Physical Zero-Knowledge Proof for Ball Sort Puzzle

Suthee Ruangwises
The University of Electro-Communications, Tokyo, Japan

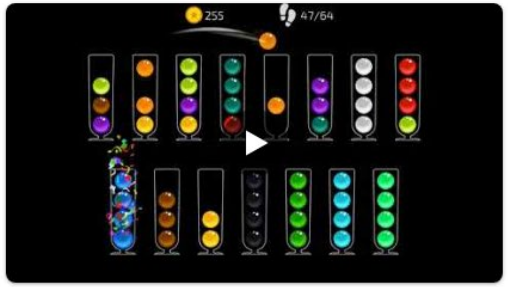
CiE 2023 - Batumi, Georgia

July 24, 2023

Introduction

Ball Sort Puzzle

- A popular logic puzzle in smartphone apps



Ball Sort Master - Puzzle Game
Kasur Games
4.6 ★

Ball Sort Puzzle - Color Games
EasyFun Game
4.7 ★

Color Ball Sort Puzzle
Sonatgame
4.5 ★

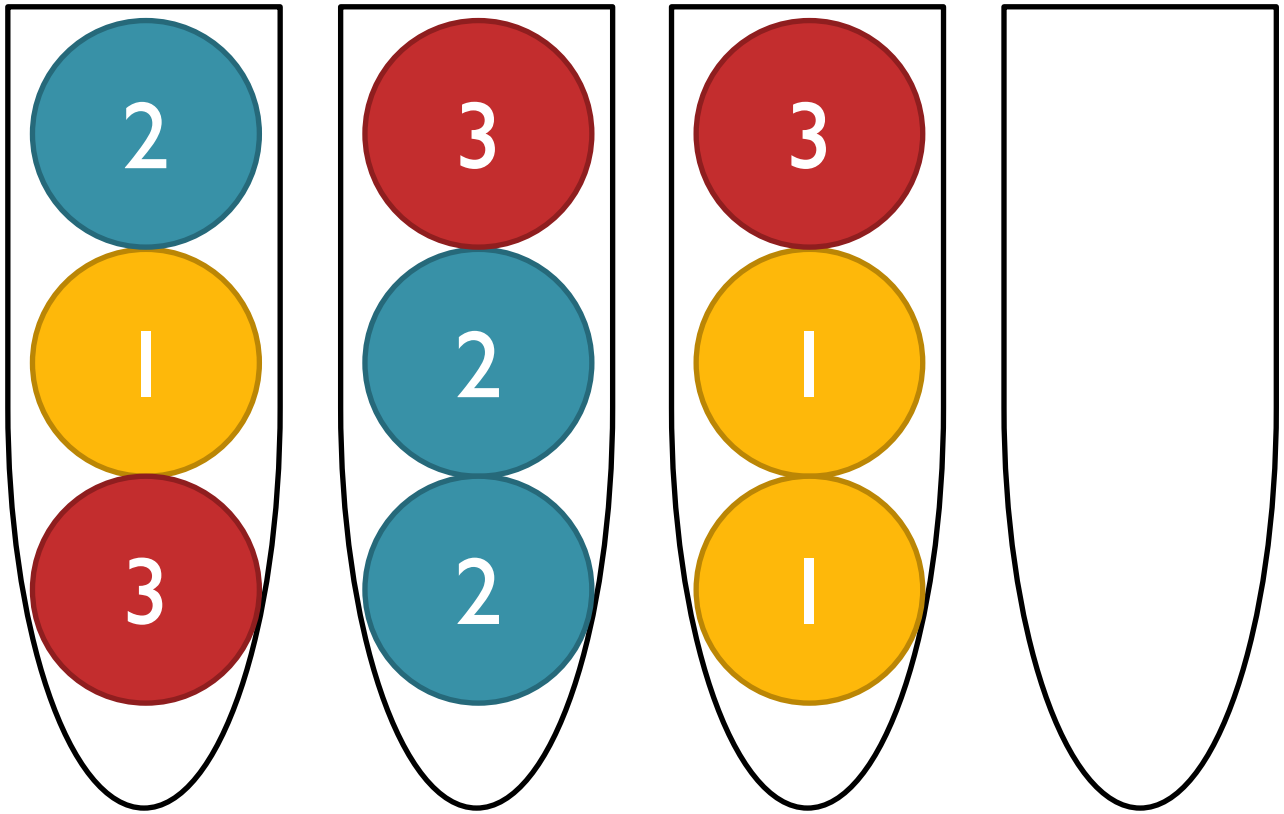
Ball Sort Puzzle – Egg Sort
Apollo Game Studio
4.7 ★

Ball Sort: Color Sorting Games
Suga Technology
4.8 ★

Ball Games Color Sorting Games
Peachu Pacha Games
3.8 ★

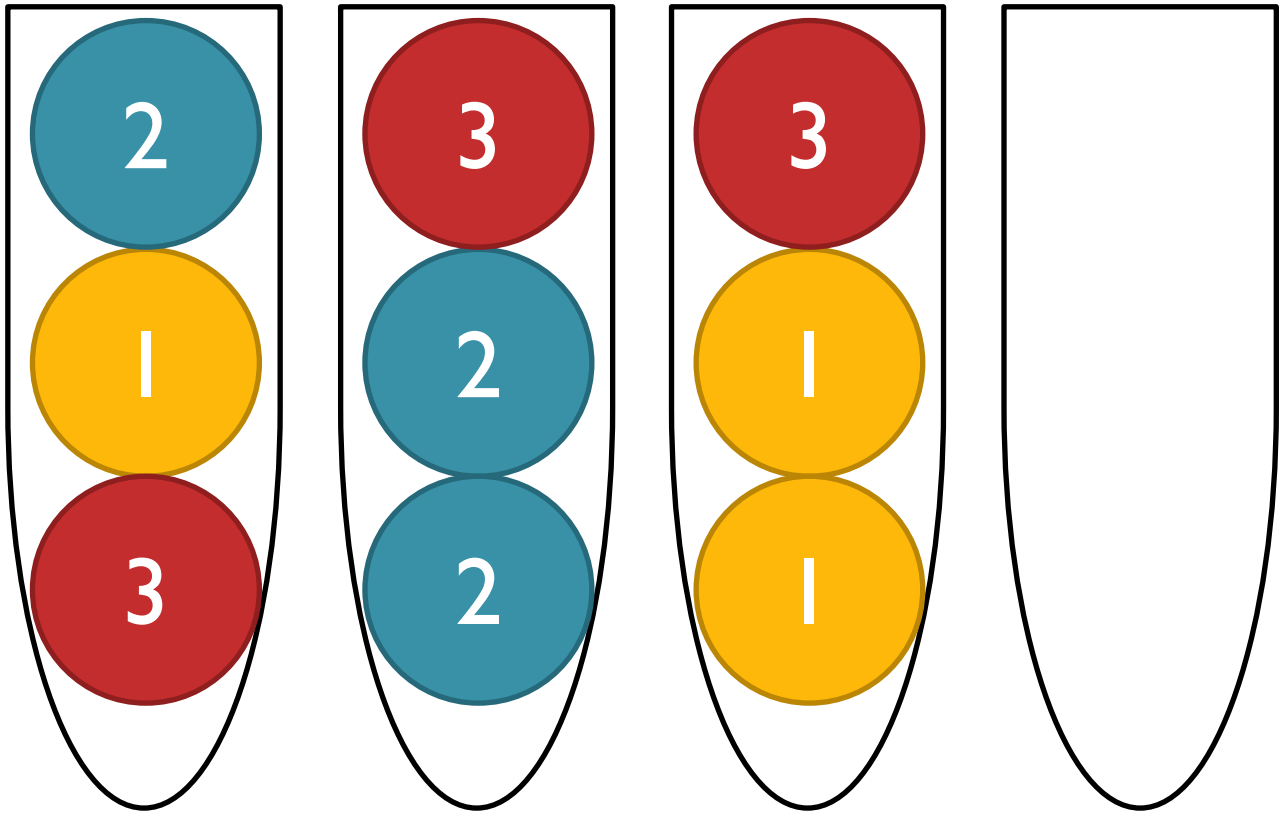
Ball Sort Puzzle

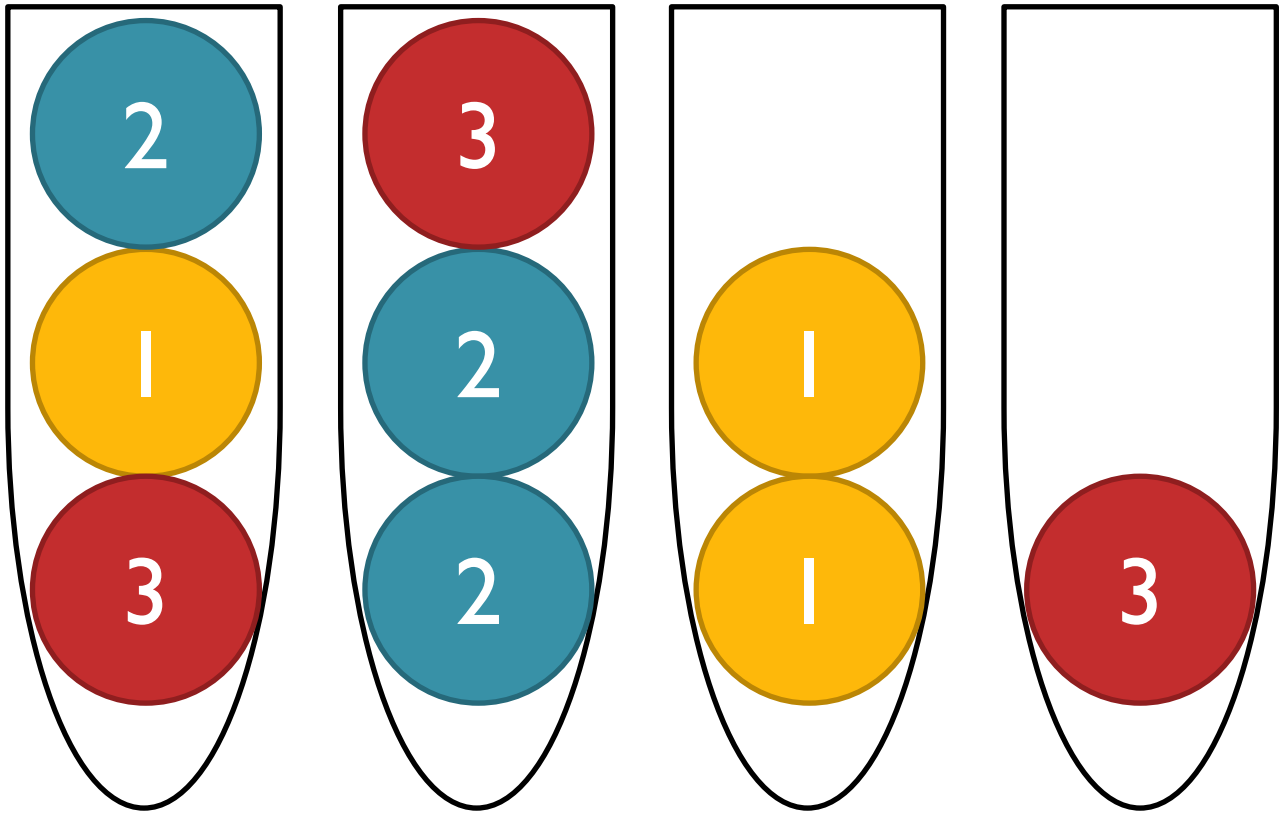
- Given several bins containing balls of n colors, and some empty bins
- Has to sort the balls by color, i.e. make each bin containing balls of single color

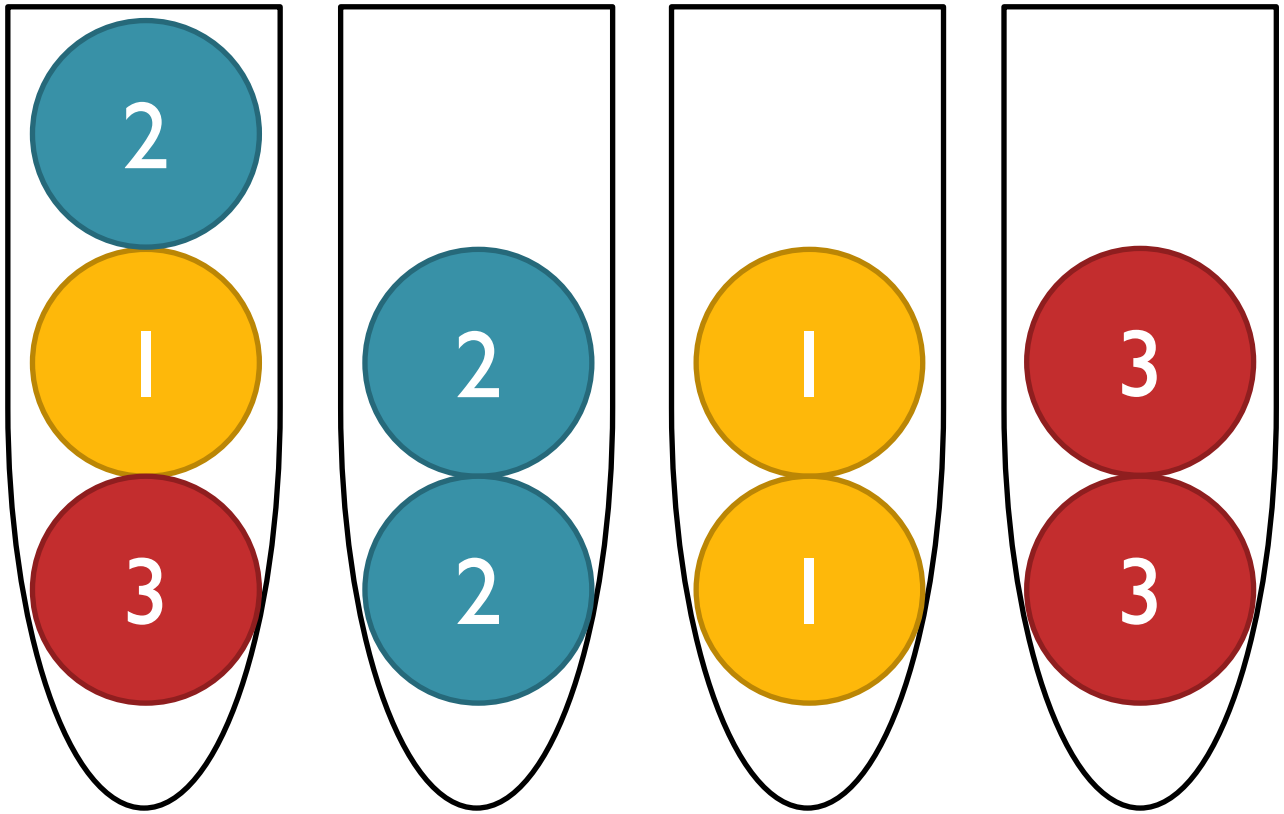

2
1
3
3
2
2
3
1
1

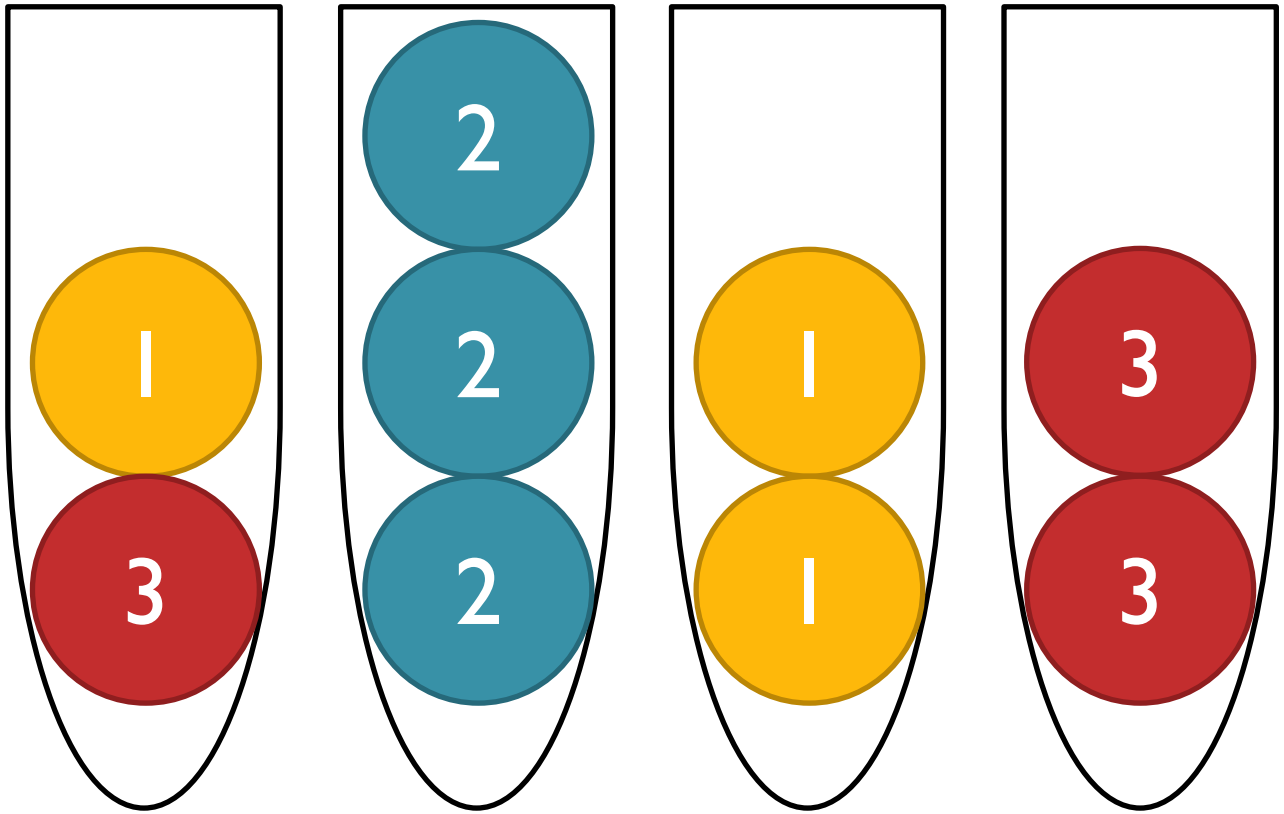
Ball Sort Puzzle

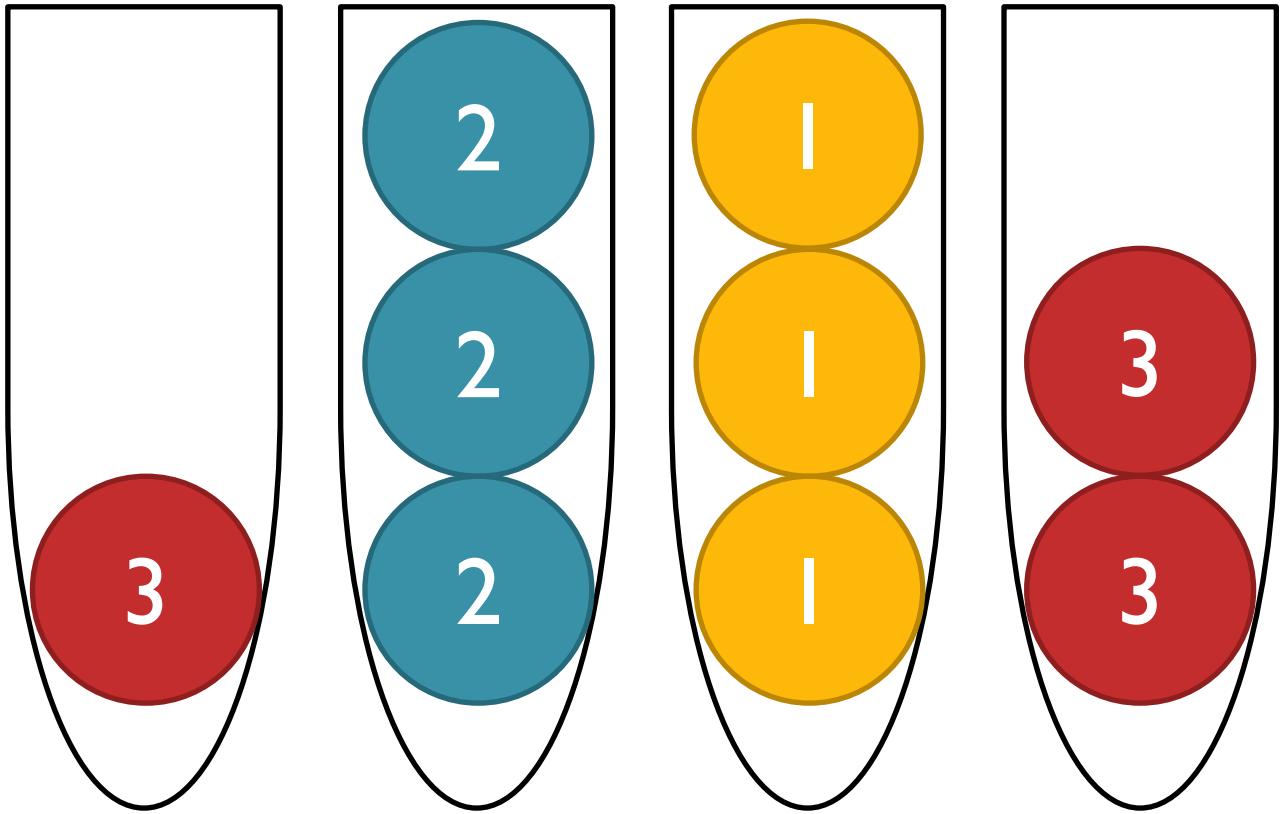
- Each bin works like a stack (LIFO: last-in first-out order).
  - Player can pick only the top ball of a bin, and put it on top of another non-full bin.
- Another restriction is that, if the destination bin is not empty, the color of its top ball must be the same as the moved ball.

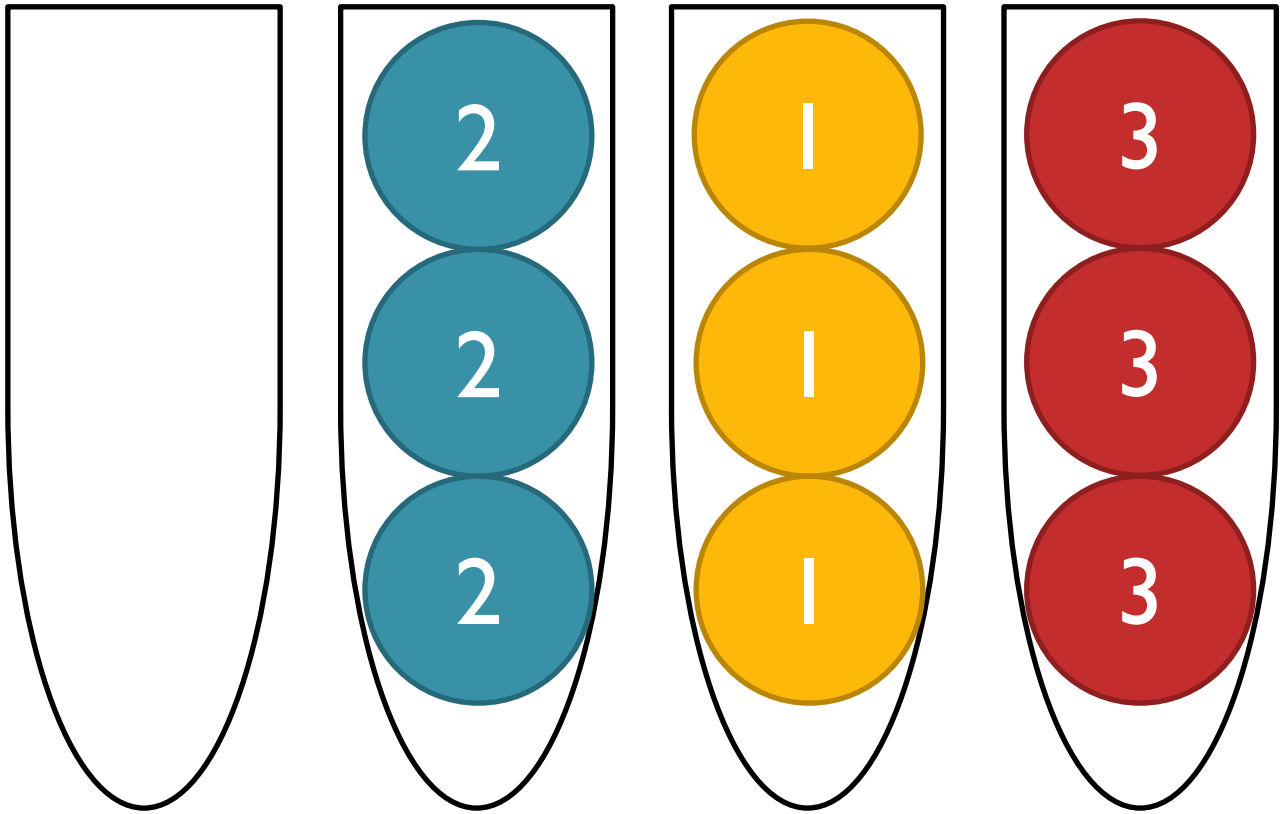

2
1
3
3
2
2
3
1
1


2
1
3
3
2
2
1
1
3


2
1
3
2
2
1
1
3
3


1
3
2
2
2
1
1
3
3


3
2
2
2
1
1
1
3
3


2
2
2
1
1
1
3
3
3

Ball Sort Puzzle

- Very recently, Ito et al. (FUN 2022) showed that determining if a ball sort puzzle instance is solvable within t moves is NP-complete.
  - Or even whether it is solvable at all is also NP-complete.
- Solvable if and only if its corresponding *water sort puzzle* instance is solvable.

Zero-Knowledge Proof

- **P**aimon creates a difficult Ball Sort Puzzle and challenges her friend **V**enti to solve it.
- He can't solve it and doubts whether it really has a solution.
- Paimon needs to convince him that her puzzle has a solution *without revealing it*.
- She needs a *zero-knowledge proof* (ZKP).

Zero-Knowledge Proof

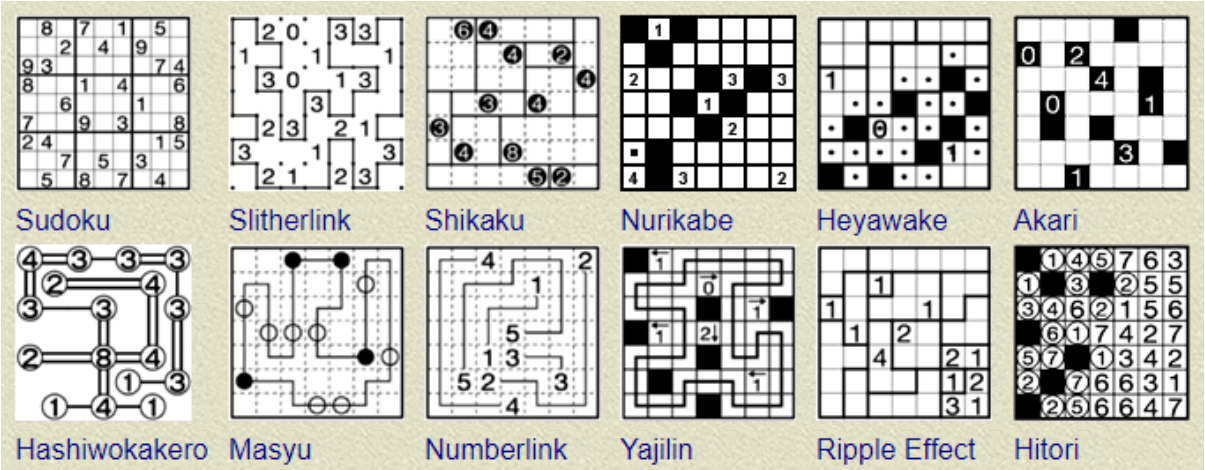
- Interactive proof between a prover P and a verifier V.
- **Completeness:** If P knows the solution, then P can convince V.
- **Soundness:** If P doesn't know the solution, then P can't convince V.
- **Zero-knowledge:** V learns nothing about P's solution.

Card-based Protocols

- Does not require computer
- Uses only small, portable objects
- Easy for observers to verify the correctness and security, even for non-experts
- Suitable for teaching purpose

Card-based ZKP for Logic Puzzles

- Sudoku
- Makaro
- Kakuro
- Akari
- Takuzu
- Juosan
- Numberlink
- etc.



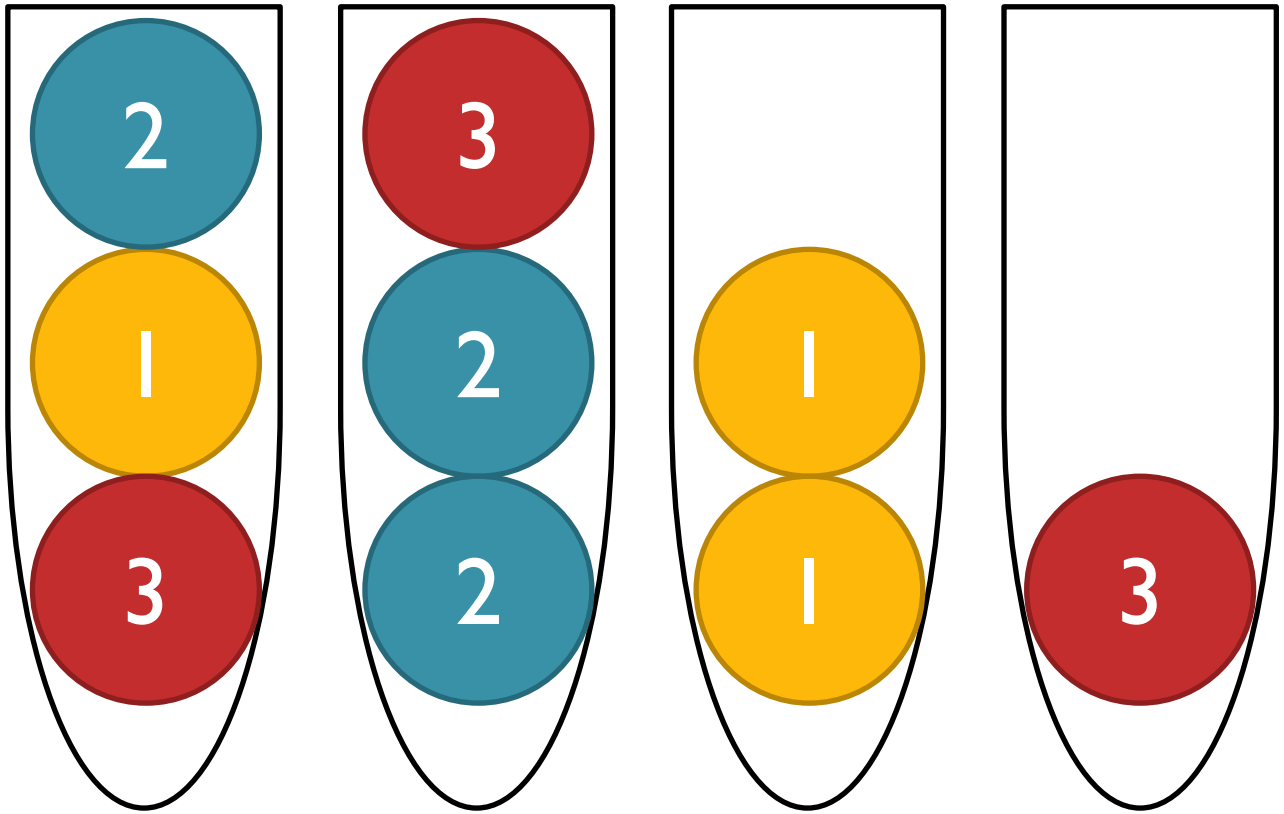
Our Contribution

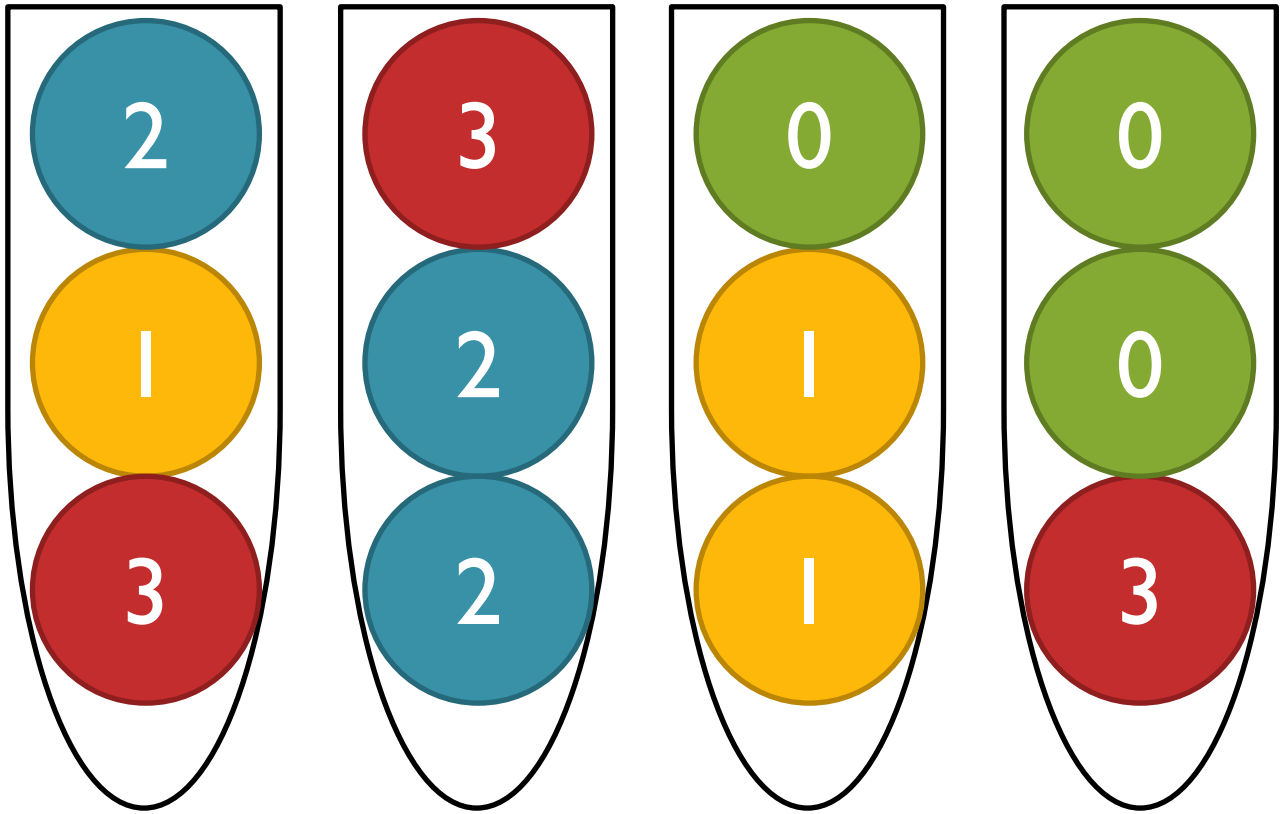
- Develop a ZKP for the ball sort puzzle
- Allowing P to show that he/she knows the solution with t moves
- The first card-based ZKP protocol for interactive puzzle (where a solution involves moving object, not just a written answer)

Our Protocol

Our Protocol

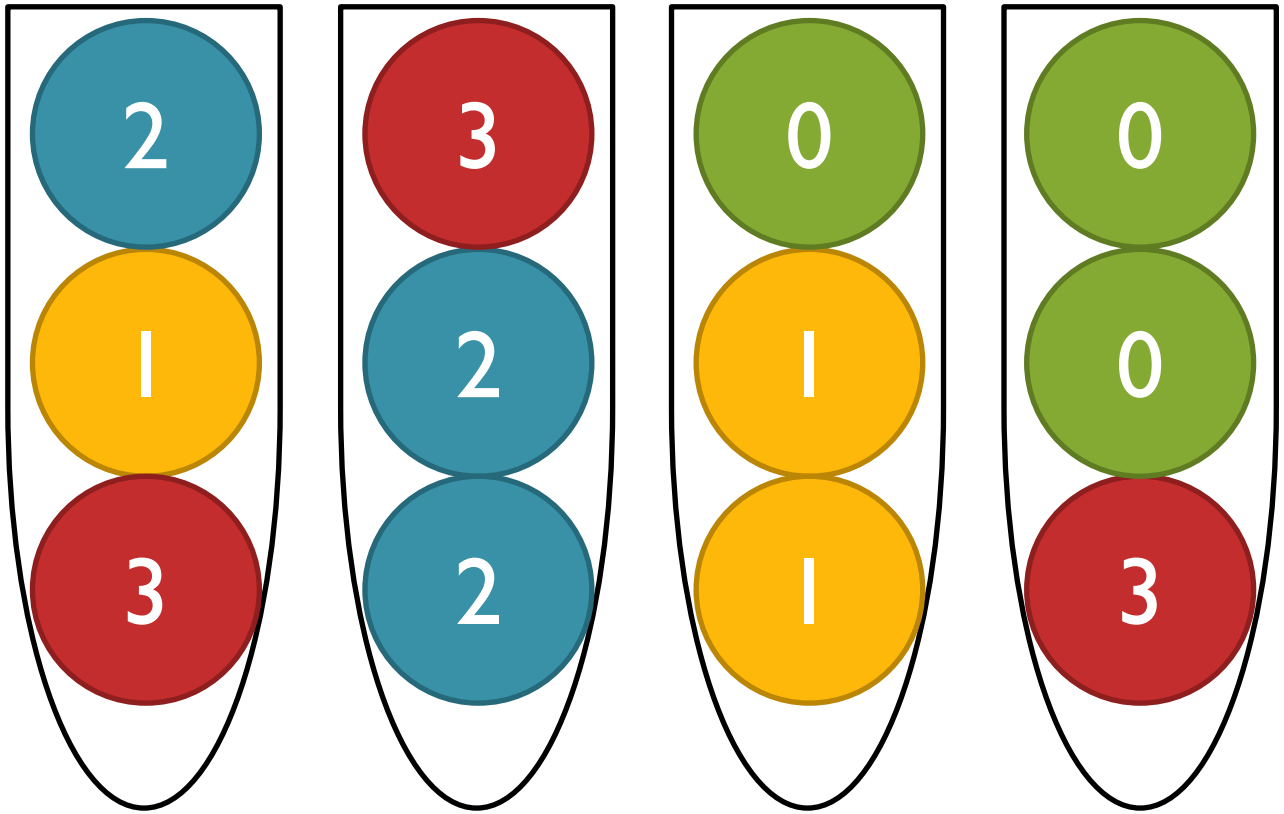
- The key idea is that we fill empty spaces with "dummy balls" with number 0.

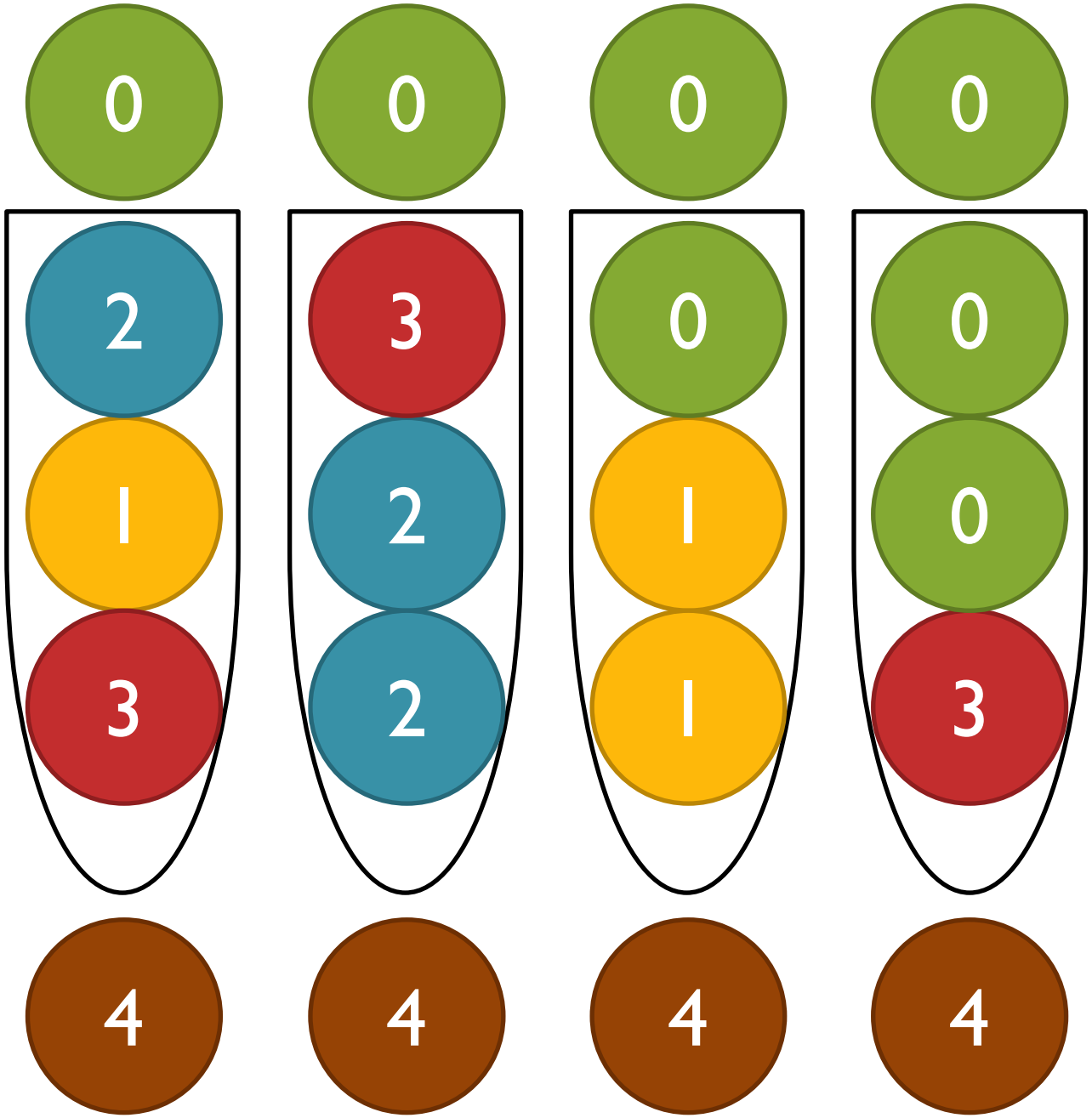

2
1
3
3
2
2
1
1
3


2
1
3
3
2
2
0
1
1
0
0
3

Our Protocol

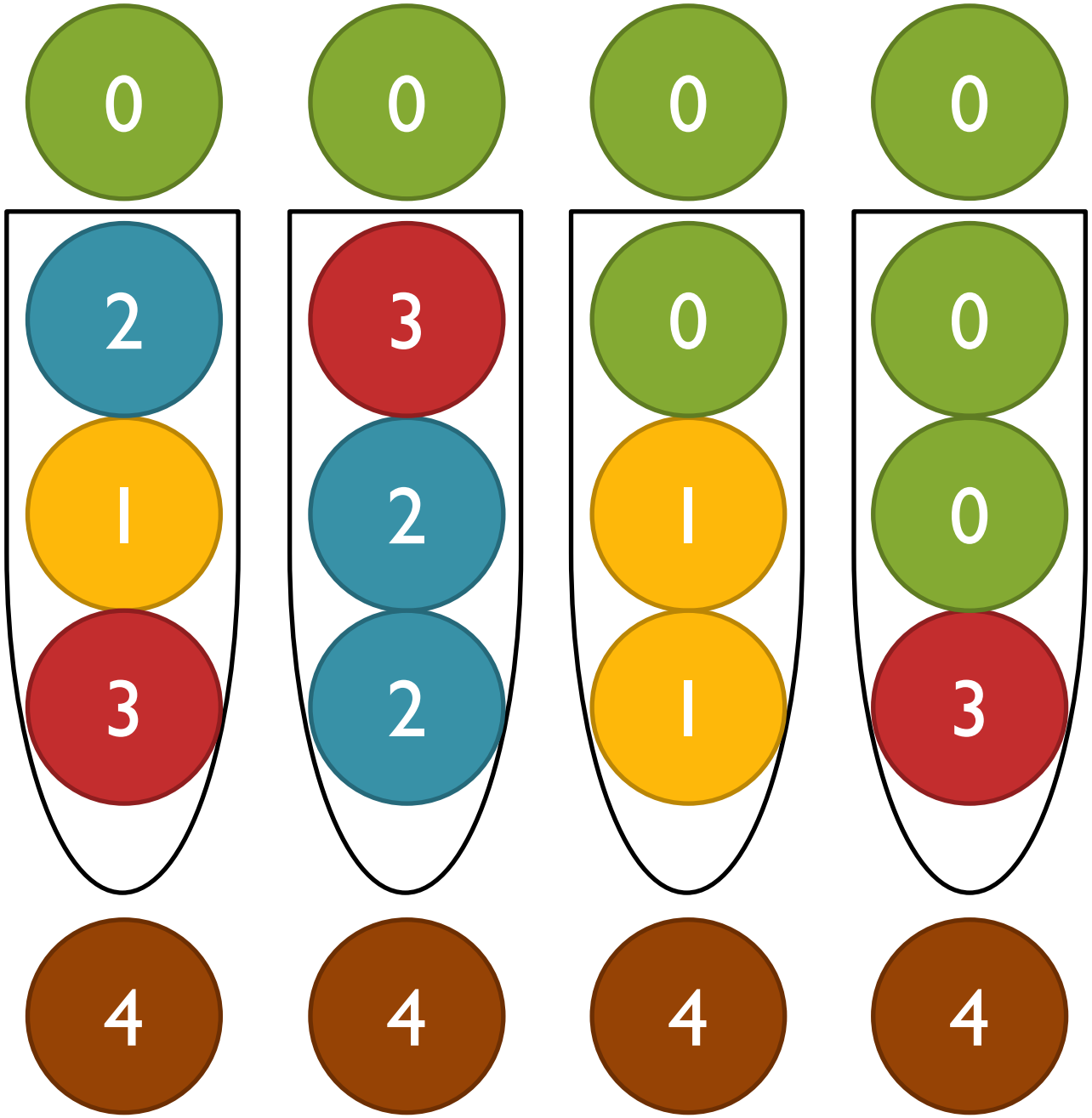
- Also, put a dummy ball with number 0 above each bin.
- Put a dummy ball with number $n + 1$ under each bin.

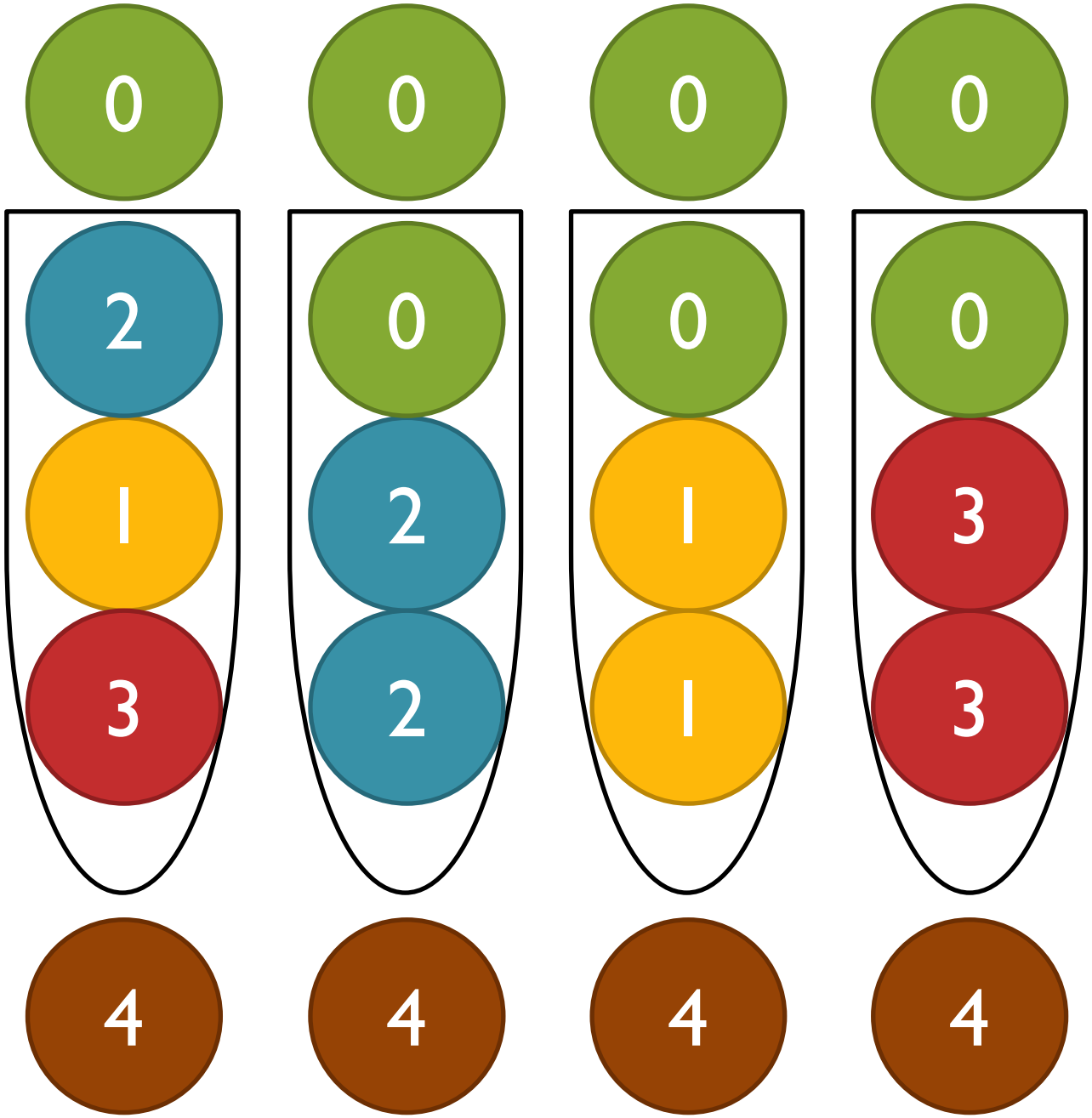

2
1
3
3
2
2
0
1
1
0
0
3


0
0
0
0
2
3
0
0
1
2
1
0
3
2
1
3
4
4
4
4

Our Protocol

- Moving a ball to another bin is equivalent to swapping it with a dummy ball.


0
0
0
0
2
3
0
0
1
2
1
0
3
2
1
3
4
4
4
4


0
0
0
0
2
0
0
0
1
2
1
3
3
2
1
3
4
4
4
4

0	0	0	0
2	3 a_x	0	0
1	2	1	0 b_y
3	2	1	3
4	4	4	4

0	0 a_{x-1}	0	0
2	3 a_x	0	0 b_{y-1}
1	2	1	0 b_y
3	2	1	3 b_{y+1}
4	4	4	4

Moving a Ball

- Conditions to check
  - $1 \leq a_x \leq n$
  - $a_{x-1} = 0$
  - $b_y = 0$
  - $b_{y-1} = 0$
  - either $b_{y+1} = a_x$ or $b_{y+1} = n + 1$
- Then, swap a_x with b_y.

0	♥	♥	♥
1	♣	♥	♥
2	♥	♣	♥
3	♥	♥	♣
4	♣	♣	♣

Moving a Ball

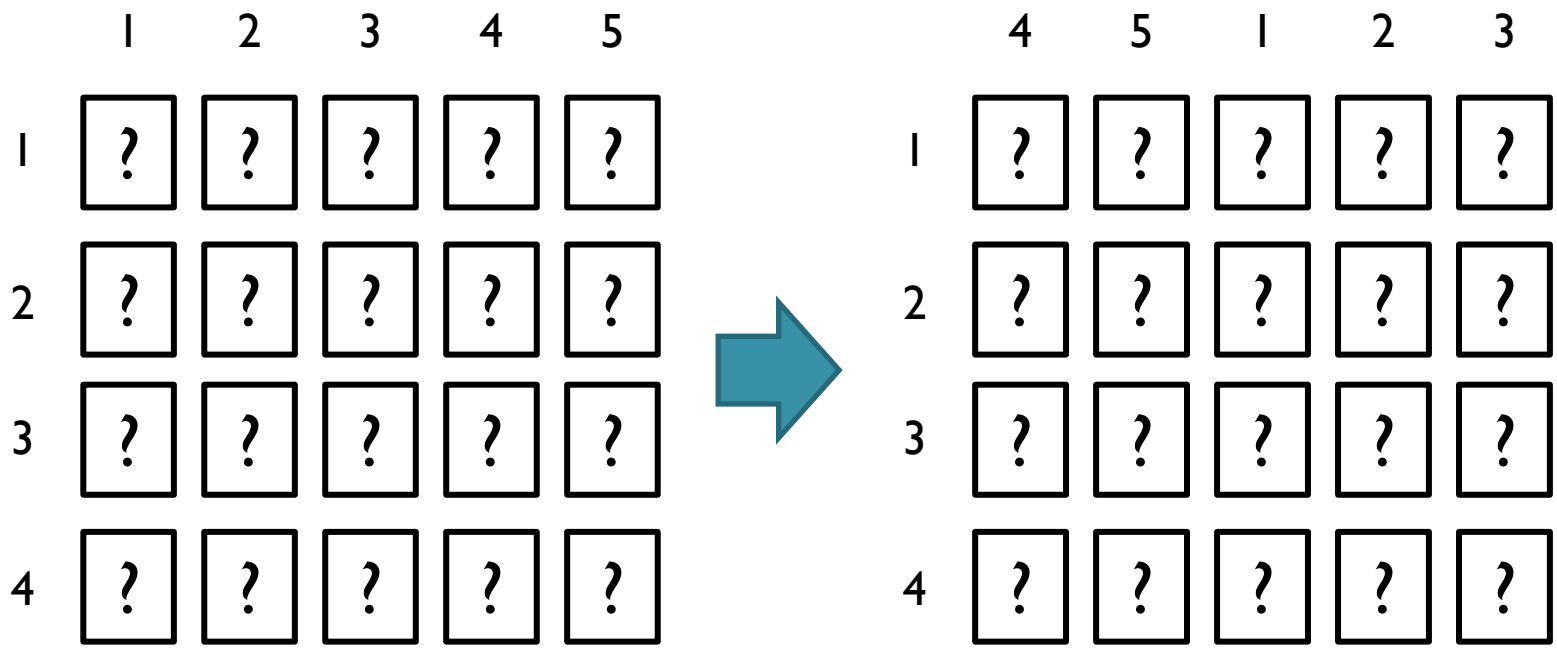
- Conditions to check
  - $1 \leq a_x \leq n$
  - $a_{x-1} = 0$ ✓
  - $b_y = 0$ ✓
  - $b_{y-1} = 0$ ✓
  - $\boxed{\text{either } b_{y+1} = a_x \text{ or } b_{y+1} = n + 1}$
- Then, swap a_x with b_y.

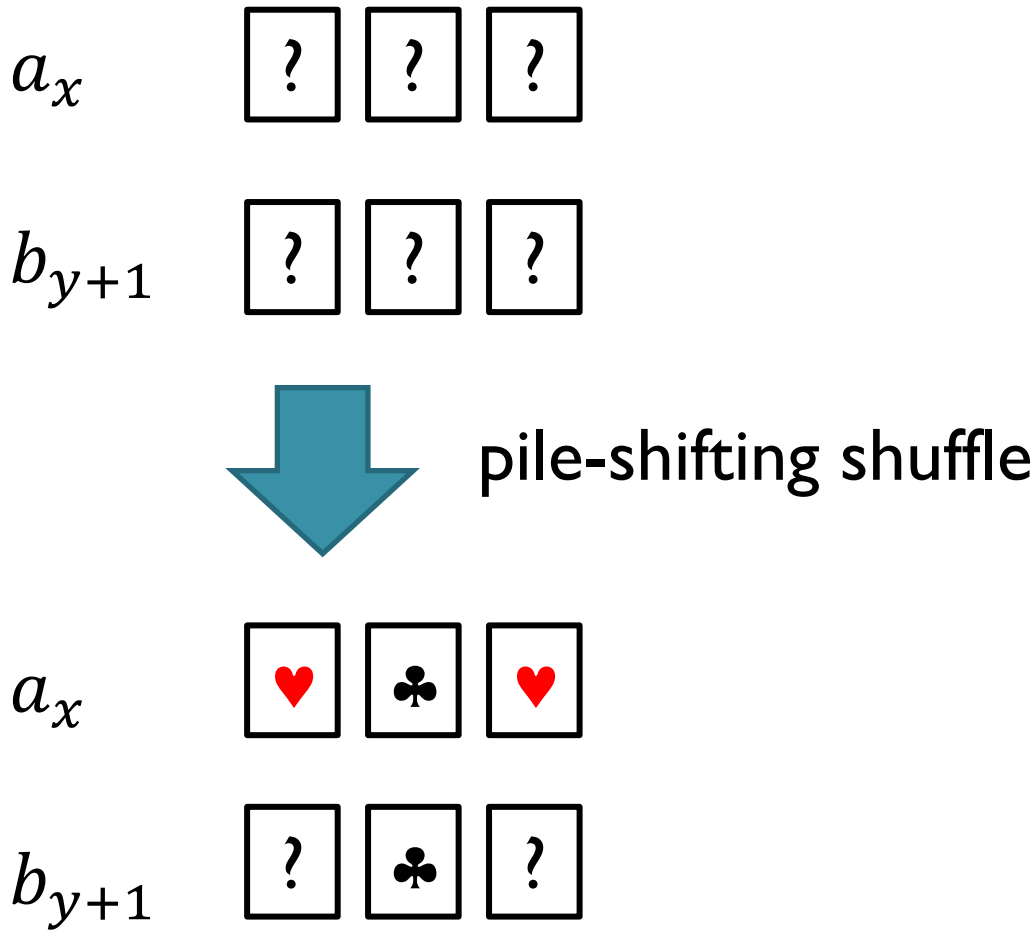
a_x ? ? ?

b_{y+1} ? ? ?

pile-shifting shuffle

Pile-Shifting Shuffle




a_x
? ? ?
b_{y+1}
? ? ?
pile-shifting shuffle
a_x
♥ ♣ ♥
b_{y+1}
? ♣ ?

Chosen Pile Cut Protocol

- Allows P to select a pile of cards he/she wants without revealing to V which one.
- Developed by Koch and Walzer (2020).
- P applies it twice, choosing the column and then the card.

Future Work

Future Work

- Develop a card-based ZKP for water sort puzzle
  - Similar puzzle with more restrictive rules
  - Consecutive balls with the same color are connected and must be moved together.

Questions and Comments