産学連携によるカードベース暗号の数理的未解決問題と新課題の整理

カードベースZKPプロトコル

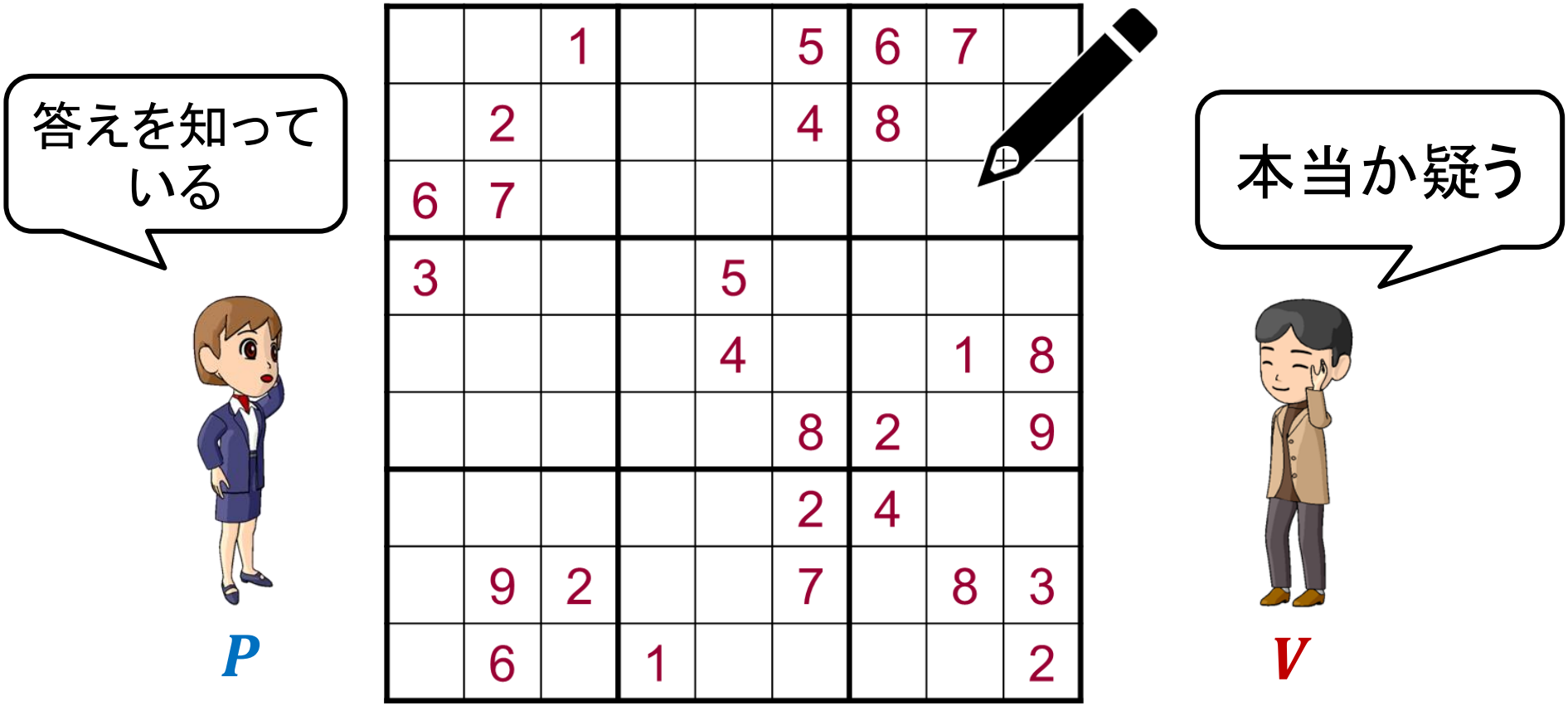
電気通信大学 情報理工学研究科
宮原 大輝

目次

1. パズルZKPの概要
2. Gradwohlらのプロトコル
3. 未解決問題

ペンシルパズルに対するZKPの概要

- ***P***はパズルの答えを知っていると***V***に納得させたい
- ***P***は答えそのものは***V***に見せたくない（知識を漏らさない＝ゼロ知識）



		1			5	6	7	
	2				4	8		
6	7							
3				5				
				4			1	8
					8	2		9
					2	4		
	9	2			7		8	3
	6		1					2

アプリケーションの例

- あるパズル雑誌に掲載されたパズルの問題に答えが存在することを、その雑誌の出版社（＝P）が購入者（＝V）に保証する

- パズルはしばしばNP完全であるため、その解を知っていることに価値がある場合がある
  - 賞金や名誉が懸かったパズルの解を自分だけが知っていることを証明する

- [物理道具を用いるメリット] 計算機に頼らずに簡単にZKPを実演できると、セキュリティ教育に活用できる[Gradwohlら、FUN07]

研究目的

- 様々なパズルに対するZKPを現実的な時間・カード枚数で実行可能になることを目指す
  - NPであればZKPが存在するが[Goldreichら、J.ACM91]、問題から直接構成したZKPは効率的
  - 数独を中心に効率性の改良が行われている[田中ら、SCIS23]

- パズルを解くのと同じようにZKPを構成でき、楽しい

計算量解明
ex.) へびいちご

ZKPを構成
ex.) スリザーリンク

効率改良
ex.) 数独

カードベースZKPプロトコルの流れ

- 2017年以前までは海外の研究者による研究成果が散発的に発表されている

著者	パズル	文献
Gradwohlら	数独	FUN07 -> TCS
Chienら	ノノグラム	FUN10
Bultelら	美術館など（4つ）	FUN16

- これらは全て健全性エラーを許している、つまり答えが入力されなくても検証を通過する確率が存在する
- カード列を複製するプロトコル[Hashimotoら、ICITS17]を活用することで健全性エラー確率を0にできる（後述）

目次

1. パズルZKPの概要
2. Gradwohlらのプロトコル
3. 未解決問題

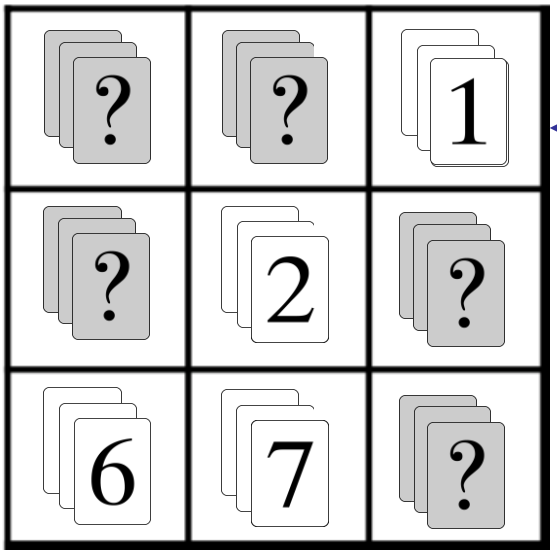
（一般化）数独（NP完全問題）

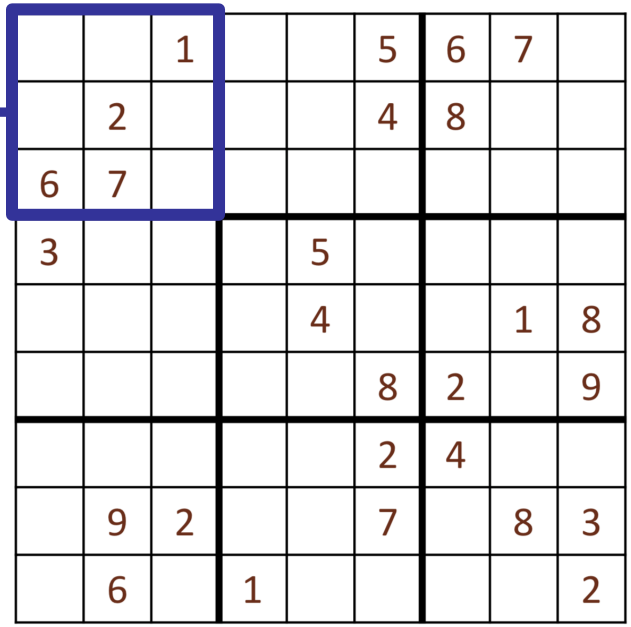
- 全ての空きマスに1~nの数字を埋める
- 各行/各列/各ブロック内の数字は重複しない

		1			5	6	7	
	2				4	8		
6	7							
3				5				
				4			1	8
					8	2		9
					2	4		
	9	2			7		8	3
	6		1					2

準備

- ***P***は答えに従って各マスに**3**枚ずつ数字カードを伏せて置く
- 予め数字が埋まっているマスには表向きに置く

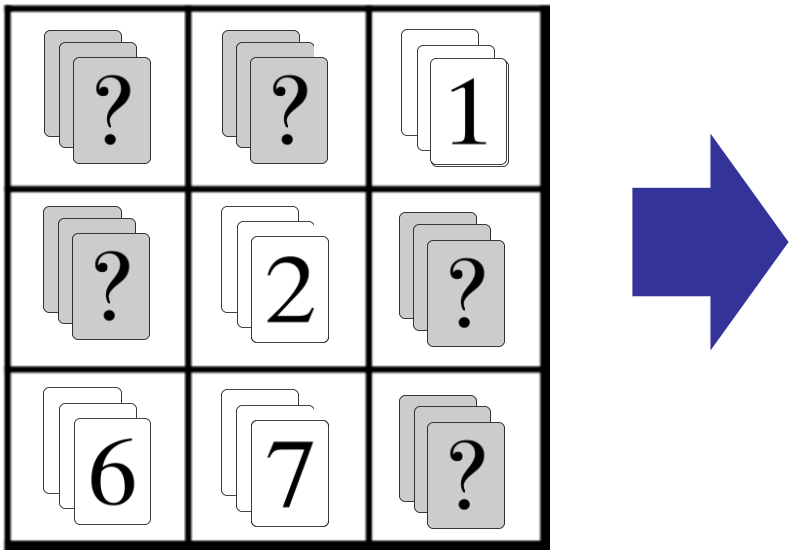




		1			5	6	7	
	2				4	8		
6	7							
3				5				
				4			1	8
					8	2		9
					2	4		
	9	2			7		8	3
	6		1					2

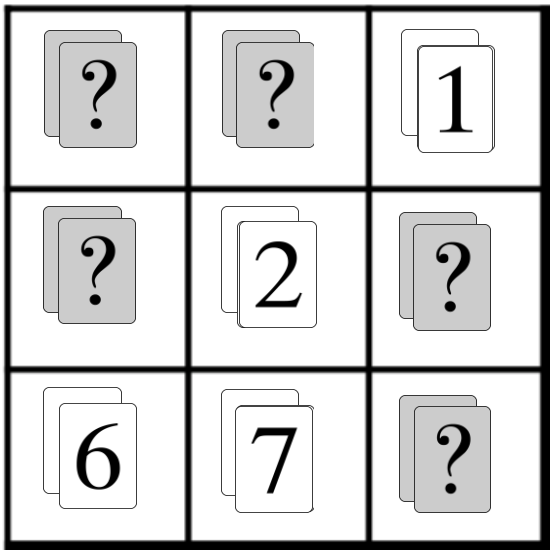
検証

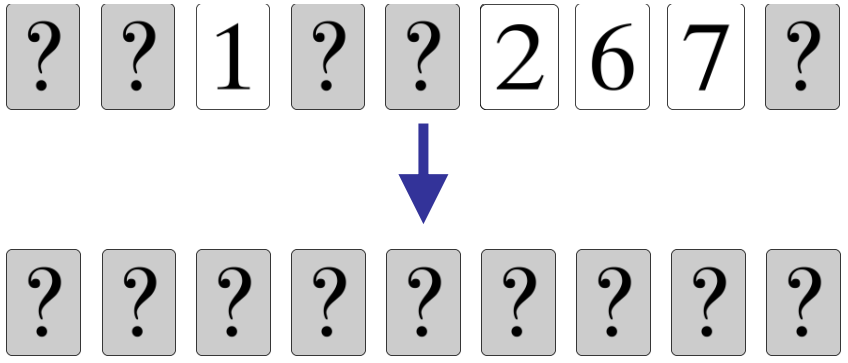
- Vは検証したい行・列・ブロックに置かれたカードを1枚ずつ取り出し、n枚のカード列を作る
- 表向きのカードを裏返す



検証

- Vは検証したい行・列・ブロックに置かれたカードを1枚ずつ取り出し、n枚のカード列を作る
- 表向きのカードを裏返す

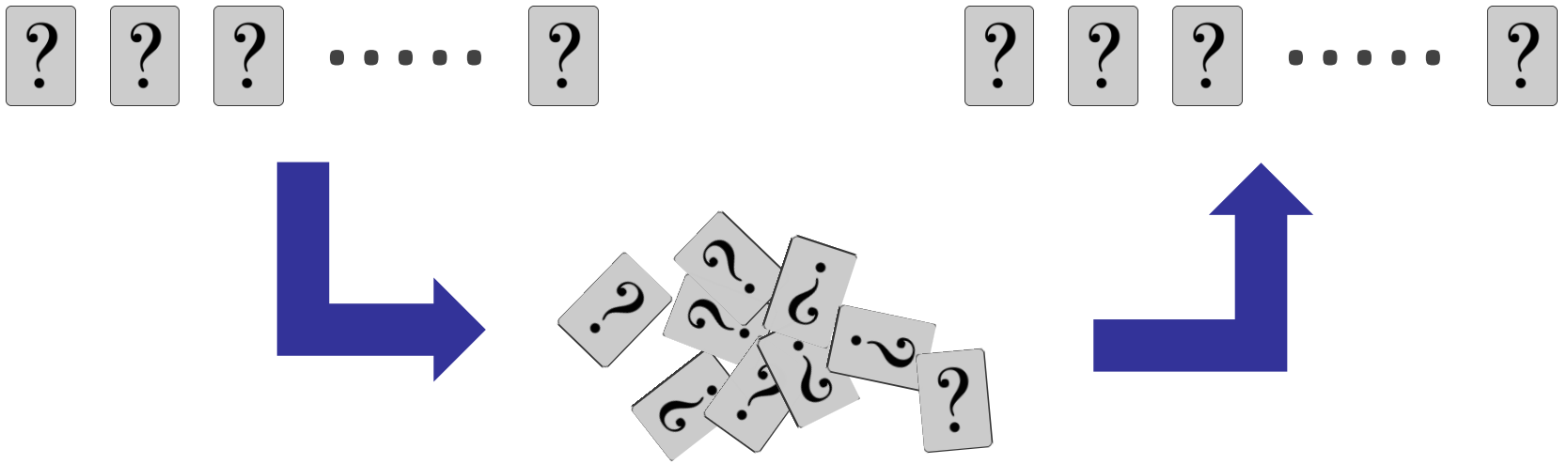




1~nの数字が含まれているか検証したい

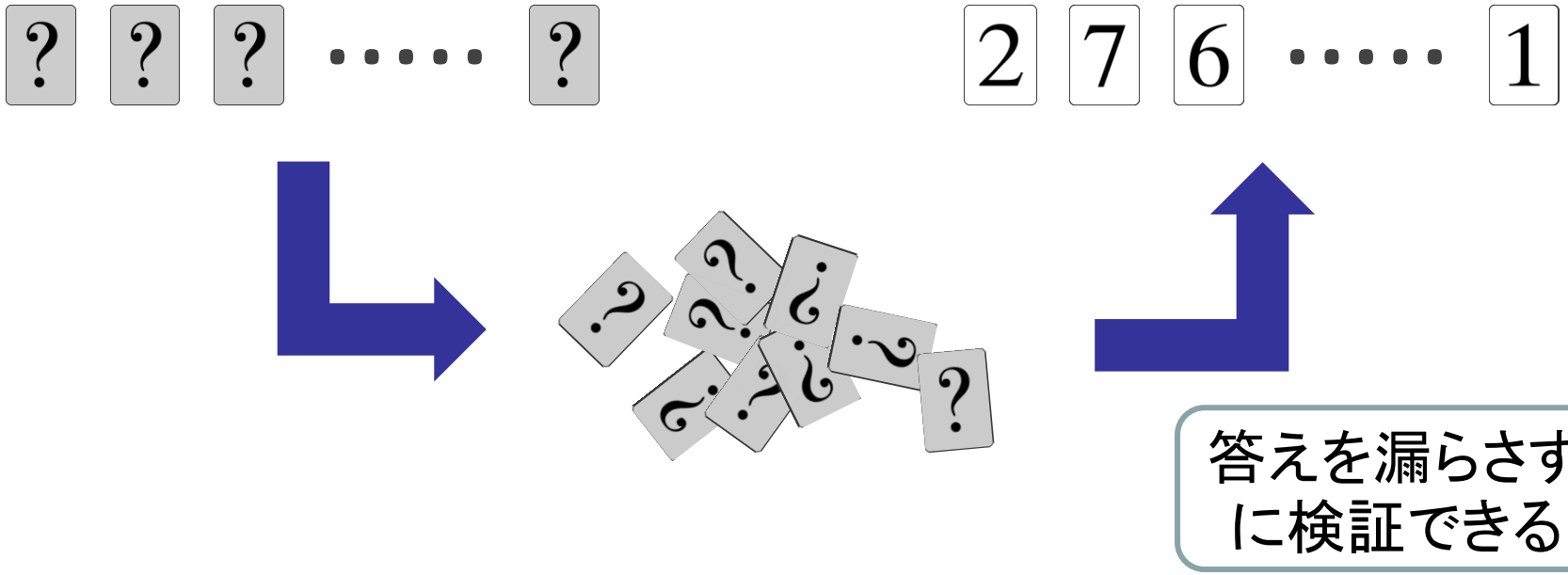
シャッフル

- Vはn個のカードをシャッフルする



情報を漏らさずに納得させる

- Vはn個のカードをシャッフルする
- カードをめくり数字が重複していないことを確かめる
- 残りの行・列・ブロックに対して同様の操作を行う



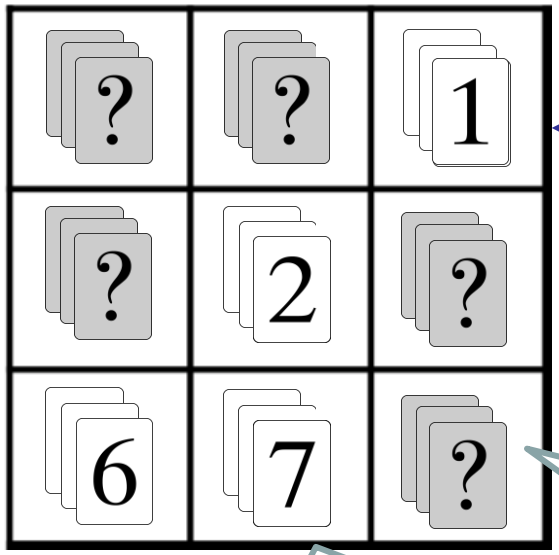
同様の検証を繰り返す

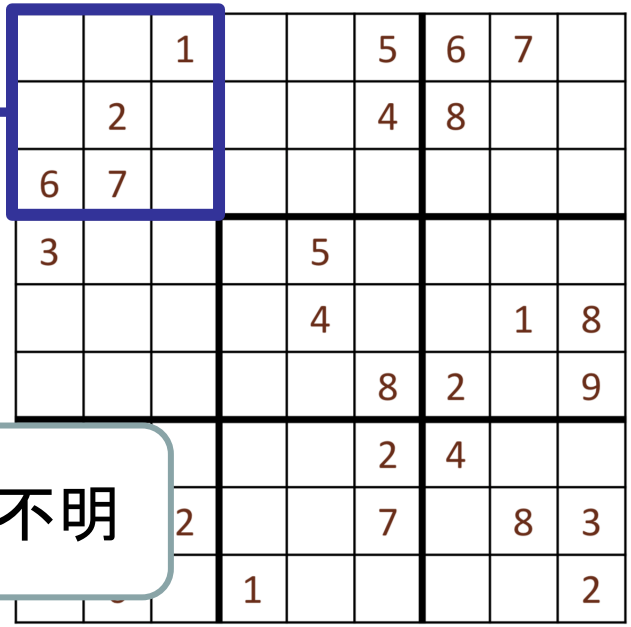
- Vは残りの行・列・ブロックに対して同様の検証を行うと、は答えが存在することを納得する

		1			5	6	7	
	2				4	8		
6	7							
3				5				
				4			1	8
					8	2		9
					2	4		
	9	2			7		8	3
	6		1					2

健全性エラーが存在する理由

- ***P***が各マスに置いた3枚の数字カードが等しいことを確かめていない
- 答えを知らない***P***がマスに異なる数字カードを置くことで、***V***を納得させてしまう場合がある





等しいか不明

Hashimotoらの技術を活用して複製[Sasakiら、FUN18]

目次

1. パズルZKPの概要
2. Gradwohlらのプロトコル
3. 未解決問題（4つ）

[再掲] 研究目的

- 様々なパズルに対するZKPを現実的な時間・カード枚数で実行可能になることを目指す
  - NPであればZKPが存在するが[Goldreichら、J.ACM91]、問題から直接構成したZKPは効率的
  - 数独を中心に効率性の改良が行われている[田中ら、SCIS23]

- パズルを解くのと同じようにZKPを構成でき、楽しい

計算量解明
ex.) へびいちご

ZKPを構成
ex.) スリザーリンク

効率改良
ex.) 数独

未解決問題(1/4):数独

- Sasakiら[TCS20]、Ruangwises[NGCO22]、田中ら[SCIS23]によって必要な枚数・シャッフル数が改良された

著者	枚数	シャッフル数	必要なデッキ
Gradwohlら	243	27	トランプ27組
Sasakiら	90	45	トランプ9組
Ruangwises	120	322	トランプ2組
田中ら*	90	11	UNO2組

*シャッフルの実装に工夫あり

- 現実的な時間で実行可能になるためには？
- 他のパズルに対するZKPは効率化できるか？

未解決問題(2/4):他のペンシルパズル

- ZKPプロトコルが構成されていない(ニコリ社の)数字パズルは約25個

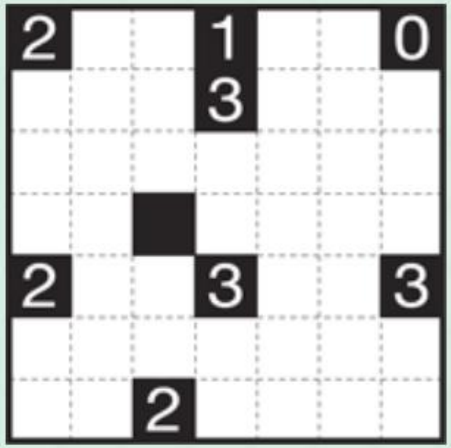
因子の部屋、ウソワン、お家へ帰ろう、カックロ、キンコンカン、クロット、黒どこ(黒マスはどこだ)、碁石ひろい、さしがね、さとがえり、サムライン、四角に切れ、シャカシャカ、縦横さん、推理パズル、数コロ、数独、ストストーン、スラローム、スリザーリンク、ダブルチョコ、チェンブロ、チョコバナナ、月か太陽[IWSEC23で発表]、ドッスンフワリ、ドッチループ、流れるループ、ナンスケ、ナンバーリンク、ぬりかべ、ぬりみさき、ぬりめいず、のりのり、波及効果、橋をかけろ、バッグ、美術館、ひとりにしてくれ、フィルオミノ、ふくめん算、へびいちご、へやわけ、ヘルゴルフ、ペンシルズ、マカロ、ましゅ、マックロ、ミッドループ、虫くい算、やじさんかずさん、ヤジリン、よせなべ、LITS

下線はZKPに関する発表がされていないパズル(宮原調べ)

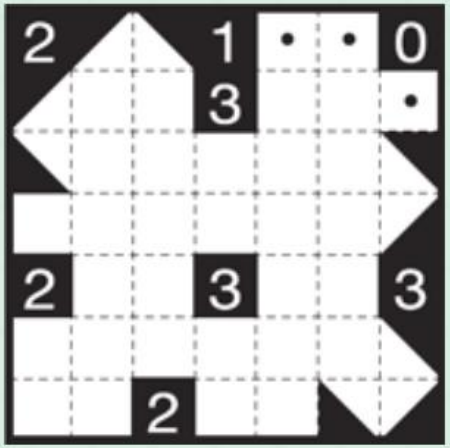
* 数字のパズル一覧:https://www.nikoli.co.jp/ja/puzzles/

未解決問題(2/4):シャカシャカ

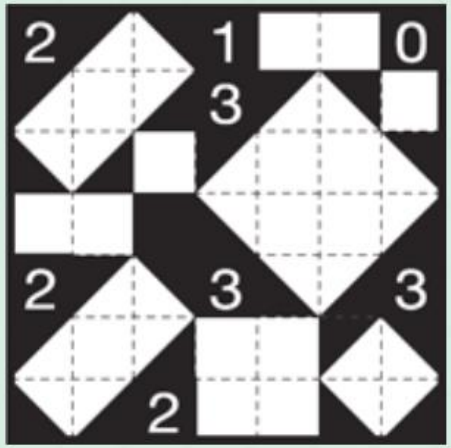
- 特に図形を扱うパズル(下のシャカシャカなど)は難易度が高い
  - 四角に切れは長方形の面積が既知なので、そのZKP [Ruangwises、FUN22]はそのまま適用できない
  - 図形が長方形であることの定義に立ち返る必要がある



例題



途中経過

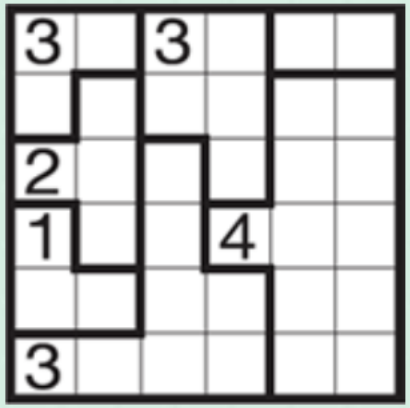


答え

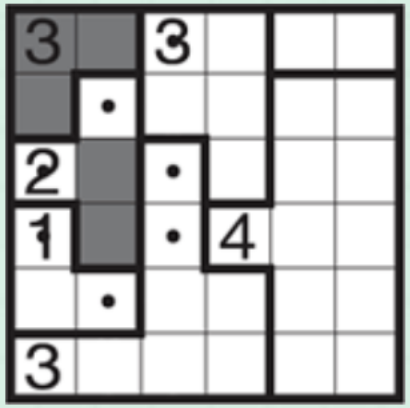
* 図はhttps://www.nikoli.co.jp/ja/puzzles/shakashaka/ から引用

未解決問題(2/4):ストストーン

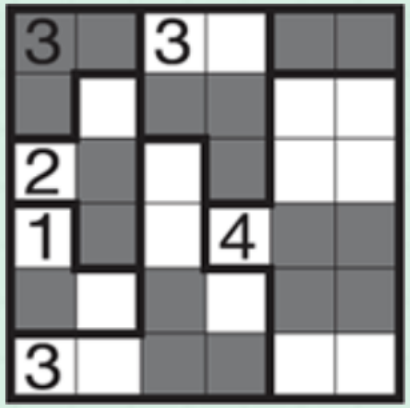
- 下のストストーンは重力を扱う
  - 縦1列だけを見ても解決しない
- テトリスのような落下を、図形の形状・位置を秘密にしたまま計算できれば良い



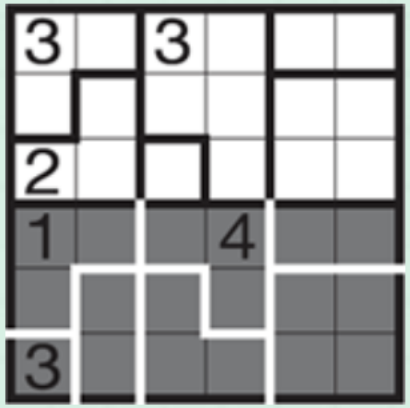
例題



途中経過



答え

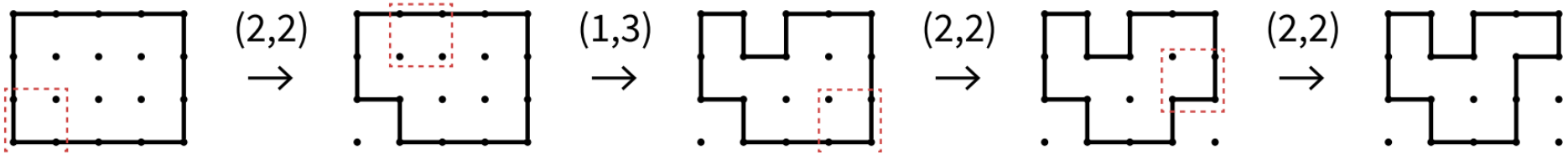


落ちたとき

* 図はhttps://www.nikoli.co.jp/ja/puzzles/sto-stone/ から引用

未解決問題(3/4):対話型 vs. 非対話型

- 効率性(必要なカード枚数・シャッフル回数・シャッフル操作の難易度)に差があるか研究する
- 複雑なパズルに対しては非対話型になりがち
- スリザーリンク[Lafourcadeら、ISPEC19]では、証明者が検証者と対話して盤面に1つのループを作る



- スリザーリンクに対するZKPを非対話型で構成できるか、つまり盤面に1つのループが存在することを非対話で(効率的に)検証できるのか、対話型よりも効率的なのか

未解決問題(4/4):計算機 vs. カードベース

- カードベース非対話型ZKPは定式化され[Miyaharaら、ProvSec21]、完全性・健全性・安全性(情報理論的安全性)を満たす
- 計算機ベース方式の安全性証明において用いられるrewindとの関係は十分に研究されていない
- 健全性の証明において悪意のある証明者ができる行動範囲も十分に議論されていない

- 計算機ベースにおける健全性・安全性との関係をどのように解釈していくのか今後の課題である

質疑応答

- 出版社が雑誌にNIZKを載せて、購入者が検証できると面白い
  - 詳細に検討したことがなく興味深い。遠隔で実行できる物理暗号プロトコルそのものがほぼ検討されていないので、それも含めて今後の課題である
- 解が唯一解であることのZKPはあるのか
  - 唯一解を持つかどうかを判定する決定問題はASPと呼ばれ、ASP完全という概念もある。これに対してカード組・計算機を用いたZKPはまだ取り組まれていない（宮原調べ）