Interactive Physical ZKP for Connectivity: Applications to Nurikabe and Hitori

Léo Robert, Daiki Miyahara, Pascal Lafourcade, Takaaki Mizuki

Interactive Physical ZKP for Connectivity: Applications to Nurikabe and Hitori

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

[1] LIMOS, University Clermont Auvergne, CNRS UMR 6158, France
[2] Graduate School of Information Sciences, Tohoku University, Japan
[3] Cyberscience Center, Tohoku University, Japan
[4] National Institute of Advanced Industrial Science and Technology (AIST), Japan

Abstract. During the last years, many Physical Zero-knowledge Proof (ZKP) protocols for Nikoli's puzzles [‡] have been designed. In this paper, we propose two ZKP protocols for the two Nikoli's puzzles called Nurikabe and Hitori. These two puzzles have some similarities, since in their rules at least one condition requires that some cells are connected to each other, horizontally or vertically. The novelty in this paper is to propose two techniques that allow us to prove such connectivity without leaking any information about a solution.

Keywords: Zero-knowledge proofs · Card-based secure two-party protocols · Puzzle · Nurikabe · Hitori.

1 Introduction

Zero-Knowledge Proofs (ZKP) were introduced by Goldwasser et al. [7]. Such a protocol has two parties: a prover P and a verifier V. The prover P wants to convince V that P knows the solution s of a problem without revealing any information about s. A ZKP must satisfy the following properties:
Completeness. If P knows s, then P can convince V.
Soundness. If P does not know s, then P cannot convince V.
Zero-Knowledge. V learns nothing about s. Formally, outputs of a simulator and outputs of the real protocol follow the same probability distribution.

In [5], the authors proved that for any NP-complete problem there exists an interactive ZKP protocol. A physical ZKP uses only physical algorithms with day-to-day objects such as cards, envelopes or bags while prohibiting large computations (i.e., no computer allowed). In 2007, the first physical ZKP was introduced for Sudoku [8], which is the most famous Nikoli's puzzle. In this paper we focus on two other Nikoli's puzzles, *Nurikabe* and *Hitori*.

In [10] solving even simple versions of Nurikabe was proven to be NP-complete. In [9] the authors proved that Hitori is also NP-complete. One might think that physical ZKP protocols for Nurikabe and Hitori could be constructed by transforming a known physical ZKP protocol for an NP-complete problem, such as a

[‡] Nikoli is a game publisher notoriously known for its Sudoku puzzle

lockable-box-based ZKP protocol for 3-Colorability [6]; however, such a transformation is not practical because the overhead must be included in the transformation. Besides, the transformed ZKP protocol does not capture the property of a puzzle.

Contributions: In this paper, we present physical ZKP protocols for Nurikabe and Hitori using a deck of cards. Our protocols achieve no soundness error. That is, no malicious P who does not have a solution can convince V that it has a solution. Our work is inspired by [12], where P has to convince V of a single loop property. For Nurikabe and Hitori, we take a similar strategy to [12]. That is, P first increases the number of black (or white) cells one by one so that the resulting cells are guaranteed to satisfy the constraint of connectivity; then V verifies all the remaining constraints. We note that our protocols in this paper could not be constructed by simply adapting the existing technique [12].

We emphasize that our proposed protocols can be applied to a situation where Bob cannot solve by hand a Nurikabe or Hitori puzzle Alice created. In addition to such really practical applications, we believe that one can add our protocols (with others such as 3-Colorability one for instance) to introduce the notion of a ZKP system to non-experts such as high school students.

Related Work: Efficient physical ZKP protocols for Nikoli puzzles have been proposed: Sudoku [8, 17], Akari [2], Takuzu [2, 13], Kakuro [2, 14], Kenken [2], Makaro [3], Norinori [4], Slitherlink [12], Juosan [13], and Numberlink [16]. An important step in this line of research is to achieve no soundness error. To the best of our knowledge, all the existing ZKP protocols since Sasaki et al. proposed the one for Sudoku in 2018 [17] achieve that property.

Nurikabe's rule: This puzzle is formed as a rectangular grid where some cells contain numbers as presented in the example of Figure 1. The goal is to color some cells in black as follows:

1. Each numbered cell tells the number of continuous white cells surrounded by black cells. Such a region is called an *island*.
2. An island must contain only one numbered cell.
3. The black cells form a connected figure (called a *sea*).
4. The *sea* cannot form a 2×2 area.

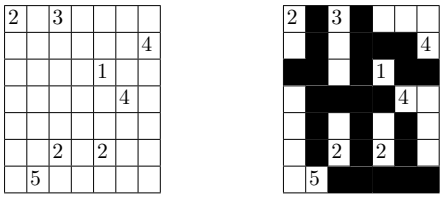


Fig. 1. Initial Nurikabe grid on the left and its solution on the right.

1	1	2	4	3	5
1	1	5	4	4	6
4	6	6	2	1	1
6	3	3	3	5	4
2	3	4	1	6	5
2	5	4	6	2	5

■	1	2	4	3	■
1	■	5	■	4	6
4	6	■	2	1	■
6	■	3	■	5	4
2	3	4	1	6	5
■	5	■	6	2	■

Fig. 2. Initial Hitori grid on the left and its solution on the right.

Hitori's rule: This puzzle is a grid where each cell contains a number as in the example of Figure 2. The goal is to color in black some cells with the following constraints:

1. Each row and each column must contain only one occurrence of a number.
2. The black cells cannot touch side to side although they can be diagonal.
3. The numbered cells must be connected to each other, horizontally or vertically.

2 Preliminaries

We introduce some notations of cards and shuffles and explain simple physical sub-protocols used in our constructions.

Card: A deck of cards used in our protocols consists of clubs $\boxed{\clubsuit}\boxed{\clubsuit}\cdots$, hearts $\boxed{\heartsuit}\boxed{\heartsuit}\cdots$, and number cards $\boxed{1}\boxed{2}\cdots$, whose back sides are identical $\boxed{?}$. We encode three colors with the order of two cards as follows:

$$\text{black} \leftarrow \boxed{\clubsuit}\boxed{\heartsuit},\ \text{white} \leftarrow \boxed{\heartsuit}\boxed{\clubsuit},\ \text{red} \leftarrow \boxed{\heartsuit}\boxed{\heartsuit}. \tag{1}$$

We call such a face-down two cards $\boxed{?}\boxed{?}$ corresponding to a color according to the above encoding rule a *commitment* to the respective color. We also use the terms, a *black commitment*, a *white commitment*, and a *red commitment*.

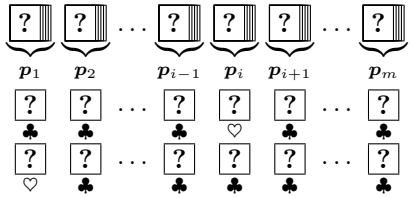
Pile-shifting shuffle [15]: This shuffling action means to *cyclically* shuffle piles of cards. More formally, given m piles, each of which consists of the same number of face-down cards, denoted by $(\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_m)$, applying a *pile-shifting shuffle* (denoted by $< \cdot | \cdots | \cdot >$) results in $(\boldsymbol{p}_{s+1}, \boldsymbol{p}_{s+2}, \ldots, \boldsymbol{p}_{s+m})$:

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

where s is uniformly and randomly chosen from $\mathbb{Z}/m\mathbb{Z}$. Implementing a pile-shifting shuffle is simple: We use physical cases that can store a pile of cards, such as boxes and envelopes; a player (or players) cyclically shuffle them by hand until nobody traces the offset.

Chosen pile protocol [4]: This is an extended version of the "chosen pile cut" proposed in [11]. Given m piles $(\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_m)$ with $2m$ additional cards, the *chosen pile protocol* enables a prover P to choose the i-th pile $\boldsymbol{p}_i$ and replace back the sequence of m piles to their original order.

1. Using $m-1$ $\boxed{\clubsuit}$s and one $\boxed{\heartsuit}$, the prover P places m face-down cards (denoted *row 2*)below the given piles such that only the i-th card is $\boxed{\heartsuit}$. We further put m cards (denoted *row 3*)below the cards such that only the first card is $\boxed{\heartsuit}$:



2. Considering the cards in the same column as a pile, apply a pile-shifting shuffle to the sequence of piles.
3. Reveal all the cards in the *row 2*. Then, one $\boxed{\heartsuit}$ appears, and the pile above the revealed $\boxed{\heartsuit}$ is the i-th pile (and hence, P can obtain $\boldsymbol{p}_i$). When this protocol is invoked, certain operations are applied to the chosen pile. Then, the chosen pile is placed back to the i-th position in the sequence.
4. Remove the revealed cards, i.e., the cards in the *row 2*. (Note, therefore, that we do not use the card $\boxed{\heartsuit}$ revealed in Step 3.) Then, apply a pile-shifting shuffle.
5. Reveal all the cards in the *row 3*. Then, one $\boxed{\heartsuit}$ appears, and the pile above the revealed $\boxed{\heartsuit}$ is $\boldsymbol{p}_1$. Therefore, by shifting the sequence of piles (such that $\boldsymbol{p}_1$ becomes the first pile in the sequence), we can obtain a sequence of piles whose order is the same as the original one without revealing any information about the order of input sequence.

Input-preserving five-card trick [13]: Given two commitments to $a, b \in \{0, 1\}$ based on the encoding: $\boxed{\clubsuit}\boxed{\heartsuit} = 0$ and $\boxed{\heartsuit}\boxed{\clubsuit} = 1$, this sub-protocol [1, 13] starts by adding extra cards and rearranging the commitment to a so that we have the negation $\overline{a}$, as follows: $\underbrace{\boxed{?}\boxed{?}}_{a}\ \underbrace{\boxed{?}\boxed{?}}_{b} \rightarrow \underbrace{\boxed{?}\boxed{?}}_{\overline{a}}\ \boxed{\heartsuit}\ \underbrace{\boxed{?}\boxed{?}}_{b}\ \boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{5}$.

The sub-protocol proceeds as follows to reveal only the value of $a \wedge b$ as well as restore commitments to a and b:

1. Rearrange the sequence of cards and then turn over the face-up cards as follows: $\boxed{?}\boxed{?}\boxed{\heartsuit}\boxed{?}\boxed{?}\boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{5} \rightarrow \begin{matrix}\boxed{?}\boxed{?}\boxed{\heartsuit}\boxed{?}\boxed{?}\\ \boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{5}\end{matrix} \rightarrow \begin{matrix}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\\ \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\end{matrix}$.
2. Regarding cards in the same column as a pile, apply a pile-shifting shuffle to the sequence. $\left\langle \begin{matrix}\boxed{?}\\ \boxed{?}\end{matrix} \middle| \begin{matrix}\boxed{?}\\ \boxed{?}\end{matrix} \middle| \begin{matrix}\boxed{?}\\ \boxed{?}\end{matrix} \middle| \begin{matrix}\boxed{?}\\ \boxed{?}\end{matrix} \middle| \begin{matrix}\boxed{?}\\ \boxed{?}\end{matrix} \right\rangle \rightarrow \begin{matrix}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\\ \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\end{matrix}$.
3. Reveal all the cards in the first row.
   (a) If the resulting sequence is $\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$ (up to cyclic shifts), we have $a \wedge b = 1$.

(b) If it is $\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}$ (up to cyclic shifts), then we have $a \wedge b = 0$.

4. After turning over all the face-up cards, apply a pile-shifting shuffle.
5. Reveal all the cards in the second row, i.e., all the number cards. Then, rearrange the sequence of piles so that the revealed number cards are in ascending order again to restore commitments to a and b.

3 ZKP Protocol for Nurikabe

We propose a ZKP protocol for Nurikabe, which is composed of three phases: the setup phase, the sea formation phase, and the verification phase. The security proof is provided in Appendix A.1.

Consider a puzzle instance of a $p \times q$ grid containing m numbered cells such that the ith numbered cell (in any order) has a number x_i for every i, $1 \leq i \leq m$. Remember that an island in the solution of a Nurikabe puzzle must contain exactly one numbered cell, and the number of white cells inside the island is indicated by the number written on the numbered cell. Thus, the number of (filled) black cells in the solution, denoted by N_b, is the difference between the number of total cells and the white cells (including the numbered cells), and hence

$$N_b = pq - \sum_{i=1}^{n} x_i.$$

Thus, this number N_b can be regarded as public information, and indeed, we use the number N_b explicitly in our protocol.

Before going into the details of our protocol, let us define a *neighbour* cell and show a sub-protocol called the *4-neighbour protocol* that is important for constructing our ZKP protocols.

Neighbour cell: Consider a target cell denoted c_t on a grid. A cell is a *neighbour* of c_t if it is next to c_t. It can be on the left, the right, the top, or the bottom of c_t but not in diagonal.

4-neighbour protocol: Given pq commitments placed on a $p \times q$ grid, a prover P wants to reveal a target commitment and another commitment that lies next to the target commitment. Here, a verifier V is convinced that the second commitment is a neighbour of the first one (without knowing in which direction it is) as well as V confirms the colors of both the commitments. To handle the case where the target commitment is at the edge of the grid, we add red commitments (as "dummy" commitments) around the grid to prevent P from choosing a commitment that is not a neighbour. Thus, the size of the new grid is $(p+2) \times (q+2)$.

This protocol uses the chosen pile protocol (explained in Section 2) twice, as follows. P first uses the chosen pile protocol to reveal a target commitment. Since a pile-shifting shuffle is a cyclic reordering, the distance between commitments are kept (up to a given modulo). That is, for a target commitment (that is not at the edge), the possible four neighbours are at distance:

- 1 for the left or right one,
- $p + 2$ for the bottom or top one.

Therefore, V and P can determine the positions of all the four neighbour commitments. Among these, P chooses one commitment by using the chosen pile protocol again, and reveals it. This convinces V that the second commitment is indeed a neighbour. The rest of the protocol is to end the second and first chosen pile protocols.

We are now ready to present our ZKP protocol for Nurikabe.

3.1 Setup Phase

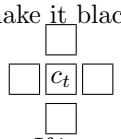
The verifier V and the prover P place a white commitment on each cell of a given $p \times q$ grid and place red commitments (as "dummy" commitments) around the grid so that we have $(p + 2)(q + 2)$ commitments on the board.

3.2 Sea Formation Phase

In this phase, P forms a sea on the board, i.e., P replaces a white commitment with a black commitment one by one according to the solution which only P knows, while hiding any information about the solution to V.

Let N_b be the number of black cells in the solution. This phase proceeds as follows.

1. P uses the chosen pile protocol to choose one white commitment which P wants to replace.
   (a) V reveals the chosen commitment; if it corresponds to white, V swaps the two cards constituting it so that the two cards become a black commitment. Otherwise, V aborts.
   (b) P and V end the chosen pile protocol to return the commitments to their original positions.
2. Repeat the following steps exactly $N_b - 1$ times:
   (a) P chooses one black commitment as a target and one white commitment among its neighbours using the 4-neighbour protocol; the neighbour is chosen such that P wants to make it black.



   (b) V reveals the target commitment. If it corresponds to black, V continues; otherwise V aborts.
   (c) V reveals the neighbour commitment (chosen by P). If it corresponds to white, V swaps the two cards constituting it to make it be a black commitment; otherwise V aborts.
   (d) P and V end the 4-neighbour protocol.
3. P and V replace every red commitment (i.e., dummy commitment) with a black commitment.

After this process, V is convinced that all the black commitments form a connected sea (rule 3).

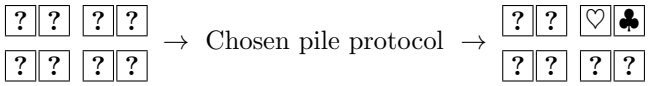
3.3 Verification Phase

V first verifies that the current commitments placed on the grid (after the sea formation phase) satisfy the rule 4 (forbidden 2×2 area). Then, V verifies the rules 1 and 2, relating to the white commitments (island constraints).

Sea rule: Forbidden area. The prover P wants to convince V that any 2×2 area contains at least one white cell. Note that all 2×2 areas are determined given an initial grid. Indeed, for a given $p \times q$ grid, there are $(p-1)(q-1)$ possible squares.

Thus, P and V consider each 2×2 area of commitments one by one (in any order) and will repeat the following for each possible square:

1. P chooses a white commitment on this square via the chosen-pile protocol applied to the four commitments.
2. V reveals the commitment marked by P. If the revealed commitment corresponds to white, then V is convinced that the square is not formed by only black commitments. Otherwise, V aborts.



Island rules. P wants to convince V that the white cells respect the constraints. There are two verifications to make. Only one numbered cell for a given region and all white commitments are connected inside the region. Those two constraints are verified in the following protocol:

Let $n \geq 2$ be the number written on a given numbered cell.[§]

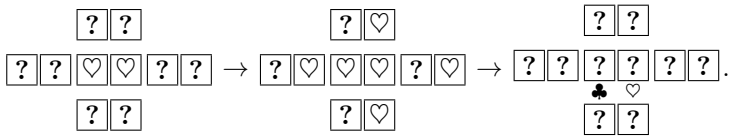
1. V reveals the commitment on the numbered cell. If it corresponds to white, V replaces it with a red commitment; otherwise V aborts.
2. Repeat the following steps exactly $n-1$ times.
   (a) P uses the 4-neighbour protocol to choose a red commitment as a target and one white commitment among its neighbours.
   (b) V reveals the target commitment. If it corresponds to red, V continues; otherwise V aborts.
   (c) V reveals the neighbour commitment (chosen by P). If it corresponds to white, V replaces it with a red commitment; otherwise V aborts.
   (d) P and V end the 4-neighbour protocol to return the commitments to their original positions.

Now, V is convinced that the size of the island consisting of white cells (including the given numbered cell) is greater than or equal to n. To show that it is equal to n, it suffices to prove that there exists no white cell around them, as follows.

3. V replaces the commitment on the numbered cell with a black commitment.

[§] For a numbered cell where 1 is written, V simply reveals the commitment on it and its four neighbours to confirm that the island is surrounded by the sea.

4. Repeat the following steps exactly $n-1$ times.
   (a) P uses the chosen pile protocol to choose a red commitment.
   (b) V reveals the chosen commitment. If it corresponds to red, V continues; otherwise V aborts.
   (c) Remember that P wants to show that any of four neighbour commitments is not white. Recall also the encoding (1), i.e., note that the right card of a black or red commitment is a heart $\boxed{\heartsuit}$. V reveals the right card of each of the four neighbours. If all of them are hearts (which means that all the commitments do not correspond to white), V replaces the chosen commitment with a black commitment; otherwise V aborts.



   (d) P and V end the chosen pile protocol to return the commitments to their original positions.

By applying the above steps to all the numbered cells, V is convinced that the placement of the commitments satisfies all the constraints, i.e., P has the solution.

4 ZKP Protocol for Hitori

We present a ZKP protocol for Hitori. The security proof is provided in Appendix A.1. Similar to our protocol for Nurikabe presented in Section 3, we let P choose a commitment which P wants to make white so that V is convinced that the resulting numbered cells are connected each other. However, we note that for Hitori the size of numbered cells could be information about the solution. That is, we cannot simply use the sea formation phase shown in Section 3.2. Therefore, we construct a sub-protocol called the *still-black protocol* as follows.

Still-black protocol: Given a black commitment, P can choose either changing it (i.e., swapping the two cards constituting the commitment) or not without V noticing it, as follows.

1. V reveals the given commitment to confirm that it is surely a black commitment.
2. If P wants to change the commitment, P places face-down club-to-heart below it; otherwise heart-to-club: $\boxed{?}\boxed{?} \rightarrow \begin{matrix}\boxed{?}\boxed{?}\\ \boxed{?}\boxed{?}\\ \clubsuit\ \heartsuit\end{matrix}$ or $\begin{matrix}\boxed{?}\boxed{?}\\ \boxed{?}\boxed{?}\\ \heartsuit\ \clubsuit\end{matrix}$.
3. Regarding cards in the same column as a pile, V applies a pile-shifting shuffle to the sequence of piles.
4. V reveals all the cards in the second row. If the revealed card on the right is a heart $\boxed{\heartsuit}$, V swaps the two cards in the first row; otherwise V does nothing.

4.1 Setup Phase

V and P put a black commitment on each cell of a given $p \times q$ grid and red commitments around the grid.

4.2 Connectivity Phase

This phase follows the same steps as the ones in the sea formation phase shown in Section 3.2 (where a white commitment is regarded as a black one and vice versa) except for Step 2c; instead of swapping the two cards, V and P use the still-black protocol so that P can choose either swapping the two cards or not. (Remember that P cannot change a white commitment into black.) Note that the steps are repeated exactly $pq - 1$ times.

After the above process, V is convinced that the resulting commitments represent a connected (white) figure (rule 3) and information about the number of the white commitments is hidden from V.

4.3 Verification phase

In this phase, V verifies all the remaining constraints, as follows.

One occurrence for each row/column. Here, V checks if each row and column contains only one occurrence of a number. The idea is that for a given row or column it suffices to look at only numbered cells that appear $k > 1$ times and confirm that the k commitments on the numbered cells correspond to either k blacks or $k - 1$ blacks. For a given row or column, this verification proceeds as follows.

1. V looks for numbered cells that appear more than once; take such a number which appears exactly $k > 1$ times. Then, V picks the corresponding k commitments.
2. P uses the chosen pile protocol to choose a white commitment among the k commitments if it exists; otherwise P uses the one to choose any commitment.
3. V reveals the $k - 1$ commitments that are not chosen by P. If all of them correspond to black (this means that the k commitments correspond to k or $k - 1$ blacks), V continues; otherwise V aborts.
4. V and P end the chosen pile protocol to return the k commitments to their original places.
5. V and P repeat the above steps for all numbers that appear twice or more.

Lonely black. V checks that black cells are isolated from each other. Let a white commitment correspond to a bit 0 and a black one correspond to 1. For each pair of adjacent commitments, V applies the input-preserving five-card trick explained in Section 2 to the two commitments. If the output is 0, V continues; otherwise V aborts.

5 Conclusion

We proposed two ZKP protocols for Nurikabe and Hitori. These two Nikoli's puzzles require that some cells of the solution are continuous without any precision on the number of cells in Hitori and without an exact number of cells in Nurikabe. We designed two methods and encoding for solving this continuity challenge and also respecting the other rules of the puzzles.

In the future, we aim at solving more challenging puzzles with other rules that also involve a kind of continuity property. For instance, in the puzzles Shikaku and Shakashaka, the goal is to draw rectangles of a certain size, which does not seem easy.

Acknowledgements. We thank the anonymous referees, whose comments have helped us to improve the presentation of the paper. This work was supported in part by JSPS KAKENHI Grant Number JP19J21153. This study was partially supported by the French ANR project ANR-18-CE39-0019 (MobiS5). This work has been partially supported by the French government research program "Investissements d´Avenir" through the IDEX-ISITE initiative 16-IDEX-0001 (CAP 20-25) and the IMobS3 Laboratory of Excellence (ANR-10-LABX-16-01).

References

1. den Boer, B.: More efficient match-making and satisfiability: *The Five Card Trick*. In: Quisquater, J., Vandewalle, J. (eds.) Advances in Cryptology - EUROCRYPT '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989, Proceedings. Lecture Notes in Computer Science, vol. 434, pp. 208–217. Springer (1989). https://doi.org/10.1007/3-540-46885-4_23
2. Bultel, X., Dreier, J., Dumas, J., Lafourcade, P.: Physical zero-knowledge proofs for akari, takuzu, kakuro and kenken. In: Demaine, E.D., Grandoni, F. (eds.) 8th International Conference on Fun with Algorithms, FUN 2016, June 8-10, 2016, La Maddalena, Italy. LIPIcs, vol. 49, pp. 8:1–8:20. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2016). https://doi.org/10.4230/LIPIcs.FUN.2016.8
3. Bultel, X., Dreier, J., Dumas, J., Lafourcade, P., Miyahara, D., Mizuki, T., Nagao, A., Sasaki, T., Shinagawa, K., Sone, H.: Physical zero-knowledge proof for makaro. In: Izumi, T., Kuznetsov, P. (eds.) Stabilization, Safety, and Security of Distributed Systems - 20th International Symposium, SSS 2018, Tokyo, Japan, November 4-7, 2018, Proceedings. Lecture Notes in Computer Science, vol. 11201, pp. 111–125. Springer (2018). https://doi.org/10.1007/978-3-030-03232-6_8
4. Dumas, J., Lafourcade, P., Miyahara, D., Mizuki, T., Sasaki, T., Sone, H.: Interactive physical zero-knowledge proof for norinori. In: Du, D., Duan, Z., Tian, C. (eds.) Computing and Combinatorics - 25th International Conference, COCOON 2019, Xi'an, China, July 29-31, 2019, Proceedings. Lecture Notes in Computer Science, vol. 11653, pp. 166–177. Springer (2019). https://doi.org/10.1007/978-3-030-26176-4_14
5. Goldreich, O., Kahan, A.: How to construct constant-round zero-knowledge proof systems for NP. Journal of Cryptology **9**(3), 167–189 (1991)

6. Goldreich, O., Micali, S., Wigderson, A.: Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. J. ACM **38**(3), 691–729 (1991). https://doi.org/10.1145/116825.116852
7. Goldwasser, S., Micali, S., Rackoff, C.: Knowledge Complexity of Interactive Proof-Systems. Conference Proceedings of the Annual ACM Symposium on Theory of Computing pp. 291–304 (1985). https://doi.org/10.1145/3335741.3335750
8. Gradwohl, R., Naor, M., Pinkas, B., Rothblum, G.N.: Cryptographic and physical zero-knowledge proof systems for solutions of sudoku puzzles. Theory Comput. Syst. **44**(2), 245–268 (2009). https://doi.org/10.1007/s00224-008-9119-9
9. Hearn, R.A., Demaine, E.D.: Games, Puzzles, and Computation. A. K. Peters, Ltd., USA (2009)
10. Holzer, M., Klein, A., Kutrib, M., Ruepp, O.: Computational complexity of NURIKABE. Fundam. Informaticae **110**(1-4), 159–174 (2011). https://doi.org/10.3233/FI-2011-534
11. Koch, A., Walzer, S.: Foundations for actively secure card-based cryptography. In: Farach-Colton, M., Prencipe, G., Uehara, R. (eds.) 10th International Conference on Fun with Algorithms, FUN 2021, May 30 to June 1, 2021, Favignana Island, Sicily, Italy. LIPIcs, vol. 157, pp. 17:1–17:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2021). https://doi.org/10.4230/LIPIcs.FUN.2021.17
12. Lafourcade, P., Miyahara, D., Mizuki, T., Sasaki, T., Sone, H.: A physical ZKP for slitherlink: How to perform physical topology-preserving computation. In: Heng, S., López, J. (eds.) Information Security Practice and Experience - 15th International Conference, ISPEC 2019, Kuala Lumpur, Malaysia, November 26-28, 2019, Proceedings. Lecture Notes in Computer Science, vol. 11879, pp. 135–151. Springer (2019). https://doi.org/10.1007/978-3-030-34339-2_8
13. Miyahara, D., Robert, L., Lafourcade, P., Takeshige, S., Mizuki, T., Shinagawa, K., Nagao, A., Sone, H.: Card-based ZKP protocols for takuzu and juosan. In: Farach-Colton, M., Prencipe, G., Uehara, R. (eds.) 10th International Conference on Fun with Algorithms, FUN 2021, May 30 to June 1, 2021, Favignana Island, Sicily, Italy. LIPIcs, vol. 157, pp. 20:1–20:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2021). https://doi.org/10.4230/LIPIcs.FUN.2021.20
14. Miyahara, D., Sasaki, T., Mizuki, T., Sone, H.: Card-based physical zero-knowledge proof for kakuro. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **102-A**(9), 1072–1078 (2019). https://doi.org/10.1587/transfun.E102.A.1072
15. Nishimura, A., Hayashi, Y., Mizuki, T., Sone, H.: Pile-shifting scramble for card-based protocols. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **101-A**(9), 1494–1502 (2018). https://doi.org/10.1587/transfun.E101.A.1494
16. Ruangwises, S., Itoh, T.: Physical zero-knowledge proof for numberlink **157**, 22:1–22:11 (2021). https://doi.org/10.4230/LIPIcs.FUN.2021.22
17. Sasaki, T., Mizuki, T., Sone, H.: Card-based zero-knowledge proof for Sudoku. In: Ito, H., Leonardi, S., Pagli, L., Prencipe, G. (eds.) 9th International Conference on Fun with Algorithms, FUN 2018, June 13-15, 2018, La Maddalena, Italy. LIPIcs, vol. 100, pp. 29:1–29:10. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2018). https://doi.org/10.4230/LIPIcs.FUN.2018.29

A Appendix: Protocol Properties

For proving that our ZKP protocols applied to Nurikabe and Hitori are secure, we need to show that they satisfy the following three properties:

– Correctness (Theorems 1 and 4): If the prover P places its cards according to the solution, then all verifications are valid. Hence, if P knows a solution, then it can always convince the verifier V.
– Soundness (Theorems 2 and 5): If P's input is invalid, then V can detect it thanks to the protocol. Therefore, if P does not know the solution, it cannot convince V.
– Zero-knowledge (Theorems 3 and 6): V learns nothing about P's solution.

A.1 Appendix: Security Proofs for Nurikabe

Theorem 1 (Completeness). *If P knows a solution of a Nurikabe grid, then it can convince V.*

Proof. Suppose that P, knowing the solution s of the grid G, runs the Setup phase as in Section 3.1. Then we show that P is able to perform the proofs for the sea formation and the verification phases.

Sea formation. In this phase, the goal of P is to convince that the black commitments form a connected figure (rule 3). Since s is a solution to the initial grid, the black cells are connected. Thus, at Step 2 (which is repeated $N_b - 1$ times), P can always pick a black commitment. The corresponding neighbour can be replaced by a black commitment, ensuring that the resulting figure is connected.

Verification. The verifier V must be convinced that rules 1, 2, and 4 hold. First, the *forbidden area* (rule 4) must be verified. Since s is a solution, there is no 2×2 only black squares on the grid. Thus, by checking each square of four cells, there will be at least one white commitment amongst the chosen cells. Hence, P can choose (via the chosen-pile protocol) the latter cell.

Secondly, the *island rules* (rules 1 and 2) must be checked. Since s is a solution, each numbered cell is in a region where there are the corresponding number of white commitments and there is no additional numbered cell. Consider a numbered cell equal to $n > 2$ (the case $n = 1$ is straightforward since it must have its four neighbours all blacks which can be checked by simply revealing them). There are $n - 1$ white commitments without counting the commitment on the numbered cell. Thus, P and V can apply the first sub-routine exactly $n-1$ times. This implies that all the white commitments are turned into red ones. From here, V is convinced that the region contains at least n white commitments. Yet this could be more than n if two regions are not separated. Hence, the second sub-routine ensures that the region is not composed of more than n white cells. Note that at this point all white cells are encoded as red commitments: $\boxed{\heartsuit}\boxed{\heartsuit}$.

Now V replaces the commitment on the numbered cell by a black commitment (i.e., $\boxed{\clubsuit}\boxed{\heartsuit}$). When revealing the right card of the four neighbours for a given previous white commitment, there are all $\boxed{\heartsuit}$ since all previous white commitments are encoded as $\boxed{\heartsuit}\boxed{\heartsuit}$. The verified commitments are then turned into black ones: $\boxed{\clubsuit}\boxed{\heartsuit}$; thus V is convinced that no white commitment is checked twice.

Finally, since all the verifications have been checked, we proved that if P has a solution then the verifications will always succeed.

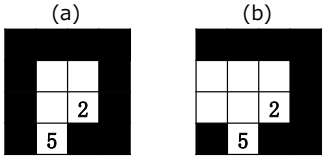
Theorem 2 (Soundness). *If P does not provide a solution of the $p \times q$ Nurikabe grid G, it is not able to convince V.*

Proof. Suppose that P does not know a solution for G. We want to show that V will always detect it.

Suppose that the commitments are correct, meaning that the black commitments form a connected figure. (If it is not the case, then P cannot use the protocol since a white commitment can be blackened if and only if one of its four neighbours is already blackened.)

We can distinguish two cases, each corresponding to a part of the verification phase:

- *Forbidden area.* V verifies all possible 2×2 squares of the grid. If one of them is composed of only black commitments, then P cannot choose a white one. Thus, V will reveal a black one since P cannot act otherwise.
- *Island rules.* Consider a numbered cell equal to $n > 2$. Two sub-cases can be discussed here. Firstly, consider the case where only $\ell\,(< n)$ white commitments are placed on a region. During Step 2c for the ℓ-th instance, the neighbour commitment cannot correspond to a white commitment; thus, V aborts. Secondly, consider that several regions are communicating; that is, there are at least two numbered cells inside the regions. There are two invalid cases: (a) a region is completely covered with another region, or (b) a part of a region is covered with another one; such examples are shown as follows.



For (a), note that when the verification is done for one of such two numbered cells, the commitment on the other numbered cell will become a black one. Thus, in Step 1 a black commitment should appear when V verifies the other numbered cell and then V aborts. For (b), this means that after Step 2 there are more white commitments around red commitments. Thus, V can detect it in Step 4c because it means that a club $\boxed{\clubsuit}$ should appear when V reveals the right card of each of four neighbours of a red commitment.

Theorem 3 (Zero-knowledge). *V learns nothing about P's solution of the given grid G.*

Proof. We use the same proof technique as in [8]: zero-knowledge is induced by a description of an efficient *simulator* which simulates interaction between a cheating verifier and a real prover. However, the simulator does not have a solution but it can swap cards for different ones during shuffles. The simulator acts as follows:

– The simulator constructs a random connected figure of size N_b.
– During the verification of the forbidden area rule, each possible 2×2 square is verified. For a given square, the corresponding commitments are shuffled; thus, the simulator can swap the targeted commitment via the chosen-pile protocol by a white commitment.
– During the verification of the island rule, the simulator replaces the target commitment by a white one and its corresponding neighbour by a red commitment for the first sub-routine.
  For the second sub-routine, the simulator changes the target commitment by a red commitment and also change the right card of the four neighbour by red cards.

Note that the chosen-pile and 4-neighbour protocols use shuffle techniques; thus, the simulator is able to replace shuffled cards when applying those protocols. The simulated proofs and the real proofs are indistinguishable; thus, V learns nothing about P's solution.

A.2 Appendix: Security Proofs for Hitori

Theorem 4 (Completeness). *If P knows a solution of a Hitori grid, then it can convince V.*

Proof. Suppose that P knows the solution s of the grid G and runs the setup phase. We show that P can perform the connectivity phase and the verification without aborting.

Connectivity. Since s is a solution, the white cells form a connected figure. Hence, for Step 2 P can always choose a black commitment to turn one of its neighbours into a white one. Thus, Step 2 is never aborted. Note that P can start this phase with any black commitment placed on a white cell of s (for Steps 1 and 1a). Next, P uses the still-white protocol. Note that the protocol can turn a black commitment into a white one depending on P's will (and V cannot notice it). Let us consider two cases: The first one is that P wishes to change the black commitment. The configuration is then:

Thus, after applying a pile-shifting shuffle, if the configuration is the same, then the right card of the second row is a heart $\boxed{\heartsuit}$; thus, V will swap the cards of the first row, leading to: $\boxed{\heartsuit}\boxed{\clubsuit}$. Thus, the resulting commitment is white. But if the configuration has changed after applying a pile-shifting shuffle, the resulting configuration is now:

Thus, V will not change the first row (as the right card of the second row is now a club $\boxed{\clubsuit}$). The commitment now corresponds to a white one.

The second case where P wants the black commitment still black is analogous to the first case.

Verification. Since s is a solution, each row and each column includes at most one occurrence of a given numbered cell. Thus, when an integer appears k times in a given row/column, at least $k-1$ of them are blackened; otherwise s is not a solution. Hence, if s is a solution, the uniqueness verification never aborts. The last verification concerns the black cells. s is a solution so for a given black commitment, its four neighbours are white commitments. Thus any combination of pair of those five commitments is different from the pair formed by only black commitments. Hence, each two adjacent commitments will be different from the pair formed by two black commitments, leading to always output 0 for the five-card trick.

Theorem 5 (Soundness). *If P does not provide a solution of the $p \times q$ Hitori grid G, then it is not able to convince V.*

Proof. Suppose that P does not know a solution for G. We want to show that V will always detect it. Since the construction of the connectivity phase enforces that the white commitments are connected (via the still-black protocol), P needs to ensure this property to continue the protocol. Note that the still-black protocol enables to ensure V that P is not cheating. Indeed, P could try to open the path with white cells and then close it, which breaks the connectivity rule. If P tries to turn back a white cell into a black cell, then V will notice it since the target cell is revealed (step 1). Thus, P can only turn black cells into white ones but not the other way.

Suppose that the commitments are correct (i.e., white cells are connected), but it does not correspond to a solution. We can distinguish two cases, each corresponding to a constraint that is not respected:

- *Uniqueness:* V looks at, for a given row (column), an integer with $k > 1$ occurrences. If this constraint is not respected, it means that more than two white commitments exist among the k commitments. V will detect it since $k-1$ commitments among them are revelaed.
- *Lonely black:* V checks **all** possible two-adjacent commitments. Thus, if P tries to blackened more cells than needed (e.g., for passing the uniqueness verification), then V will detect it.

Hence, if P provides correct commitments which not correspond to a solution then V will detect it. Finally, if P passes all the verifier's checks, it has the solution which concludes the soundness proof.

Theorem 6 (Zero-knowledge). *V learns nothing about P's solution of the given grid G.*

Proof. We use again the same proof technique as in [8]: zero-knowledge is induced by a description of an efficient *simulator* which simulates interaction between a cheating verifier and a real prover. The simulator acts as follows:

– Connectivity phase. The simulator chooses a random cell on the grid to turn it white. Then it applies the routine $pq - 1$ times using the 4-neighbour and still-black protocols without changing anything. Thus the grid contains only one white cell (which is a connected figure).
– During the verification phase, uniqueness is ensured since all but one cells are blackened. Thus no numbered card cannot appear more than once. For the lonely black, the verifier takes two adjacent commitments and the simulator swaps one of the two piles with a pile of white commitment. Hence, the five-card trick always output 0. Note that when the two piles include the already white cell, the simulator does nothing.

The simulated proofs and the real proofs are indistinguishable. Thus, V learns nothing about P's solution.