Card-Based ZKP Protocol for Nurimisaki

Léo Robert[1] Daiki Miyahara[2] Pascal Lafourcade[3] Takaaki Mizuki[4,5]

[1]XLIM, Université de Limoges, France

[2]Graduate School of Information Sciences, Tohoku University, Sendai, Japan

National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan

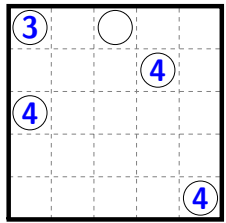
[3]Université Clermont-Auvergne, CNRS, Mines de Saint-Étienne, LIMOS

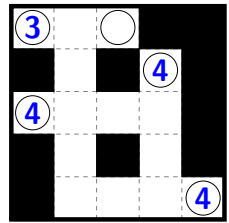
[4]Cyberscience Center, School of Engineering, Tohoku University, Sendai, Japan

[5]Department of Information Science, Ochanomizu University, Tokyo, Japan

November 17, 2022

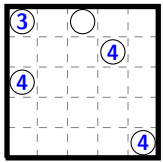
Nurimisaki

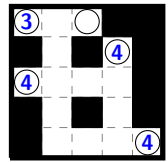




- ○ $\Leftrightarrow$ Misaki: only one neighbour is white.
- **Number Rule:** Number of white cells in straight line from Misaki.
- **Square Rule:** No 2×2 square is composed of all blacks/whites.
- **Connectivity Rule:** White cells are connected.

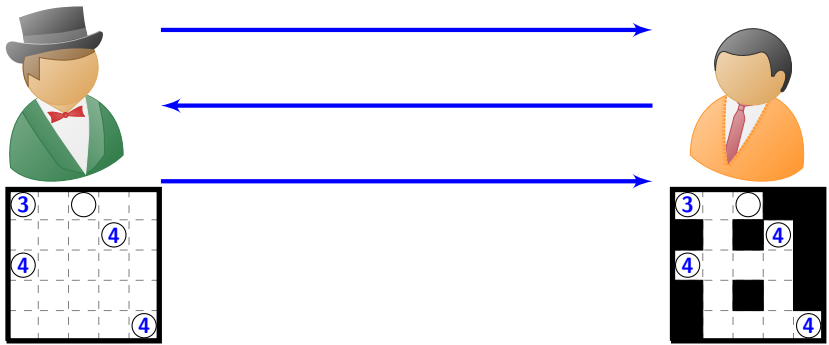
Zero-Knowledge Proof (ZKP) Protocol



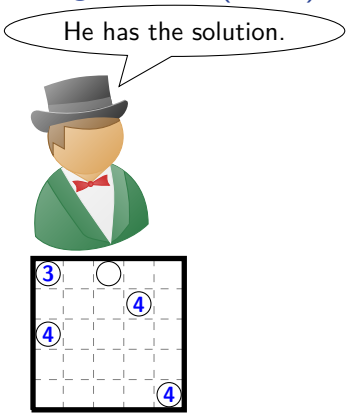


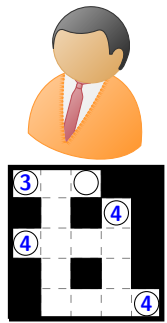
NP-complete

Zero-Knowledge Proof (ZKP) Protocol



Zero-Knowledge Proof (ZKP) Protocol





ZKP properties

Completeness

If P knows the solution then it can convince V.

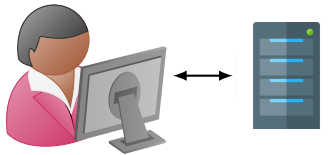
Extractability

If P does not have the solution then V can notice it.

Zero-Knowledge

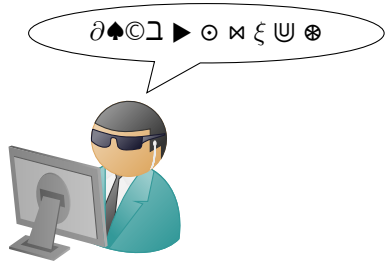
V learns nothing about the solution.

ZKP for real...




VOTE


BLOC 46
Transaction 92
Transaction 93
Transaction 94
Transaction 95
BLOC 47
Transaction 96
Transaction 97
Transaction 98
Transaction 99
BLOC 48
Transaction 100
Transaction 101
Transaction 102
Transaction 103
BLOC 49
Transaction 104
Transaction 105
Transaction 106
Transaction 107

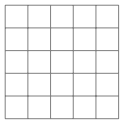

∂♠©⊐ ▶ ⊙ ⋈ ξ ⋓ ⊛

Encoding

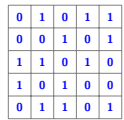
0/black → ♣ ♥

1/white → ♥ ♣

dummy → ♥ ♥



G



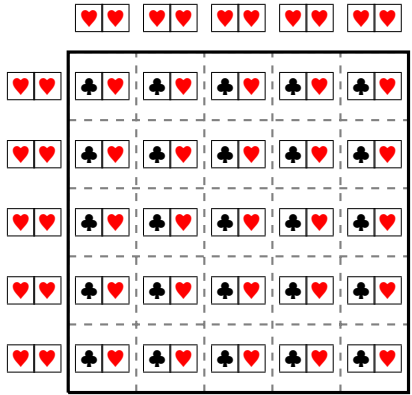
S

Shuffle

$$\left\langle \underbrace{?}_{\mathbf{p}_1} \,\middle\|\, \underbrace{?}_{\mathbf{p}_2} \,\middle\|\, \cdots \,\middle\|\, \underbrace{?}_{\mathbf{p}_m} \right\rangle \rightarrow \underbrace{?}_{\mathbf{p}_{s+1}} \; \underbrace{?}_{\mathbf{p}_{s+2}} \; \cdots \; \underbrace{?}_{\mathbf{p}_{s+m}}$$

Our protocol - Setup phase

P and V place black commitments on each cell + dummy around G



Roadmap

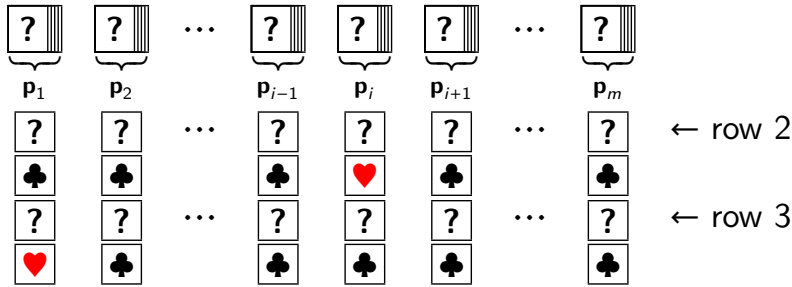
Connectivity

- Chosen Pile Protocol;
- 4-Neighbour Protocol;
- Forming the polyomino.

Verifications

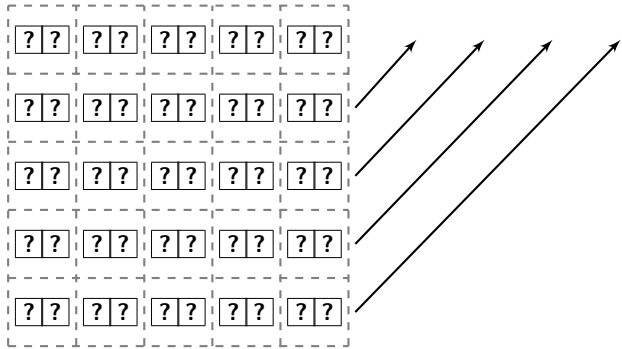
- No 2×2 square;
- Misaki;
- No circle $\iff$ No Misaki.

Chosen Pile Protocol



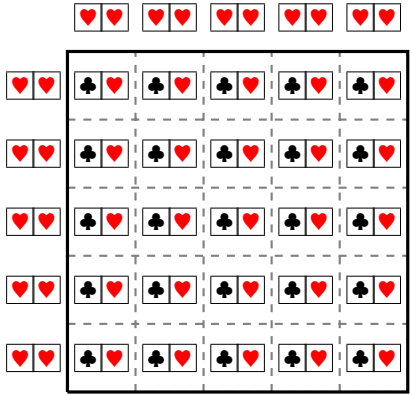
J-G. Dumas, P. Lafourcade, D. Miyahara, T. Mizuki, T. Sasaki, H. Sone,
Interactive Physical Zero-Knowledge Proof for Norinori. 166-177 2019 COCOON

Choose a Neighbour



? ? ? ? ? ? ? ? ⋯ ? ? ? ? ? ?

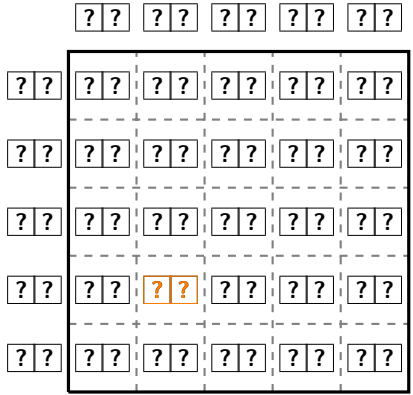
Forming White Polyomino



L. Robert, D. Miyahara, P. Lafourcade, T. Mizuki:

Card-Based ZKP for Connectivity: Applications to Nurikabe, Hitori, and Heyawake. New Gener. Comput. 40(1): 149-171 (2022)

Forming White Polyomino



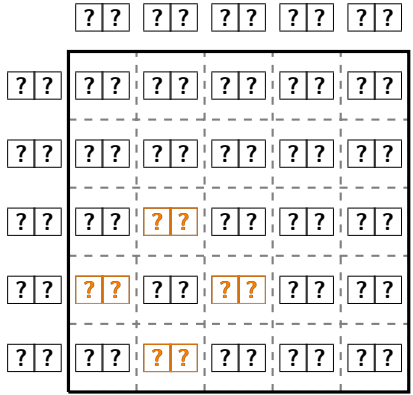
P: Chosen Pile Protocol

V: Swap to white

L. Robert, D. Miyahara, P. Lafourcade, T. Mizuki:

Card-Based ZKP for Connectivity: Applications to Nurikabe, Hitori, and Heyawake. New Gener. Comput. 40(1): 149-171 (2022)

Forming White Polyomino



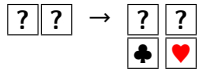
P: 4-Neighbour Protocol

L. Robert, D. Miyahara, P. Lafourcade, T. Mizuki:

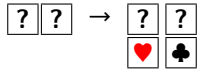
Card-Based ZKP for Connectivity: Applications to Nurikabe, Hitori, and Heyawake. New Gener. Comput. 40(1): 149-171 (2022)

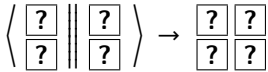
Changed/Still Commitment

Change commitment:

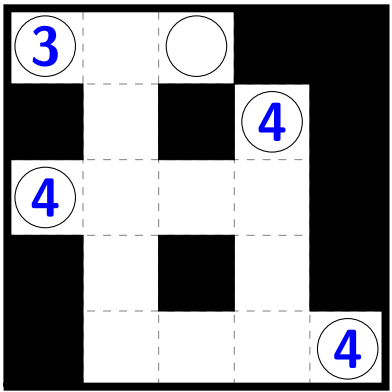


Still commitment:





Verifications of other rules

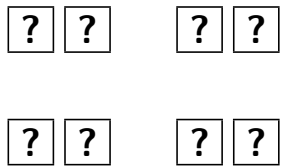


V is convinced that white cells are connected.

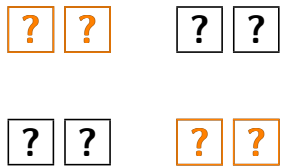
V checks that other rules are satisfied:

- 2×2 square;
- Misaki cells have only one white neighbour;
- Number indicates the number of white cells in straight line;
- No Circle $\Leftrightarrow$ No Misaki.

No 2×2 square

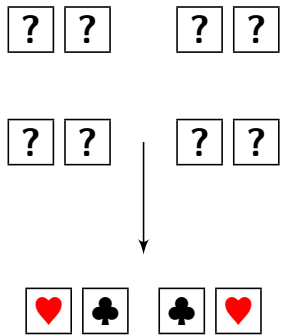


No 2×2 square



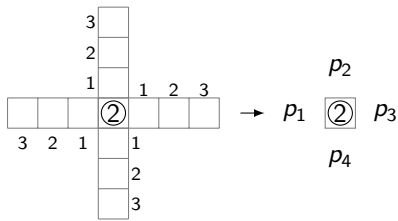
P: Chosen Pile Protocol

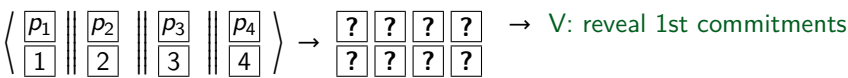
No 2×2 square



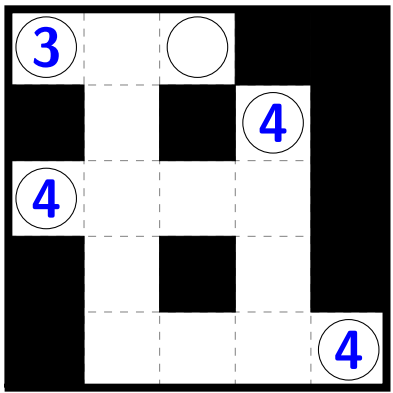
Misaki

1. Only one neighbour is white;
2. Number indicates the number of white cells in straightline.





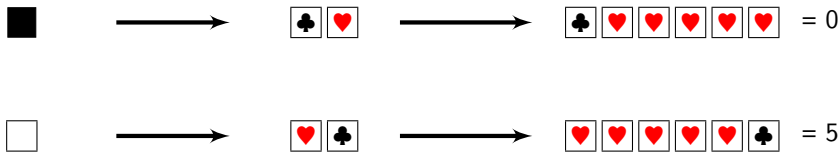
No Circle ⟺ No Misaki



White Neighbours ≥ 2

❦ Location and Number of white cells ⊂ solution.

Idea: Sum



Security Proofs

Theorem (Completeness)

If P knows the solution of a Nurimisaki grid, then P can convince V.

→ We show that all the steps will not abort.

Theorem (Soundness)

If P does not provide a solution of the $p \times q$ Nurimisaki grid, then P is not able to convince V.

→ We show that at least one step will abort.

Theorem (Zero-knowledge))

V learns nothing about P's solution of the given grid G.

→ Description of a simulator which does not have the solution but can swap cards during shuffles.

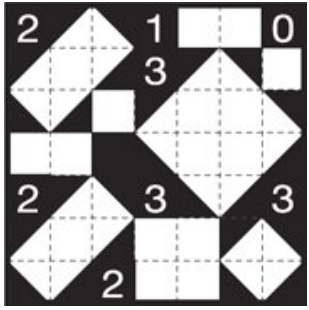
Conclusion

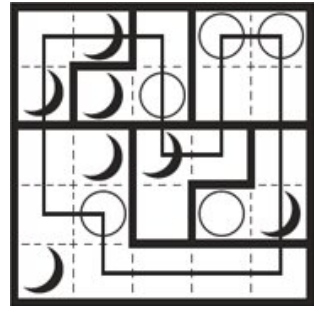
ZKP protocol: how to convince of having a secret without revealing it.

3 properties:

- Completeness;
- Soundness;
- Zero-Knowledge.

Future Works





Thank you for your attention, questions ?