When Locality Implies Globality: Card-based ZKP Protocol for Shakashaka Puzzle

Daiki Miyahara
The University of Electro-Communications, Japan
National Institute of Advanced Industrial Science and Technology, Japan

Léo Robert
MIS, Université de Picardie Jules Verne, France

Pascal Lafourcade
Université Clermont Auvergne, CNRS UMR 6158, LIMOS, France

Shohei Kaneko
The University of Electro-Communications, Japan

Abstract

Shakashaka is an NP-complete Nikoli puzzle that requires to draw white rectangles by filling a grid with black triangles. Verifying that there are only rectangles drawn in the solution was an open problem for card-based ZKP protocols designers.

In this paper, we construct a card-based ZKP protocol to show that a prover can prove to a verifier that he knows a solution of this puzzle without revealing any information. For doing this we prove a local property on all possible 2×2 subgrids drawn according to the rules of the game and such configurations are possible valid shapes for rectangles. This local property implies a global property on the shape of the constructed areas. Thanks to this local result for all 2×2 subgrids, we are able to establish that the only possible shape in the global grid are rectangles. We also verify other classical rules of Shakashaka.

2012 ACM Subject Classification Theory of computation, Computational complexity and cryptography, Cryptographic protocols

Keywords and phrases Card-based cryptography, ShakaShaka, Nicoli, ZKP.

Digital Object Identifier 10.4230/LIPIcs.FUN.2026.22

Acknowledgements We thank the anonymous referees, whose comments have helped us to improve the presentation of the paper. We also thank Alexander Koch for helpful discussions in the early stages of this work. This work was supported in part by ANR Project PRIVA-SIQ, by JSPS KAKENHI Grant Number JP23H00479, by JSPS Bilateral Joint Research Projects JPJSBP120253206, and by Institute of Mathematics for Industry, Joint Usage/Research Center in Kyushu University, 2023a020, 2024a035, and 2025a036.

1 Introduction

The study of card-based zero-knowledge proof (ZKP) protocols for pencil-and-paper puzzles gained attention following the foundational works on Sudoku [4, 17, 23], Kakuro [1, 10], and Makaro [2, 20]. These studies established physical ZKPs with perfect soundness (no soundness error), meaning that a malicious P who does not know a solution can convince V with probability 0. Building on these arithmetic constraints, recent studies have focused on geometric and topological constraints. These include verifying the formation of a single loop [5,7], a single connected component [12,15,18,22], rectangles [19], and pentominoes [9,21].

Despite these developments, however, *Shakashaka* has not yet been addressed. In this paper, we present a physical ZKP protocol for Shakashaka with a physical deck of color cards, such as blacks $\boxed{\clubsuit}\boxed{\clubsuit}\cdots\boxed{\clubsuit}$ and reds $\boxed{\heartsuit}\boxed{\heartsuit}\cdots\boxed{\heartsuit}$. It enables a prover P to convince

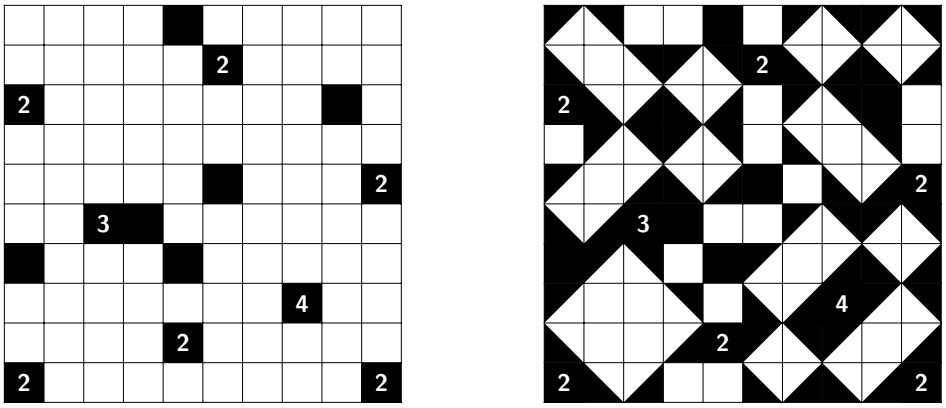


Figure 1 Example grid of Shakashaka (left) and its solution (right), taken from the Wikipedia: `https://en.wikipedia.org/wiki/Shakashaka`.

a verifier V that P knows a solution of a given Shakashaka puzzle, without revealing any information about the solution to V. We begin by introducing Shakashaka.

1.1 Shakashaka

Shakashaka is a pencil-and-paper puzzle popularized by the Japanese publisher Nikoli, similar to Sudoku. An example of a Shakashaka puzzle is given in Fig. 1. We are given a grid where some cells are colored black containing a number from zero to four. According to the Nikoli website[1], the rules are defined as follows:

1. Place black "triangles in squares" in the grid under the following rules.
2. There are four kinds of black triangles you can put in the squares: ◩, ◪, ◭, and ◮. You cannot place black triangles in the black squares.
3. The parts of the grid that remain white (uncovered by black triangles) always form a rectangle or a square.
4. The numbers indicate how many black triangles are around it, vertically and horizontally.

In all Nikoli puzzles, there is an extra implicit rule that says that the solution is unique. Solving Shakashaka offers a sense of achievement, as the triangles reveal a structured pattern of rectangles. This visual result is one of its best feature. From a mathematical perspective, however, Shakashaka is quite challenging. This puzzle has been shown to be NP-complete in [3] when generalized to $m \times n$ grids.

1.2 Contributions

In this paper, we construct a card-based ZKP protocol for Shakashaka. Shakashaka presents a unique partitioning problem; while it shares the goal of forming rectangular areas with *Shikaku* [19], it possesses several distinct features that prevent the direct application of existing techniques:

- Implicit Boundaries: In Shikaku, rectangles are explicitly defined by numerical clues that specify their area, whereas in Shakashaka, the rectangular white areas are implicitly formed as a byproduct of placed triangles.

[1] `https://www.nikoli.co.jp/en/puzzles/shakashaka/`

- Lack of Numerical Constraints: Unlike Shikaku, where the total number and sizes of rectangles are easily inferable, Shakashaka provides no such direct information.
- 45° Rotation: Most crucially, while Shikaku only involves axis-aligned rectangles, Shakashaka allows for rectangles rotated by 45°.

Beyond the first construction of a specific protocol for this puzzle, our work offers two major contributions to the community.

Our first contribution is to identify that the "global" requirement of Shakashaka can be perfectly characterized by "local" geometric constraints. We prove that the correctness of the entire board is guaranteed if and only if every 2×2 square of cells follows one of 138 valid patterns. These patterns ensure that every interior angle of the white areas is 90°. While it is well-known in geometry that such a constraint on angles results in a set of rectangles [13], our major contribution is to employ this property in the context of ZKPs, reducing the global requirement to local pattern-matching task totaling $O(mn)$ steps.

To implement the above verification of 138 patterns, we propose a second contribution with a generalized ZKP protocol for *set membership*. This protocol enables P to convince V that a sequence of face-down cards s belongs to a public set $\mathcal{S} = \{s_1, s_2, \ldots, s_{|\mathcal{S}|}\}$, where each s_i is a sequence of face-up cards, without revealing which specific element of $\mathcal{S}$ corresponds to s. While similar techniques have been addressed, either explicitly or implicitly, to verify 2×2 forbidden patterns [15, 16] or specific valid positions [5, 7, 14], we extend these approaches into a generic construction, handling any arbitrary set of sequences of cards.

2 Preliminaries

We define a deck of cards used in our protocol and a card-based ZKP protocol.

2.1 Encoding

To encode a solution of a Shakashaka puzzle, we use a deck of two-color cards: blacks [♣] and [♥], whose backs are all identical, denoted by [?]. Each cell is encoded by a sequence of four cards as follows.

- □ cell is encoded by: [♥][♥][♥][♥].
- ◪ cell is encoded by: [♣][♥][♥][♥].
- ◹ cell is encoded by: [♥][♣][♥][♥].
- ◺ cell is encoded by: [♥][♥][♣][♥].
- ◿ cell is encoded by: [♥][♥][♥][♣].
- ■ cell is encoded by: [♣][♣][♣][♣].

We note that each triangle cell contains exactly one [♣], which makes the verification of numbers in black cells (Rule 4) straightforward.

2.2 Pile-Scramble Shuffle

To introduce randomness into the protocol, we employ a *pile-scramble* shuffle [11]. This primitive uniformly randomizes the order of multiple sequences of cards, while preserving the internal order of cards within each sequence. Formally, given k sequences $(s_1, s_2, \ldots, s_k)$, each consisting of the same number of cards, a pile-scramble shuffle applies a random permutation π drawn uniformly at random from the symmetric group of degree k, denoted by $\mathfrak{S}_k$: $(s_1, s_2, \ldots, s_k) \to (s_{\pi(1)}, s_{\pi(2)}, \ldots, s_{\pi(k)})$.

2.3 Card-Based ZKP Protocol

A card-based ZKP protocol [8] should satisfy the following three requirements.

- **Completeness**: If a prover P knows a valid solution of a given puzzle and follows the protocol, then V always accepts the proof with probability 1.
- **Knowledge Soundness**: If P does not know a valid solution, V rejects the proof with a certain probability (or with probability 1 in the case of *perfect soundness*). This ensures that P cannot pass the verification unless they have correctly encoded a solution onto the board. Formally, this property implies the existence of a *knowledge extractor* that can retrieve the solution from any P who succeeds in the protocol.
- **Zero-knowledge**: V learns no information about P's specific solution other than the fact that P knows it. This is formally guaranteed if there exists a *simulator* that can produce a transcript of the protocol indistinguishable from a real execution, without having access to the solution.

3 Generalized ZKP for Set Membership

We generalize existing protocols to obtain an original ZKP protocol for set membership (simply, the membership protocol).

3.1 Description

The membership protocol allows a prover P to convince a verifier V that a sequence of ℓ face-down cards, denoted by s, belongs to a public set of sequences of ℓ cards, denoted by $\mathcal{S} = \{s_1, s_2, \ldots, s_{|\mathcal{S}|}\}$, without revealing any further information about s:

$$s\colon \underbrace{\boxed{?}\boxed{?}\cdots\boxed{?}}_{\ell \text{ cards}} \in \mathcal{S}\colon \{s_1\colon \underbrace{\boxed{\heartsuit}\boxed{\heartsuit}\cdots\boxed{\heartsuit}}_{\ell \text{ cards}}, s_2\colon \underbrace{\boxed{\heartsuit}\boxed{\heartsuit}\cdots\boxed{\clubsuit}}_{\ell \text{ cards}}, \ldots, s_{|\mathcal{S}|}\colon \underbrace{\boxed{\heartsuit}\boxed{\clubsuit}\cdots\boxed{\clubsuit}}_{\ell \text{ cards}}\}.$$

Given s and $\mathcal{S}$ with their faces down, the membership protocol proceeds as follows.[2]

1. P privately "appends" a face-down card c_i with each s_i to construct a pair (s_i, c_i), such that $c_i = \boxed{\heartsuit}$ iff $s = s_i$. This means that exactly one card in $\{c_1, c_2, \ldots, c_{|\mathcal{S}|}\}$ is $\boxed{\heartsuit}$.

$$\begin{array}{c} c_1\colon \boxed{?} \\ s_1\colon \boxed{?}\boxed{?}\cdots\boxed{?} \end{array} \quad \begin{array}{c} c_2\colon \boxed{?} \\ s_2\colon \boxed{?}\boxed{?}\cdots\boxed{?} \end{array} \quad \cdots \quad \begin{array}{c} c_{|\mathcal{S}|}\colon \boxed{?} \\ s_{|\mathcal{S}|}\colon \boxed{?}\boxed{?}\cdots\boxed{?} \end{array}.$$

2. Apply a pile-scramble shuffle to the $|\mathcal{S}|$ pairs.
3. Reveal all c_i to determine exactly one $\boxed{\heartsuit}$. Let p be the index such that $c_p = \boxed{\heartsuit}$. Note that p is a random number uniformly chosen from $\{1, 2, \ldots, |\mathcal{S}|\}$ due to the previous shuffling step.

$$\begin{array}{c} c_p\colon \boxed{\heartsuit} \\ s_p\colon \boxed{?}\boxed{?}\cdots\boxed{?} \end{array}.$$

4. Replace s_p with s to update $\mathcal{S}$. Note that $\mathcal{S}$ is identical to the original $\mathcal{S}$ iff $s = s_p$.
5. Apply a pile-scramble shuffle to $\mathcal{S}$.
6. Finally reveal all cards in $\mathcal{S}$. If it is identical to the original $\mathcal{S}$, then V is convinced of $s \in \mathcal{S}$.

[2] This protocol is an adaptation of the chosen pile cut technique [6].

A notable feature of this protocol is "non-destructive." Since s is replaced with an equivalent s_p in Step 4, the input s is preserved. Furthermore, by simply flipping the revealed cards back face-down in Step 6, the set $\mathcal{S}$ is restored, ready for subsequent use.

3.2 Proofs

The proofs of the three properties for the membership protocol are given as follows:

- **Completeness**: Suppose that P knows $s \in \mathcal{S}$. Let $s = s_j \in \mathcal{S}$. Then in Step 1, P can place $c_j =$ 🂱 and 🃑 for all other positions. Therefore, the protocol should replace $s_p = s_j$ with s in Step 3, and $\mathcal{S}$ should be identical to the original one.
- **Knowledge Extractor**: If V accepts the proof, then it means that $s_p = s$ since they are replaced in Step 4. Here, s_p is selected by P appending exactly one 🂱 to it in Step 1. Therefore, we define a knowledge extractor as an algorithm that just reveals $c_1, c_2, \ldots, c_{|\mathcal{S}|}$ to extract P's knowledge, where the position of 🂱 indicates which element in $\mathcal{S}$ is identical to s.
- **Zero-knowledge**: In Steps 3 and 6, the protocol reveals a sequence of cards. In Step 3, the position of the revealed 🂱 denoted by p is a random number, which can be simulated without having the knowledge of $s \in \mathcal{S}$. In Step 6, the updated $\mathcal{S}$ is revealed, but it is identical to the original one (if V accepts the proof), which can be also simulated.

4 Locality Implies Globality

Recall that the goal is to prove that a grid contains only (white) rectangles without revealing them and without knowing how many rectangles there are. To understand our approach, we first outline the intuition behind the protocol.

First, our proposed protocol for Shakashaka works as follows: a prover P places cards on each cell of a given Shakashaka grid, according to the encoding defined in Section 2.1. Then for every 2×2 subgrid (so that the entire grid is *scanned*), P and V execute the membership protocol presented in Section 3, to check that four sequences placed in each 2×2 cell belong to one of 138 valid configuration.

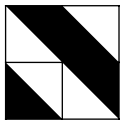
These configurations serve as the basic building blocks for constructing rectangles: given a 2×2 cell in a valid configuration, the shape can always be extended to form part of a rectangle. We will then show that if every 2×2 subgrid of the grid is in a valid configuration, the entire grid must consist only of rectangles.

We now formalize the notion of a valid configuration in order to fully characterize how a 2×2 cell can be extended to form a (white) rectangle.

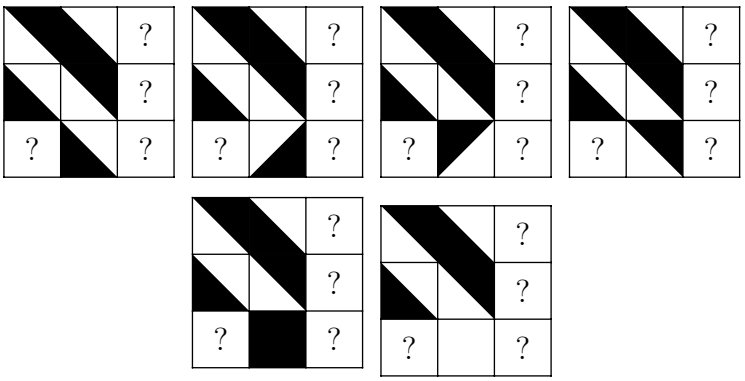
▶ **Definition 1** (Valid Configuration)**.**
We say that a configuration of 2×2 *cells is* valid *if its white part can form either a right angle or a straight line.*

In appendix, we list all valid configurations for 2×2 cells. We have a total of $138 = 4 + 10 + 76 + 48$ valid configuration over all $6^4 = 1296$ possible configurations of 2×2 cells. In Figure 2, we list all the 138 valid configurations, grouped by number of symmetries. We obtain this by analyzing all 1296 possibilities manually.

Notice that the following configuration is not valid, as well as all corresponding symmetries.



Indeed it is not possible to construct rectangles with a width of $\frac{\sqrt{2}}{2}$. Without loss of generality, we show that it is not possible to construct a rectangle on the right side. For this, we have the following 6 possibilities for the next cell wich is not a "?". All are impossible girds, except the first one that does not close the rectangle but just shifts the problem to the next cell. Hence this configuration is not valid.



In Theorem 2, we prove that if all connected white regions in the grid are rectangles then all 2×2 subgrids of the grid are one of the 138 valid configurations.

▶ **Theorem 2.** *If all white areas are form only white rectangles in a grid then the grid contains only valid configurations of* 2×2 *cells.*

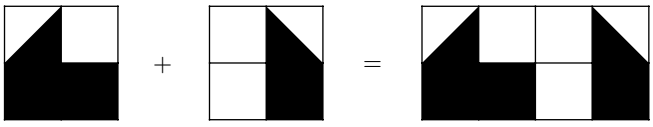
Proof. If all white areas are only white rectangles in a grid. Then by construction of the 138 valid configurations, the grid contains only valid configurations. ◀

In Theorem 3, we prove that if all 2×2 subgrids of the grid belong to one of the 138 valid configurations, then all connected white regions in the grid are necessarily rectangles.

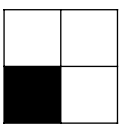
▶ **Theorem 3.** *If a grid contains only valid configurations of* 2×2 *cells, then all white areas are form only white rectangles.*

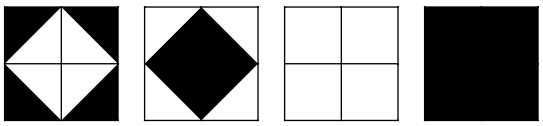
Proof. If a grid contains only valid configurations of 2×2 cells, then the composition (concatenation) of two valid configurations is composed only of valid configurations.

For example, the composition (concatenation) of the two following valid configurations is not a valid configuration.

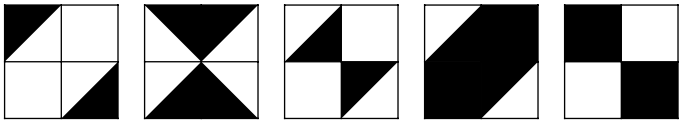


Because it does not contain only valid configuration, indeed it contains the following invalid configuration.

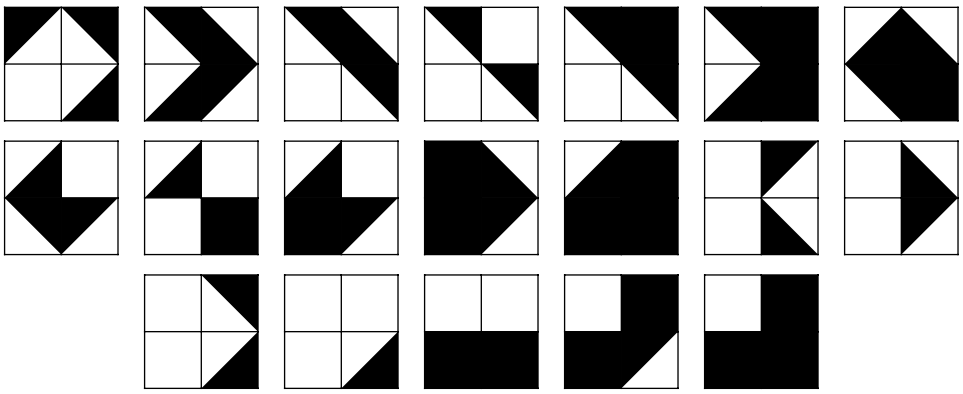




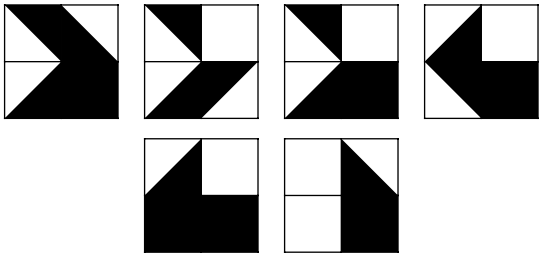
(a) No symmetry: 4 configurations, for a total of $4 \times 1 = 4$.



(b) Two symmetries: 5 configurations, for a total of $5 \times 2 = 10$.



(c) Four symmetries: 19 configurations, for a total of $19 \times 4 = 76$.



(d) 8 symmetries: 6 configurations, for a total $6 \times 8 = 48$.

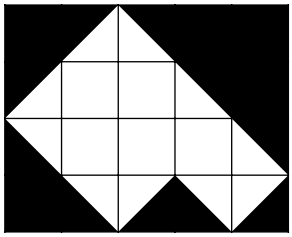
Figure 2 All $138 = 4 + 10 + 76 + 48$ possible valid configurations.

Then if a grid contains only valid configurations of 2×2 cells, then all white areas are composed only of straight lines and right angles by definition of a valid configuration.

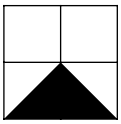
Now, we have only three possibilities for the combinations of straight lines and right angles:

1. They construct rectangles, which is exactly what we want.

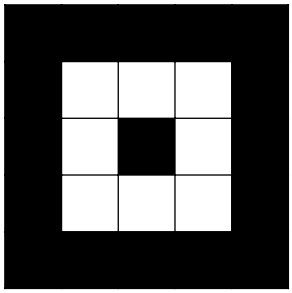
2. They form white shapes constructed with several white rectangles as follows:



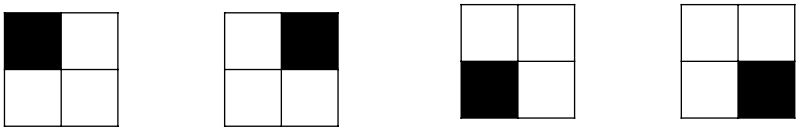
But such situations are not possible because they contain at least one invalid configuration (one of the symmetries of the following configuration), in this example the invalid configuration is the following:



3. Finally, we can have some white shapes with black rectangles insides as follows:



But such areas are not possible because they contain invalid configurations, in this example the following configurations are invalid configurations:



This ensures that a grid with only 4×4 valid configurations contains only white rectangles. It concludes the proof. ◀

Consequently, it suffices to locally verify that each 2×2 subgrid avoids all invalid configurations (*i.e.,* those that cannot be extended to form a rectangle) in order to infer that the global grid consists exclusively of rectangular white regions.

5 Main Protocol

We are ready to present our ZKP protocol for Shakashaka.

5.1 Procedure

Given an $m \times n$ grid $(m, n > 1)$, our protocol proceeds as follows.

1. P places a sequence of four face-down cards on each white cell to represent a solution according to the encoding defined in Section 2.1. Additionally, P and V place a sequence of four black cards on each black cell. Let $\sigma_{i,j}$ denote the sequence of cards placed on each cell (i, j), where $1 \leq i \leq m$ and $1 \leq j \leq n$. Note that $(1, 1)$ is located at the top-left corner of the grid.
2. For each i and j with $0 \leq i \leq m$ and $0 \leq j \leq n$, execute the membership protocol presented in Section 3. In this execution, the input sequence s is the concatenation of four sequences:

   $$s = (\sigma_{i,j}, \sigma_{i,j+1}, \sigma_{i+1,j}, \sigma_{i+1,j+1}),$$

   and the public set $\mathcal{S} = \{s_1, s_2, \ldots, s_{138}\}$ represents the 138 valid 2×2 configurations defined in Section 4. Each $s_k \in \mathcal{S}$ represents one of these 138 configurations (in any order) with a sequence of 16 cards, just as s is. To handle the grid "boundaries," the following conditions are applied in the execution:
   - Any sequence $\sigma_{x,y}$ with $x \in \{0, m+1\}$ or $y \in \{0, n+1\}$ is a fixed sequence of four black cards. This means that the $(m \times n)$ grid is surrounded by black cells.
   - If s includes any sequence $\sigma_{x,y}$ that represents a known black cell, then reveal $\sigma_{x,y}$ after executing the membership protocol. This ensures that it indeed represents a black cell.
3. For each black cell (i, j) containing a number $k \in \{0, 1, 2, 3, 4\}$, execute the following steps (assuming that any sequence of four cards placed on a black cell has been removed).
   - **a.** If $k = 0$, then reveal the four sequences around it, i.e., $\sigma_{i-1,j}$, $\sigma_{i,j-1}$, $\sigma_{i,j+1}$, and $\sigma_{i+1,j}$ (if they exist), to confirm that each revealed sequence represents a white cell. Otherwise, just shuffle them.
   - **b.** Reveal all the shuffled cards to confirm that the total number of revealed $\boxed{\clubsuit}$ is exactly k.

5.2 Efficiency

Our proposed protocol uses $O(mn)$ cards and $O(mn)$ shuffles. The number of shuffles is counted as follows:

- Step 2 uses exactly $(m+1)(n+1)$ shuffles, since the membership protocol, which needs a single shuffle, is executed $(m+1)(n+1)$ times.
- The number of shuffles used in Step 3 is at most mn.

The total number of cards used in this protocol is $4mn + 2358$, which is counted as follows:

- For the $m \times n$ grid, P places four cards on each cell in Step 1, totaling $4mn$ cards.
- In the execution of the membership protocol in Step 2, the set $\mathcal{S}$ of size 138 is prepared, each with $4 \times 4 = 16$ cards. Additionally, P appends one card to each element, totaling $17 \times 138 = 2346$ cards.
- The remaining 12 cards is used to handle the grid boundaries. In any execution, at most three sequences of four cards (12 cards in total) represent black cells, and they can be reused since they are all revealed after the execution.

5.3 Proofs

We prove that our proposed protocol satisfies the three requirements of a ZKP as follows.

▶ **Theorem 4.** *Our proposed protocol satisfies completeness.*

Proof. Suppose that P knows a solution. This implies that the placement of cards provided by P in Step 1 respects all the rules. First, by Theorem 2, 16 cards placed in every 2×2 cell represent one of the 138 valid configurations, and P can correctly replace the one with the identical one during the execution in Step 2. As we noted in Section 2.1, each triangle cell is encoded with exactly one $\boxed{\clubsuit}$, meaning that the total number of $\boxed{\clubsuit}$ revealed in Step 3 will always be identical to k. This completes the proof. ◀

▶ **Theorem 5.** *Our proposed protocol satisfies perfect knowledge soundness.*

Proof. First, the placement of cards provided by P in Step 1 directly represents a candidate solution. We define a knowledge extractor as an algorithm that has the ability to reveal these cards to extract P's knowledge at the end of Step 1. We show that if V accepts the proof, then the extracted knowledge must be a solution to the given Shakashaka puzzle.

The protocol executes the membership protocol for every 2×2 cell in Step 2, to ensure that it matches one of the 138 valid configurations. By Theorem 3, this implies that the extracted knowledge represents a figure composed entirely of white rectangles. Finally, Step 3 reveals the cards around each black cell with a number. As we described above, the number of revealed $\boxed{\clubsuit}$ is identical to the number of triangle cells around it in the extracted knowledge.

Since all the rules are respected, the extracted knowledge is a solution. Thus, the protocol satisfies perfect knowledge soundness. ◀

▶ **Theorem 6.** *Our proposed protocol satisfies perfect zero-knowledge.*

Proof. Step 2 just repeats to execute the membership protocol, which can be perfectly simulated by a simulator S. In Step 3, V only observes that the number of $\boxed{\clubsuit}$ matches k. Since all cards are shuffled beforehand, any other information remains hidden. Thus, S can perfectly simulate the protocol using only the public information. This completes the proof. ◀

6 Conclusion

We propose a first ZKP protocol for the Nikoli's game Shakashaka. This game is different to other Nikoli's games because it has to construct a rectangles thanks to placing only small triangles in the grid of the game. The geometric aspect is the originality of this game. It is why was not yet studied. In this paper, we use an original approach to address this open problem: verifying a local property to satisfy a global property in ZKP. To the best of our knowledge it is the first time such idea is used to construct a card-based ZKP protocol. Thanks to this idea we were able to construct the first ZKP for Shakashaka.

References

1 Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas, and Pascal Lafourcade. Physical zero-knowledge proofs for Akari, Takuzu, Kakuro and KenKen. In Erik D. Demaine and Fabrizio Grandoni, editors, *Fun with Algorithms*, volume 49 of *LIPIcs*, pages 8:1–8:20, Dagstuhl, Germany, 2016. Schloss Dagstuhl. URL: `https://doi.org/10.4230/LIPIcs.FUN.2016.8`.

2 Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas, Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Atsuki Nagao, Tatsuya Sasaki, Kazumasa Shinagawa, and Hideaki Sone. Physical zero-knowledge proof for Makaro. In Taisuke Izumi and Petr Kuznetsov, editors, *Stabilization, Safety, and Security of Distributed Systems*, volume 11201 of *LNCS*, pages 111–125. Springer, 2018. URL: https://doi.org/10.1007/978-3-030-03232-6_8.

3 Erik D. Demaine, Yoshio Okamoto, Ryuhei Uehara, and Yushi Uno. Computational complexity and an integer programming model of Shakashaka. *IEICE Trans. Fundam.*, 97-A(6):1213–1219, 2014. URL: https://doi.org/10.1587/transfun.E97.A.1213.

4 Ronen Gradwohl, Moni Naor, Benny Pinkas, and Guy N. Rothblum. Cryptographic and physical zero-knowledge proof systems for solutions of Sudoku puzzles. *Theory of Computing Systems*, 44(2):245–268, 2009. URL: https://doi.org/10.1007/s00224-008-9119-9.

5 Samuel Hand, Alexander Koch, Pascal Lafourcade, Daiki Miyahara, and Léo Robert. Efficient card-based ZKP for single loop condition and its application to Moon-or-Sun. *New Gener. Comput.*, 42:449–477, 2024. URL: https://doi.org/10.1007/s00354-024-00274-1.

6 Alexander Koch and Stefan Walzer. Foundations for actively secure card-based cryptography. In Martin Farach-Colton, Giuseppe Prencipe, and Ryuhei Uehara, editors, *Fun with Algorithms*, volume 157 of *LIPIcs*, pages 17:1–17:23, Dagstuhl, Germany, 2020. Schloss Dagstuhl. URL: https://doi.org/10.4230/LIPIcs.FUN.2021.17.

7 Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Léo Robert, Tatsuya Sasaki, and Hideaki Sone. How to construct physical zero-knowledge proofs for puzzles with a "single loop" condition. *Theor. Comput. Sci.*, 888:41–55, 2021. URL: https://doi.org/10.1016/j.tcs.2021.07.019.

8 Daiki Miyahara, Hiromichi Haneda, and Takaaki Mizuki. Card-based zero-knowledge proof protocols for graph problems and their computational model. In Qiong Huang and Yu Yu, editors, *Provable and Practical Security*, volume 13059 of *LNCS*, pages 136–152, Cham, 2021. Springer. URL: https://doi.org/10.1007/978-3-030-90402-9_8.

9 Daiki Miyahara, Léo Robert, Pascal Lafourcade, and Takaaki Mizuki. ZKP protocols for Usowan, Herugolf, and Five Cells. *Tsinghua Science and Technology*, 29(6):1651–1666, 2024. URL: https://doi.org/10.26599/TST.2023.9010153.

10 Daiki Miyahara, Tatsuya Sasaki, Takaaki Mizuki, and Hideaki Sone. Card-based physical zero-knowledge proof for Kakuro. *IEICE Trans. Fundam.*, 102(9):1072–1078, 2019. URL: https://doi.org/10.1587/transfun.E102.A.1072.

11 Takaaki Mizuki, Isaac Kobina Asiedu, and Hideaki Sone. Voting with a logarithmic number of cards. In Giancarlo Mauri, Alberto Dennunzio, Luca Manzoni, and Antonio E. Porreca, editors, *Unconventional Computation and Natural Computation*, volume 7956 of *LNCS*, pages 162–173, Berlin, Heidelberg, 2013. Springer. URL: https://doi.org/10.1007/978-3-642-39074-6_16.

12 Koji Nuida. Card-based protocol counting connected components of graphs. *New Gener. Comput.*, 43:18, 2025. URL: https://doi.org/10.1007/s00354-025-00304-6.

13 Joseph o'Rourke. *Computational geometry in C*. Cambridge university press, 1998.

14 Taisei Otsuji, Peter Fulla, and Takuro Fukunaga. NP-Completeness and physical zero-knowledge proof of Hotaru Beam. In Yong Chen, Xiaofeng Gao, Xiaoming Sun, and An Zhang, editors, *Computing and Combinatorics*, pages 239–251, Singapore, 2024. Springer. URL: https://doi.org/10.1007/978-981-96-1090-7_20.

15 Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. Card-based ZKP for connectivity: Applications to Nurikabe, Hitori, and Heyawake. *New Gener. Comput.*, 40:149–171, 2022. URL: https://doi.org/10.1007/s00354-022-00155-5.

16 Léo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki. Physical ZKP protocols for Nurimisaki and Kurodoko. *Theor. Comput. Sci.*, 972:114071, 2023. URL: https://doi.org/10.1016/j.tcs.2023.114071.

17 Suthee Ruangwises. Two standard decks of playing cards are sufficient for a ZKP for Sudoku. *New Gener. Comput.*, 40:49–65, 2022. URL: https://doi.org/10.1007/s00354-021-00146-y.

18 Suthee Ruangwises and Toshiya Itoh. Physical ZKP for connected spanning subgraph: Applications to Bridges puzzle and other problems. In Irina Kostitsyna and Pekka Orponen, editors, *Unconventional Computation and Natural Computation*, pages 149–163, Cham, 2021. Springer. URL: https://doi.org/10.1007/978-3-030-87993-8_10.

19 Suthee Ruangwises and Toshiya Itoh. How to physically verify a rectangle in a grid: A physical ZKP for Shikaku. In Pierre Fraigniaud and Yushi Uno, editors, *Fun with Algorithms*, volume 226 of *LIPIcs*, pages 24:1–24:12, Dagstuhl, 2022. Schloss Dagstuhl. URL: https://doi.org/10.4230/LIPIcs.FUN.2022.24.

20 Suthee Ruangwises and Toshiya Itoh. Physical ZKP for Makaro using a standard deck of cards. In Ding-Zhu Du, Donglei Du, Chenchen Wu, and Dachuan Xu, editors, *Theory and Applications of Models of Computation*, volume 13571 of *LNCS*, pages 43–54, Cham, 2022. Springer. URL: https://doi.org/10.1007/978-3-031-20350-3_5.

21 Suthee Ruangwises and Mitsugu Iwamoto. Printing protocol: Physical ZKPs for decomposition puzzles. *New Gener. Comput.*, 42:331–343, 2024. URL: https://doi.org/10.1007/s00354-024-00266-1.

22 Shun Sasaki and Kazumasa Shinagawa. Physical zero-knowledge proof for Sukoro. *New Gener. Comput.*, 42:381–398, 2024. URL: https://doi.org/10.1007/s00354-024-00271-4.

23 Tatsuya Sasaki, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone. Efficient card-based zero-knowledge proof for Sudoku. *Theor. Comput. Sci.*, 839:135–142, 2020. URL: https://doi.org/10.1016/j.tcs.2020.05.036.

A All possible 2×2 subgrids

For completeness, we list all possible 2×2 subgrids.