

ハミルトン閉路問題に対する カードベースゼロ知識証明とその応用

千葉工業大学 猪狩紫雲

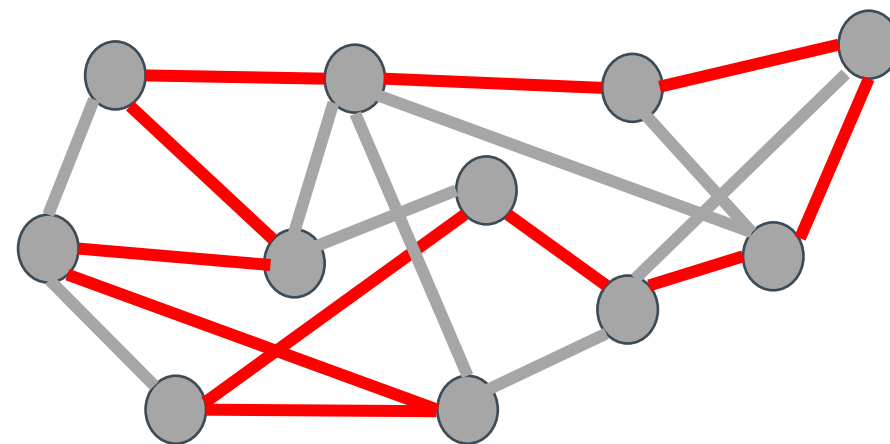
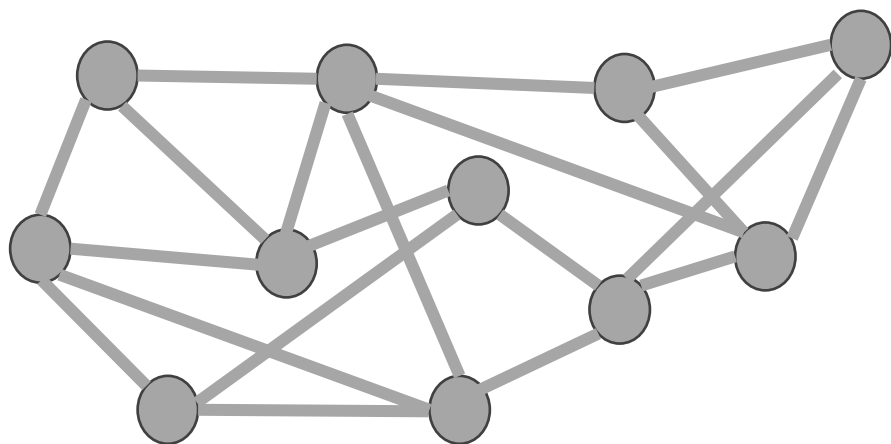
本発表は、以下論文の内容となっています

Ren Igari, Shun Odaka, Yuichi Komano, Takaaki Mizuki, “Efficient Physical ZKP Protocols for Hamiltonian Cycle Problem and Traveling Salesman Problem,” IEICE Trans. Fundam. Electron. Commun. Comput. Sci., vol.E109-A, no.9, 2026.9

もくじ

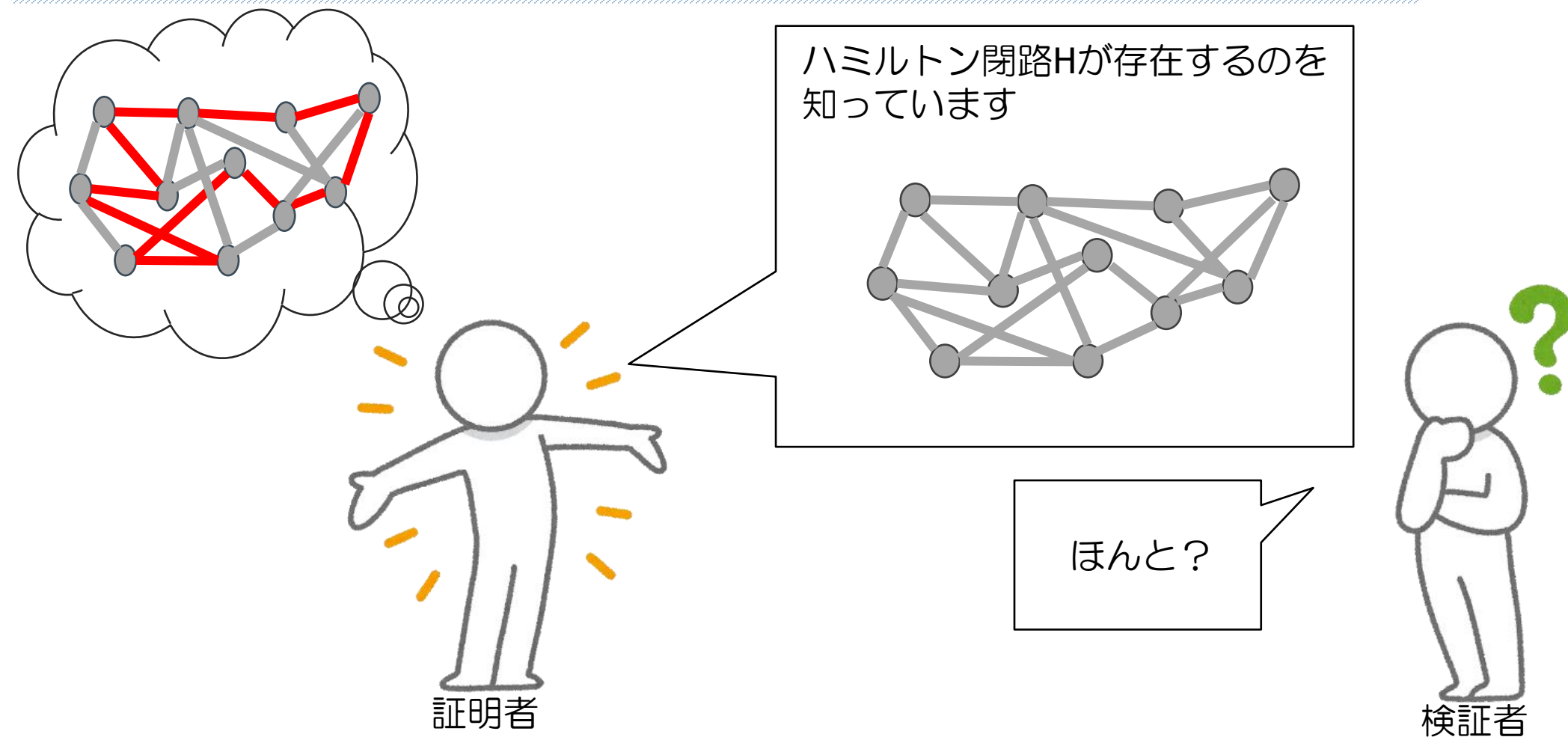
1. ハミルトン閉路とゼロ知識証明
 - グラフとハミルトン閉路
 - ハミルトン閉路のゼロ知識証明
 - ゼロ知識証明の安全性
2. プロトコル
3. プロトコルの応用
4. まとめ
5. 後続研究

グラフとハミルトン閉路



- グラフとは、辺と頂点の集合である $G=(V_G, E_G)$
 - 本発表では無向グラフを扱う
- ハミルトン閉路 H とは、グラフ上のすべての頂点を1度ずつ通る閉路
 - ハミルトン閉路が存在するのか判定するのは難しい(NP完全問題)

ハミルトン閉路のゼロ知識証明



閉路そのものは教えずに閉路を知っていることのみを証明する

ゼロ知識証明の安全性

完全性

証明者と検証者が正しく振舞うなら、証明は受理される

健全性

証明者が嘘をついても、検証者が正しく振舞うならば証明は棄却される

ゼロ知識性

証明者と検証者が正しく振舞うなら、検証者に秘密はもれない

もくじ

1. ハミルトン閉路とゼロ知識証明
2. プロトコル
 - プロトコルの概要と性能
 - プロトコル紹介
 - 安全性
3. プロトコルの応用
4. まとめ
5. 後続研究

ハミルトン閉路のゼロ知識証明プロトコル

- ① 既存方式（既存方式1,2, Ruangwises-Itoh^[1]）
- ② 提案方式（提案方式1,1の変形版,2, 猪狩ら^[2]）

方式	シャッフル回数	カード枚数
既存方式1	$2(n-1)(2m-n-\Delta+1)$	$4(\Delta+3)(n+1)+4\Delta+2m+5$
既存方式2	$O(1)^*$	$n^2+O(n)^*$
提案方式1	$n+2$	$m+n\Delta$
提案方式1_変形版	3	$m+n(\Delta+2)$
提案方式2	3	n^2+2n

*既存方式2は[1]の脚注に概要が記載されているだけであり詳細は不明

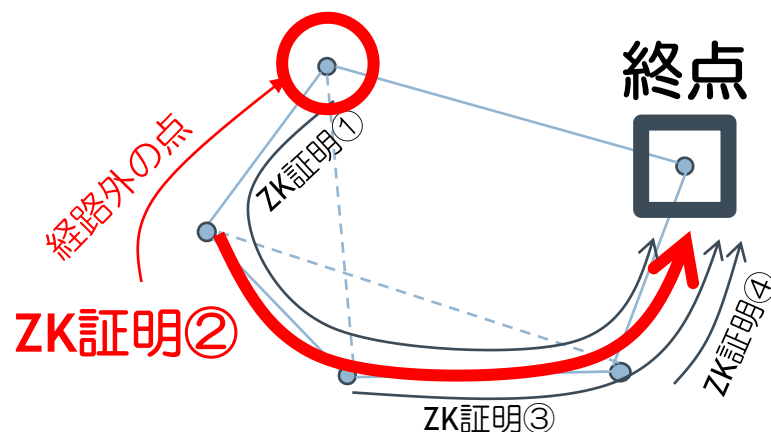
[1]Suthee Ruangwises,Toshiya Itoh. Physical ZKP for connected spanning subgraph: Applications to Bridges Puzzle and other problems. In Unconventional Computation and Natural Computation (UCNC,2021), Vol. 12984 of LNCS, Cham, 2021. Springer.

[2] Ren Igari, Shun Odaka, Yuichi Komano, Takaaki Mizuki, “Efficient Physical ZKP Protocols for Hamiltonian Cycle Problem and Traveling Salesman Problem,” IEICE Trans. Fundam. Electron. Commun. Comput. Sci., vol.E109-A, no.9, 2026.9

既存方式1、既存方式2[1]

頂点に着目したハミルトン閉路のゼロ知識証明を行っている

既存方式 1



既存方式 2



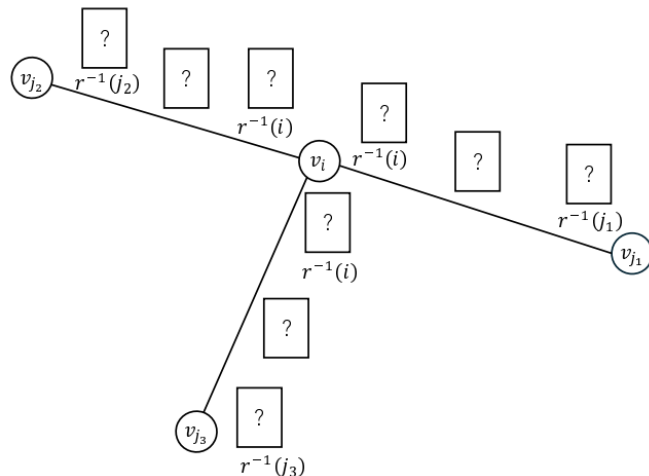
- 頂点ごとに閉路のための確認を繰り返す

提案方式[2]

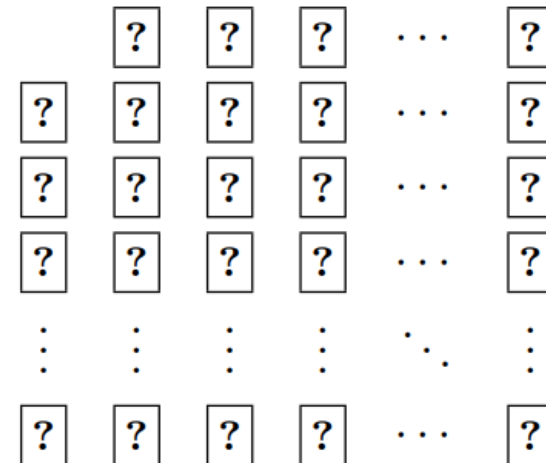
提案方式では、グラフの辺を起点に考える

提案方式1：各辺にハミルトン閉路Hの辺であるかを示すカードをそれぞれ配置する

提案方式2：ハミルトン閉路Hの辺であるかを示すカードの行列を作成する



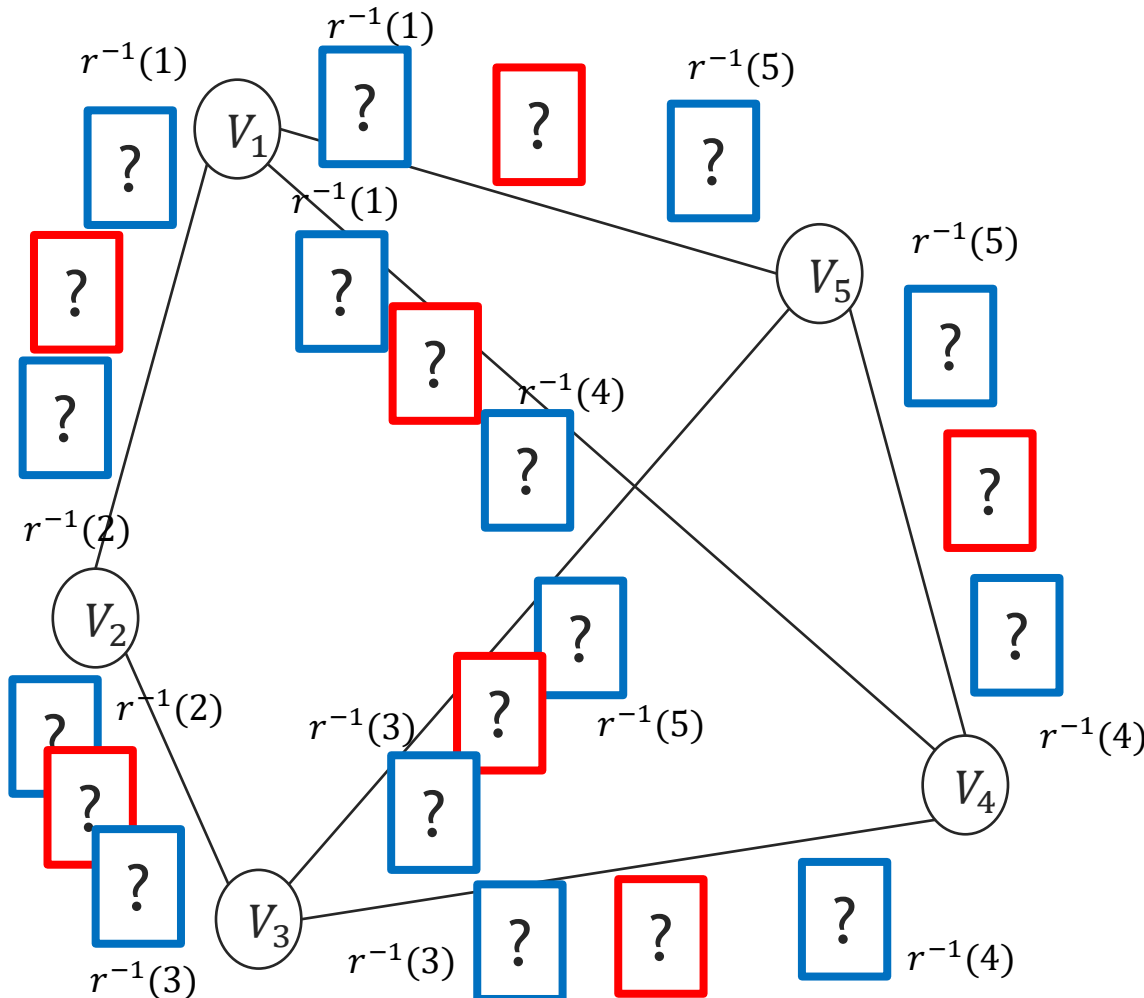
提案方式1のイメージ



提案方式2のイメージ

提案方式1 [2]

頂点ではなく、ハミルトン閉路Hの辺を起点とする



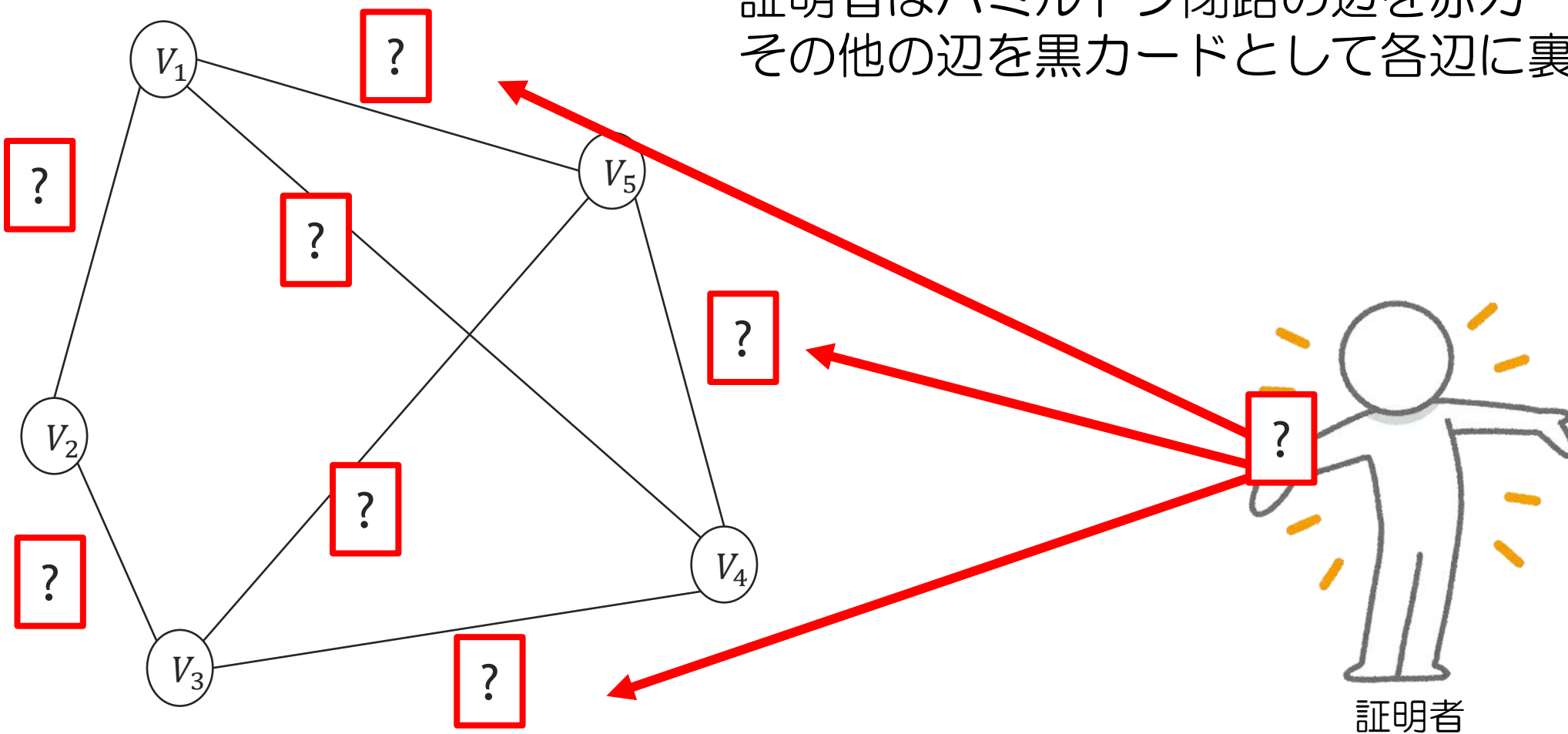
概要

1. 各辺に黒赤カードを裏返して配置
2. 頂点の仮名カード(数字カード)を作成し裏返して配置
3. 各辺のカードを束ねてPSシャッフル
4. 閉路の確認

次のページから詳しく説明

1.各辺に黒赤カードを裏返して配置

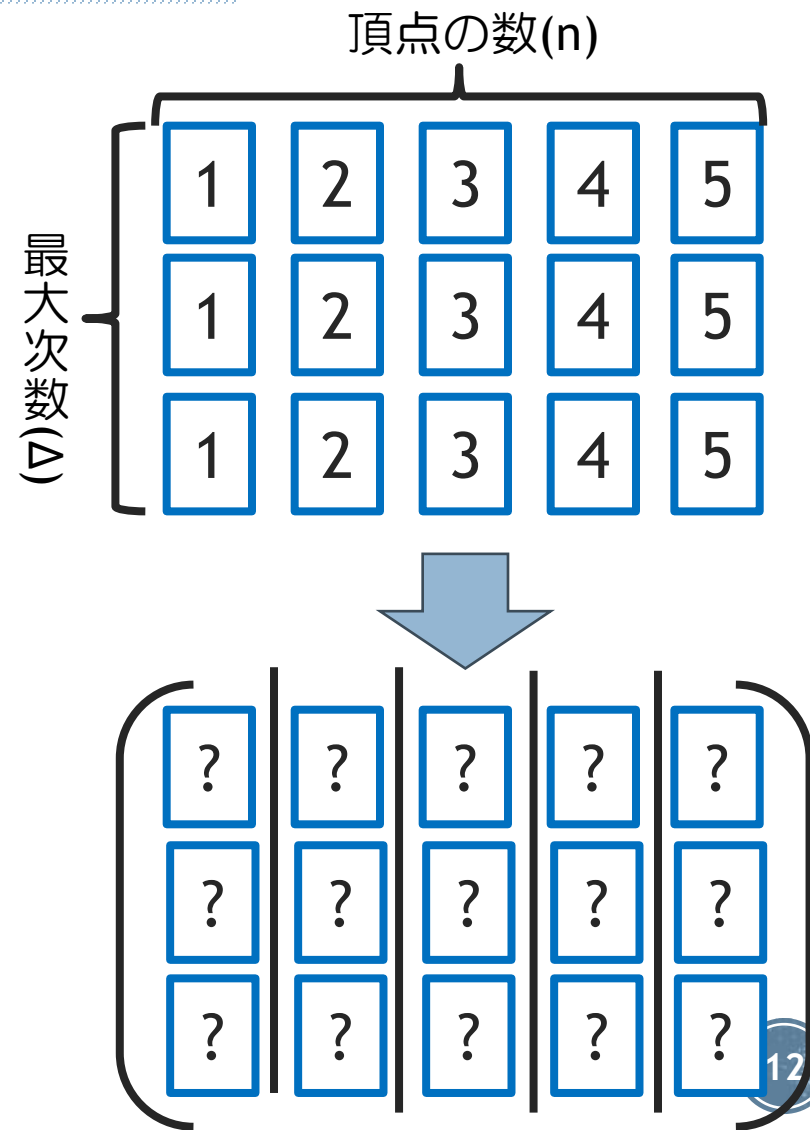
証明者はハミルトン閉路の辺を赤カード
その他の辺を黒カードとして各辺に裏返して配置する



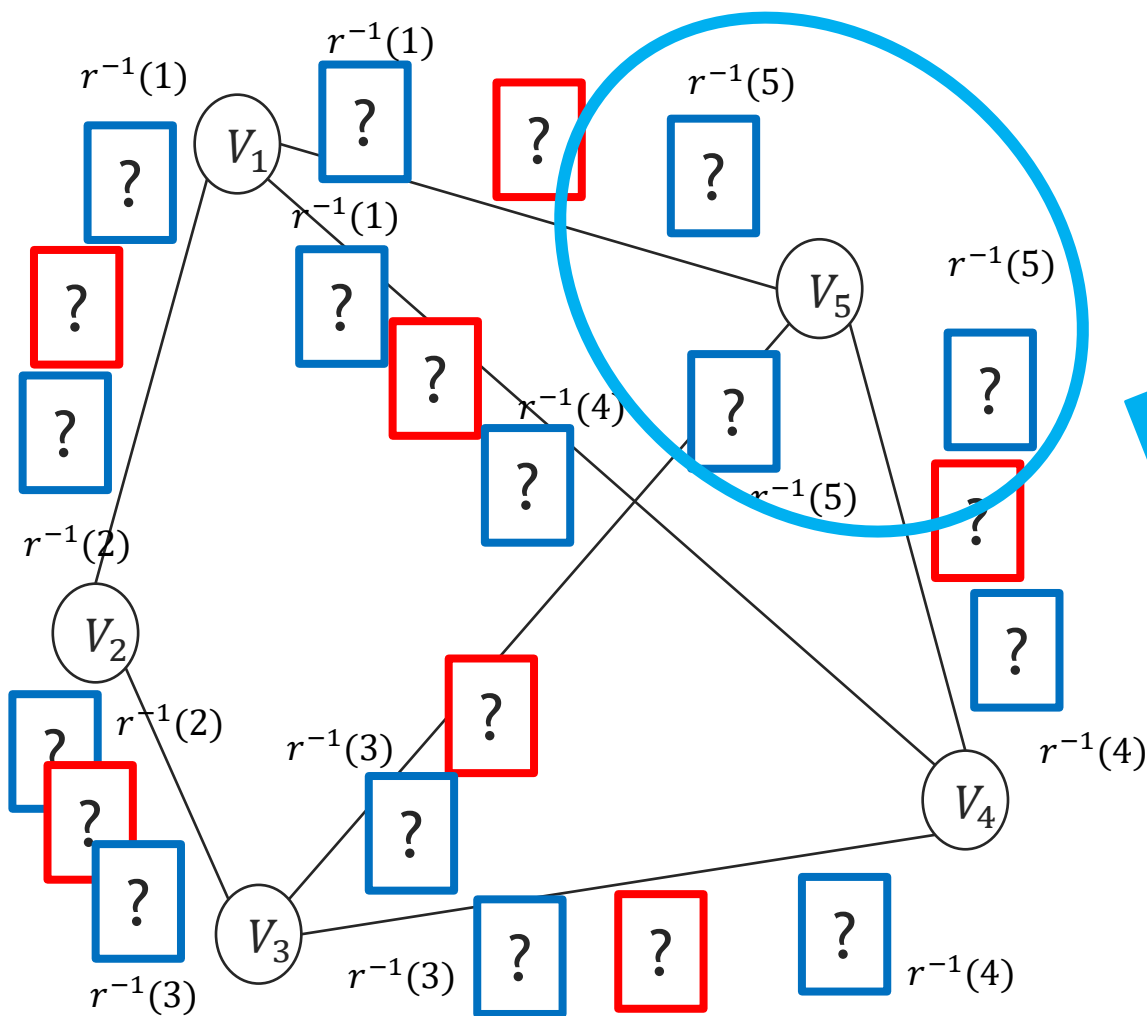
2. 頂点の仮名カードを作成し配置(1/2)

仮名カードの作成方法(数字カードを使用)

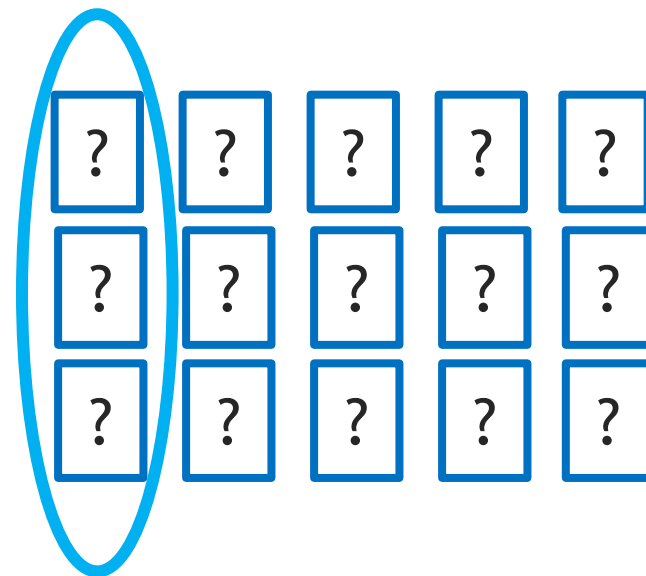
1. グラフの最大次数(Δ) $\times$ 頂点の数(n)の行列を作成
2. 列方向にPSシャッフル



2. 頂点の仮名カードを作成し配置(2/2)

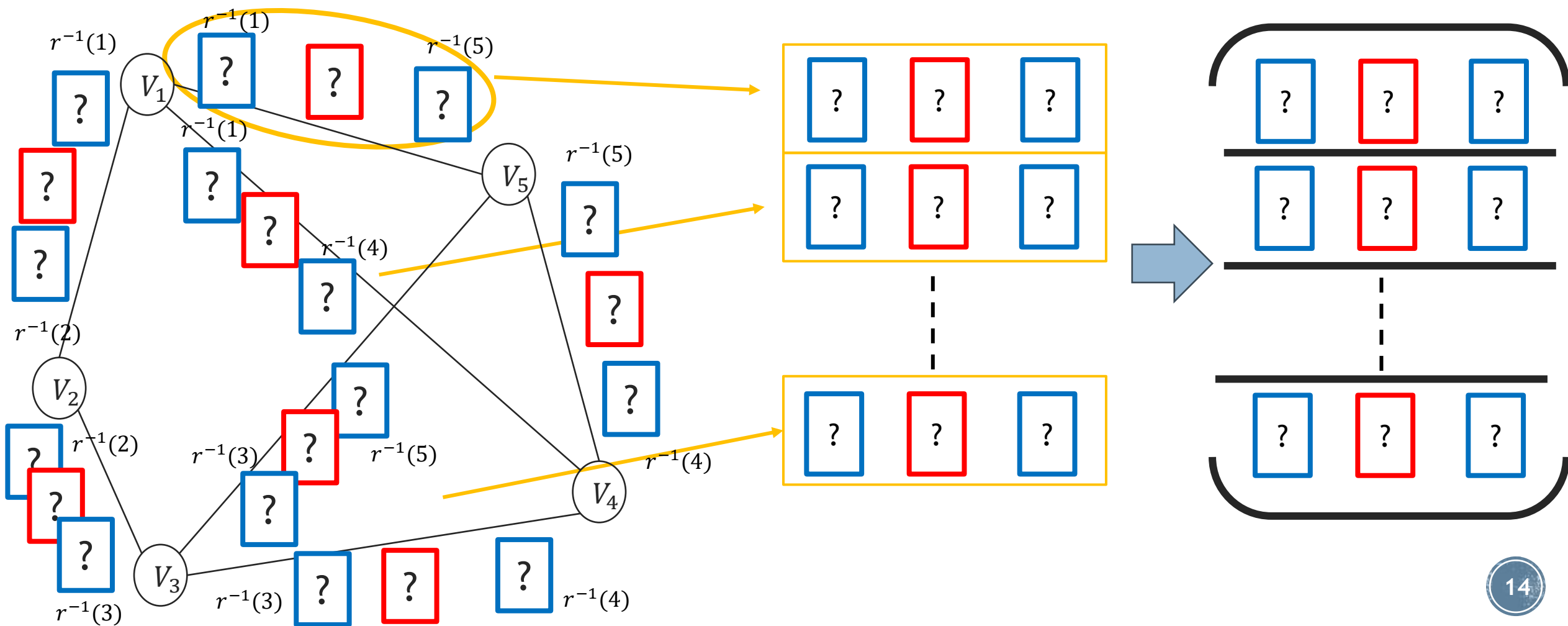


PSシャッフルされたカードを頂点 V_i ごとに、 V_i に接続する各辺の端点に $r^{-1}(i)$ のカードを配置する

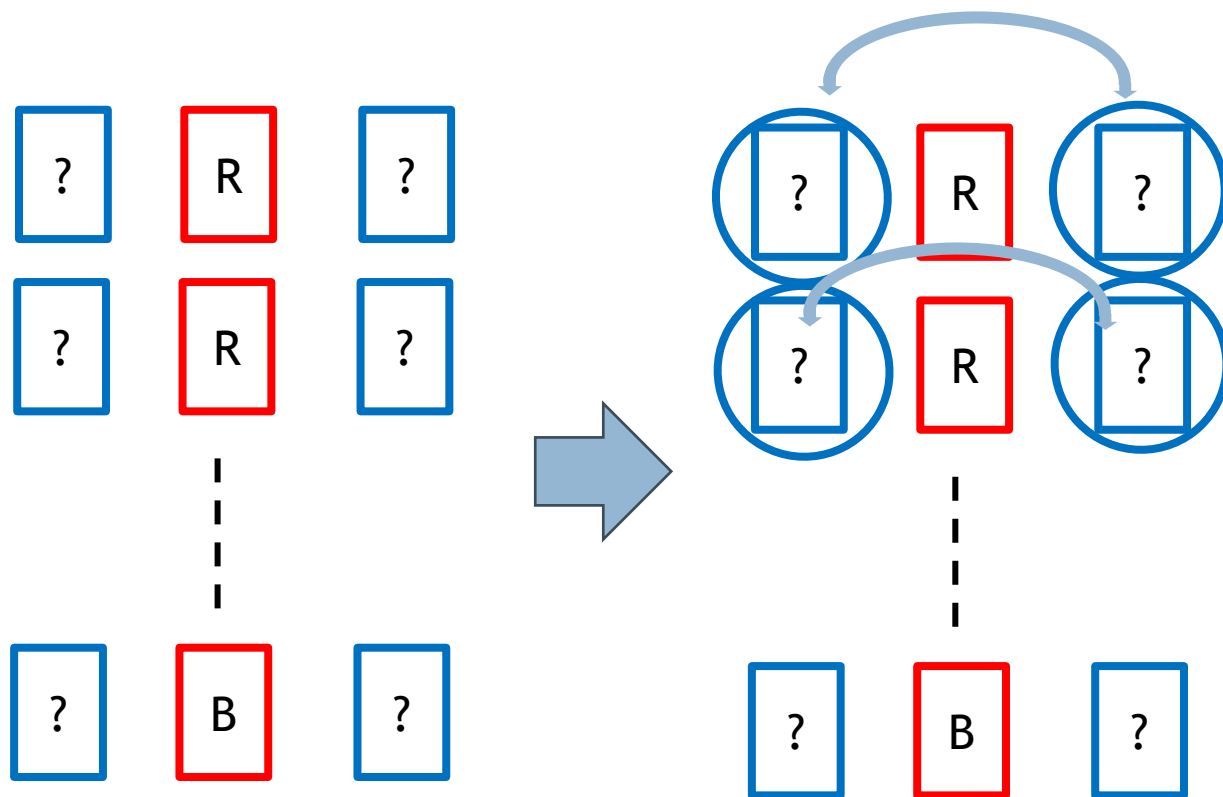


3. 各辺のカードを束ねてPSシャッフル

各辺に配置された3枚のカードを束ねて行方向にPSシャッフル

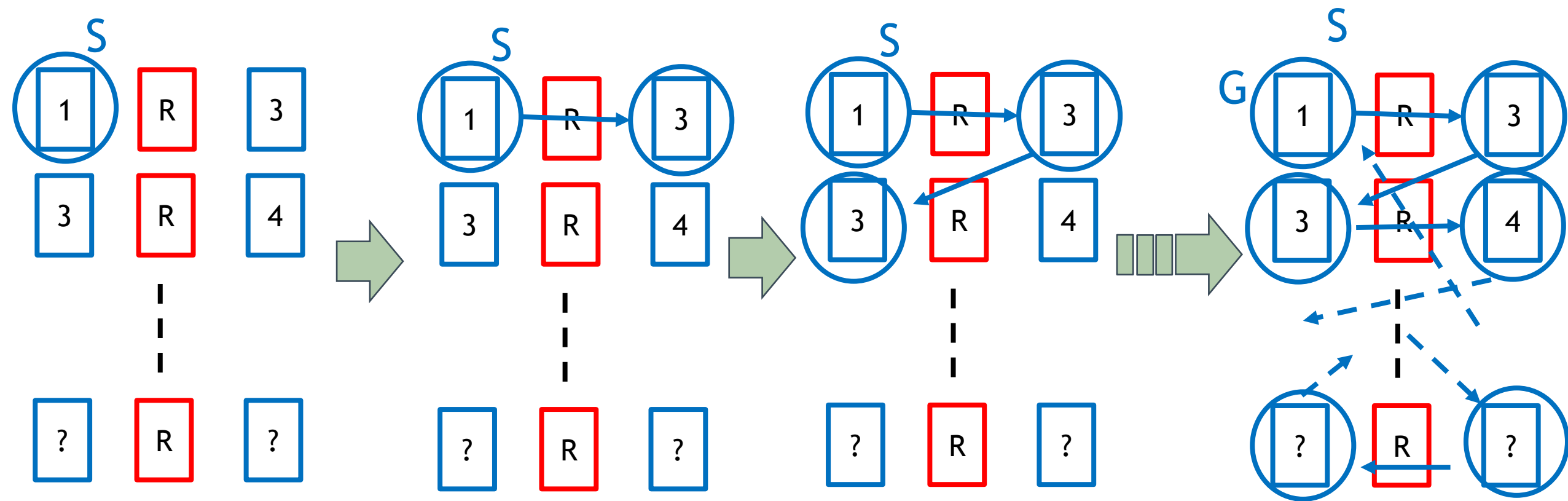


4.閉路の確認(1/2)



1. 黒赤カードをめくる
(ハミルトン閉路の辺は赤カードが配置されている)
2. 赤カードがある行の仮名カードをPSシャッフルする
(グラフの形状からの情報漏洩を防ぎハミルトン閉路Hの辺を特定させないため)

4.閉路の確認(2/2)



赤カード(ハミルトン閉路)の存在する行を抽出し

1～nの数字がそれぞれ2枚ずつあるのかを確認する

ハミルトンの辺の仮名の頂点が巡回路を与えることを確認する

提案方式1 [2] について

方式	シャッフル回数	カード枚数
既存方式1	$2(n-1)(2m-n-\Delta+1)$	$4(\Delta+3)(n+1)+4\Delta+2m+5$
既存方式2	$O(1)^*$	$n^2+O(n)^*$
提案方式1	$n+2$	$m+n\Delta$
提案方式1_変形版	3	$m+n(\Delta+2)$
提案方式2	3	n^2+2n

現在、表の青枠で囲まれている提案方式1の説明をした

提案方式1では、シャッフル数、カード枚数共に既存方式より削減できた

提案方式1 [2]の変形版について

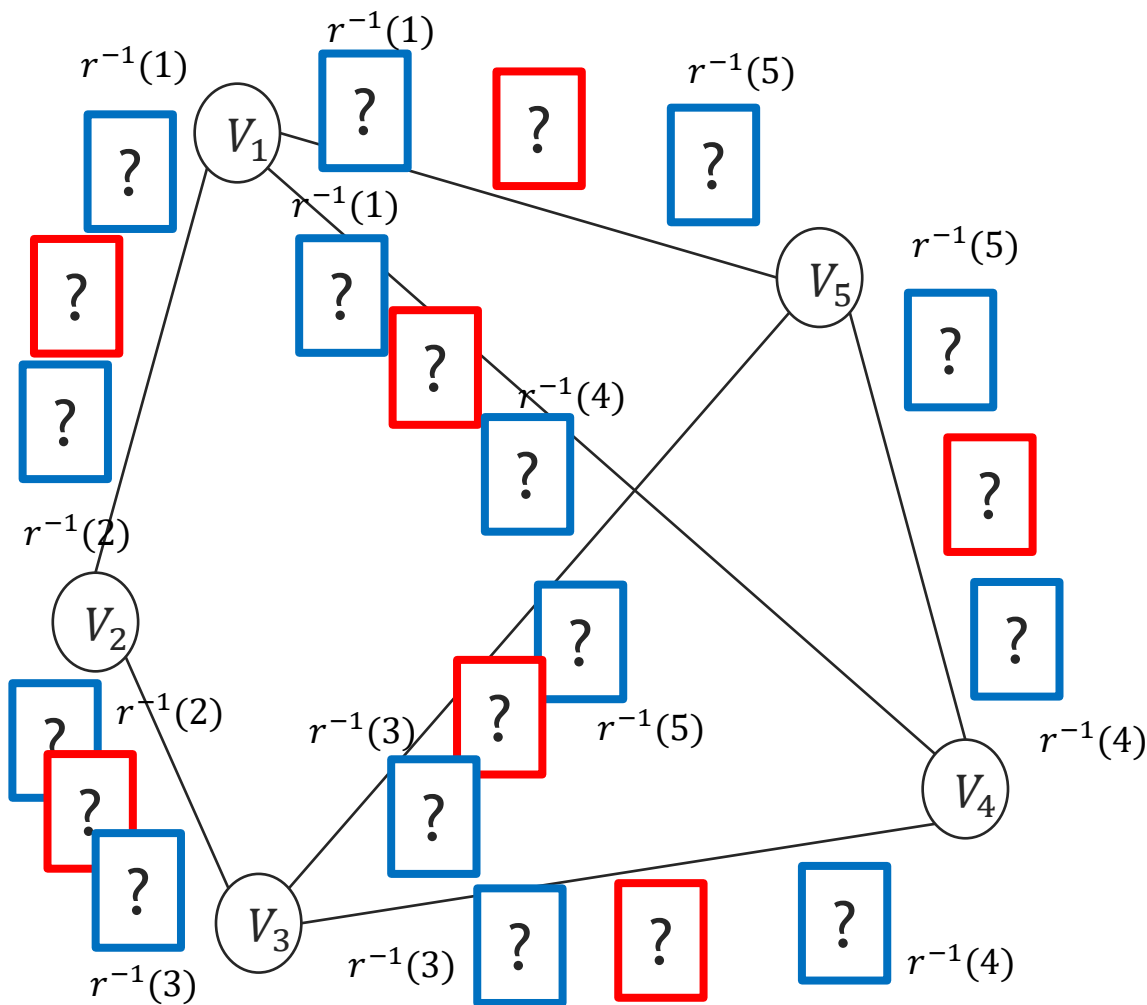
方式	シャッフル回数	カード枚数
既存方式1	$2(n-1)(2m-n-\Delta+1)$	$4(\Delta+3)(n+1)+4\Delta+2m+5$
既存方式2	$O(1)^*$	$n^2+O(n)^*$
提案方式1	$n+2$	$m+n\Delta$
提案方式1_変形版	3	$m+n(\Delta+2)$
提案方式2	3	n^2+2n

次に、提案方式1_変形版について説明する

提案方式1_変形版ではカード枚数は増えるがシャッフル数が3回に固定される

提案方式1 [2]の変形版

頂点ではなく、ハミルトン閉路Hの辺を起点とする



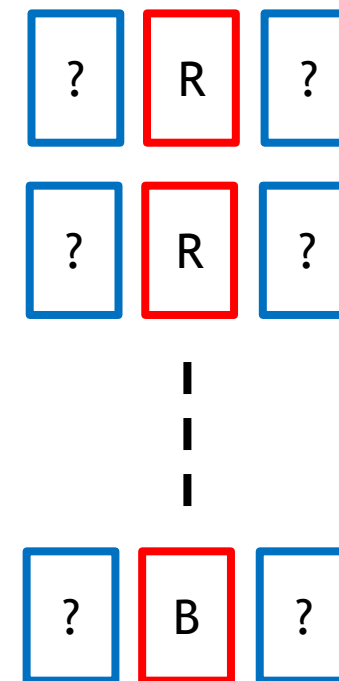
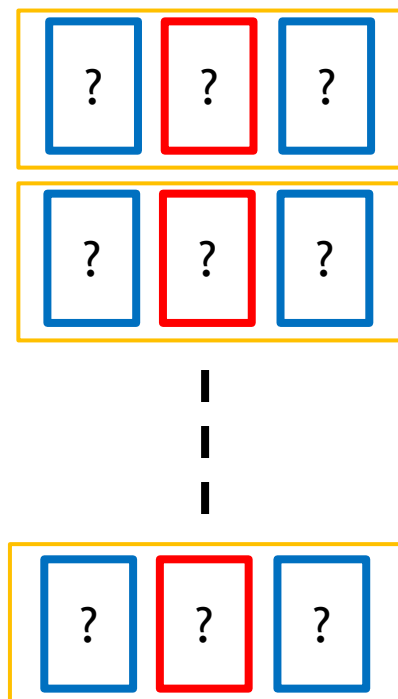
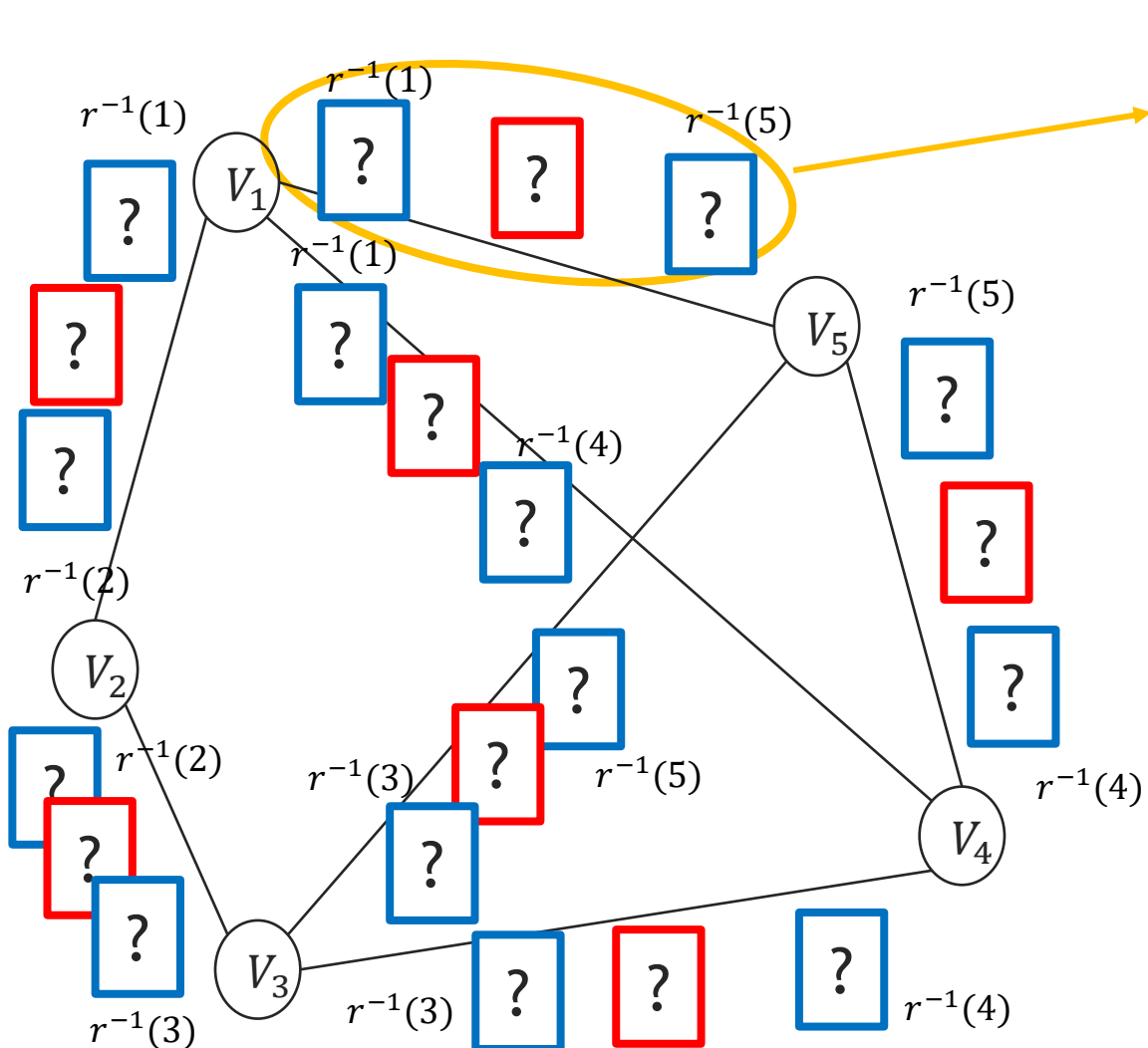
概要

1. 各辺に**黒赤カード**を裏返して配置
2. 頂点の**仮名カード(数字カード)**を作成し裏返して配置
3. 各辺のカードを束ねてPSシャッフル
4. **閉路の確認**

「閉路の確認」が変形される

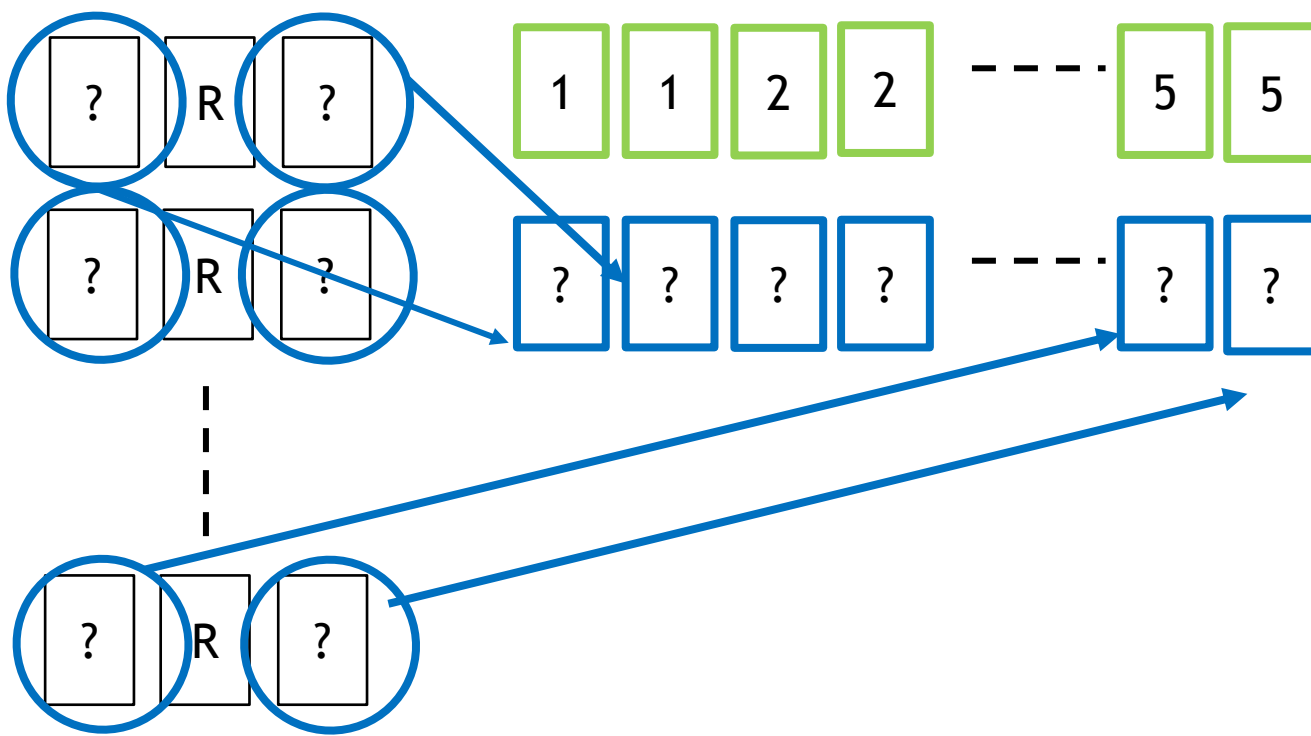
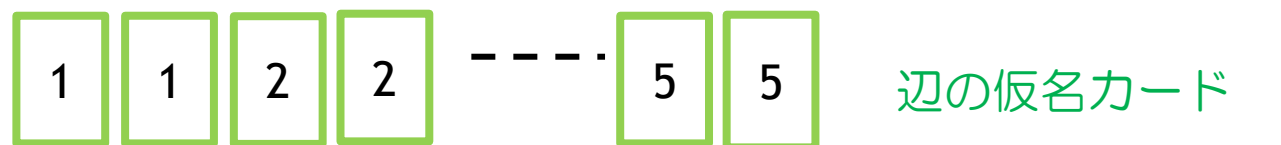
※1,2,3までは提案方式1と同じプロトコル

変形版: 4.閉路の確認(1/3)



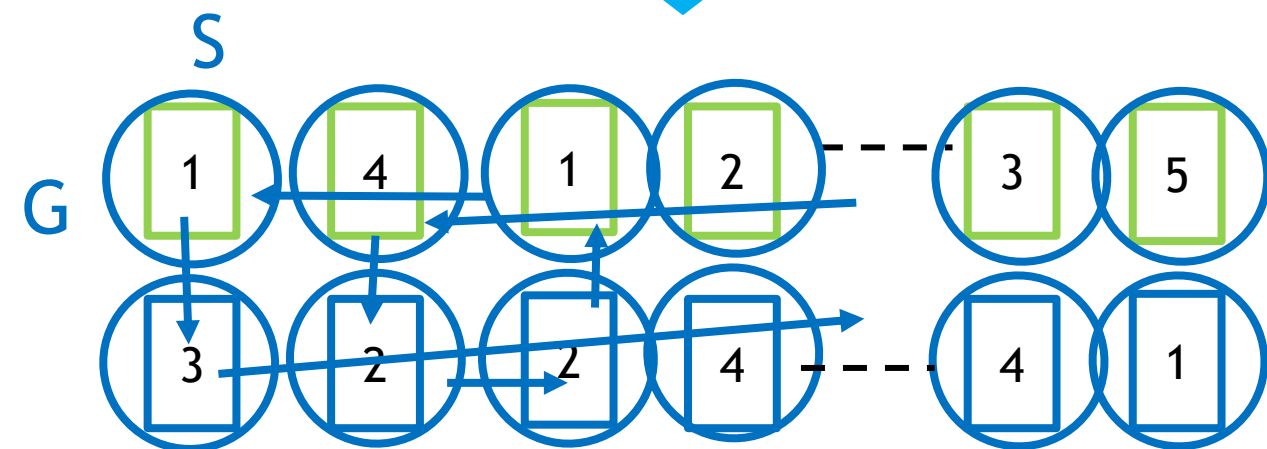
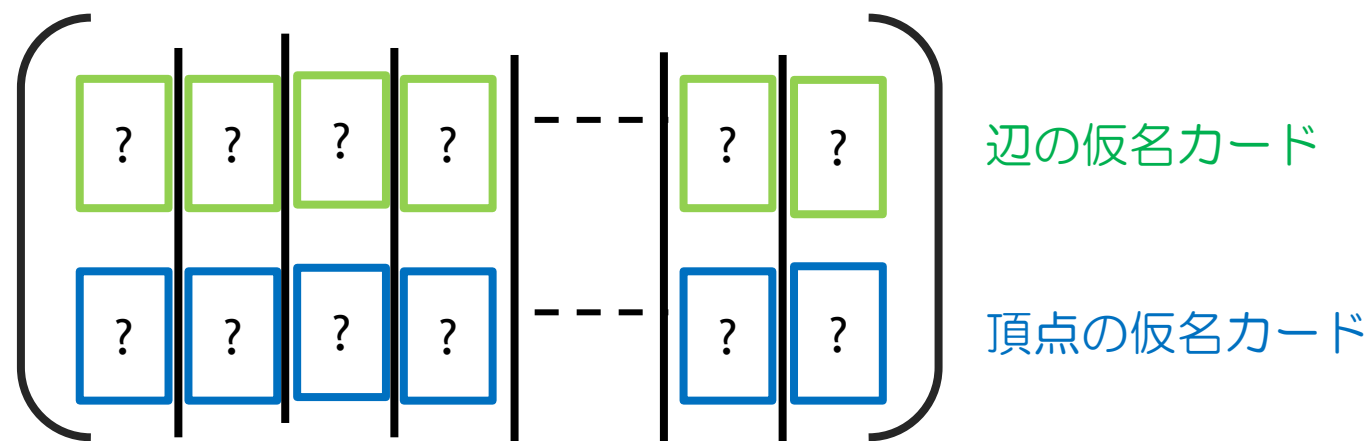
黒赤カード(ハミルトン閉路は赤カード)
をめぐり、赤カードのある行を抽出する

変形版: 4.閉路の確認(2/3)



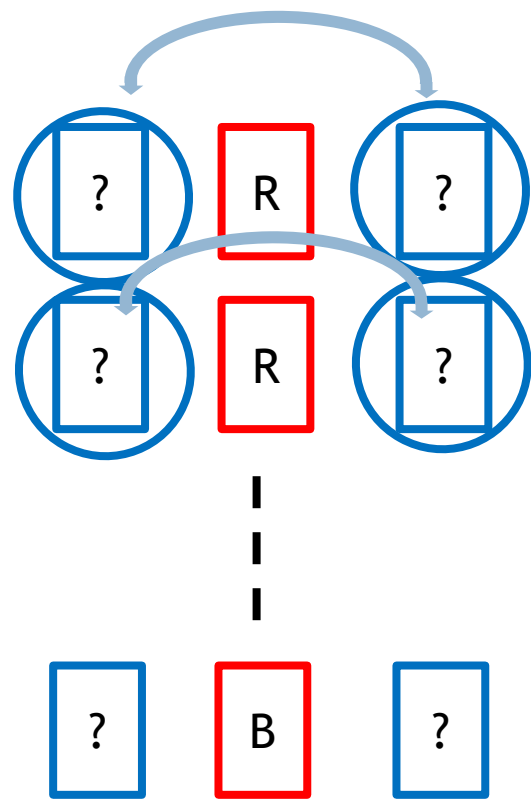
1. 辺の仮名カード $((1 \sim n) \times 2)$ を追加する
2. 用意した辺の仮名カードの下にそれぞれ、頂点の仮名カードを裏返しのまま配置する
3. 辺の仮名カードも裏返す

変形版: 4.閉路の確認(3/3)

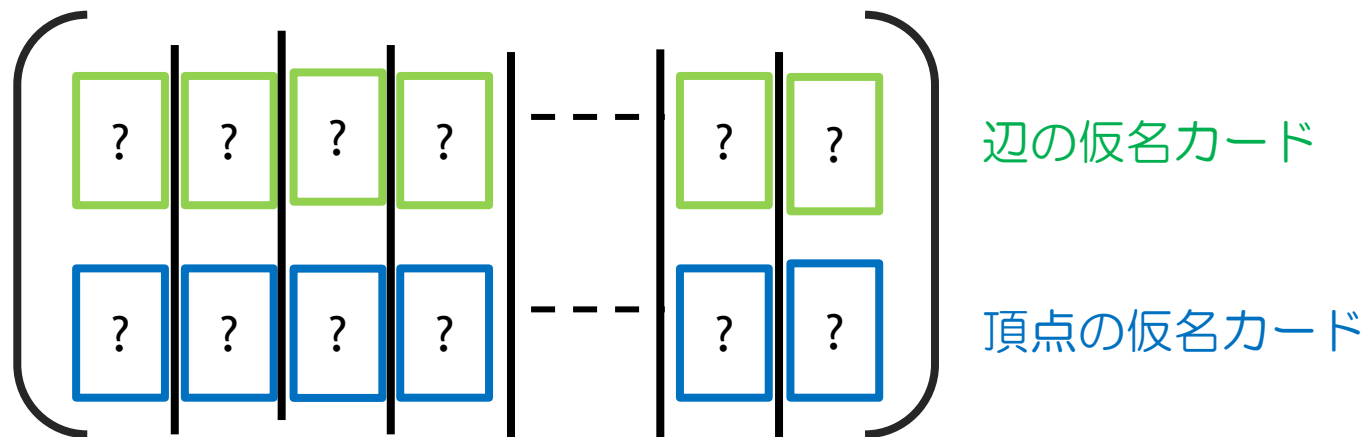


4. 辺の仮名カードと頂点の仮名カードを列でPSシャッフル
5. ハミルトンの辺の仮名の頂点が巡回路を与えることを確認
6. 2行目の表向きの $2n$ 枚の数字カードすべてを巡回して、最初に特定したカードに戻ることを確認する。戻ることが確認されたら証明を受理し、そうでない場合は証明を棄却

提案方式1とシャッフル数が異なる理由



提案方式1



提案方式1_変形版

グラフの形状からの情報漏洩を防ぎHの辺を特定させないために各行ごとに行っていたシャッフルを、辺の仮名カードを用いて一括シャッフルすることにより、頂点の仮名カードに関する情報を秘匿し1回のシャッフルで情報が漏洩を防ぐことができる

提案方式2^[2]について

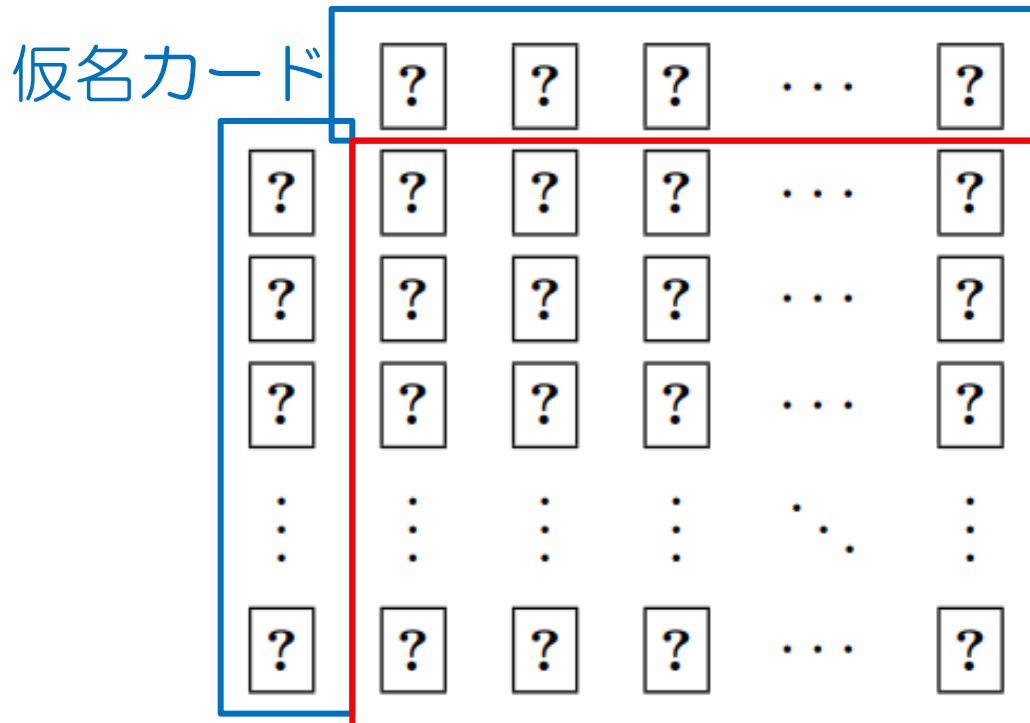
方式	シャッフル回数	カード枚数
既存方式1	$2(n-1)(2m-n-\Delta+1)$	$4(\Delta+3)(n+1)+4\Delta+2m+5$
既存方式2	$O(1)^*$	$n^2+O(n)^*$
提案方式1	$n+2$	$m+n\Delta$
提案方式1_変形版	3	$m+n(\Delta+2)$
提案方式2	3	n^2+2n

以上のように提案方式1_変形版はシャッフル数が3回である
次に、提案方式2について説明する

提案方式2は行列に基づくプロトコルで、シャッフル数が3回に固定される

提案方式2 [2]

頂点ではなく、ハミルトン閉路Hの辺を起点とする



Hの辺であるかを示す
黒赤カード

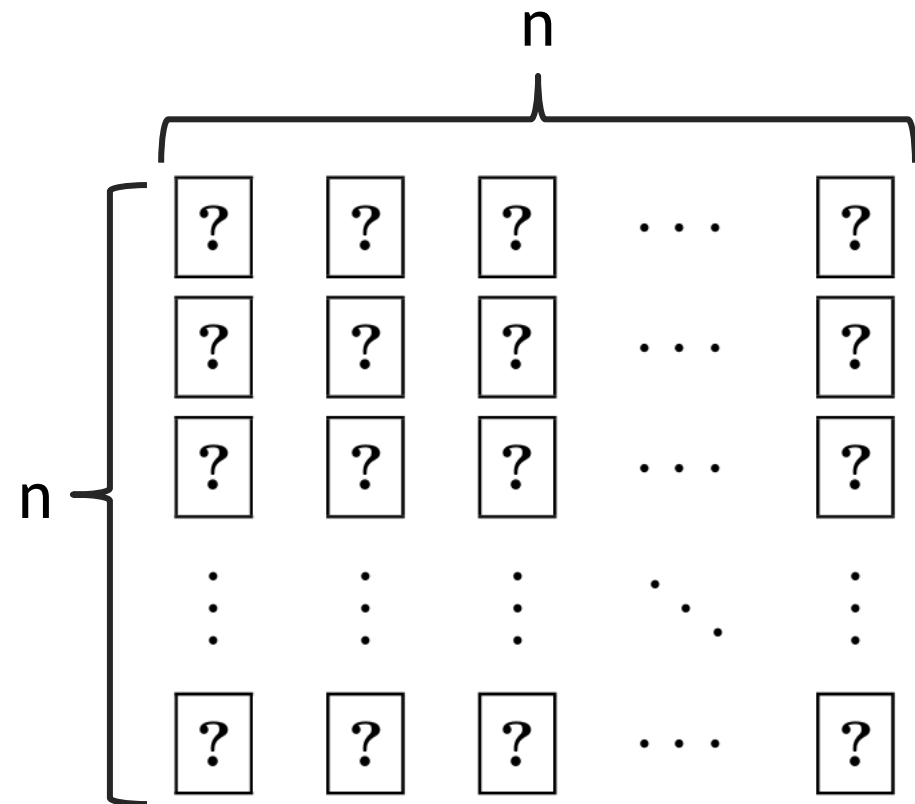
概要

1. ハミルトン閉路Hの辺であるかを示す黒赤カードの行列を作成
2. 頂点の仮名カードをPSシャッフルを用いて2組作成し行と列に配置
3. 行と列をそれぞれPSシャッフル
4. カードをオープンし、各行に赤カードが1枚ずつあるか確認(不正な入力の検知)
5. 仮名カードを用いて閉路を確認

次のページから詳しく説明

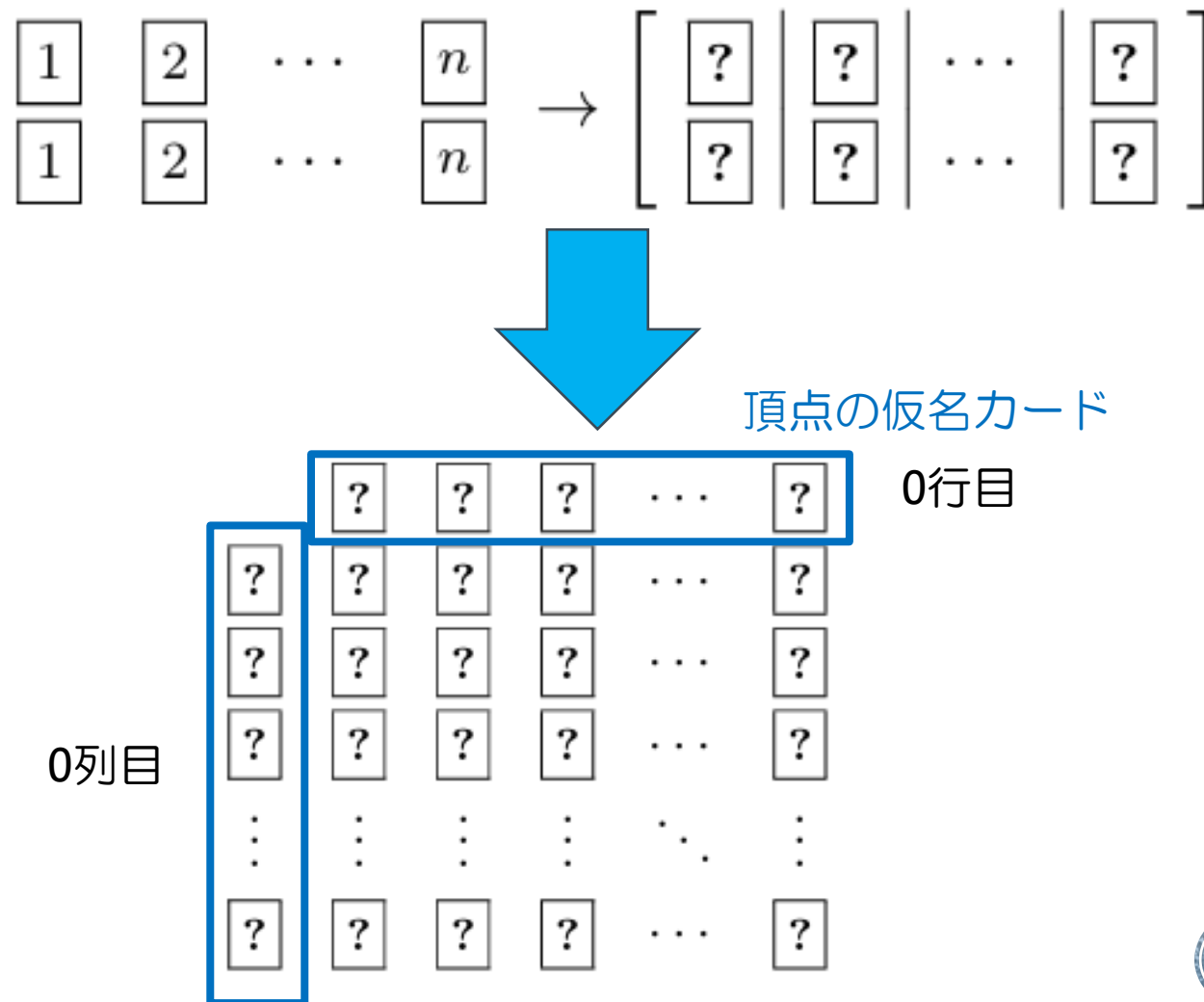
1.ハミルトン閉路Hの辺であるかを示す黒赤カードの行列を作成

サイズが $n \times n$ であり、頂点 v_i と v_j の間に
辺が存在するときに赤カード、辺が存在
しないときに黒カードを (i,j) 成分に裏返
して配置した行列を作成する



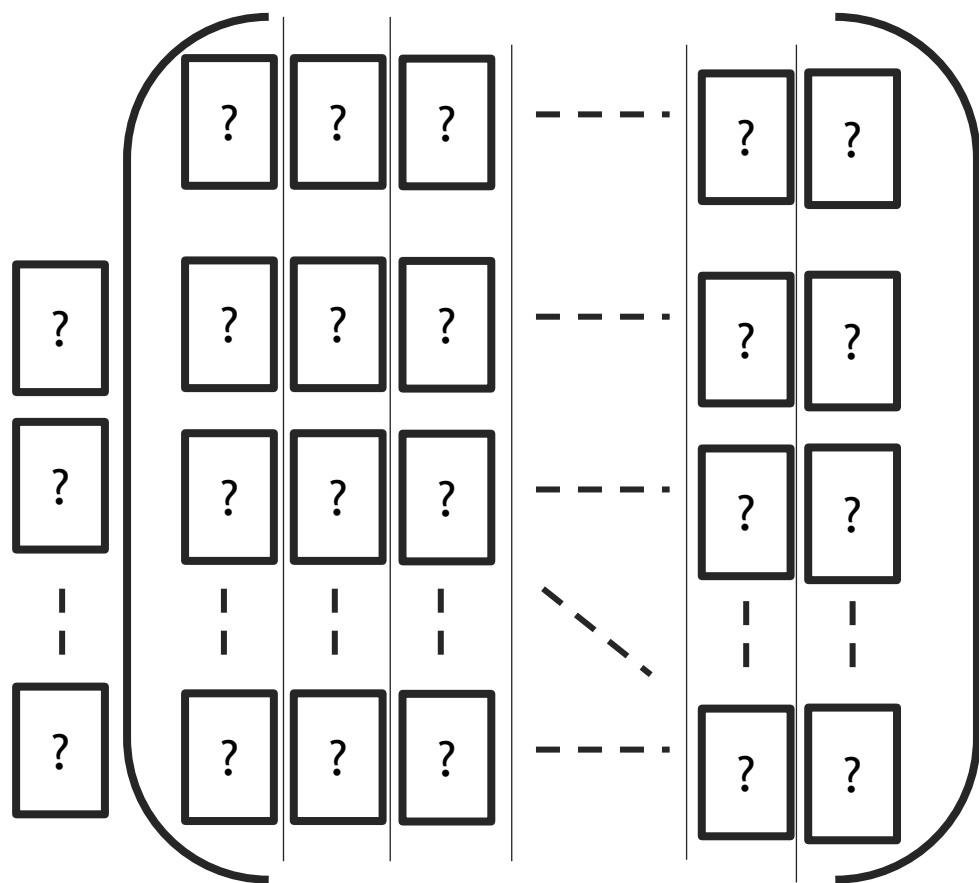
2.頂点の仮名カードをPSシャッフルを用いて2組作成し行と列に配置

1. 2枚ずつの1からnまでの数字カードを右図のように配置する
2. 裏返したのちPSシャッフルを行い頂点の仮名カードを作成する
3. 作成した頂点の仮名カードを行列の0行0列目に配置する

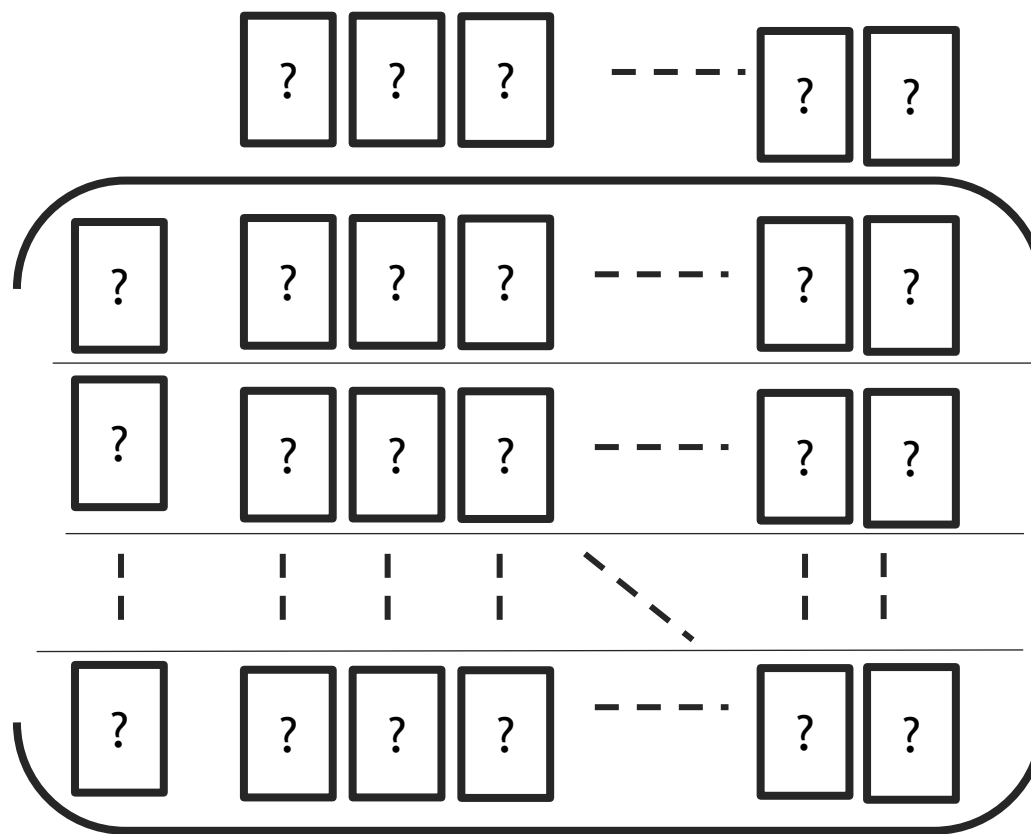


3. 行と列をそれぞれPSシャッフル

1列目から n 列目、1行目から n 行目にPSシャッフルを行う



列のPSシャッフル

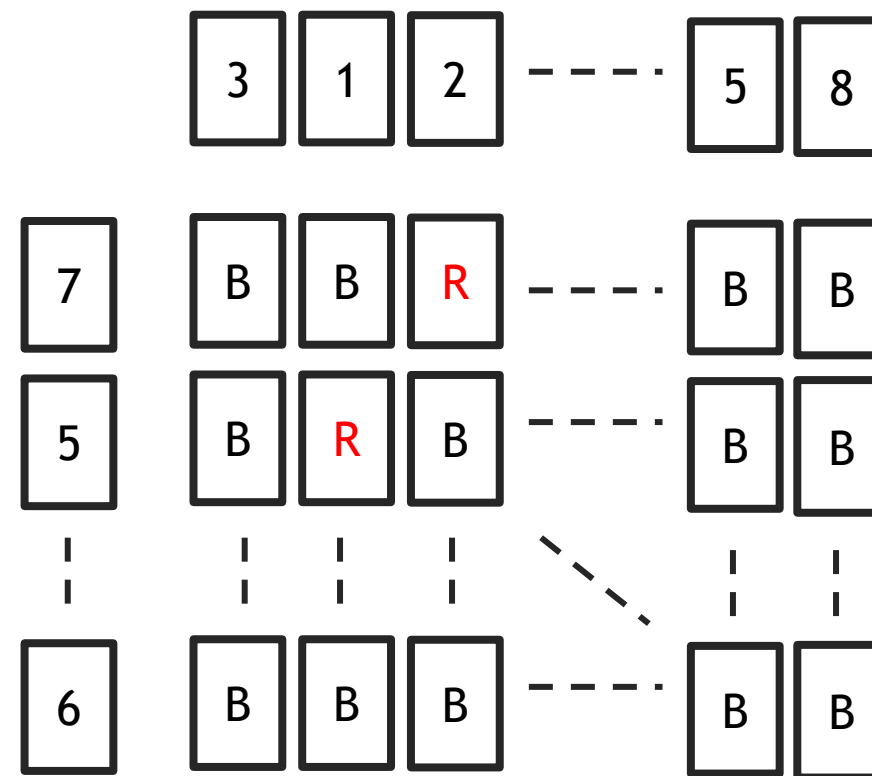


行のPSシャッフル

4.カードをオープンし、各行に赤カードが1枚ずつあるか確認

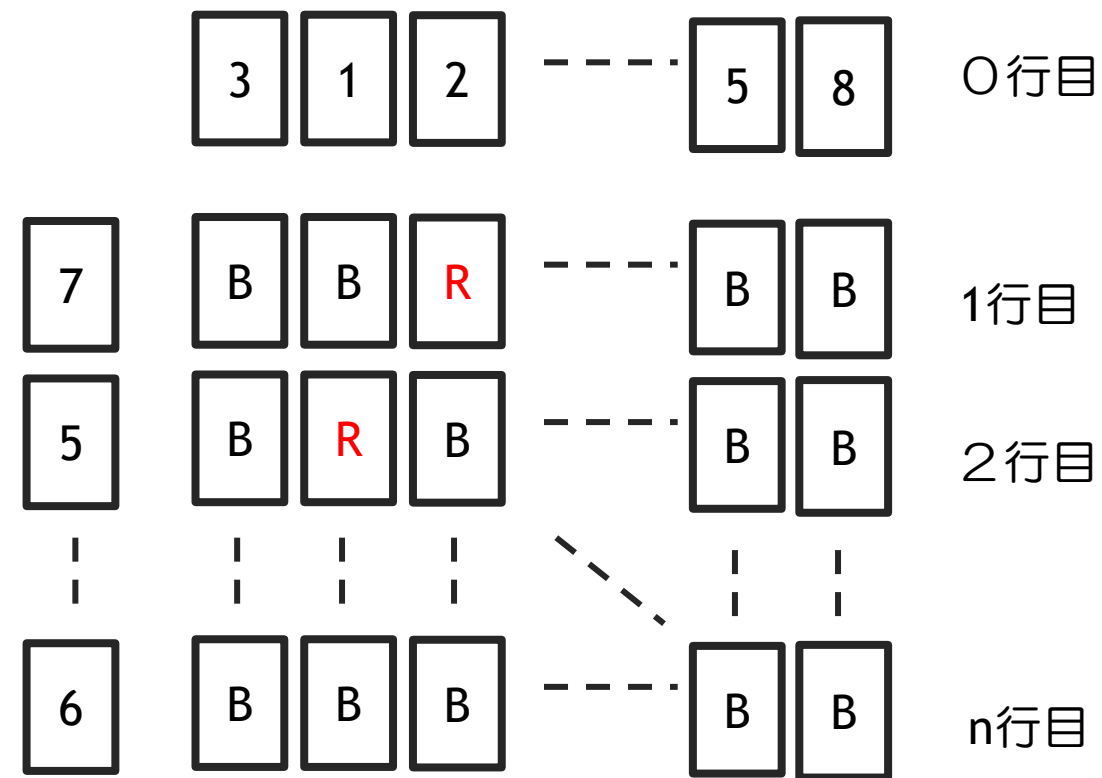
すべてのカードをオープンし、
各行に赤カードが1枚ずつ現れ
ているか確認する。

現れていなければ、棄却する



5. 仮名カードを用いて閉路を確認

1. 1行目の左端の数字カードの番号を $s_1 \in [1, n]$ とする
2. s_1 を始点としハミルトンの辺の仮名の頂点が巡回路を与えることを確認
3. すべての仮名カード(数字カード)を巡回したとき、証明を受理する。そうでない場合は、証明を棄却する。



安全性

完全性（証明者と検証者が正しく振舞うなら、証明は受理される）

- 証明者が部分グラフ $H \subseteq G$ の辺に赤カードを正しく配置したとき、証明はどの段階でも拒否されず、最後まで受理される。

健全性（証明者が嘘をつくことができない）

- 頂点の仮名はのちに開示されるため、ハミルトン閉路ではない不正カード配置は、閉路確認の際に検出される。

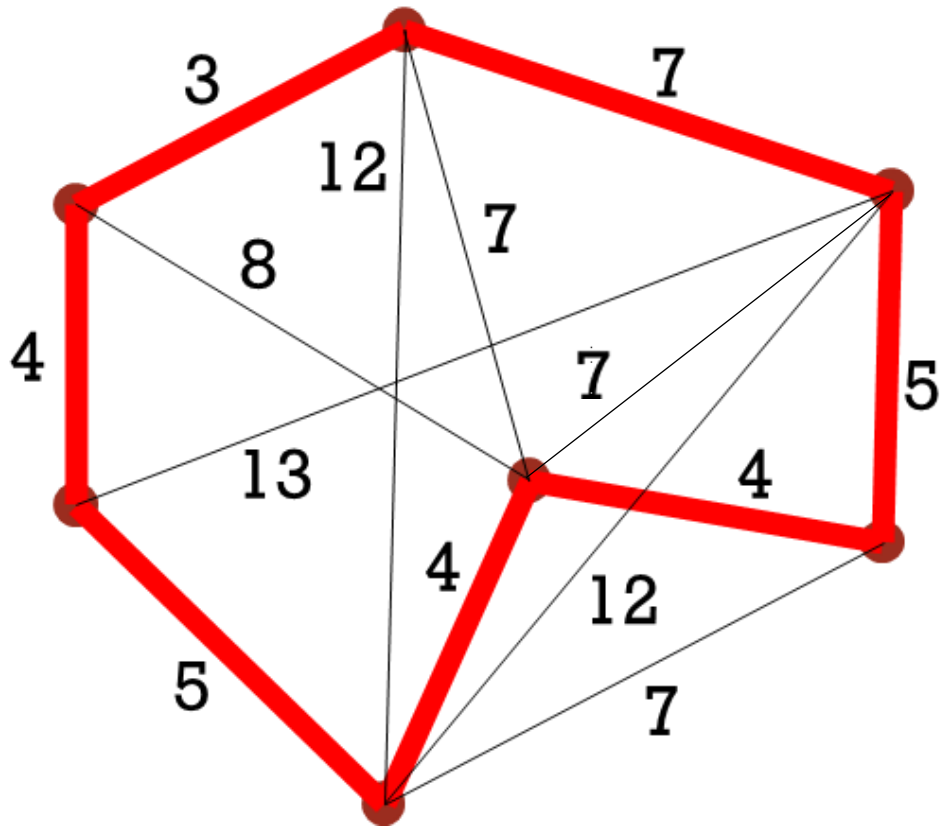
ゼロ知識性（検証者に知識が漏れない）

- カードを開示する直前でシャッフルを行うことで、カードの対応箇所情報が秘匿される。

もくじ

1. ハミルトン閉路とゼロ知識証明
2. プロトコル
3. プロトコルの応用
 - 巡回セールスマン問題のゼロ知識証明
4. まとめ
5. 後続研究

巡回セールスマン問題

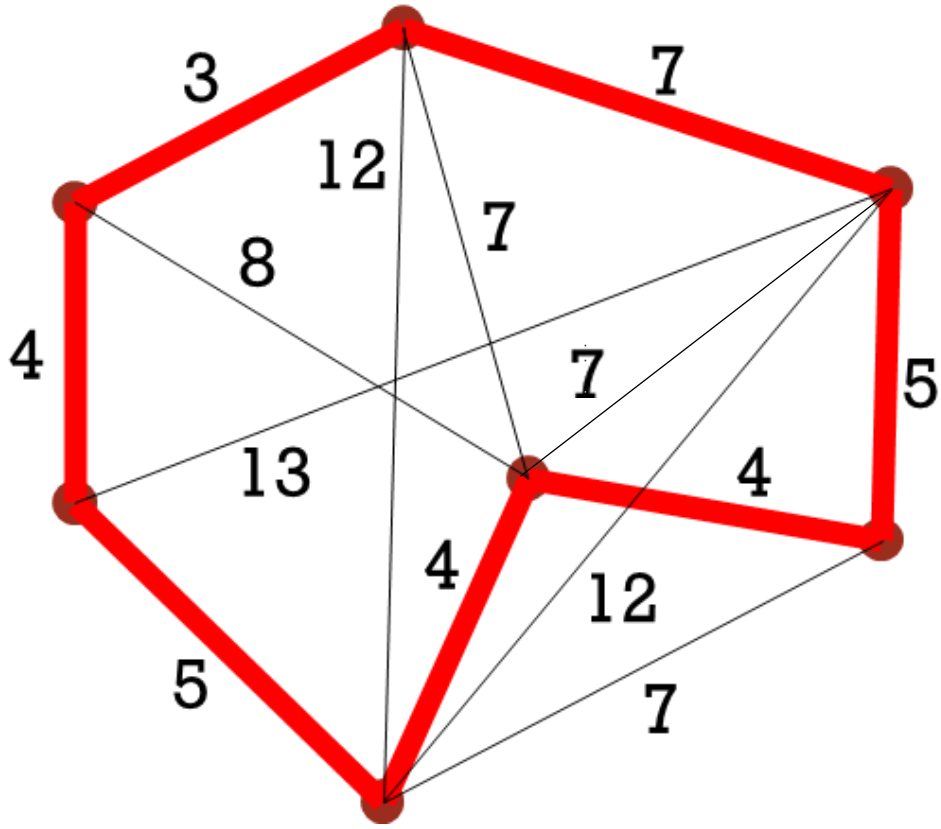


各辺は距離を持つ

各都市を必ず1度訪れて出発点に戻り、移動距離が最短になる経路を求める

輸送・配送ルート最適解導出の鍵になる概念

巡回セールスマン問題

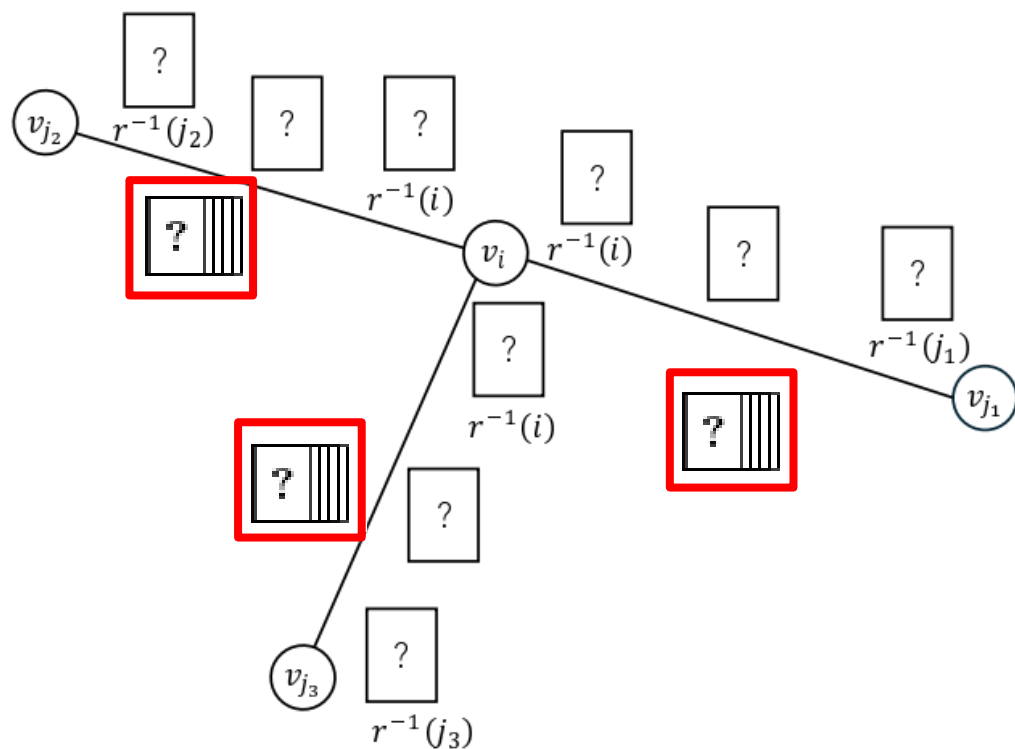


今回提案するゼロ知識証明では、
総移動距離が x km以下の経路の
存在を示す

距離を秘匿する場合は、
距離の大小比較を行う
※今回は、大小比較の説明は省く

巡回セールスマン問題のゼロ知識証明

ハミルトン閉路 + 距離



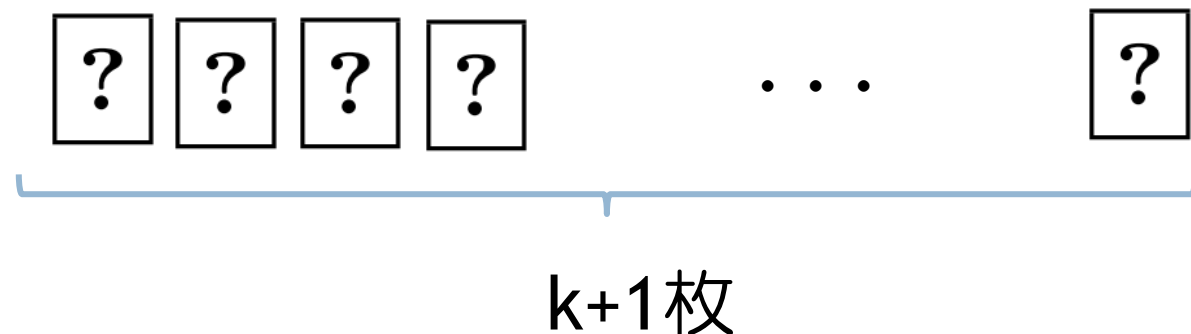
- 閉路であること
→ ハミルトン閉路のZKPより確認
- 距離が所定の値以下であること
→ 距離を加算し、総和を求める

巡回セールスマン問題のZKPとなる

距離コミットメントと加算

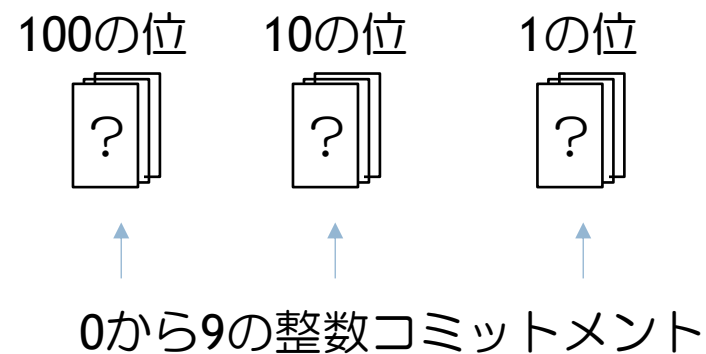
整数コミットメント

$k+1$ 枚のカードを用いて $0 \sim k$ の整数を表す



桁表記された整数コミットメント

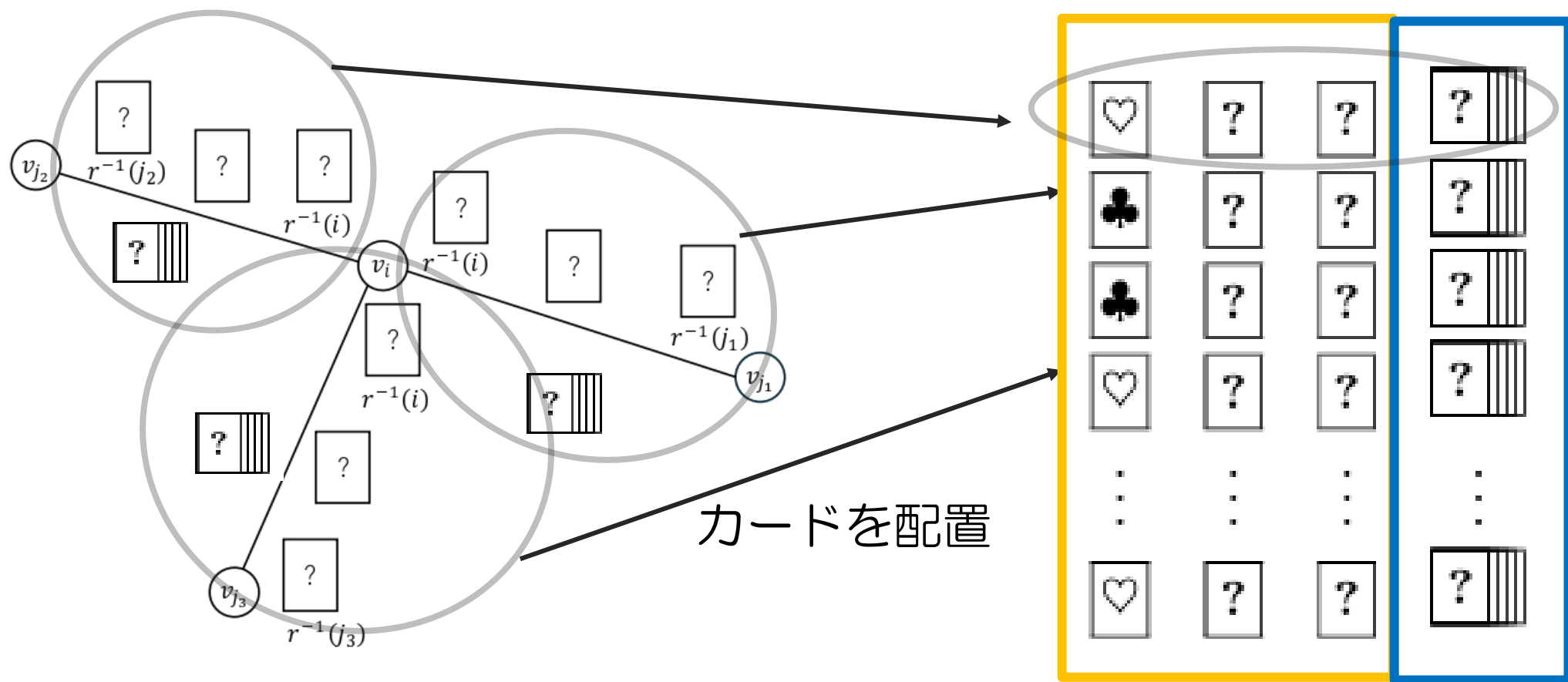
整数 k を表すために $O(\log_{10} k)$ 枚のカードで十分



加算

桁表記された整数コミットメントの加算を行う

巡回セールスマン問題への応用



ハミルトン閉路であることを確認

加算して、距離の総和を確認

もくじ

1. ハミルトン閉路とゼロ知識証明
2. プロトコル
3. プロトコルの応用
4. まとめ
5. 後続研究

まとめ

1. ハミルトン閉路問題とゼロ知識証明についての解説
2. ハミルトン閉路問題の物理的ゼロ知識証明について紹介した
 - 応用として、巡回セールスマン問題の物理的ゼロ知識証明も紹介

もくじ

1. ハミルトン閉路とゼロ知識証明
2. プロトコル
3. プロトコルの応用
4. まとめ
5. 後続研究

関連する後続研究

1. 藤原愛斗（茨城大学）、品川和雅（筑波大学／産業技術総合研究所）
「ハミルトン閉路問題に対するカードベースゼロ知識証明とHidatoへの応用」(SCIS2026)
2. 小河子竜、石田楓雅、松田眞彦、上嶋章宏（大阪電気通信大学）
「ハミルトン閉路遷移問題およびマッチング遷移問題に対する物理的ゼロ知識証明」（SCIS2026）

後続研究1

「ハミルトン閉路問題に対するカードベースゼロ知識証明とHidatoへの応用」

概要

- ハミルトン閉路問題のZKPを既存手法より効率化した
- Hidatoと呼ばれるペンシルパズルに対する、効率化したカードベースゼロ知識証明の提案

後続研究2

「ハミルトン閉路遷移問題およびマッチング遷移問題に対する物理的ゼロ知識証明」

概要

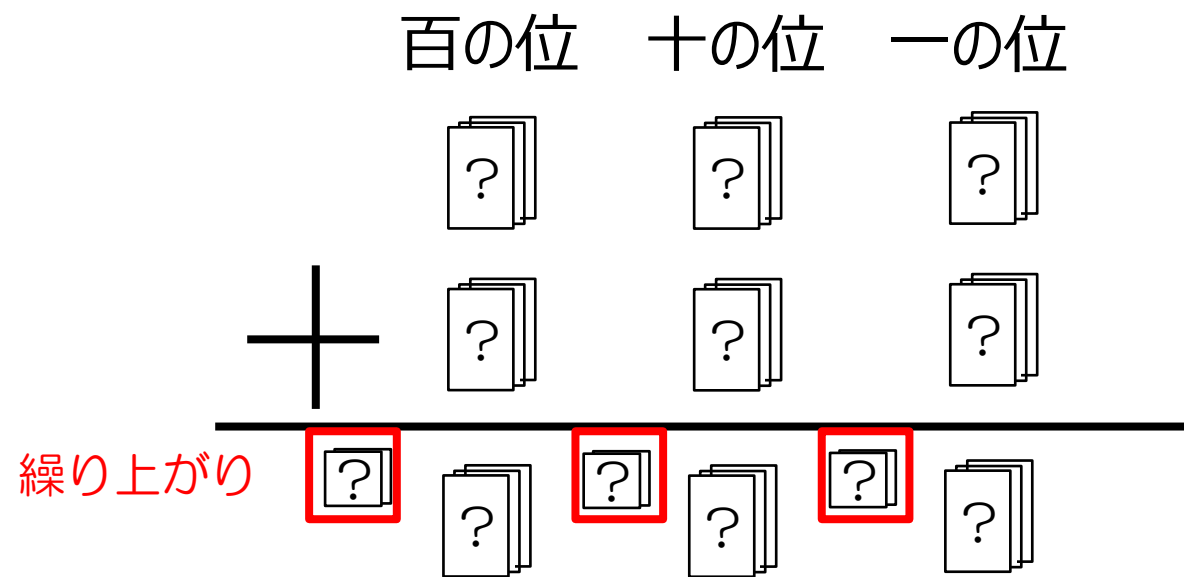
- ハミルトン閉路遷移問題に対するZKPの提案
- マッチング遷移問題に対するZKPの提案

ご清聴
ありがとうございました

追加資料

加算

イメージ図



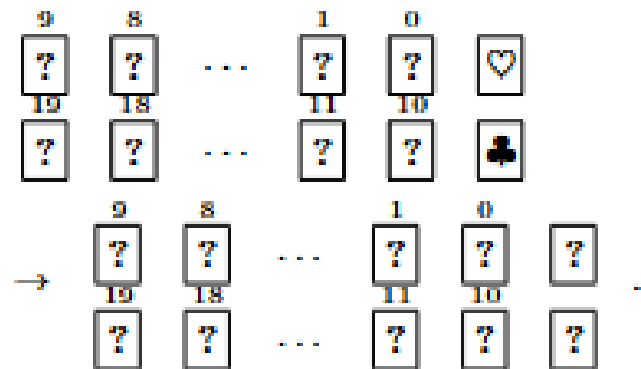
加算

①同じ桁同士を足して0～19の和を計算する



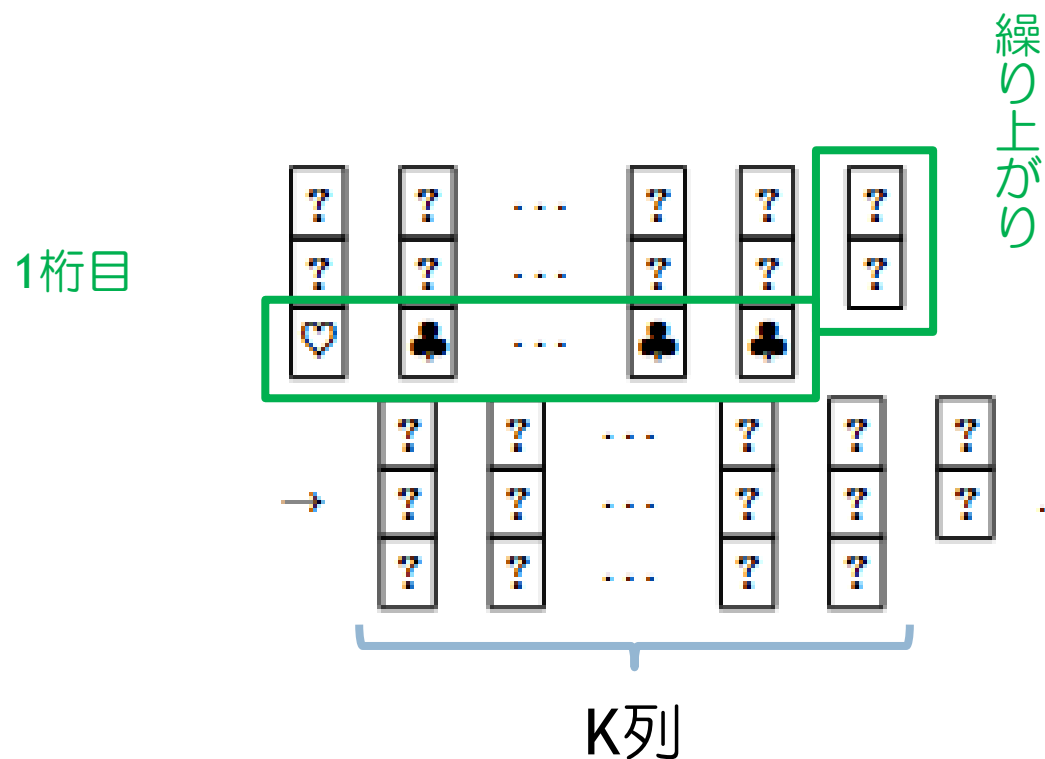
加算

②加算したカードを0～9、10～19に分けて並べる
行をまとめてPSシャッフルする



加算

③繰り上がりと加算結果の一桁目用のカードを並べる
裏返して、左10枚をPile-shiftingシャッフル



加算

④上2行のカード列の左10枚を公開して、Rが右端に来るように左10列を巡回シフトして結果を出力する

1行目と2行目のうちRを含む行の右端のカードと含まない行の右端のカードを左から順に並べると、加算の繰り上がりの計算結果となる

