}(\Delta) = \mathbf{k}(\Delta') = \mathbf{k}$ ならば, 以下は同値
   - (a) $\mathrm{Cay}(\mathbb{Z}_n, \Delta) \simeq \mathrm{Cay}(\mathbb{Z}_n, \Delta')$
   - (b) $\exists f \in P(\mathbf{k})\ s.t.\ \mathrm{Cay}(\mathbb{Z}_n, \Delta)^f = \mathrm{Cay}(\mathbb{Z}_n, \Delta')$
   - (c) $\exists f \in P(\mathbf{k})\ s.t.\ \Delta^f = \Delta'$

例 3.14. 例 3.9 より, $\Delta = \{1,5,2\}, \Delta' = \{1,5,6\} \subset \mathbb{Z}_8$ に対し $\mathbf{k}(\Delta) = \mathbf{k}(\Delta') = (0,0,1)$. 例 3.11 より, $f_{(1,3,1)} = (2\ 6)(3\ 7) \in P((0,0,1))$ であり, $\Delta^{f_{(1,3,1)}} = \Delta'$ となる. よって, $\mathrm{Cay}(\mathbb{Z}_8, \{1,5,2\}) \simeq \mathrm{Cay}(\mathbb{Z}_8, \{1,5,6\})$ である.

4 $|\Delta|$ が最小の反例

2 節で述べたように Ádám 予想 (予想 2.11) の反例が存在するような頂点数 n は完全にわかっている. そこで, 具体的な反例を全て求めることを考える. 本節では, n が 2 のべきのとき, $|\Delta|$ が最小の反例を全て求める. 補題 2.8 より連結なグラフについて考えればよい. 補題 2.8 より $\mathbb{Z}_n^*$ に属する元 $s \in \Delta$ が存在し, Δ と $s^{-1}\Delta$ は共役で $1 \in s^{-1}\Delta$ であるから, 最初から $1 \in \Delta$ と仮定してよい. 頂点数 $n = 2, 4$ で同型な巡回グラフはすべて共役なので反例は存在しない. 以降では $n = 2^\alpha, \alpha \geq 3$ とする.

補題 4.1.

(*i*) $n/2+1 \notin \Delta \subset \mathbb{Z}_n\backslash\{0\} \Rightarrow \mathbf{k}(\Delta) = \mathbf{0}$.
(*ii*) $\mathbf{0} \in K_n$ に対し, $P(\mathbf{0})$ は共役写像以外を含まない.

この補題から次のことが容易に分かる.

系 4.2. $\Delta \subset \mathbb{Z}_n\backslash\{0\}, |\Delta| \leq 2$ のとき, Ádám 予想の反例は存在しない.

$|\Delta| = 3$ の場合の反例を調べる. 補題 4.1 より $1, n/2+1 \in \Delta$ と仮定してよい. $m \in \mathbb{Z}_n, m \neq 0, 1, n/2+1$ に対し,

$$\Delta_{n,m} = \{1, 1+n/2, m\} \subset \mathbb{Z}_n\backslash\{0\}$$

とおき, $\mathrm{Cay}(\mathbb{Z}_n, \Delta_{n,m})$ を考えればよい. $\Delta_{n,m}$ のキーは次のように計算される.

命題 4.3. m を整数と考えて素因数分解した際に現れる 2 の指数を e とする. このとき,

$$\mathbf{k}(\Delta_{n,m}) = (\overbrace{0, \ldots, 0}^{\alpha-e}, \overbrace{1, \ldots, 1}^{e}).$$

命題 4.4. m が奇数のとき, $\mathrm{Cay}(\mathbb{Z}_n, \Delta_{n,m})$ に対して, Ádám 予想の反例は存在しない.

証明. 命題 4.3 より, $\mathbf{k}(\Delta_{n,m}) = \mathbf{0}$. よって, 補題 4.1(ii) より $P(\mathbf{k}(\Delta_{n,m}))$ は共役写像以外を含まないので, Ádám 予想の反例は存在しない. □

われわれの主結果は次の通りである.

定理 4.5. $n = 2^\alpha, \alpha \geq 3, m \in \mathbb{Z}_n, 2|m, 0 < m < n/2$ とする. このとき, $\Delta_{n,m}$ と $\Delta_{n,m+n/2}$ は共役でなく,

$$\mathrm{Cay}(\mathbb{Z}_n, \Delta_{n,m}) \simeq \mathrm{Cay}(\mathbb{Z}_n, \Delta_{n,m+n/2})$$

が成り立つ. すなわち, これらの巡回グラフは Ádám 予想の反例を与える.

証明の概略は次の通りである. まず, $\Delta_{n,m}$ と $\Delta_{n,m+n/2}$ が共役でないことは簡単にわかる. 次に, 命題 4.3 から $\mathbf{k}(\Delta_{n,m}) = \mathbf{k}(\Delta_{n,m+n/2})$ である. 定義 3.10 より

$$\mathbf{m} = (\overbrace{1, \ldots, 1}^{\alpha-e-1}, 1+2^{\alpha-e-1}, \overbrace{1, \ldots, 1}^{e}) \in \mathbb{Z}_n^{**}(\mathbf{k}(\Delta_{n,m}))^o$$

に対して, $f_{\mathbf{m}} \in P(\mathbf{k}(\Delta_{n,m}))$ とわかる. この $f_{\mathbf{m}}$ に対し, $\Delta_{n,m}^{f_{\mathbf{m}}} = \Delta_{n,m+n/2}$ となるので定理 3.13 より $\mathrm{Cay}(\mathbb{Z}_n, \Delta_{n,m}) \simeq \mathrm{Cay}(\mathbb{Z}_n, \Delta_{n,m+n/2})$ である.

$|\Delta| = 3$ のとき, Ádám 予想の反例は定理 4.5 で挙げたものに限られる. $m = n/2$ のとき, $\mathbf{k}(\Delta_{n,m})$ とキーが等しくなる Δ が存在しないため, 反例は存在しない. それ以外の場合は補題 4.1 と命題 4.3 よりキーが $\mathbf{0}$ となり, 補題 4.1 より反例が存在しない.

参考文献

[1] A.Ádám, 'Research problems 2-10' J. Combin. Theory 2 (1967) 393.

[2] Alspach, Brian; Parsons, T. D. Isomorphism of circulant graphs and digraphs. Discrete Math. 25 (1979), no. 2, 97–108.

[3] Egorov, V. N.; Markov, A. I. Ádám's conjecture for graphs with circulant adjacency matrices. (Russian) Dokl. Akad. Nauk SSSR 249 (1979), no. 3, 529–532; translation in Soviet Math. Dokl. 20 (1979), 1292–1296.

[4] Elspas, Bernard; Turner, James. Graphs with circulant adjacency matrices. J. Combinatorial Theory 9 (1970), 297–307.

[5] Mans, Bernard; Pappalardi, Francesco; Shparlinski, Igor. On the spectral Ádám property for circulant graphs. Discrete Math. 254 (2002), no. 1-3, 309–329.

[6] Muzychuk, Mikhail. Ádám's conjecture is true in the square-free case. J. Combin. Theory Ser. A 72 (1995), no. 1, 118–134.

[7] Muzychuk, Mikhail. On Ádám's conjecture for circulant graphs. Discrete Math. 176 (1997), no. 1-3, 285–298.

[8] Muzychuk, M. A solution of the isomorphism problem for circulant graphs. Proc. London Math. Soc. (3) 88 (2004), no. 1, 1–41.

[9] Pálfy, P. P. Isomorphism problem for relational structures with a cyclic automorphism. European J. Combin. 8 (1987), no. 1, 35–43.