Some Recent Advancements in Monotone Circuit Complexity

Susanna F. de Rezende

Lund University

STACS, Jena

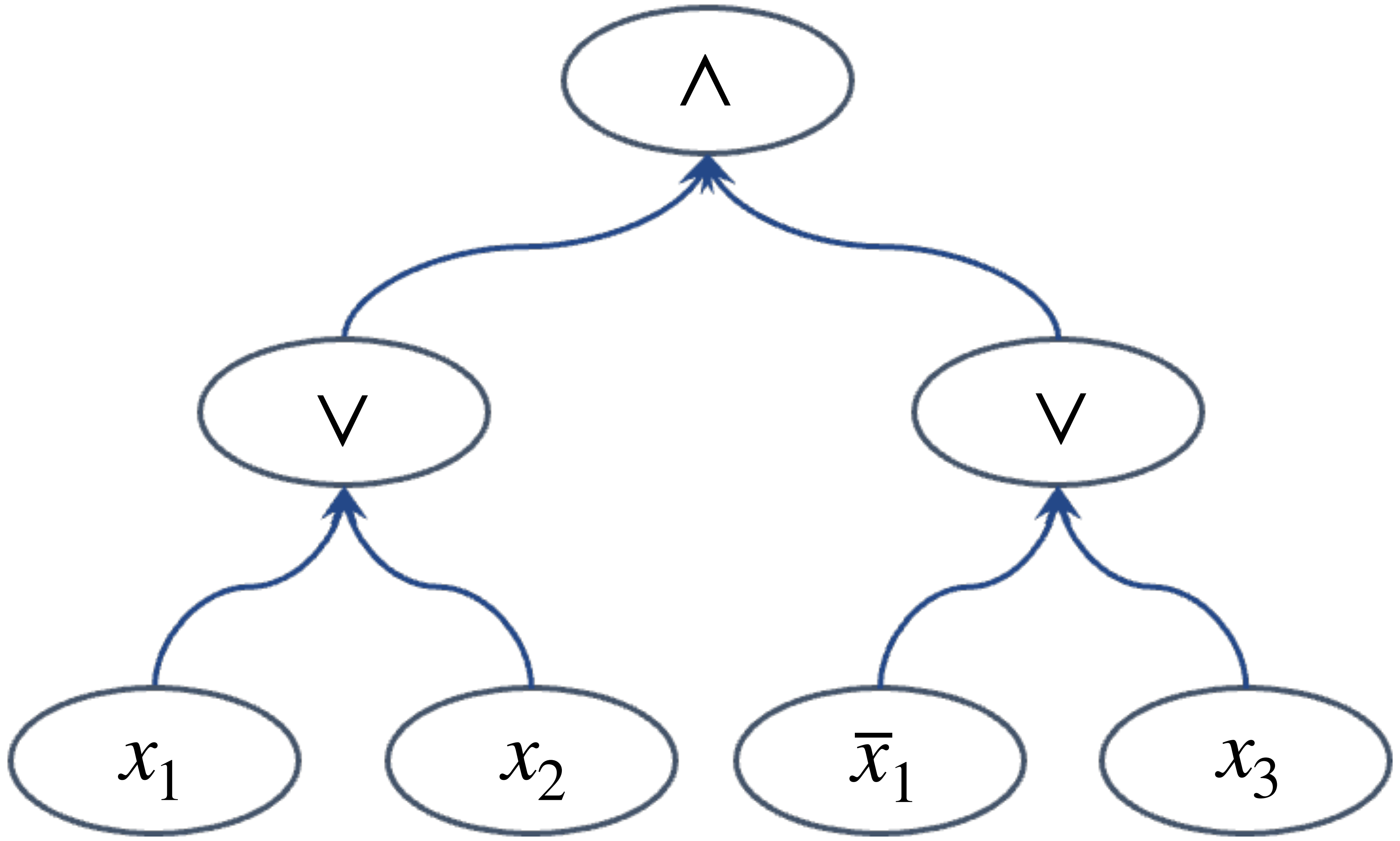
March 7, 2025

SYMPOSIUM ON THEORETICAL ASPECTS OF COMPUTER SCIENCE

Boolean Circuits

The difficulty in proving that a given boolean function has high complexity lies in the nature of our adversary: the circuit. Small circuits may work in a counterintuitive fashion, using deep, devious, and fiendishly clever ideas. How can one prove that there is no clever way to quickly compute the function? [Jukna '12]

- Input gates (Boolean literals) and $\wedge$, $\vee$ gates*
- **Size**: # of gates, **Depth**: length of longest path
- *Monotone* if only variable as inputs
- *Formula* if DAG is a tree
- Depth-d lower bound (fan-in 2) for f
  $\Rightarrow$ formula size-$2^{\Omega(d)}$ lower bound for f



* DeMorgan Boolean circuits: poly-equivalent to Boolean circuits

Boolean Circuits

- Most functions require circuits of size $2^n/n$ [Shanon '49]
- Goal: exhibit hard functions and understand why they are hard
- Best lower bound until recently was $3n$ [Blum '84]
  - Improved to $(3 + 1/86)n$ [Find, Golovnev, Hirsch, and Kulikov '16]
  - Improved to $3.1n$ [Li, Yang '22]

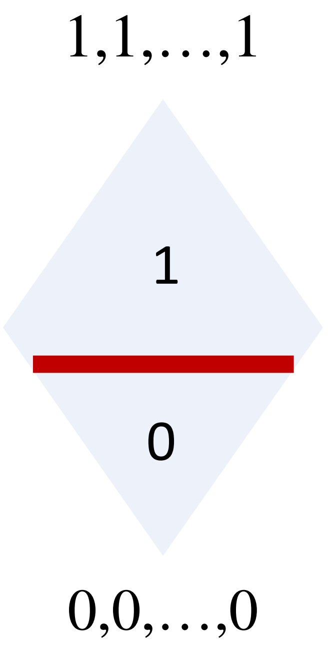
Why Study Monotone Boolean Circuits

- Natural computation model for monotone functions

> Why should one care about monotone circuits? The point is that this model has a purely "practical" importance. Namely, lower bounds for such circuits imply the same lower bounds for (min, +)-circuits, and hence, for dynamic programming. [Jukna '12]

- Connections to non-monotone: equally powerful* for slice functions

$$f(x) = \begin{cases} 1 & \text{if } |x| > k \\ g(x) & \text{if } |x| = k \\ 0 & \text{if } |x| < k \end{cases}$$



* up to constant factor and small additive factor [Berkowitz '82, Valiant '86]

Monotone Complexity of Boolean Functions

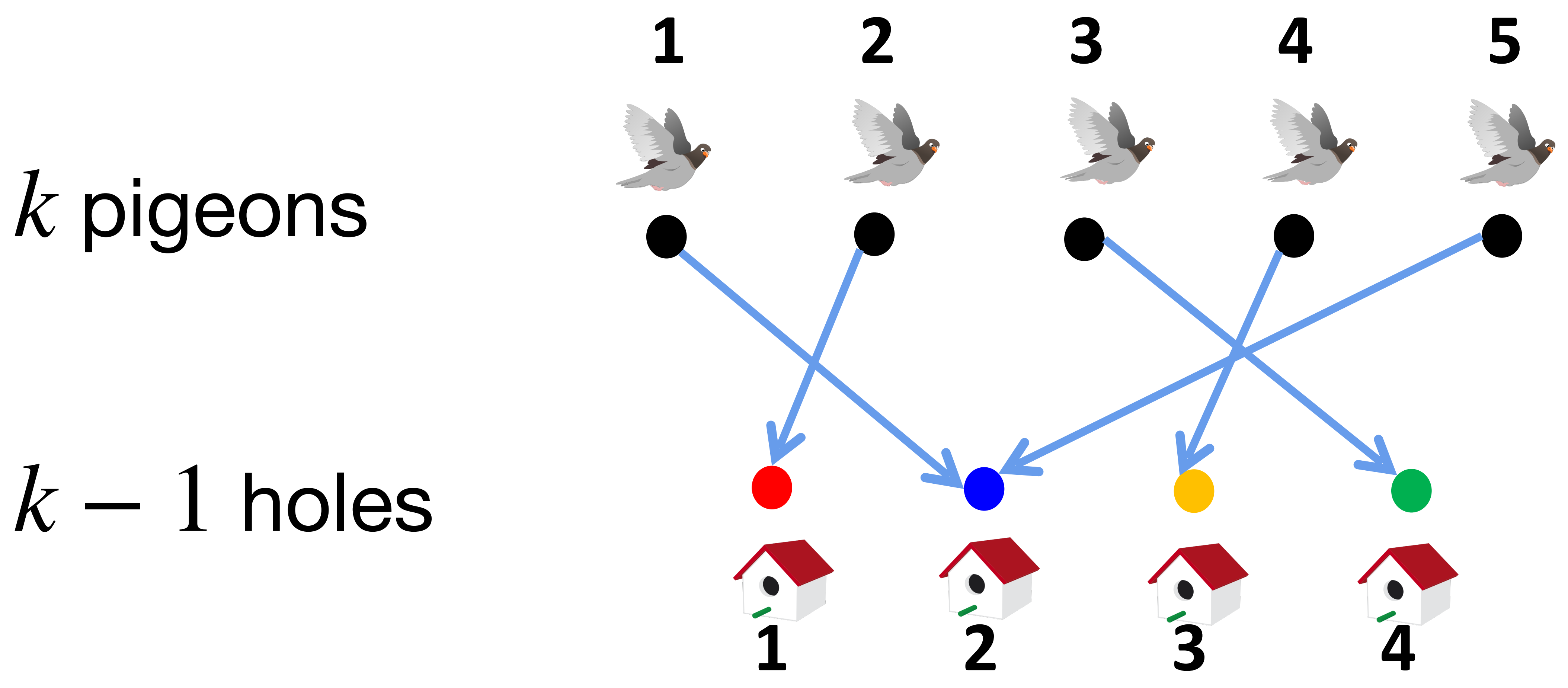
- Best lower bound for ***monotone circuits/formulas*** for f in NP? And for f in P?
  - And for f in AC^i or NC^i?
  - Or even in AC^0? [Grigni and Sipser '92]

NC^i = poly-size depth-$O(\log^i n)$ fan-in 2 circuits
AC^i = poly-size depth-$O(\log^i n)$ unbounded fan-in circuits

- Best **separations** for:
  - Monotone formulas and monotone circuits
  - Monotone AC^i and NC^i, for different levels i
- Does it make sense to consider monotone circuits of ***(supercritical) depth*** $> n$? Are they stronger than monotone circuits of depth $\leq n$?
- What is the complexity of functions like: st***-connectivity, perfect matching, clique?***

* *We will not talk about other monotone model of computations (such as monotone span programs)*

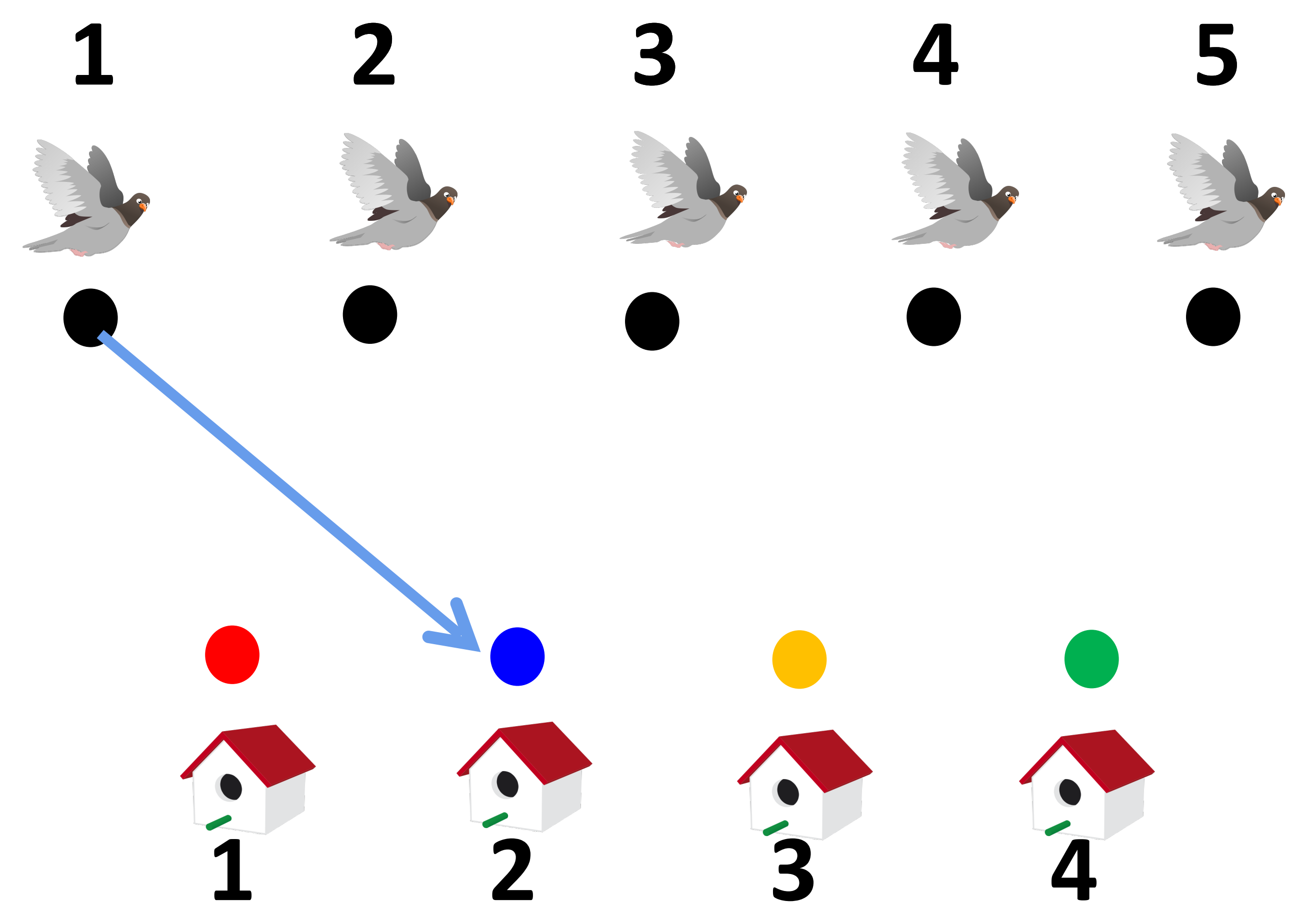
Warm Up: Find a Collision Problem



Warm Up: Find a Collision Problem

k pigeons

$k-1$ holes



- Ask where any pigeons flies and write it on the blackboard (1 line)
- How many queries until guaranteed to find collision?
- Allow you to erase: how many lines need to have (simultaneously) to find collision?

Plan

After Jukna's 2012 book: "Boolean Function Complexity: Advances and Frontiers"

Part I: Classical results

- 1985: exponential lower bounds
- 1990: Karchmer-Wigderson game for depth
- 1997: Raz-McKenzie lifting theorem for depth

Part II: Recent results

- More lower bounds
- 2017: Karchmer-Wigderson game for size
- 2018: Lifting theorem for size
- 2019-2025: Improvements and consequences

- Open problems

Part I: Classical results

Exponential Lower Bounds for Monotone Circuits

- Until 1985: only linear lower bounds for both monotone and non-monotone
- $n^{\Omega(\log n)}$-size lower bound for **clique** and **perfect matching** [Razborov '85]
- $\exp(\Omega(n^{\epsilon}))$-size lower bound for ***Andreev function*** [Andreev '85]

independent

Lower bound for f in P

- Improved above to: [Alon and Boppana '87]
  - $n^{\Omega(\sqrt{k})}$ lower bound for k-**clique** for $k \leq n^{2/3}$
  - $\exp\left(\tilde{\Omega}(n^{1/4})\right)$ lower bound for **Andreev function**

Common: approximation method

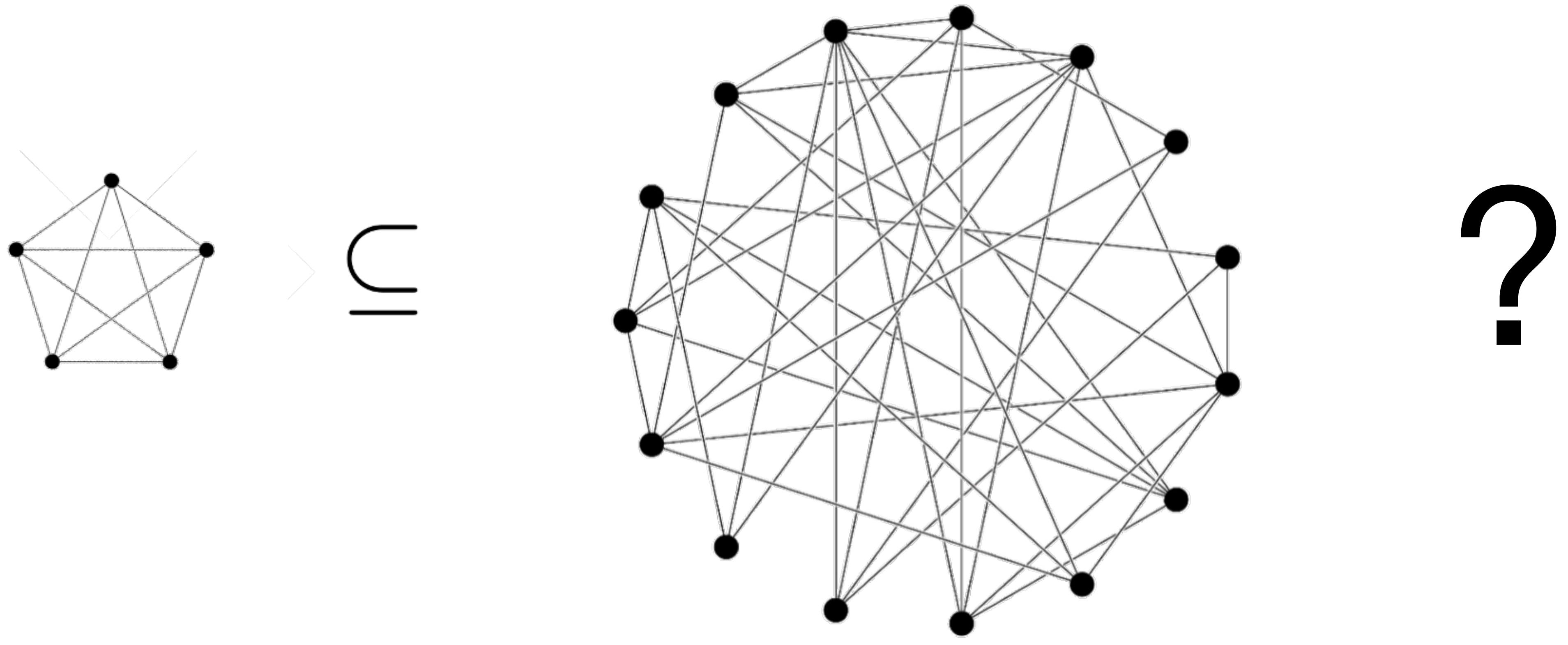
Lower bound for f in NP

- $\exp\left(\tilde{\Omega}(n^{1/3})\right)$ lower bound for **Andreev function** [Andreev '87]

Best known until 2020

A Famous NP-hard Graph Problem: Clique

- Does G have a clique of size k?



- Brute-force: time $n^{O(k)}$
- Requires $n^{\Omega(k)}$ assuming ETH [Impagliazzo, Paturi '01, Chen, Huang, Kanj, Zia '04]

Another Famous NP-Hard Graph Problem: Colouring

- Is there a proper colouring of vertices of G with c colours?
- G cannot have a k-clique and be $(k-1)$-colourable: how hard to distinguish?

$$\text{Clique-Col}_k(G) := \begin{cases} 1 & \text{if } G \text{ has a } k\text{-clique,} \\ 0 & \text{if } G \text{ is } (k-1)\text{-colorable,} \\ * & \text{otherwise.} \end{cases}$$

- This is in P (because Lovász ϑ function is in P and distinguishes)
- [Razborov '85, Alon and Boppana '87]: also applies for clique-colouring
- $\exists$ monotone function that distinguishes [Tardos '88]

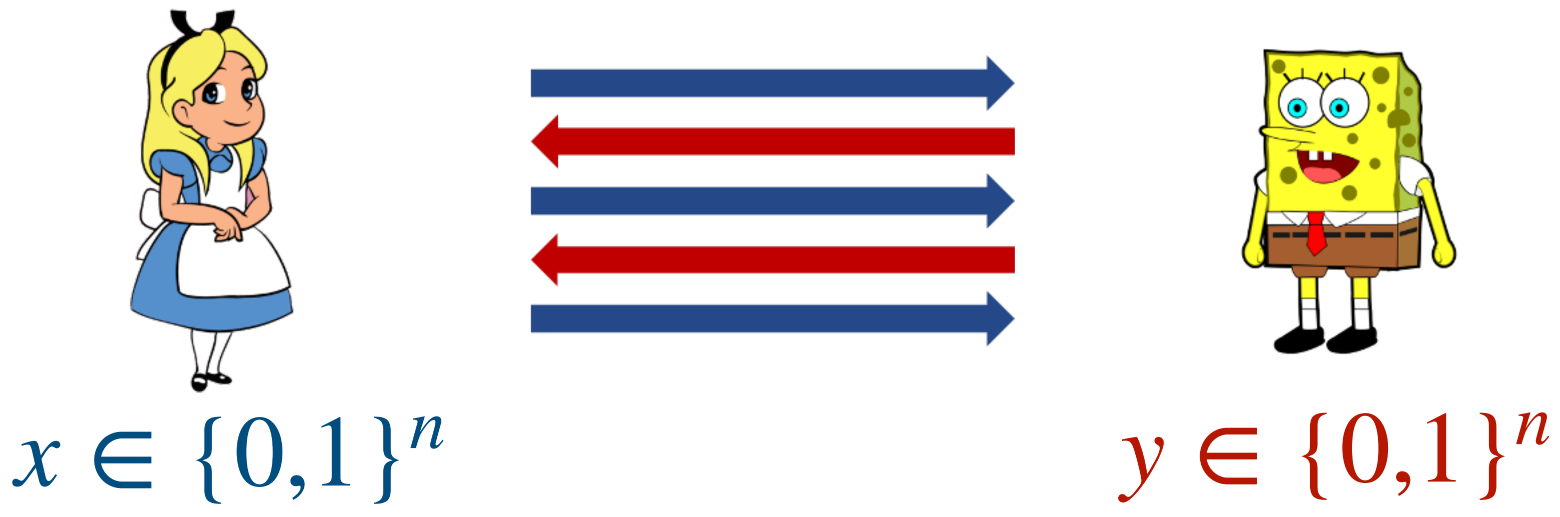
Lower bound for f in P: $\exp(\tilde{\Omega}(n^{1/6}))$

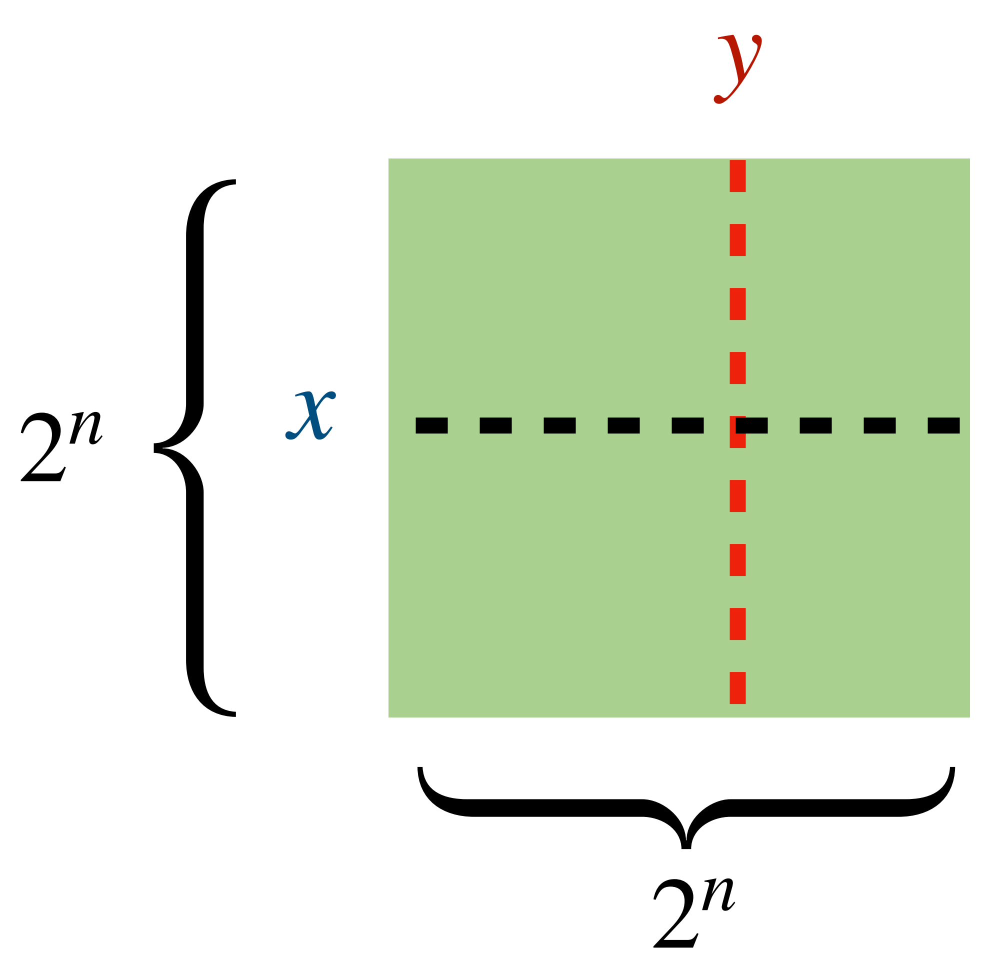
Best known until 2025

Communication complexity

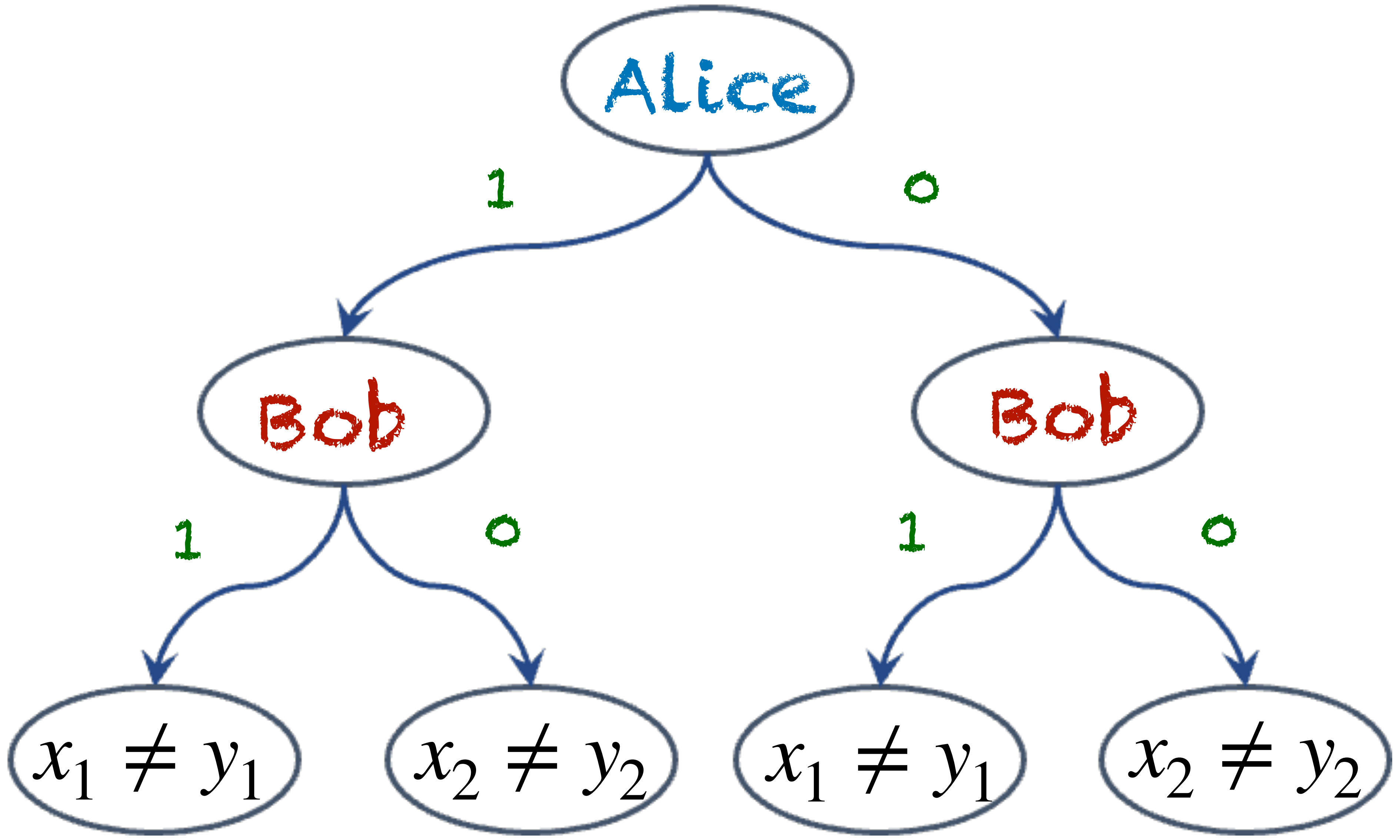
understanding circuit depth

Game: Find a Differing Bit

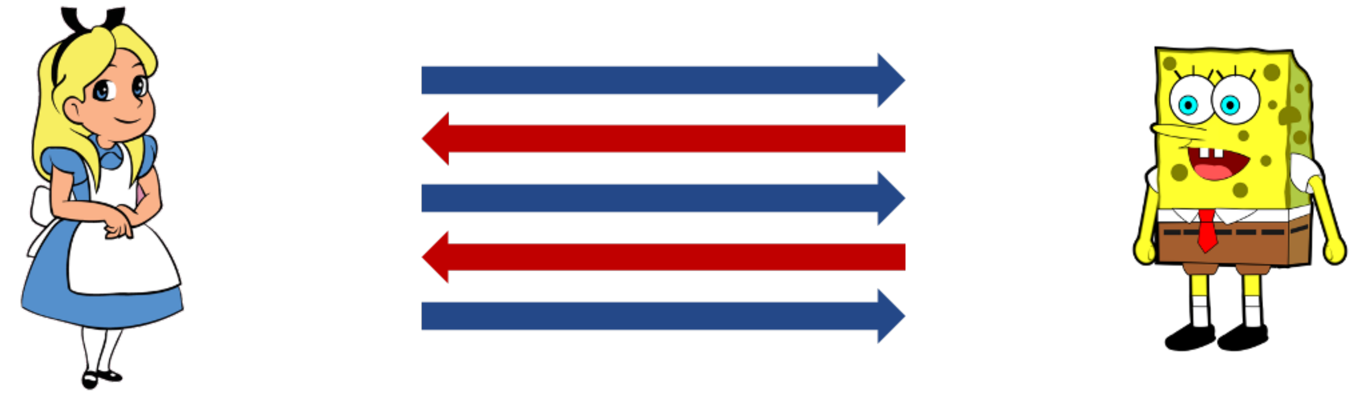




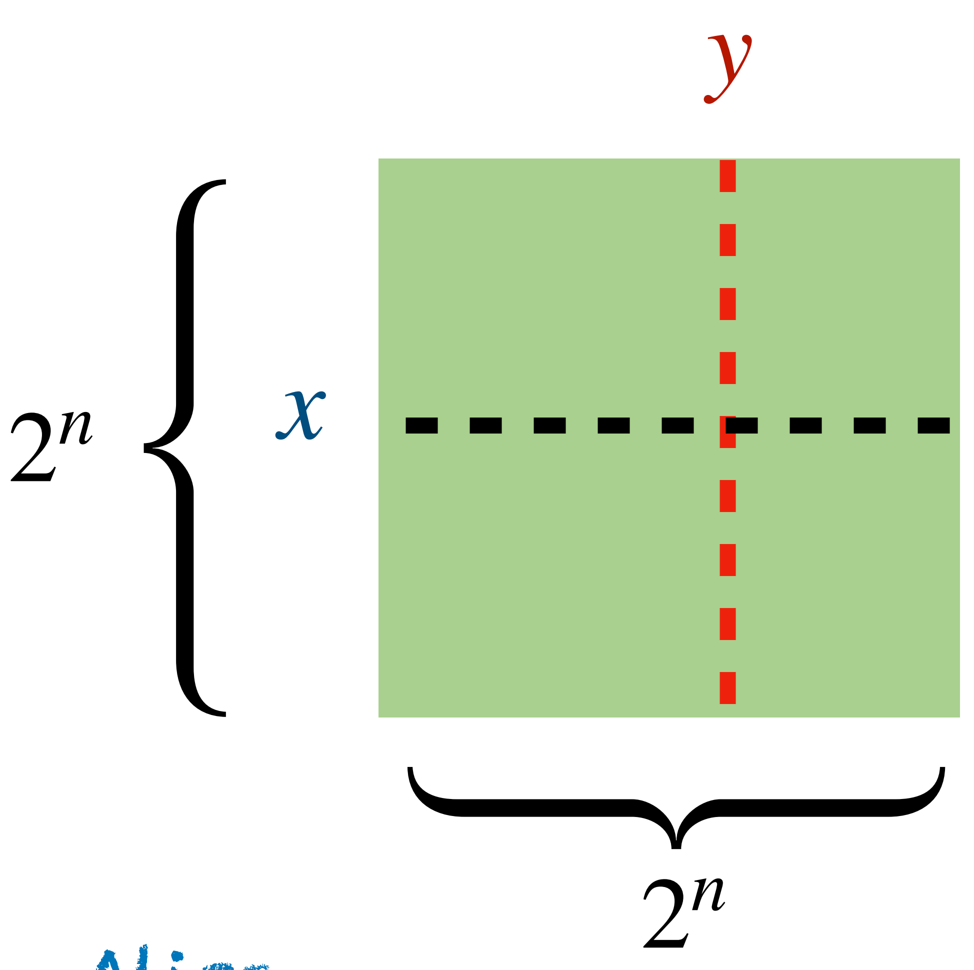
- Goal: communicate min # bits to find i s.t. $x_i \neq y_i$
- Before seeing input, decide communication protocol:
  - "strategy tree": who speaks when, what message means



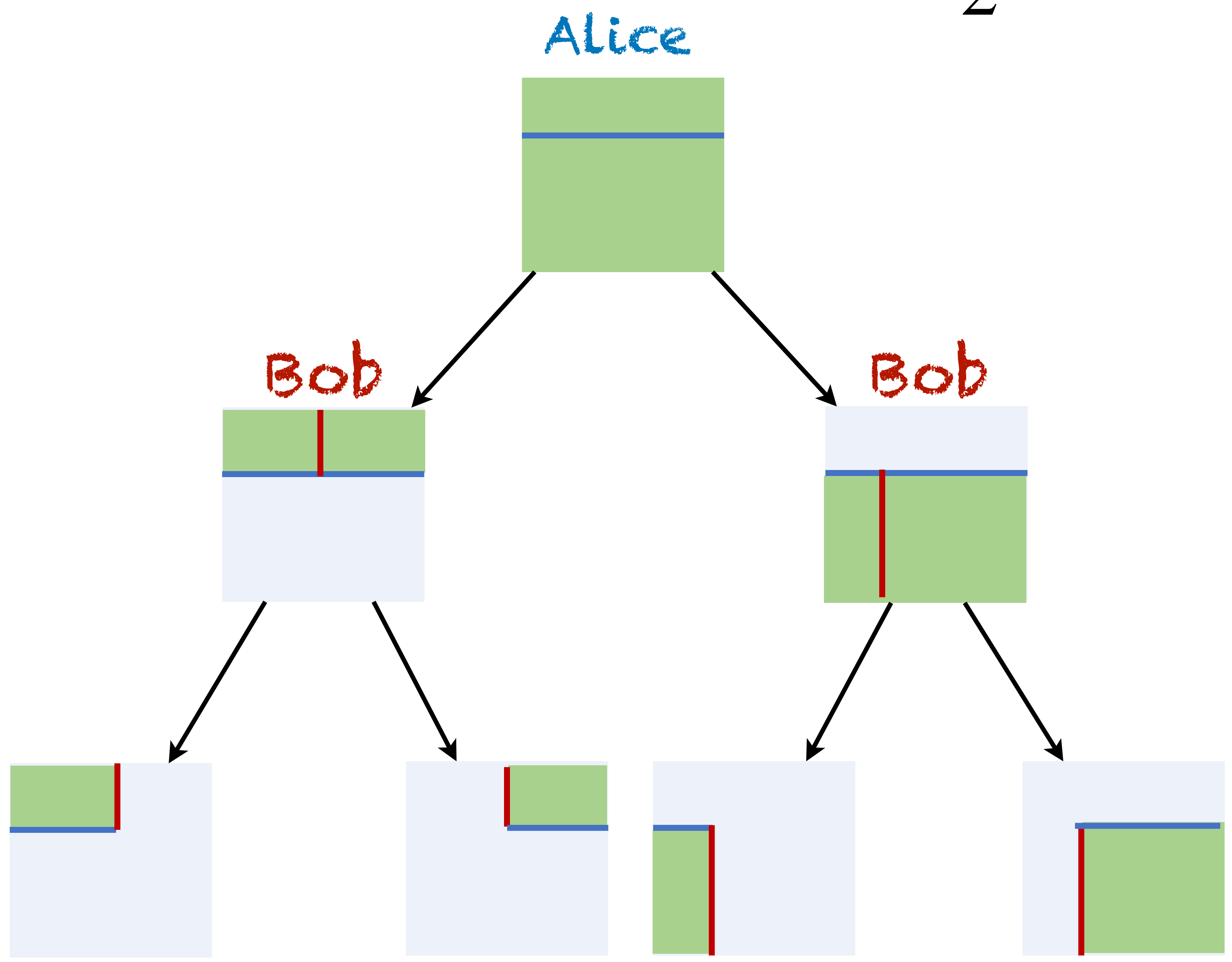
Game: Find a Differing Bit



$x \in \{0,1\}^n$ $y \in \{0,1\}^n$

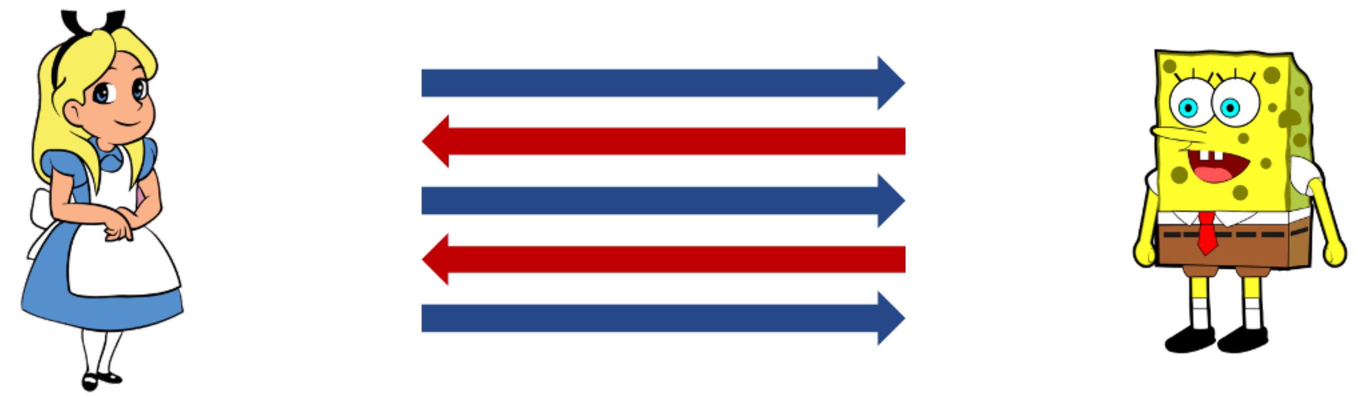


- Goal: communicate min # bits to find i s.t. $x_i \neq y_i$
- Before seeing input, decide communication protocol:
  - “strategy tree”: who speaks when, what message means
- Worst-case: how many bits?



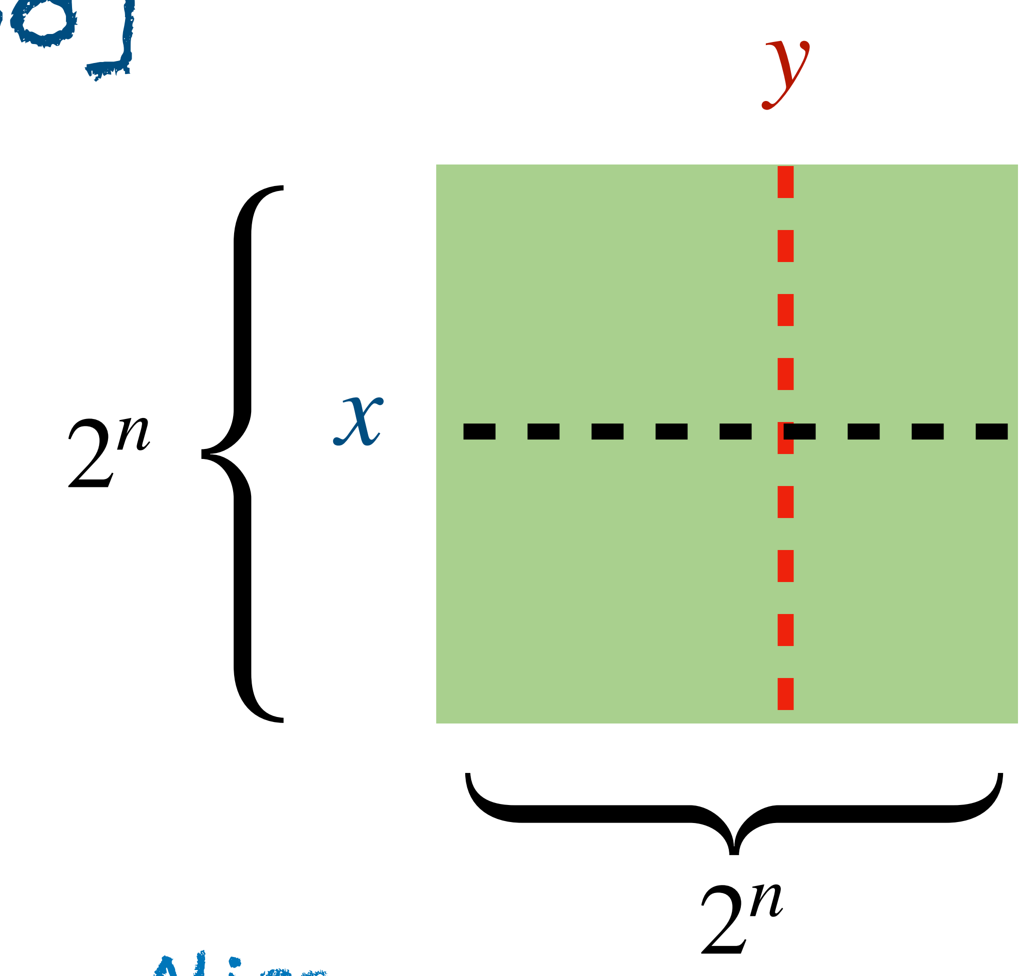
Karchmer-Wigderson game KW(f) [KW'90]

- Given f

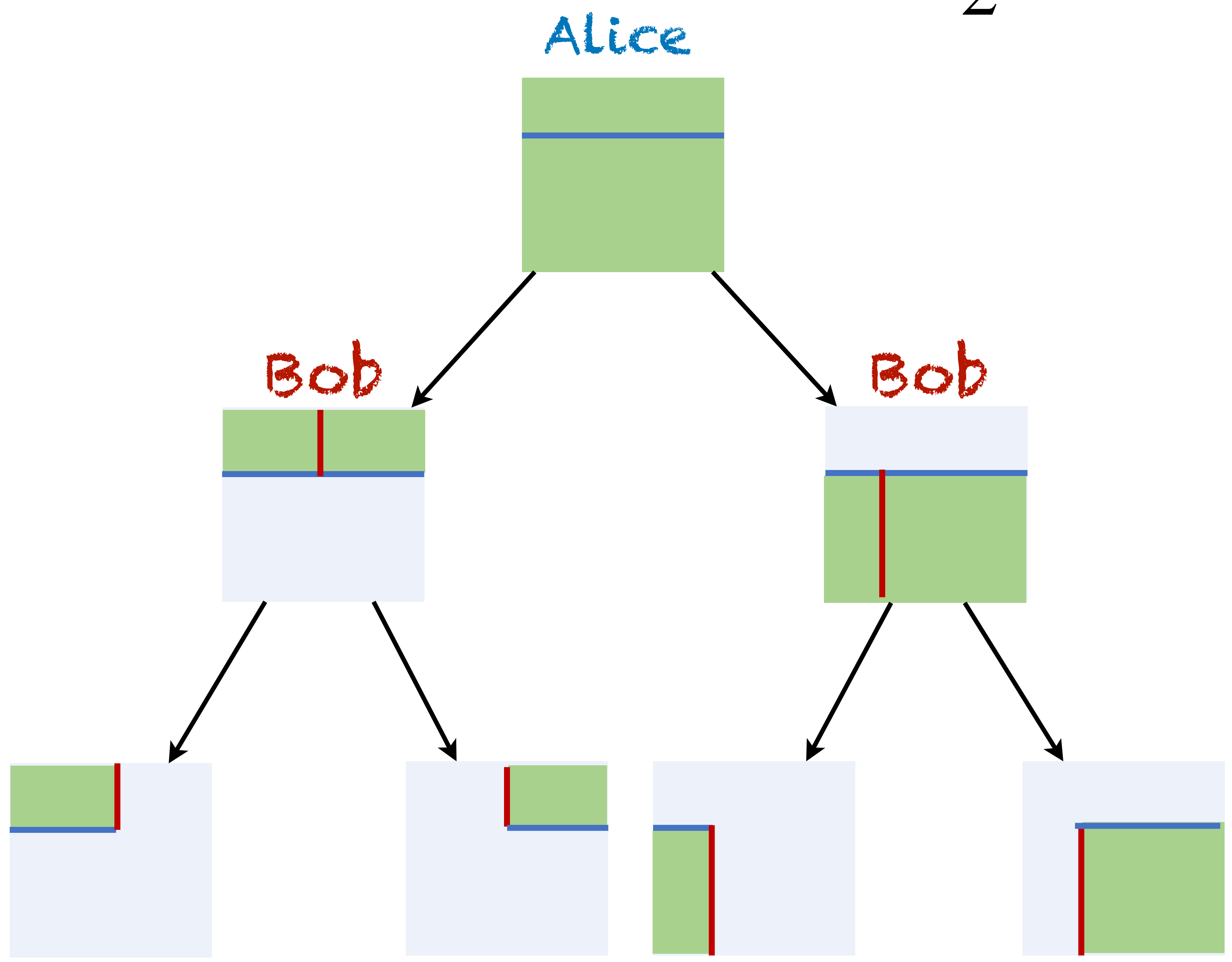


$x \in \{0,1\}^n$ $\quad$ $y \in \{0,1\}^n$

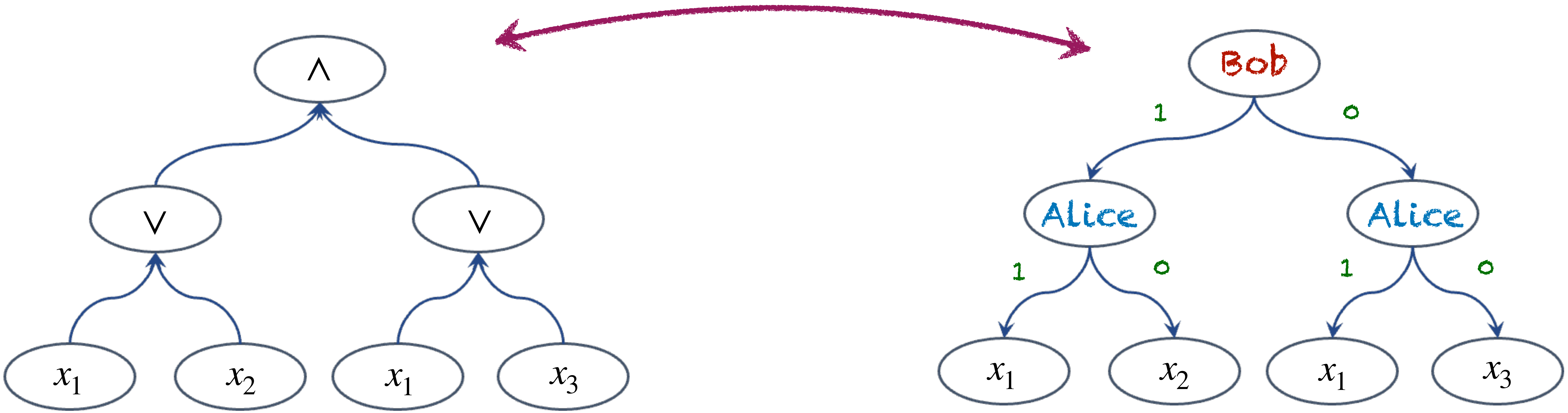
$x \in f^{-1}(1)$ $\quad$ $y \in f^{-1}(0)$



- Goal: communicate min # bits to find i s.t. $x_i \neq y_i$
- Before seeing input, decide communication protocol:
  - "strategy tree": who speaks when, what message means
- Worst-case: how many bits?



Formulas = communication protocols



∃ depth-d formula computing f ⇔
∃ depth-d communication protocol for KW(f)

[KW'90]

- Result is stronger: really the same object (even graph structure is preserved)

Monotone Karchmer-Wigderson game [KW'90]

- KW(f) : given $x \in f^{-1}(1), y \in f^{-1}(0)$ **find i s.t. $x_i \neq y_i$**

i.e. $x \geq y \Rightarrow f(x) \geq f(y)$

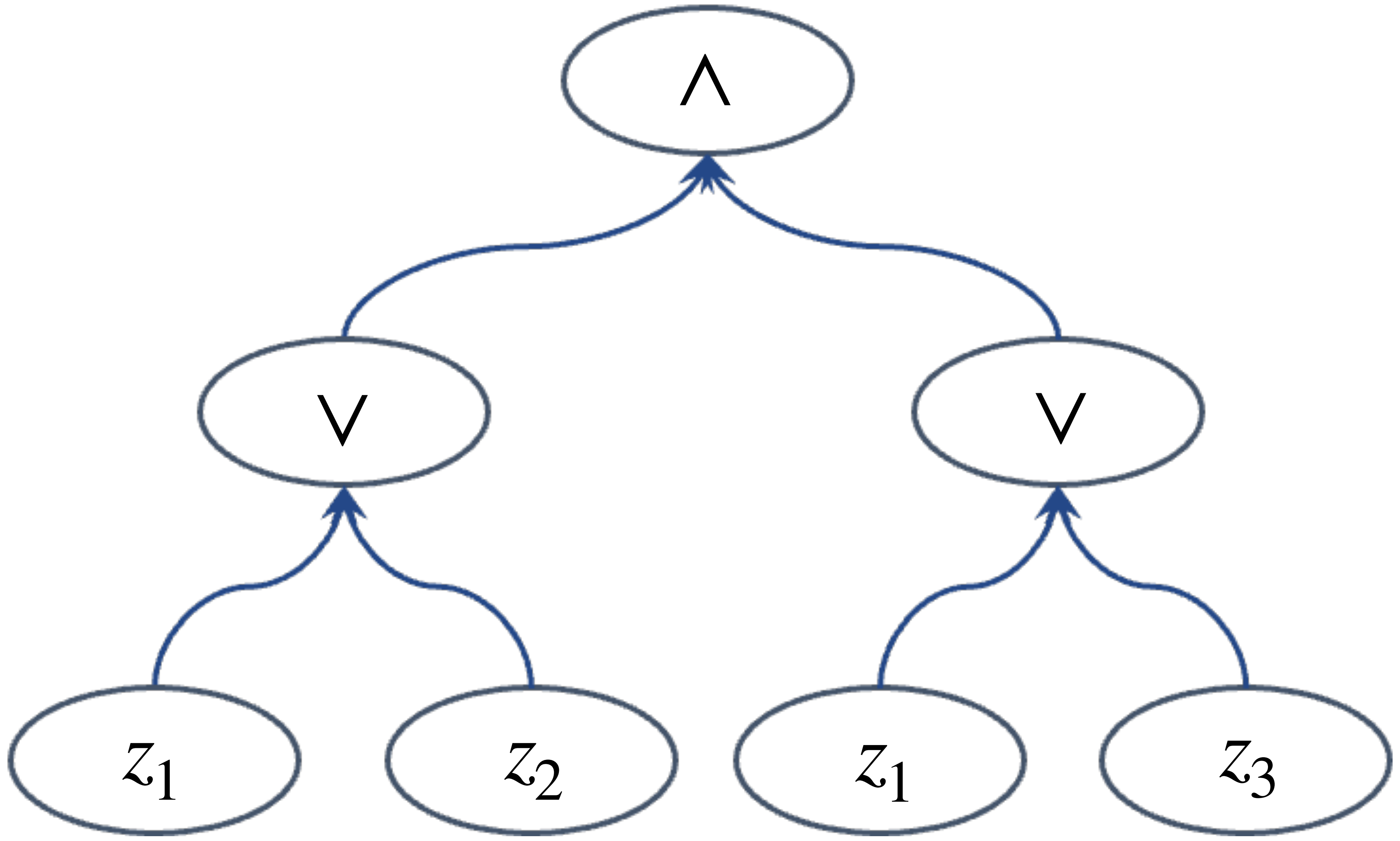
- For f monotone, mKW(f) *harder* problem: **find i s.t. $x_i > y_i$**

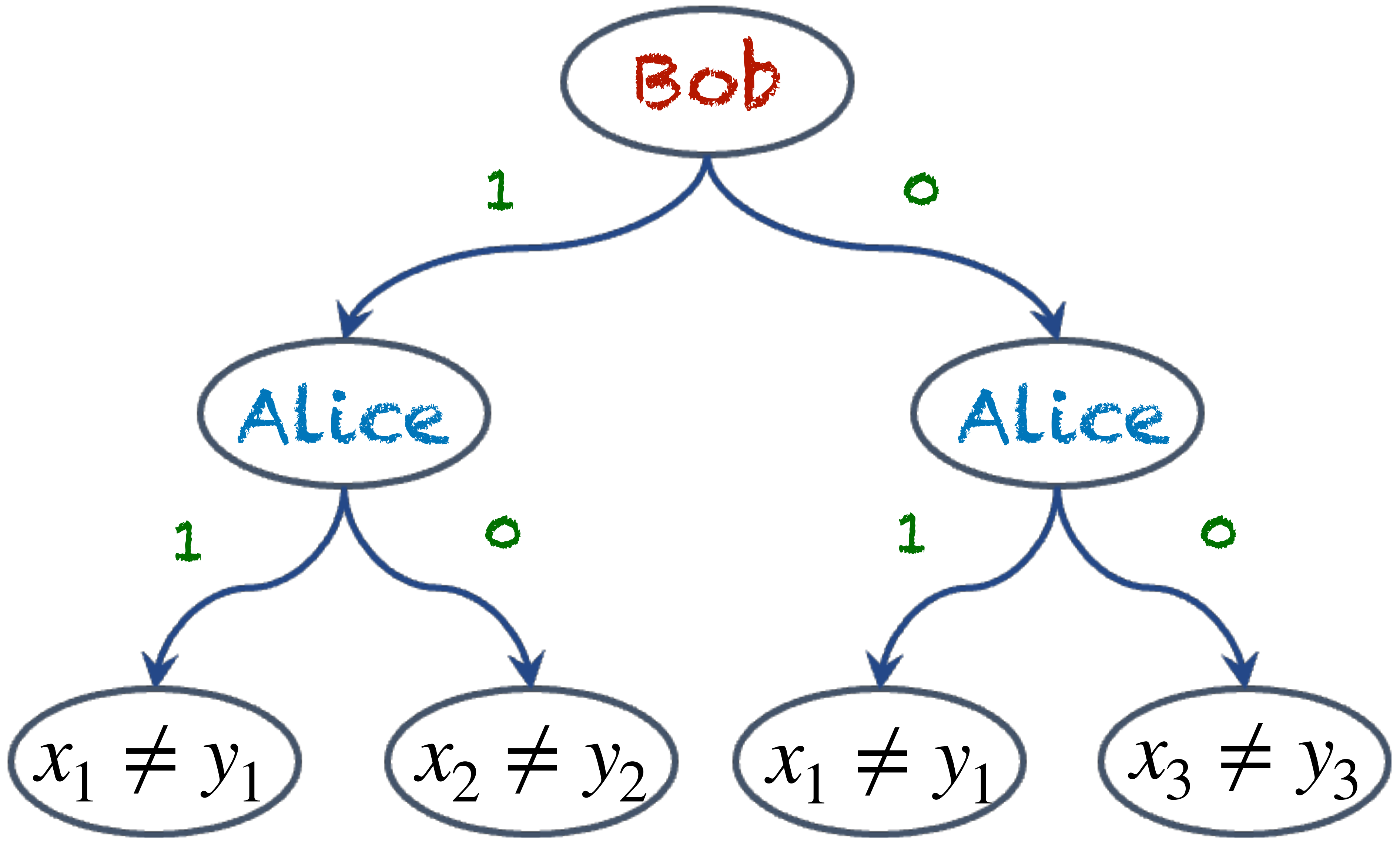
∃ depth-d monotone formula computing f ⇔
∃ depth-d communication protocol for mKW(f)

Example: f = majority

- $x = (1,1,0,1,0)$
- $y = (0,1,1,0,0)$
- 1,3,4 valid answer for KW(f)
- 1,4 valid for mKW(f) but not 3

Formulas = communication protocols

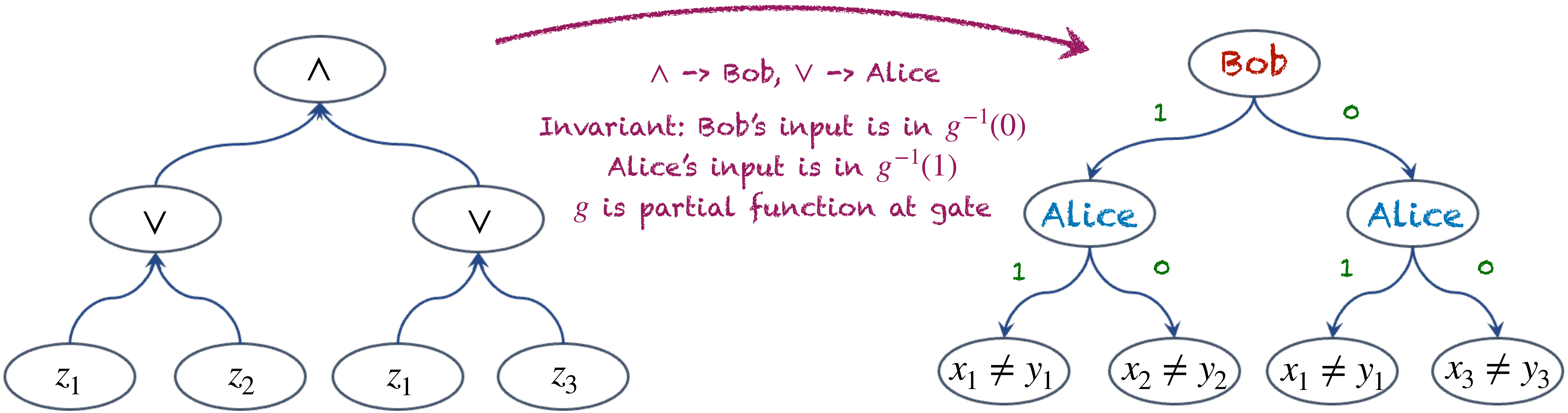




$\exists$ depth-d (monotone) formula computing $f \Leftrightarrow$
$\exists$ depth-d protocol for (monotone) KW(f)

[KW'90]

Formulas = communication protocols

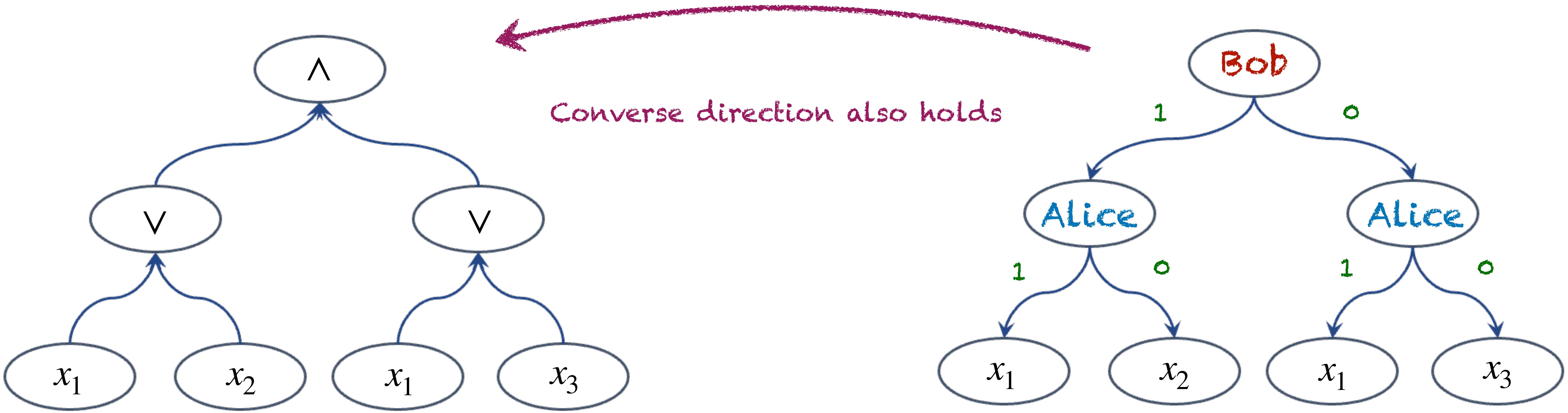


$\exists$ depth-d (monotone) formula computing $f \Leftrightarrow$
$\exists$ depth-d protocol for (monotone) KW(f)

[KW'90]

- Result is stronger: really the same object (even graph structure is preserved)

Formulas = communication protocols



$\exists$ depth-d (monotone) formula computing $f \Leftrightarrow$
$\exists$ depth-d protocol for (monotone) KW(f)

[KW'90]

- Result is stronger: really the same object (even graph structure is preserved)

Depth lower bound for st-connectivity [KW'90]

- Framework used for $\Omega(\log^2 n)$ depth lower bound for st-connectivity
- Separates mon-NC^1 and mon-NC^2
- KW(f) is a *total search problem*
  - Total search problem S $\subseteq I \times O$ s.t. $\forall z \in I \;\; \exists o \in O : (z, o) \in$ S
  - KW$(f) \subseteq \left(f^{-1}(1) \times f^{-1}(0)\right) \times [n]$

Raz-McKenzie: Lifting Theorem [RM '97]

- Idea: sometimes structured protocols (communicates bits of input) are best possible
  - $\exists$ special gadget $g : X \times Y \to \{0,1\}$
  - $\forall$ total search problem $\mathsf{S} \subseteq \{0,1\}^n \times O$

given $x \in X^n$, $y \in Y^n$ find $o \in O$
s.t. $(z, o) \in \mathsf{S}$ for $z_i = g(x_i, y_i)$

If $\mathsf{S} \circ g$ requires structured protocol of depth $\geq c \Rightarrow$
any protocol for $\mathsf{S} \circ g$ has depth $\Omega(c)$

- Structured protocol for $\mathsf{S} \circ g$ can only simulate decision trees for S

depth-d decision tree lower bound for $\mathsf{S} \Rightarrow$
depth-$\Omega(d \log n)$ communication protocol lower bound for $\mathsf{S} \circ g$

Raz-McKenzie: Lifting Theorem [RM '97]

- What does this have to do with circuits? mKW is universal for total search problems

depth-d decision tree lower bound for S $\Rightarrow$
depth-$\Omega(d \log n)$ monotone circuit lower bound for f_{S}

S	f_{S}
Induction Principle	st-connectivity
Pebbling	Generation
Find collision	Clique

Depth lower bound for f in mP
$\exp(\Omega(n^{\epsilon}))$

- reproved depth-$\Omega(\log^2 n)$ for st-connectivity
- separated mon-NC^i and mon-NC^{i+1}
- depth-$\Omega(k \log n)$ for k-clique for $k \leq n^{\epsilon}$

Part II: Recent developments

Monotone depth lower bounds

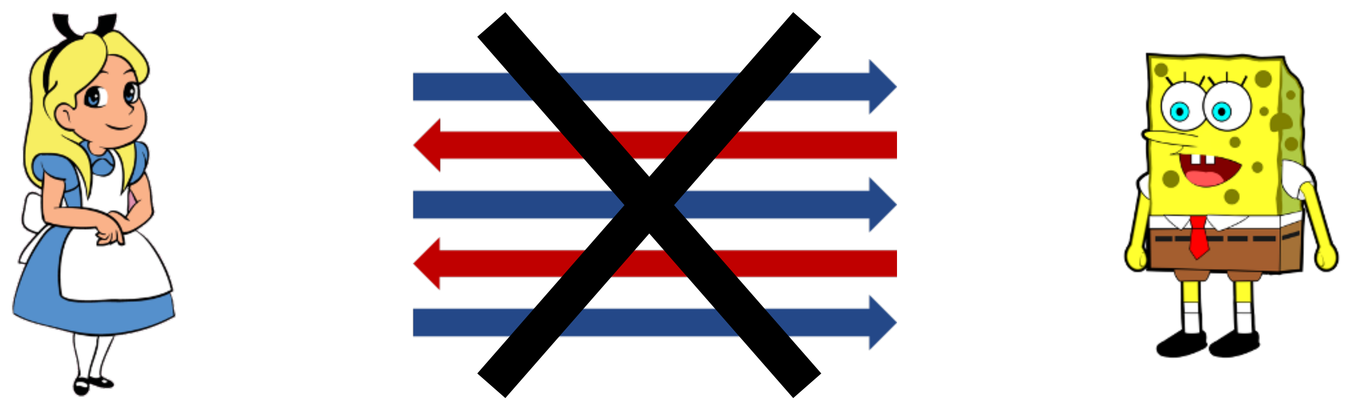
- For function in NP: $\Omega(n)$ [Pitassi, Robere '17]
  - $\Omega(n/\log n)$ [Göös, Pitassi '14], previously $\Omega(\sqrt{n})$ [Raz, Wigderson '90]
- For function in mP: $\Omega(n/(\log^{O(1)} n))$ [dR, Meir, Nordström, Pitassi, Robere, Vinyals '20]
  - $\Omega(\sqrt{n})$ [Göös, Pitassi '14], previously $\Omega(n^{\epsilon})$ [Raz, McKenzie '97]
- Bringing Raz-McKenzie to light again [Göös, Pitassi, Watson '14]
- Separated mon-AC^{i} and mon-NC^{i+1} [dR, Nordström, Vinyals '16]

DAG-like communication complexity

understanding circuit size

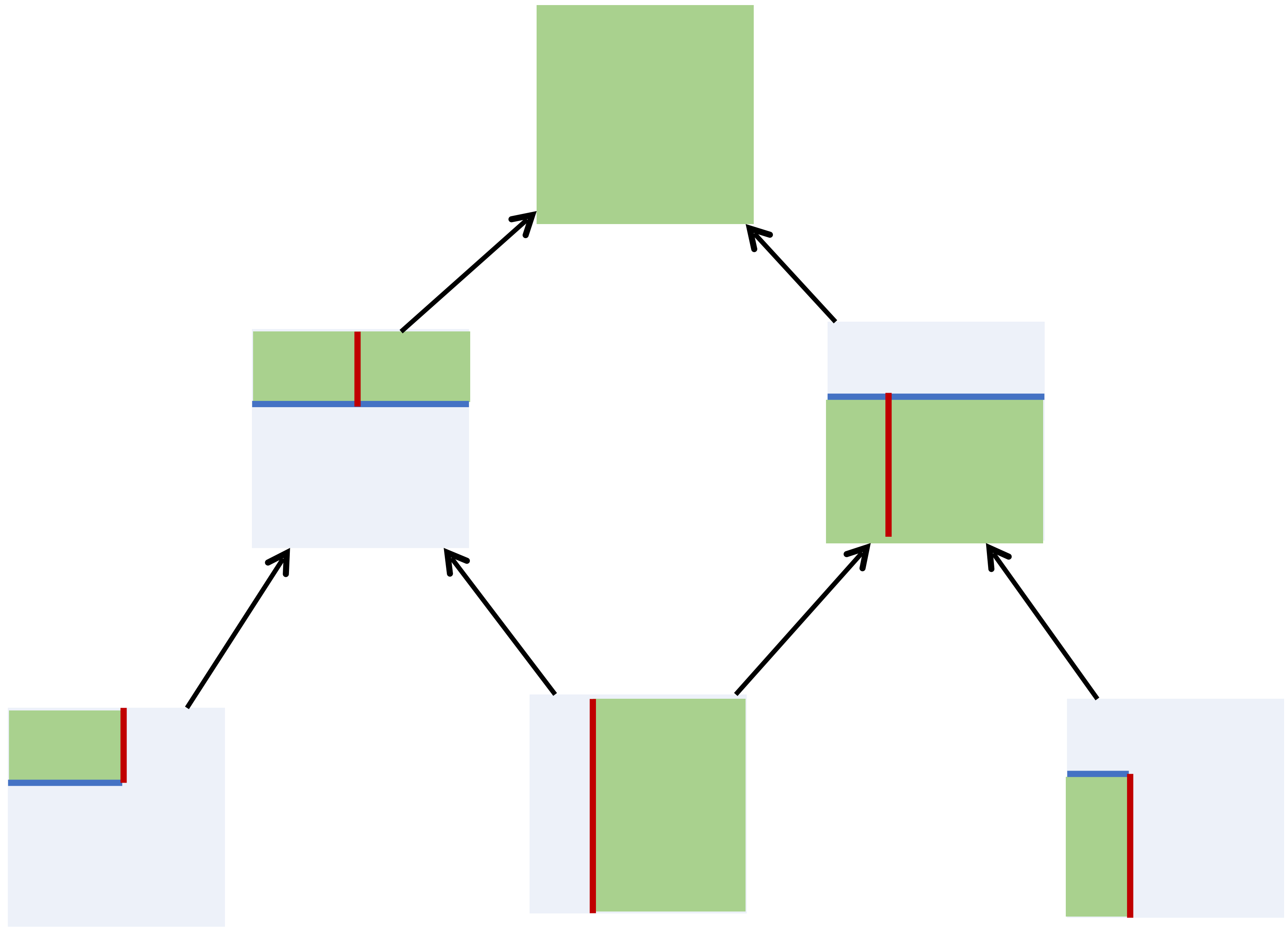
Karchmer-Wigderson for Circuits [Razborov '95, Sokolov '17]

- As before, given f



$x \in f^{-1}(1)$ $y \in f^{-1}(0)$

- Goal: find i s.t. $x_i \neq y_i$
  - Monotone case: find i s.t. $x_i > y_i$
- DAG-like protocols: *rectangle-DAGs*



Circuits = rectangle-DAGs [Razborov '95, Sokolov '17]

$\exists$ size-s (monotone) circuit computing $f \Leftrightarrow$
$\exists$ size-s rectangle-DAG for (monotone) KW(f)

- Result is stronger: really the same object (even graph structure is preserved)

Raz-McKenzie: Lifting Theorem **for Circuits**

[Garg, Göös, Kamath, Sokolov '18]

Remember "Find Collision Problem"? # lines needed when allowed to forget

width-d decision DAG lower bound for S $\Rightarrow$
size-$n^{\Omega(d)}$ monotone circuit lower bound for f_S

- Compare with [Raz, McKenzie '18]

depth-d decision tree lower bound for S $\Rightarrow$
size-$n^{\Omega(d)}$ monotone *formula* lower bound for f_S

Results for monotone circuits

- $\exp(\Omega(n^\epsilon))$-size lower bound for f in NC^2 [Göös, Kamath, Robere, Sokolov '19]
  - Follows from lifting theorem [Garg, Göös, Kamath, Sokolov '18]
- $n^{\Omega(k)}$-size lower bound for k-clique for $k \leq n^{1/2-o(1)}$
- $\exp(\tilde{\Omega}(n^{1/3}))$-size lower bound for f in P

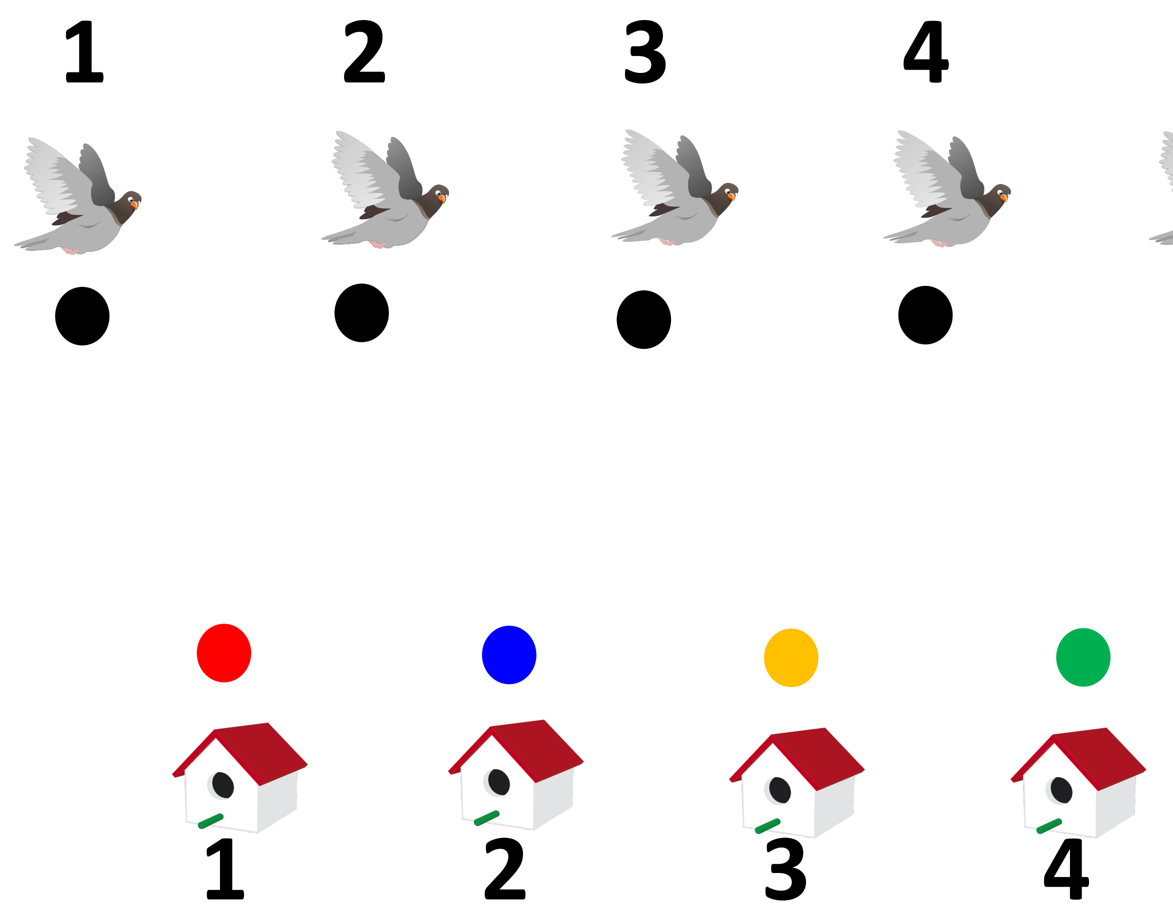
[dR, Vinyals '25] (for both results above)

  - Follows from improvement of lifting theorem [Lovett, Meka, Mertz, Pitassi, Zhang, Jiapeng '21]
  - Use simplification from [dR, Fleming, Janett, Nordström, Pang '25]

for $S \subseteq \Sigma^n \times O$, $m \gg |\Sigma| \cdot d \log(n)$

width-d decision DAG lower bound for S $\Rightarrow$
size-$m^{\Omega(d)}$ monotone circuit lower bound for S $\circ$ Ind_m

$\text{Find-collision}_k \circ \text{Ind}_m \preccurlyeq \text{mKW}(\text{Clique-Col}_{k,n=mk})$

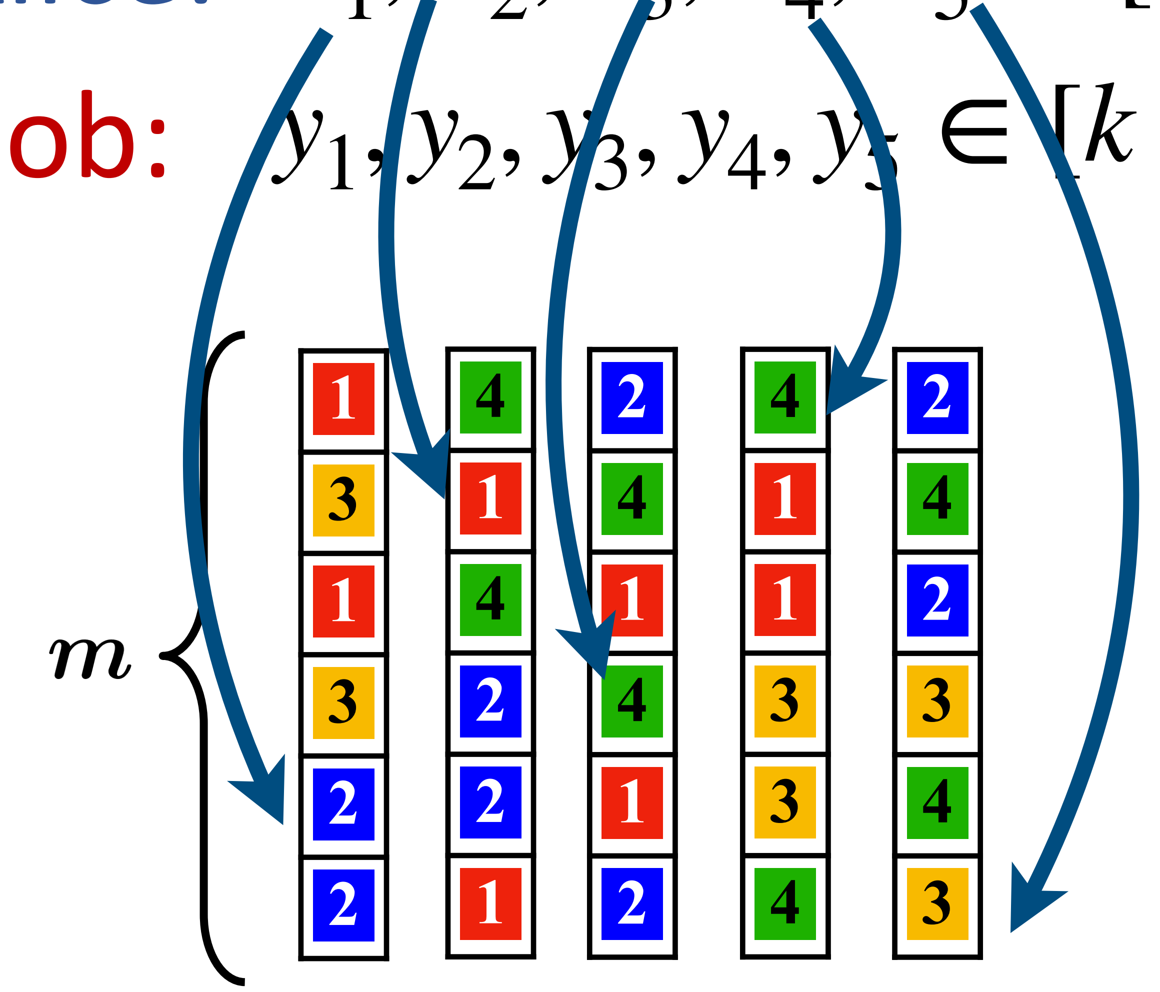


$z_i \in [k-1], \ \forall i \in n$

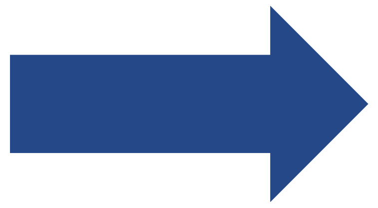
find $i \neq j$ s.t. $z_i = z_j$

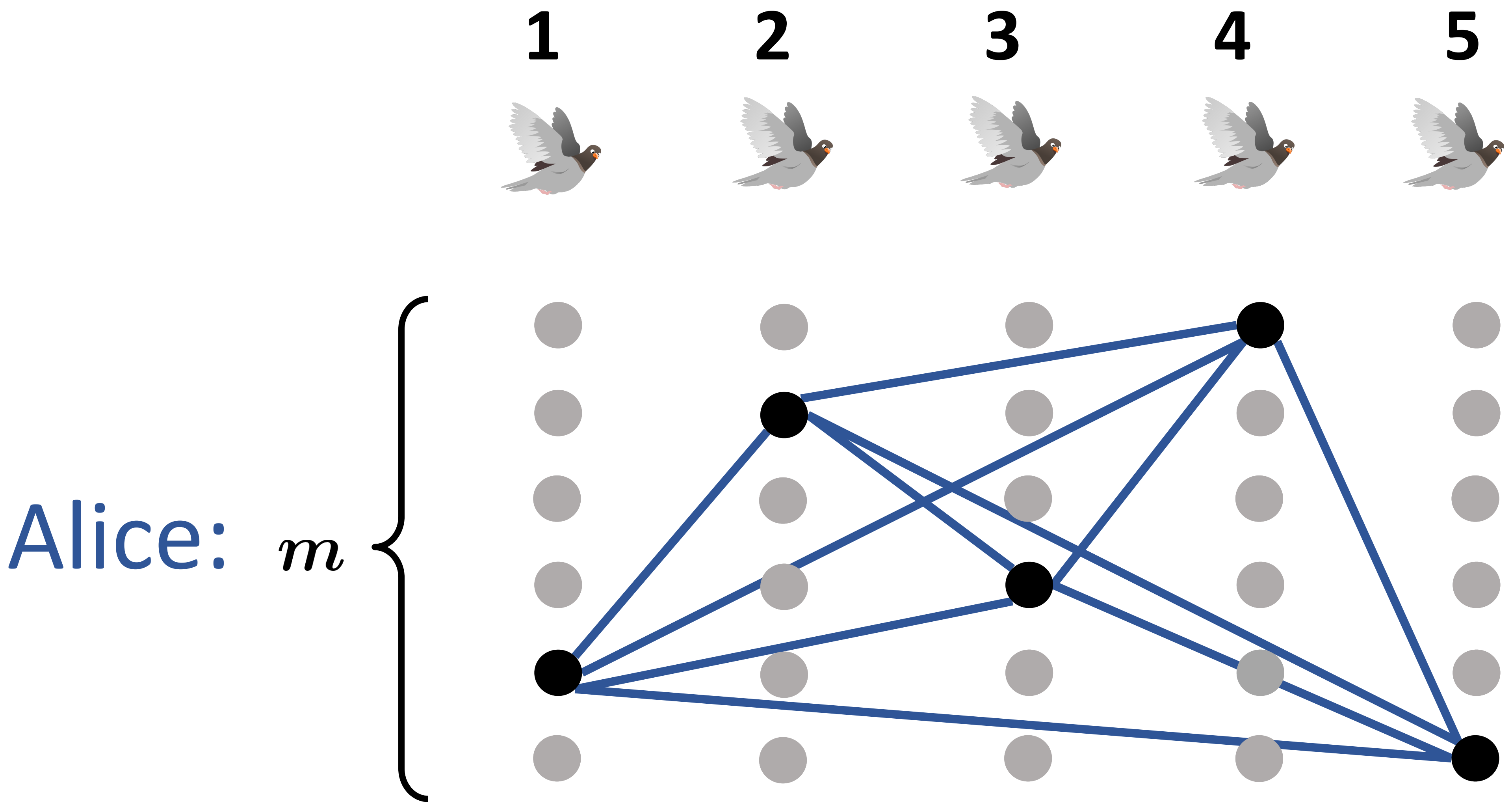
Alice: $x_1, x_2, x_3, x_4, x_5 \in [m]$

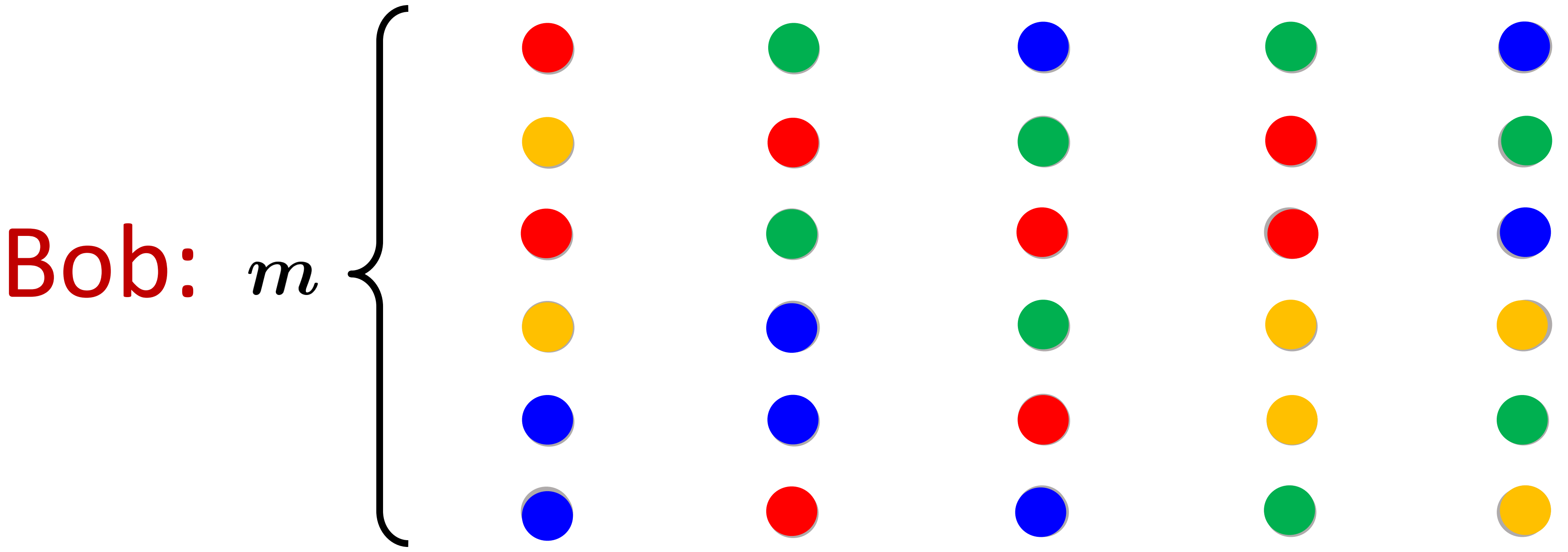
Bob: $y_1, y_2, y_3, y_4, y_5 \in [k-1]^m$



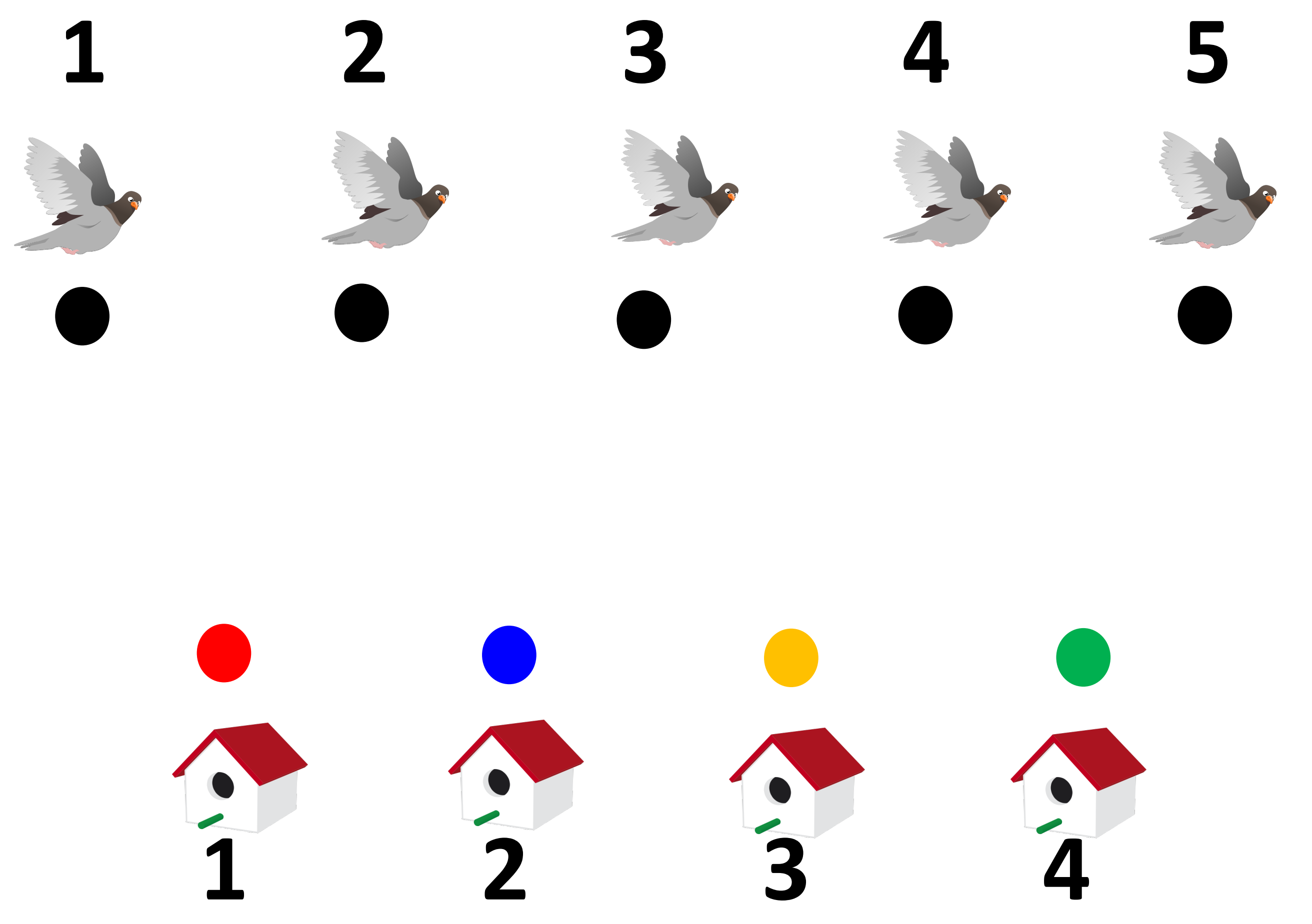
find $i \neq j$ s.t. x_i and x_j point to same number







Find-collision$_k \circ \mathrm{Ind}_m \preccurlyeq$ mKW(Clique-Col$_{k,n=mk}$)

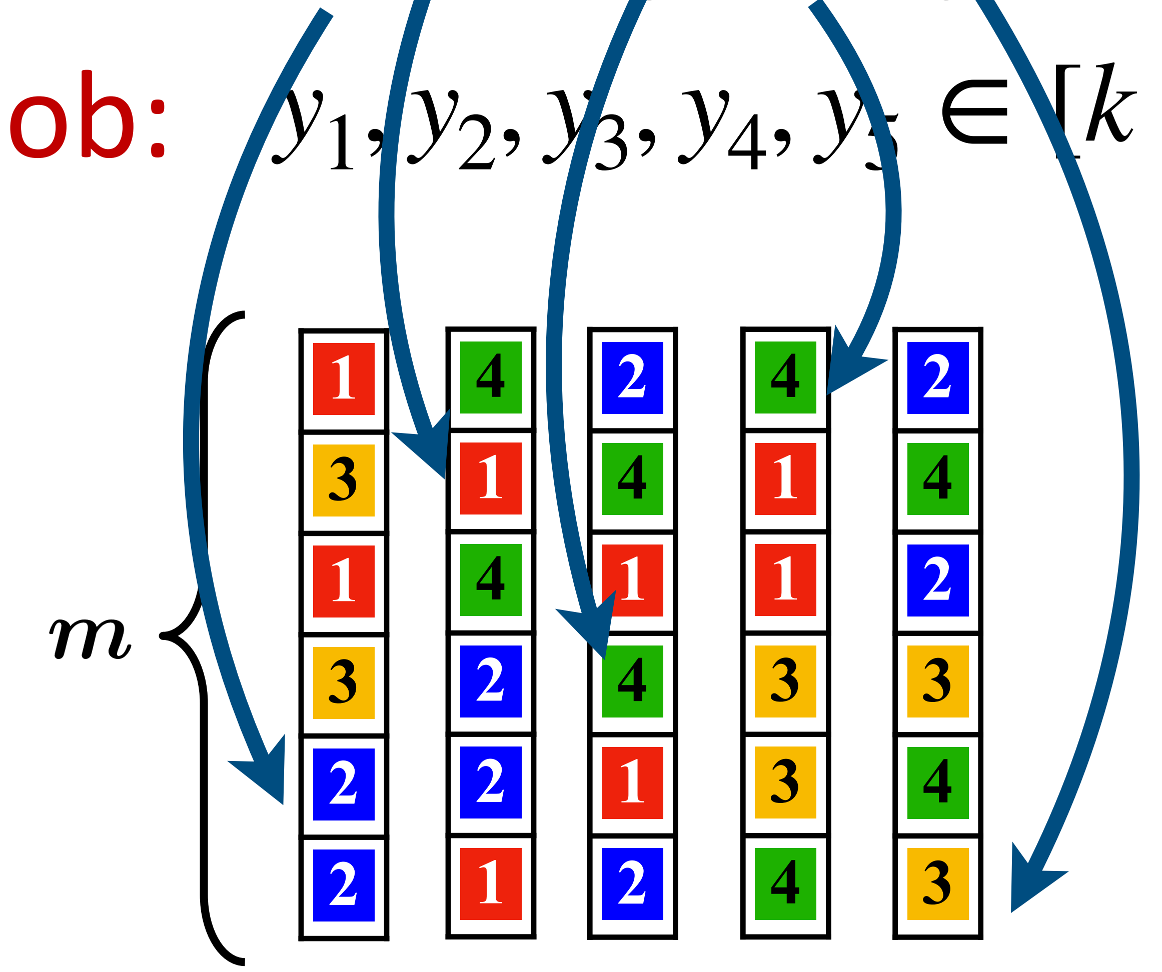


$z_i \in [k-1], \ \forall i \in n$

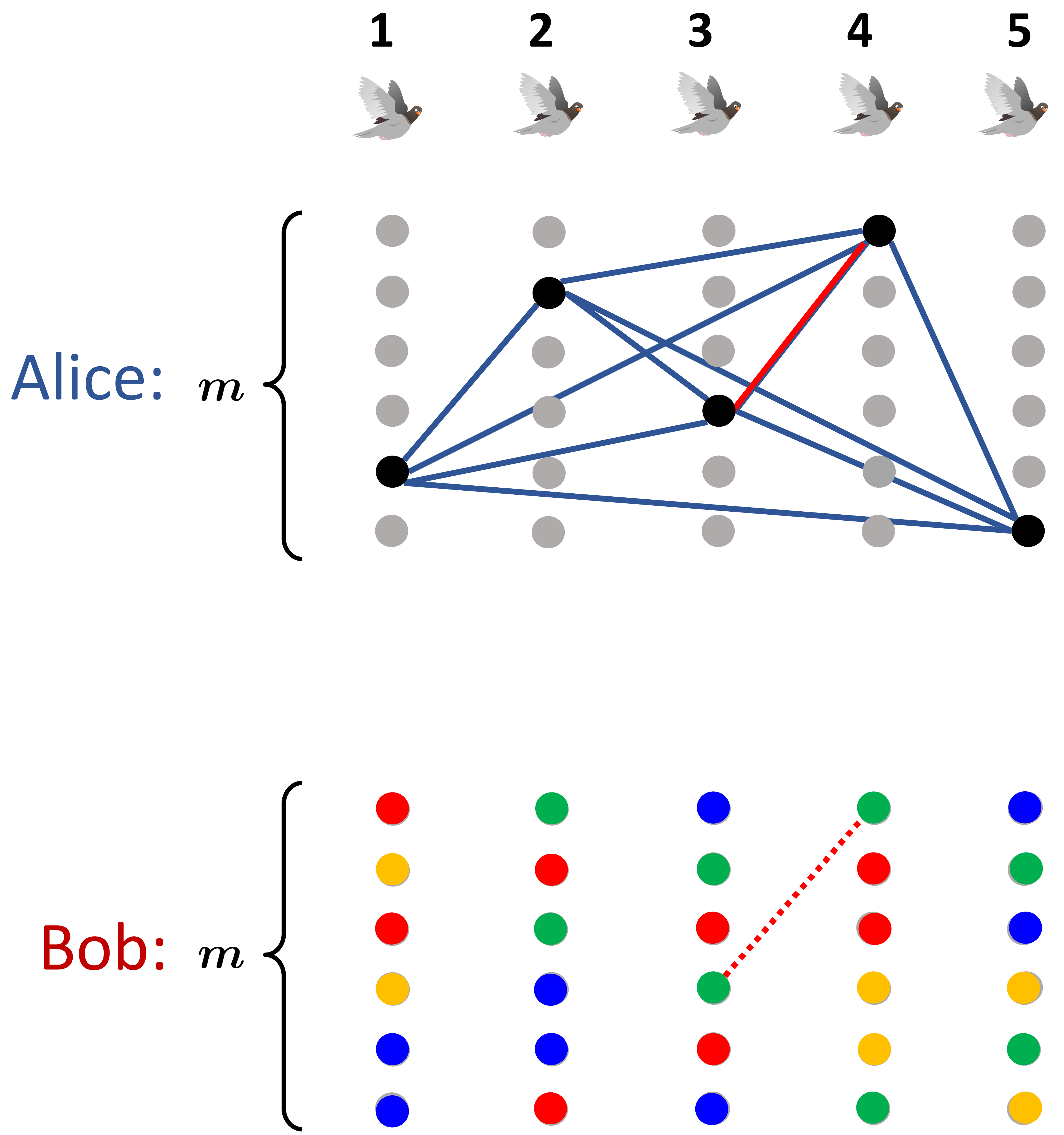
find $i \neq j$ s.t. $z_i = z_j$

Alice: $x_1, x_2, x_3, x_4, x_5 \in [m]$

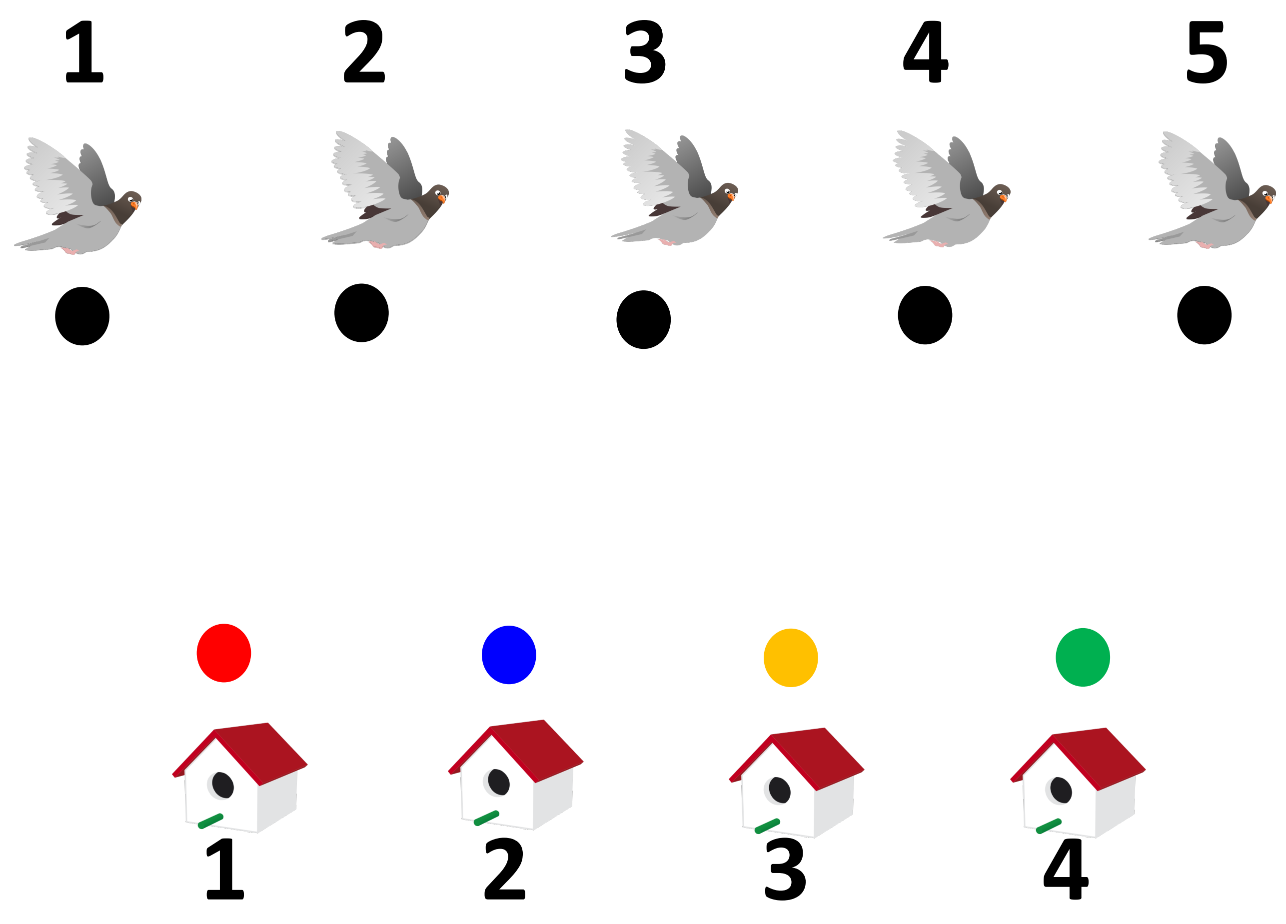
Bob: $y_1, y_2, y_3, y_4, y_5 \in [k-1]^m$



find $i \neq j$ s.t. x_i and x_j point to same number



Find-collision$_k \circ \text{Ind}_m \preccurlyeq$ mKW(Clique-Col$_{k,n=mk}$)

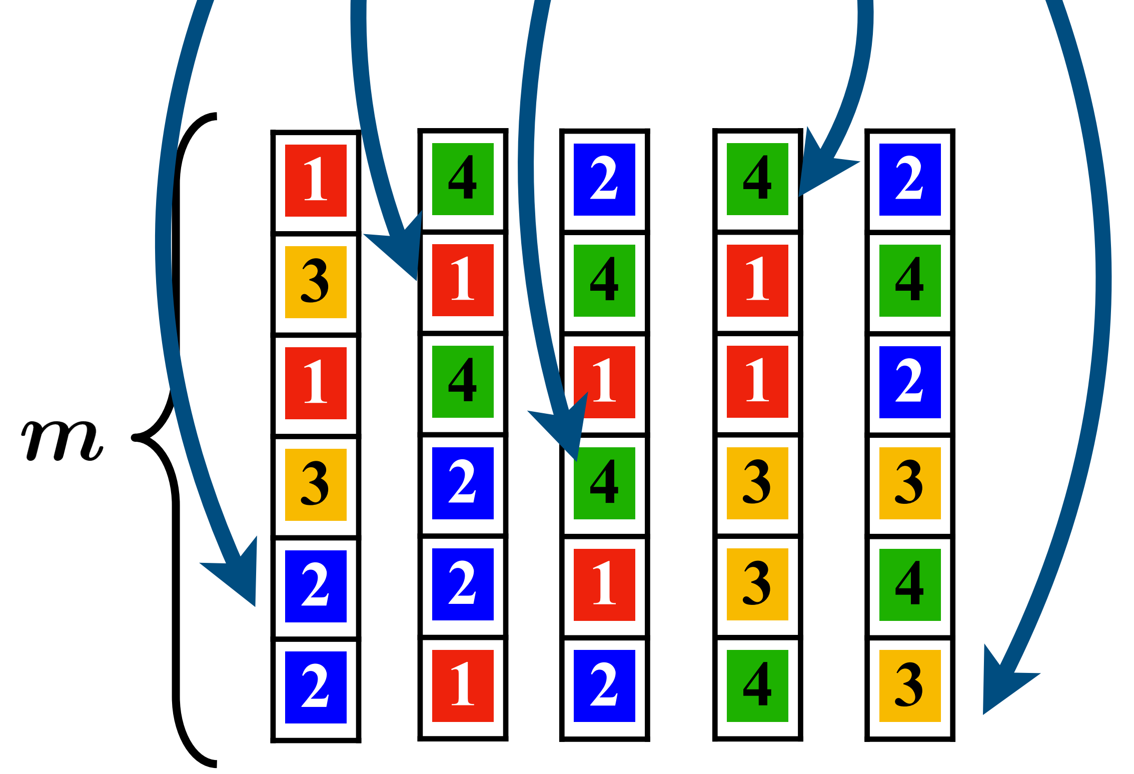


$z_i \in [k-1], \ \forall i \in n$

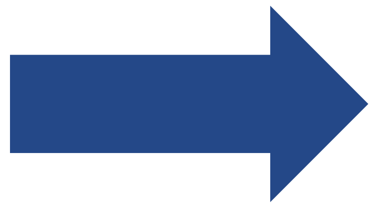
find $i \neq j$ s.t. $z_i = z_j$

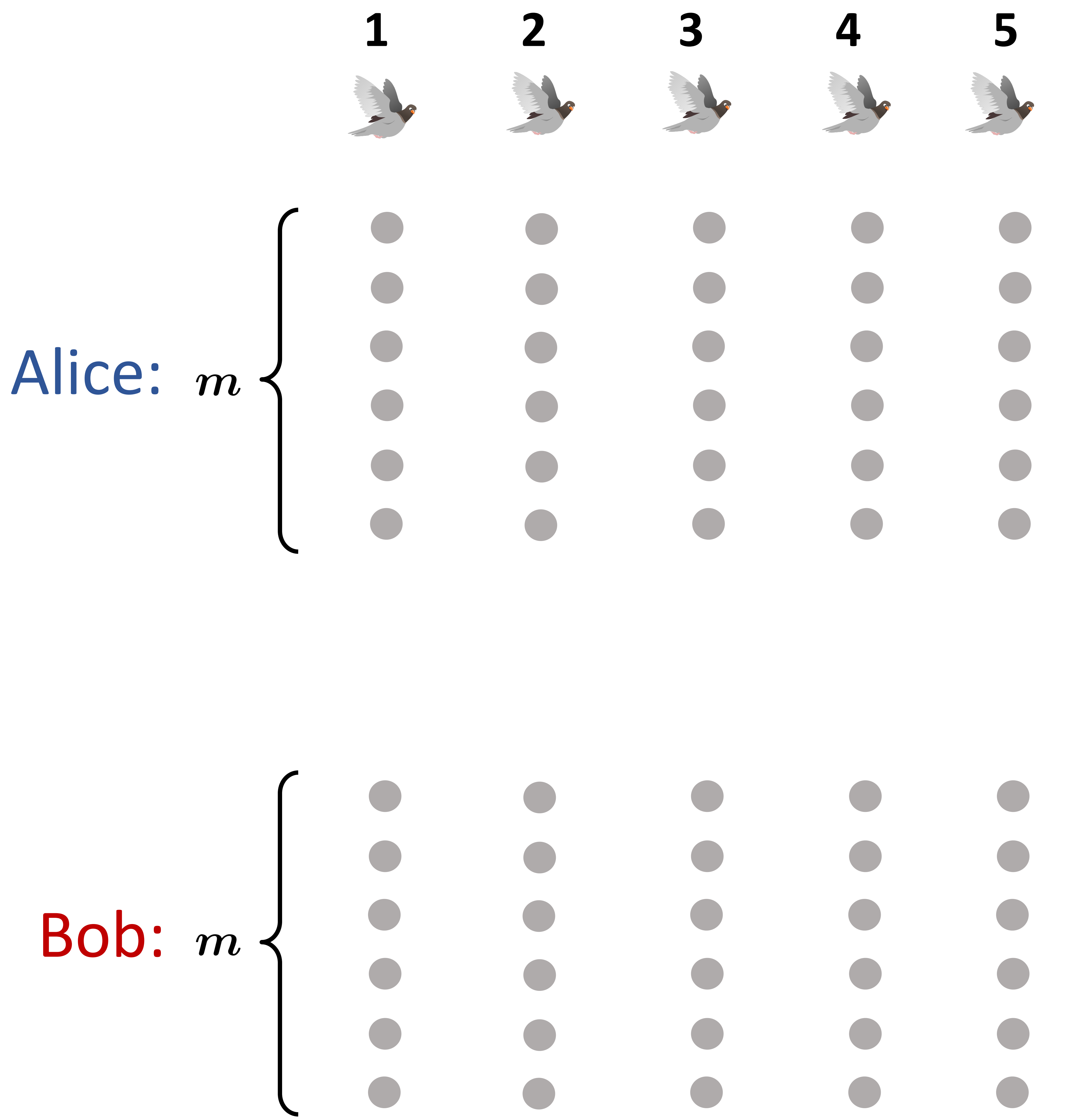
Alice: $x_1, x_2, x_3, x_4, x_5 \in [m]$

Bob: $y_1, y_2, y_3, y_4, y_5 \in [k-1]^m$

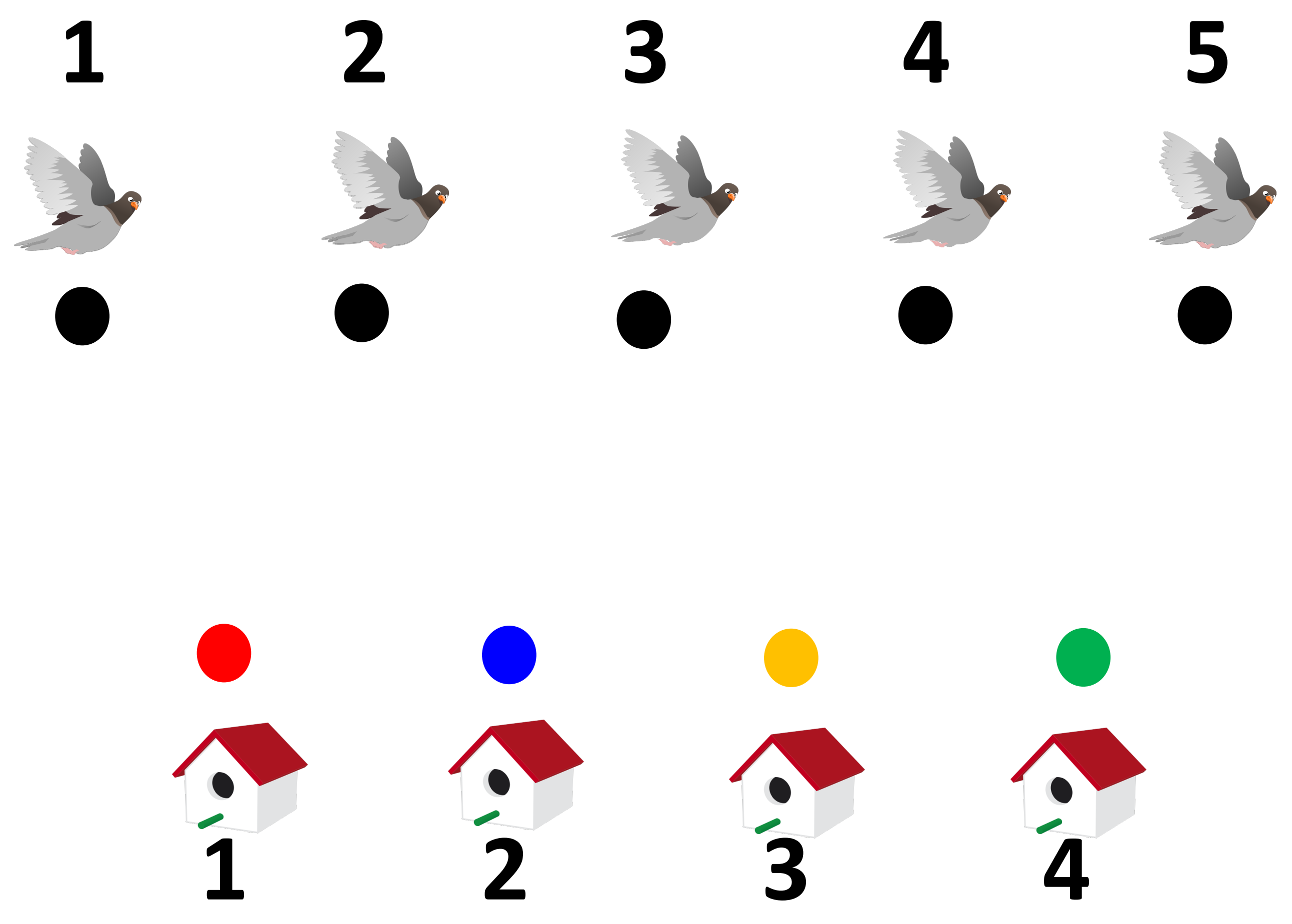


find $i \neq j$ s.t. x_i and x_j point to same number





Find-collision$_k$ ∘ $\mathrm{Ind}_m \preccurlyeq$ mKW(Clique-Col$_{k,n=mk}$)

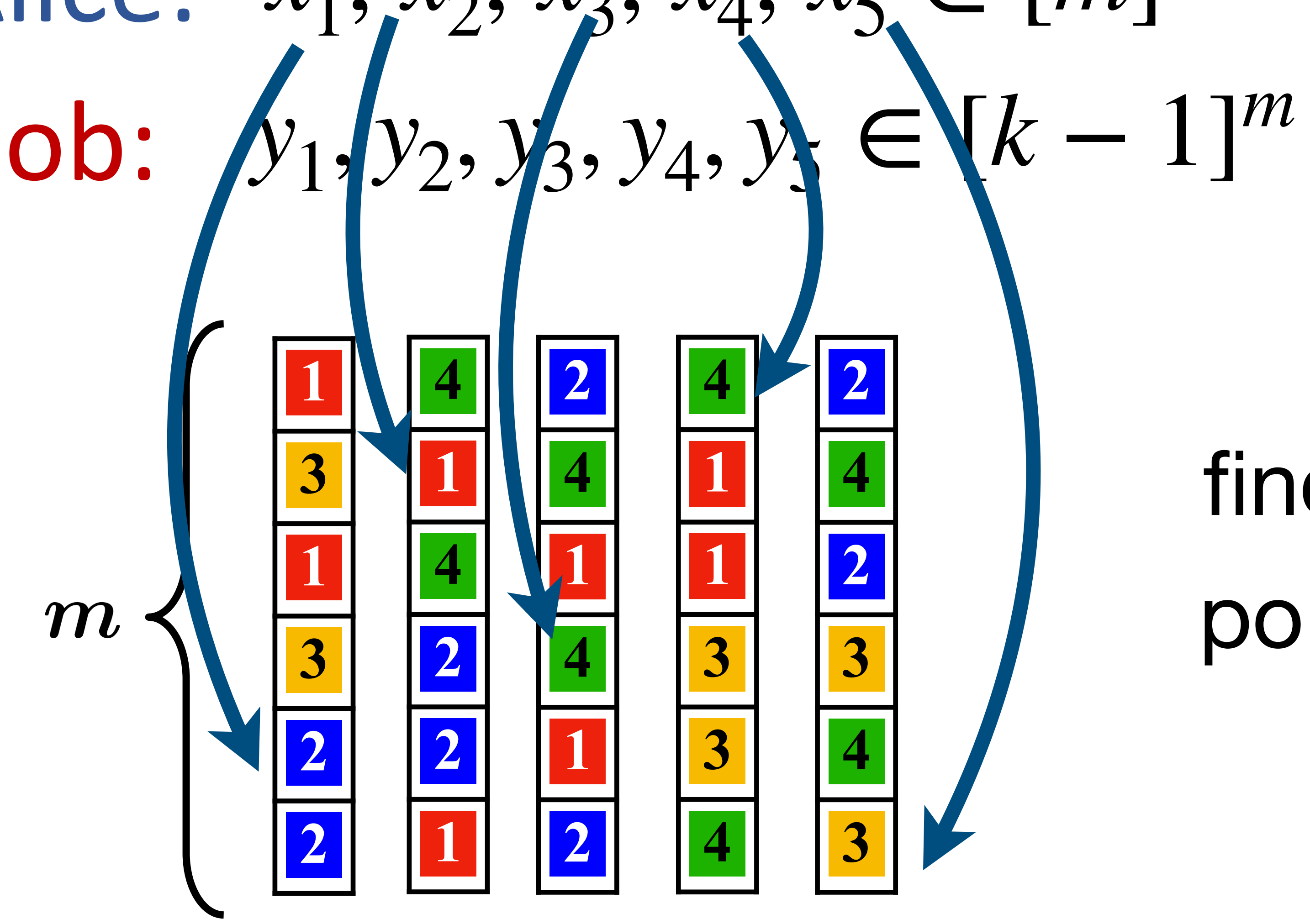


$z_i \in [k-1], \;\; \forall i \in n$

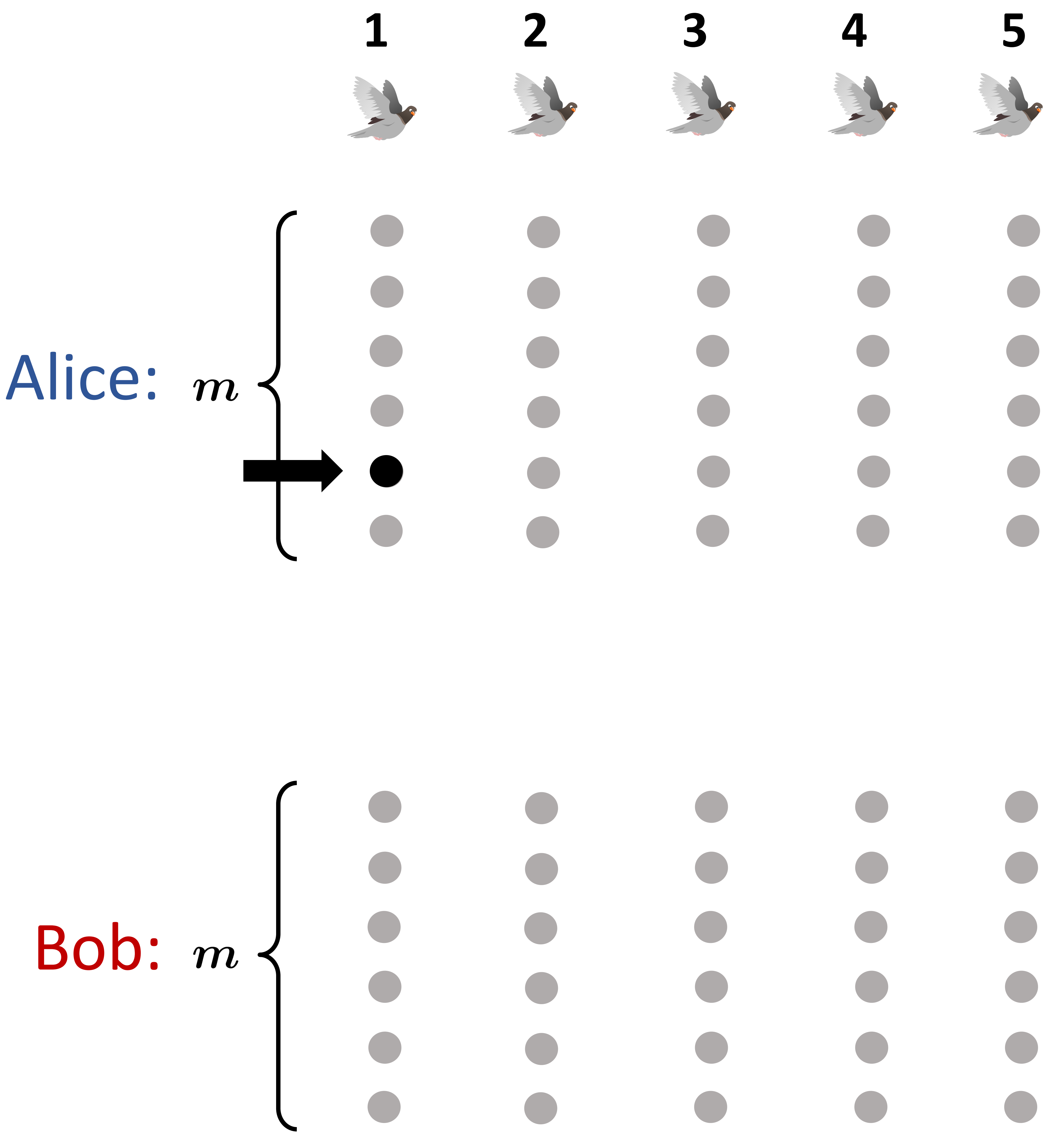
find $i \neq j$ s.t. $z_i = z_j$

Alice: $x_1, x_2, x_3, x_4, x_5 \in [m]$

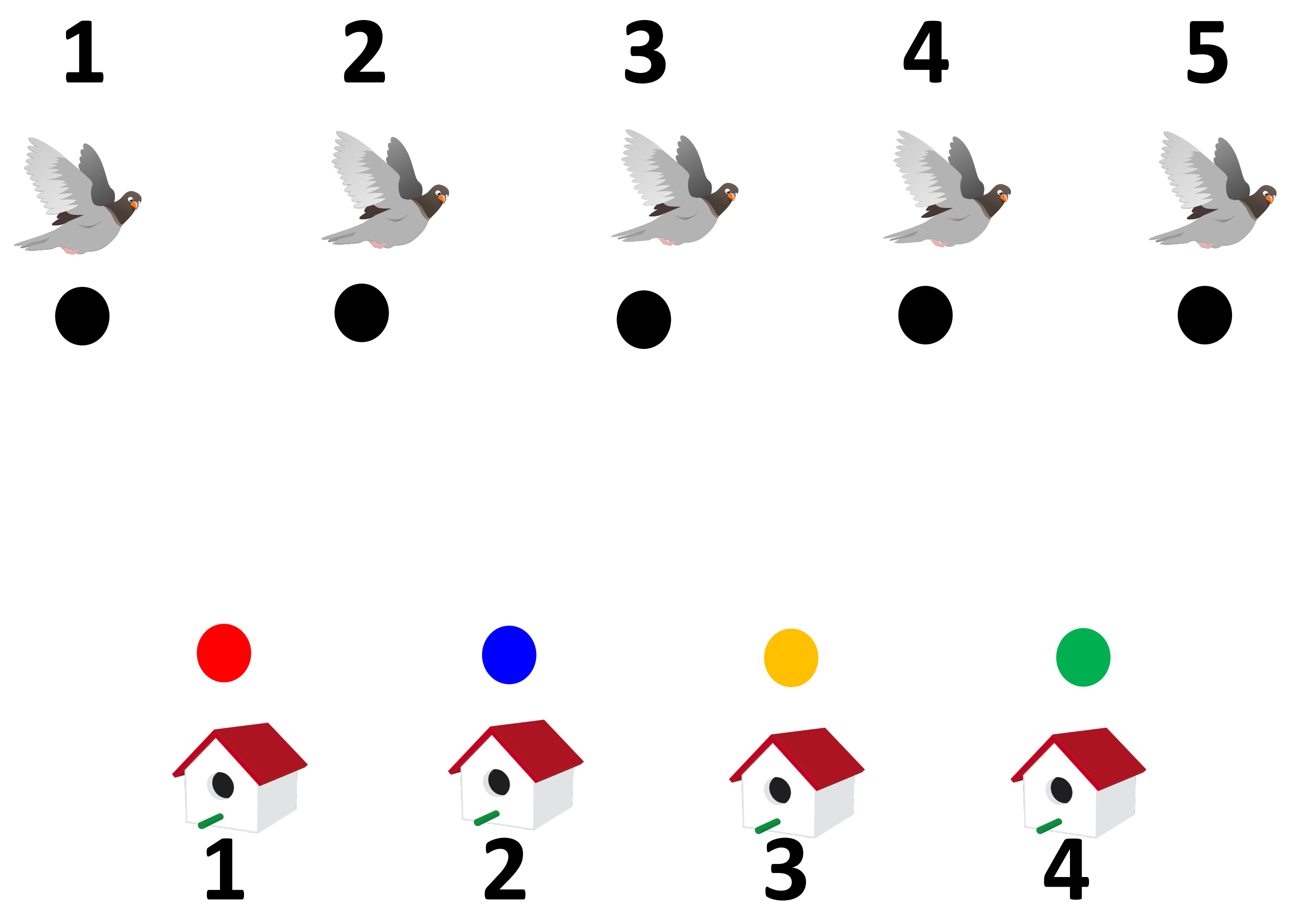
Bob: $y_1, y_2, y_3, y_4, y_5 \in [k-1]^m$



find $i \neq j$ s.t. x_i and x_j point to same number



Find-collision$_k \circ \mathrm{Ind}_m \preccurlyeq$ mKW(Clique-Col$_{k,n=mk}$)

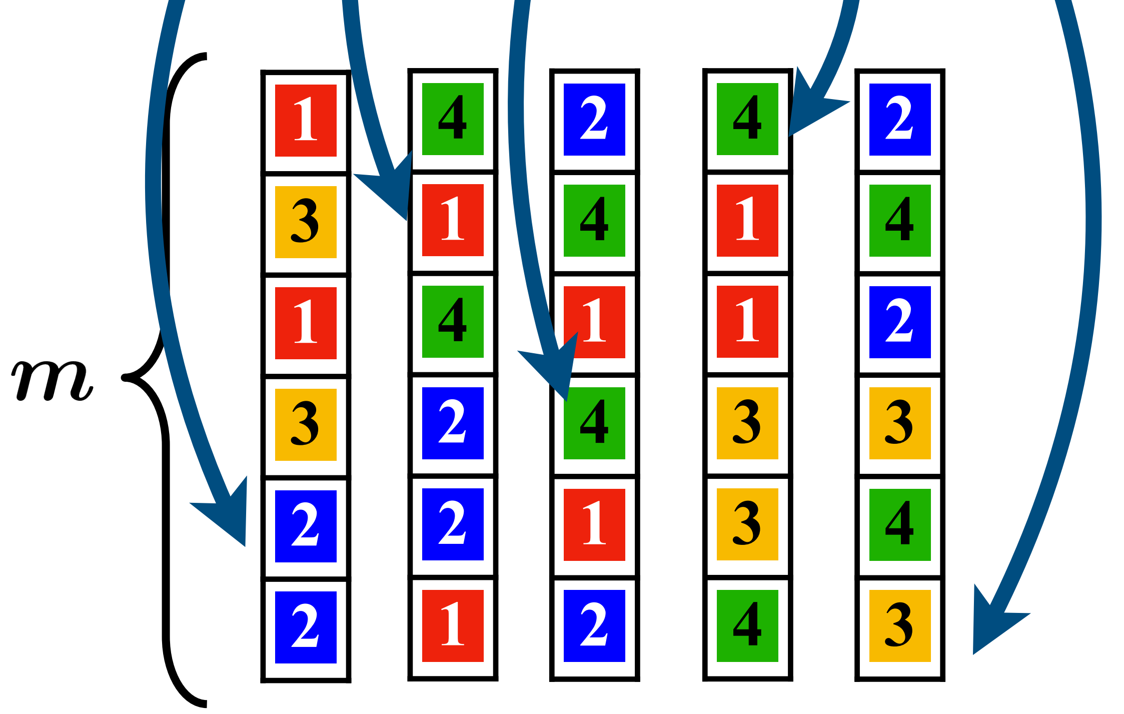


$z_i \in [k-1], \ \forall i \in n$

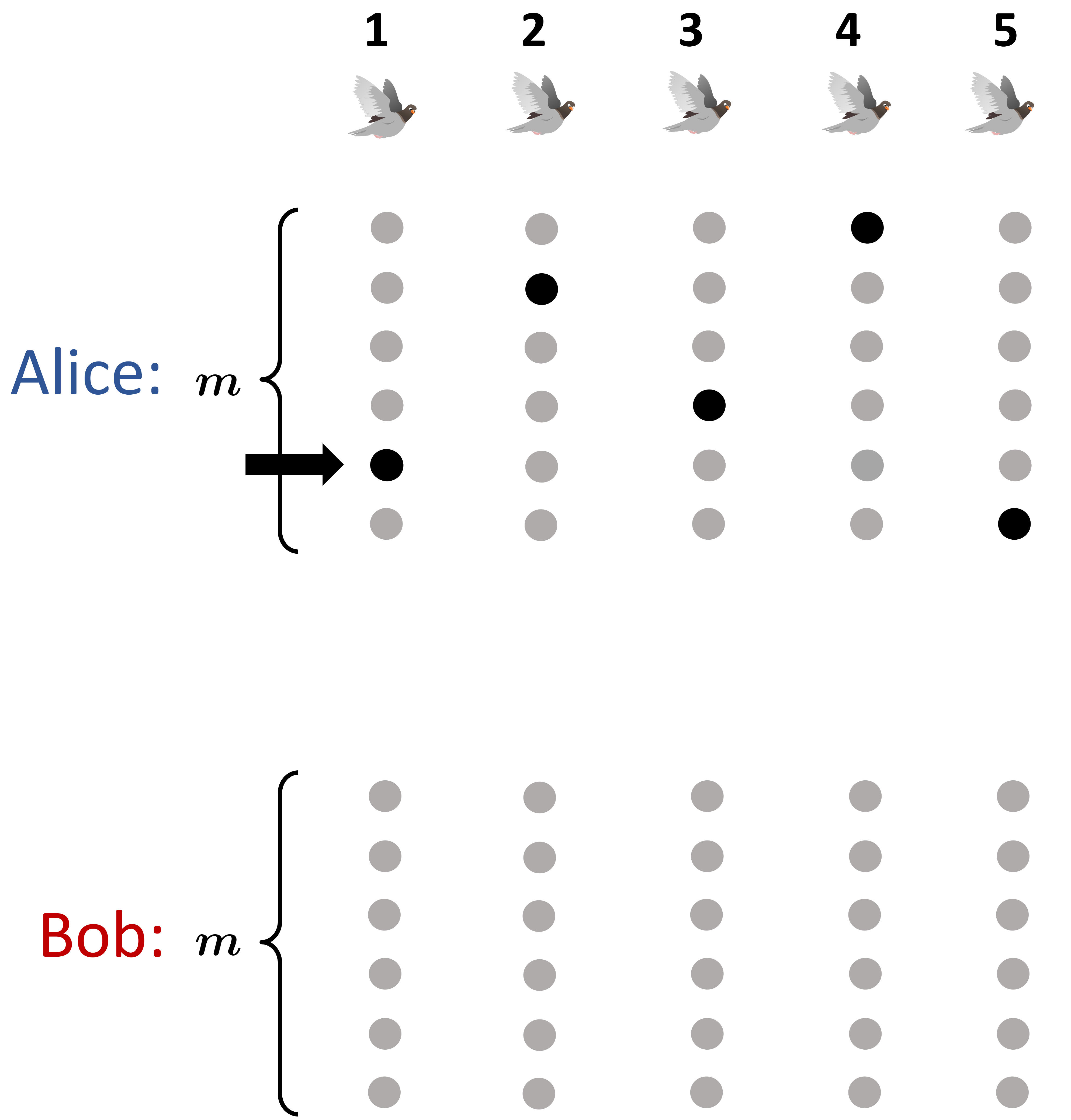
find $i \neq j$ s.t. $z_i = z_j$

Alice: $x_1, x_2, x_3, x_4, x_5 \in [m]$

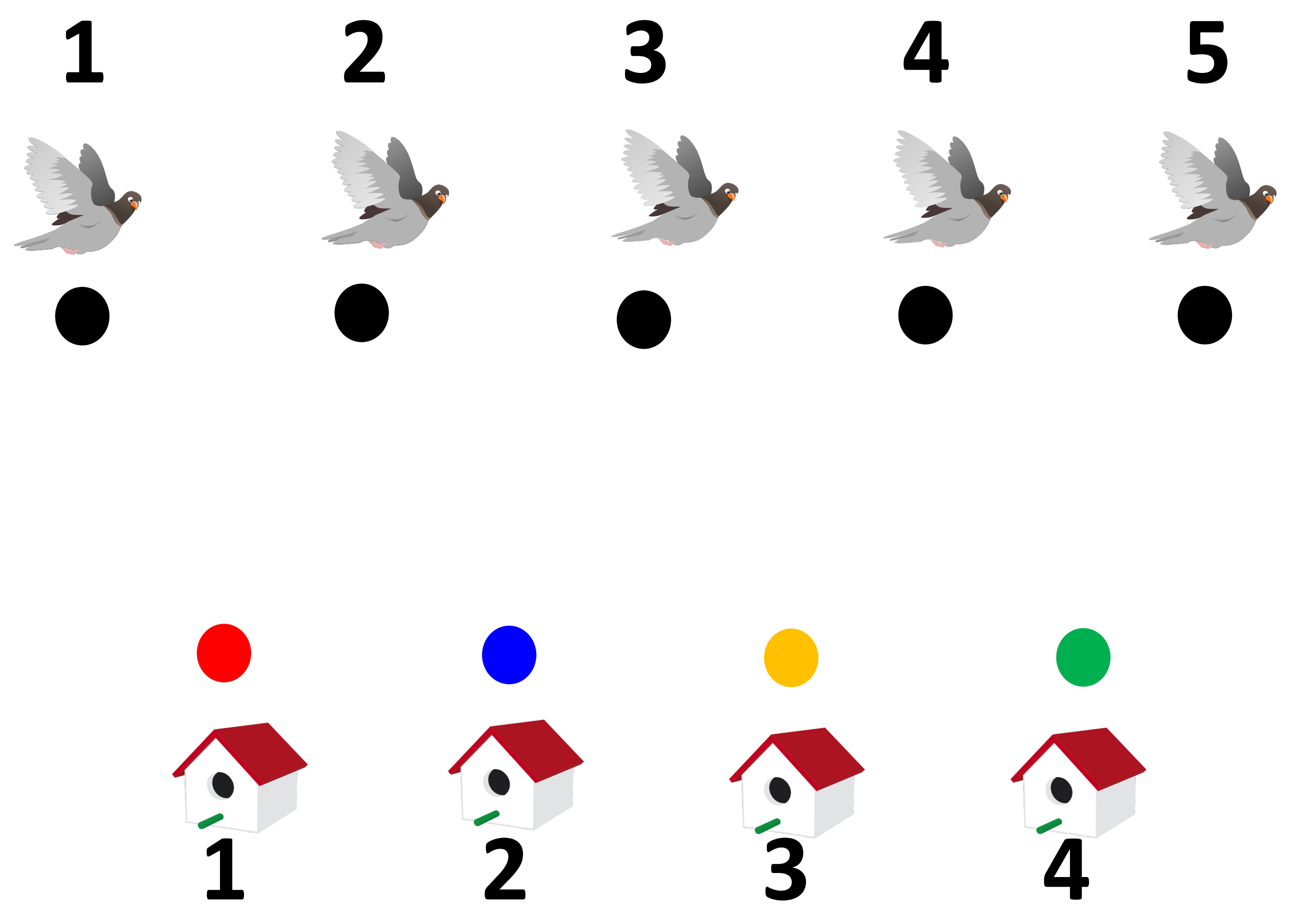
Bob: $y_1, y_2, y_3, y_4, y_5 \in [k-1]^m$



find $i \neq j$ s.t. x_i and x_j point to same number



Find-collision$_k \circ \mathrm{Ind}_m \preccurlyeq$ mKW(Clique-Col$_{k,n=mk}$)

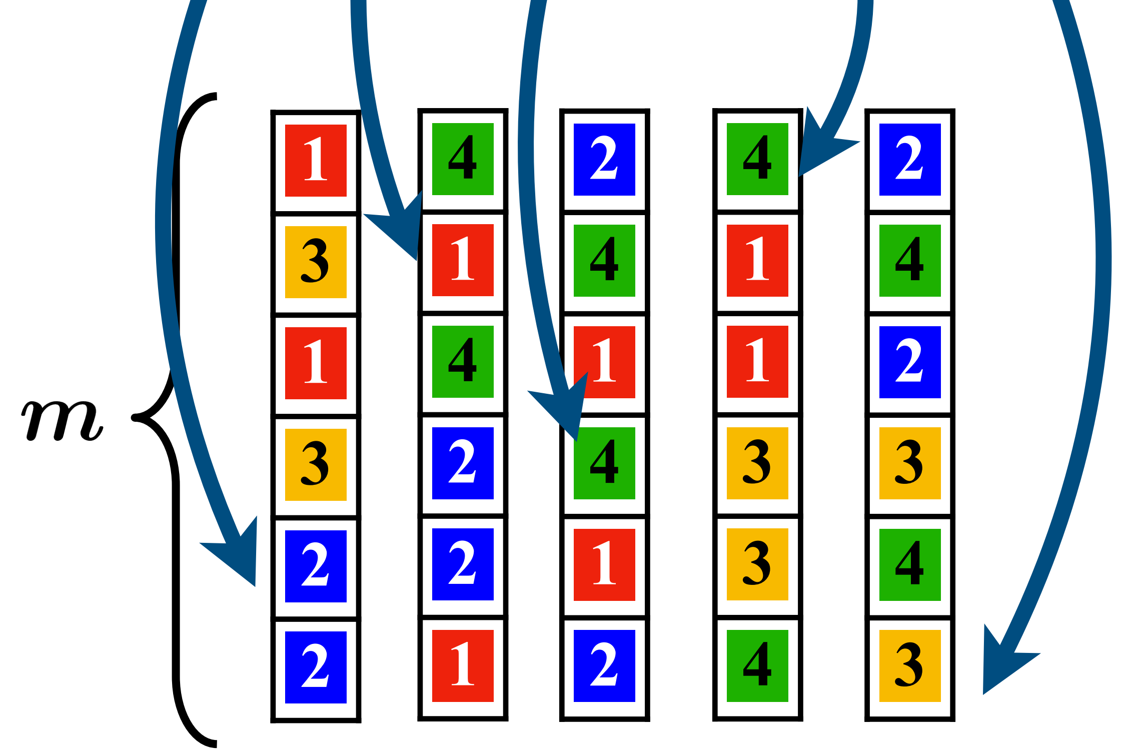


$z_i \in [k-1], \ \forall i \in n$

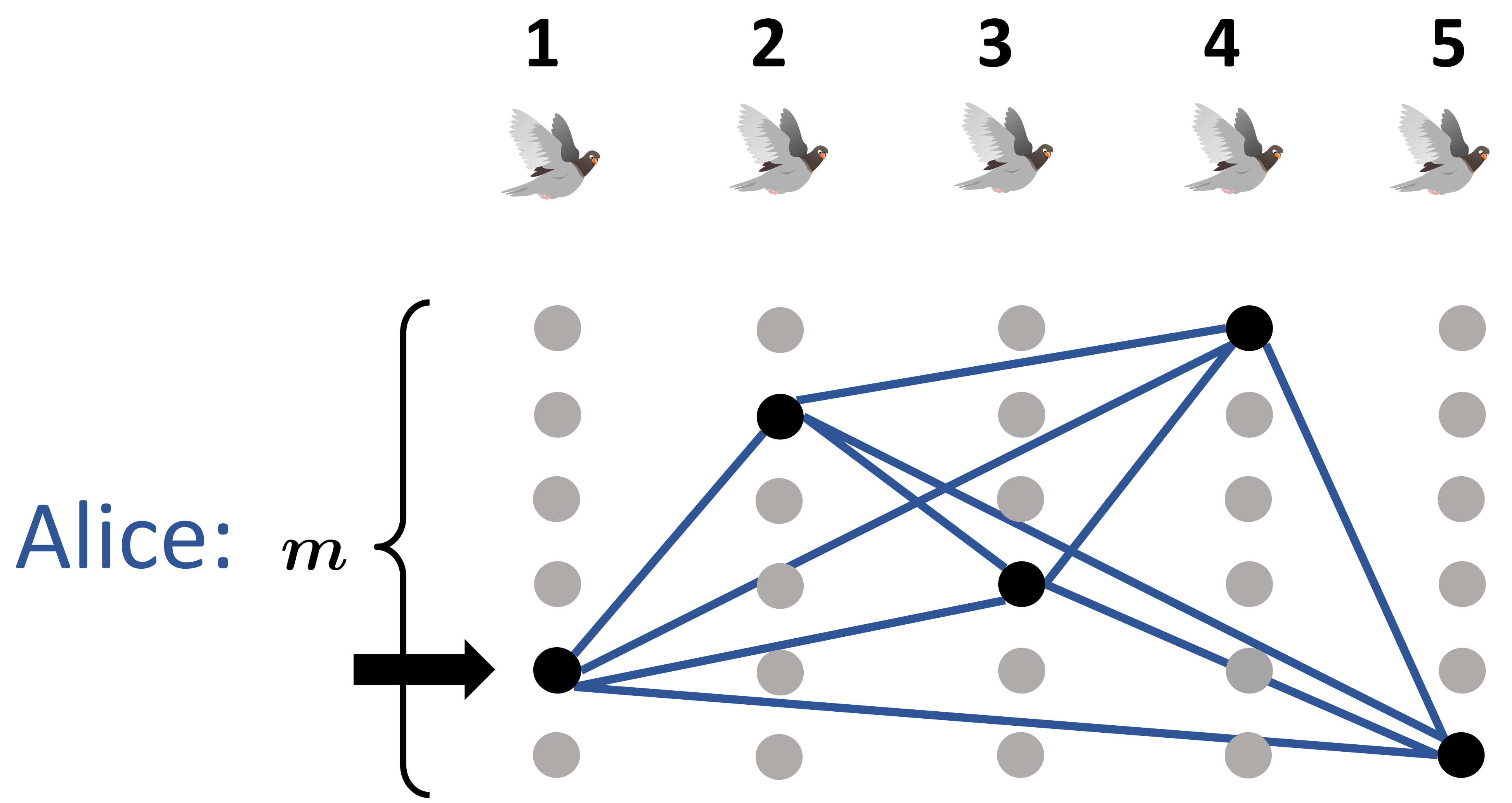
find $i \neq j$ s.t. $z_i = z_j$

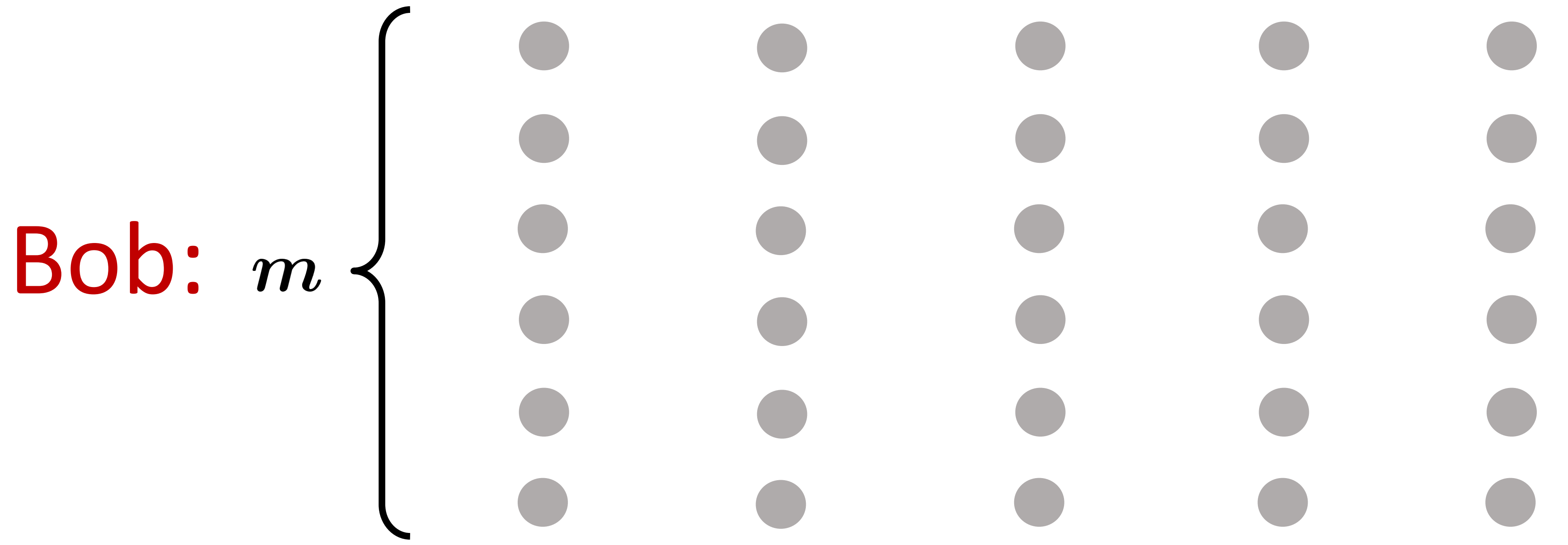
Alice: $x_1, x_2, x_3, x_4, x_5 \in [m]$

Bob: $y_1, y_2, y_3, y_4, y_5 \in [k-1]^m$

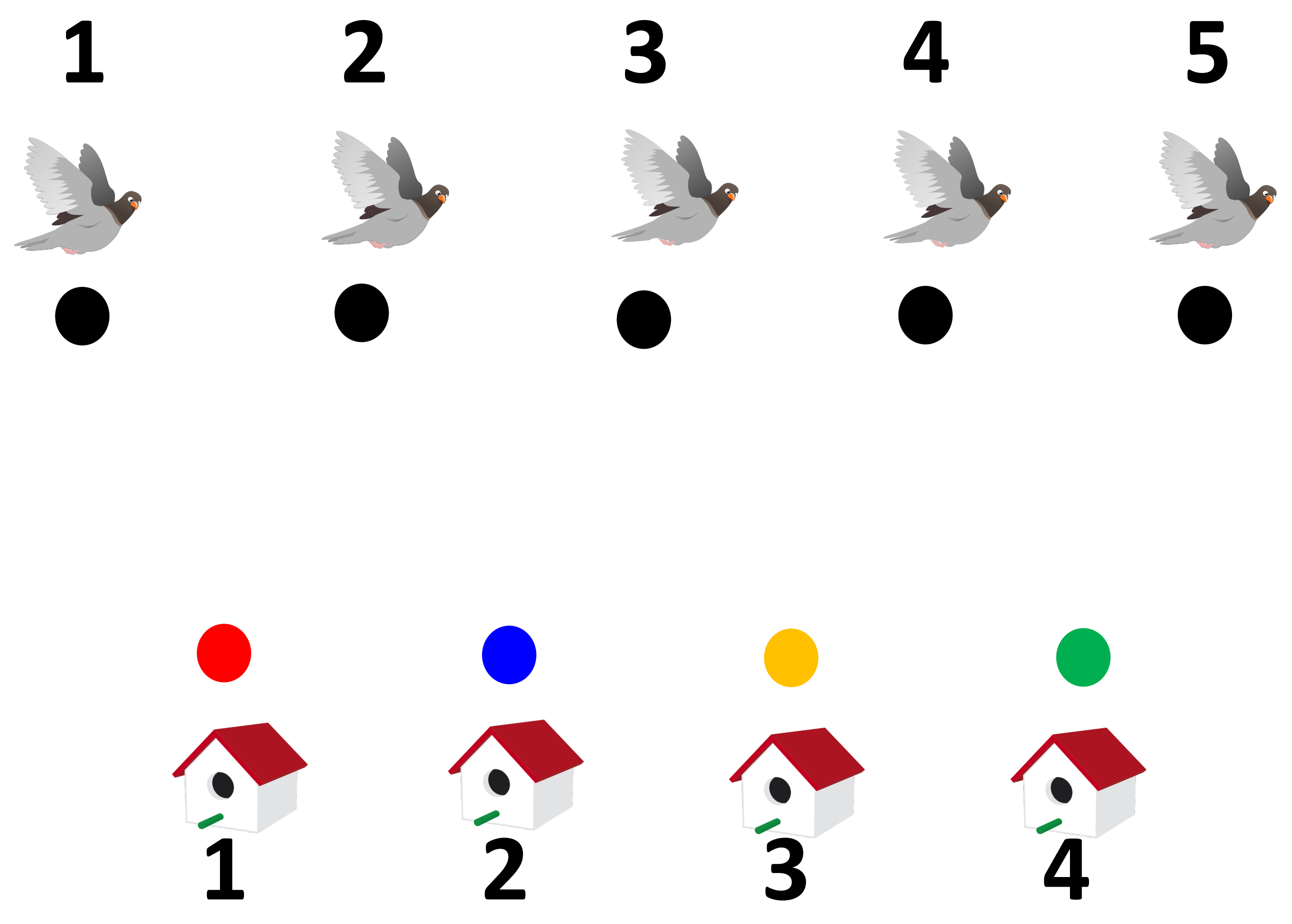


find $i \neq j$ s.t. x_i and x_j point to same number





Find-collision$_k \circ \mathrm{Ind}_m \preccurlyeq$ mKW(Clique-Col$_{k,n=mk}$)

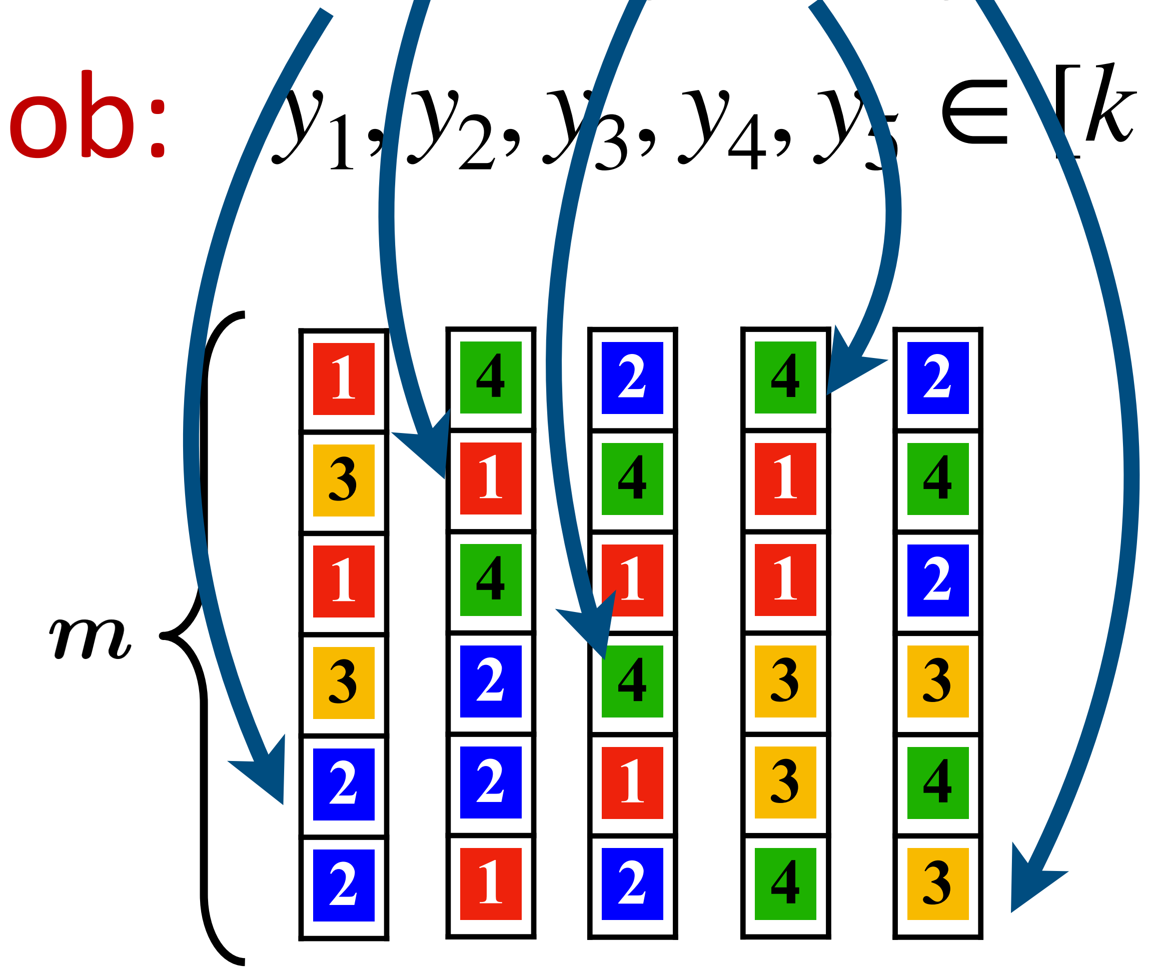


$z_i \in [k-1], \;\; \forall i \in n$

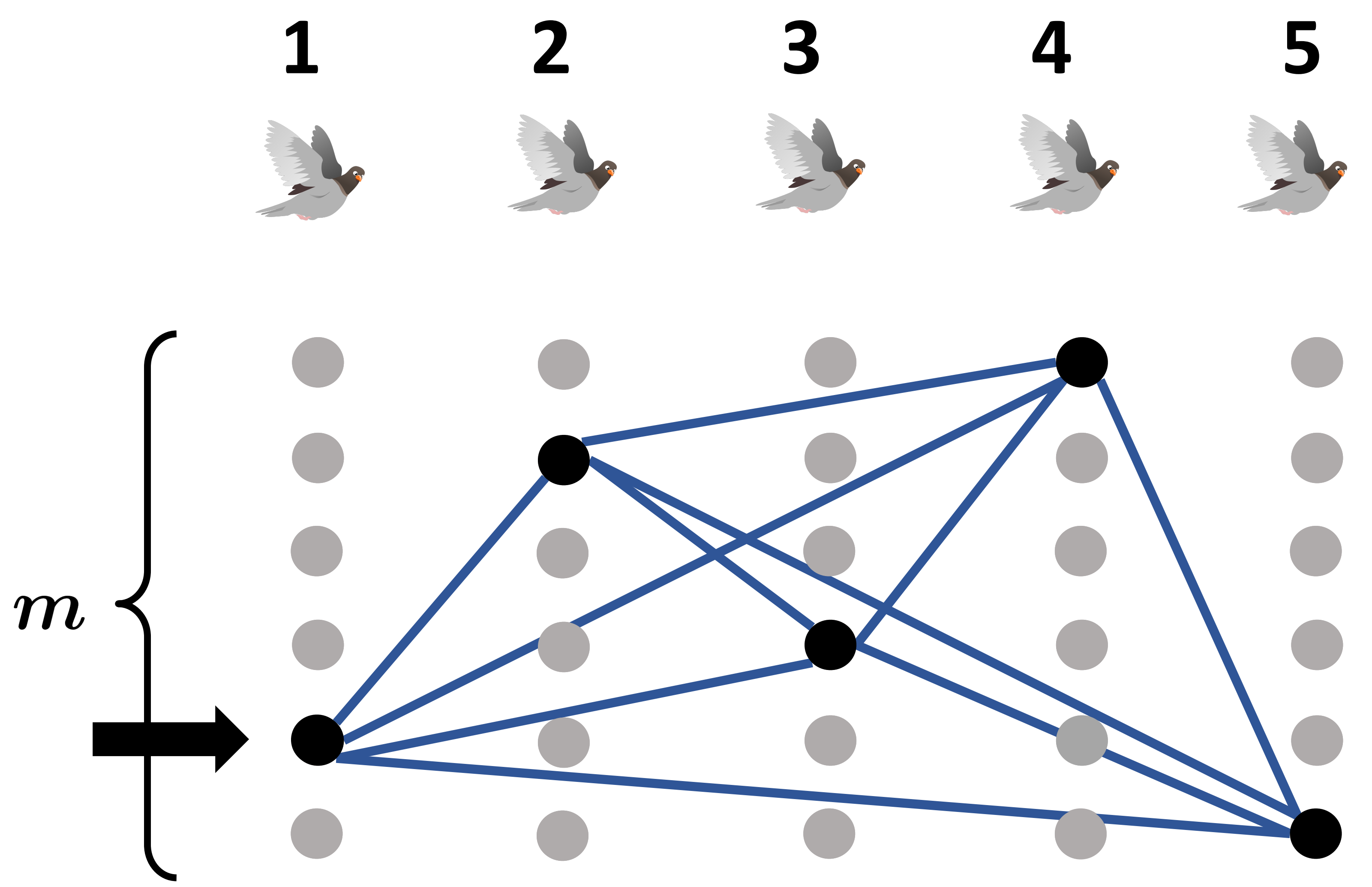
find $i \neq j$ s.t. $z_i = z_j$

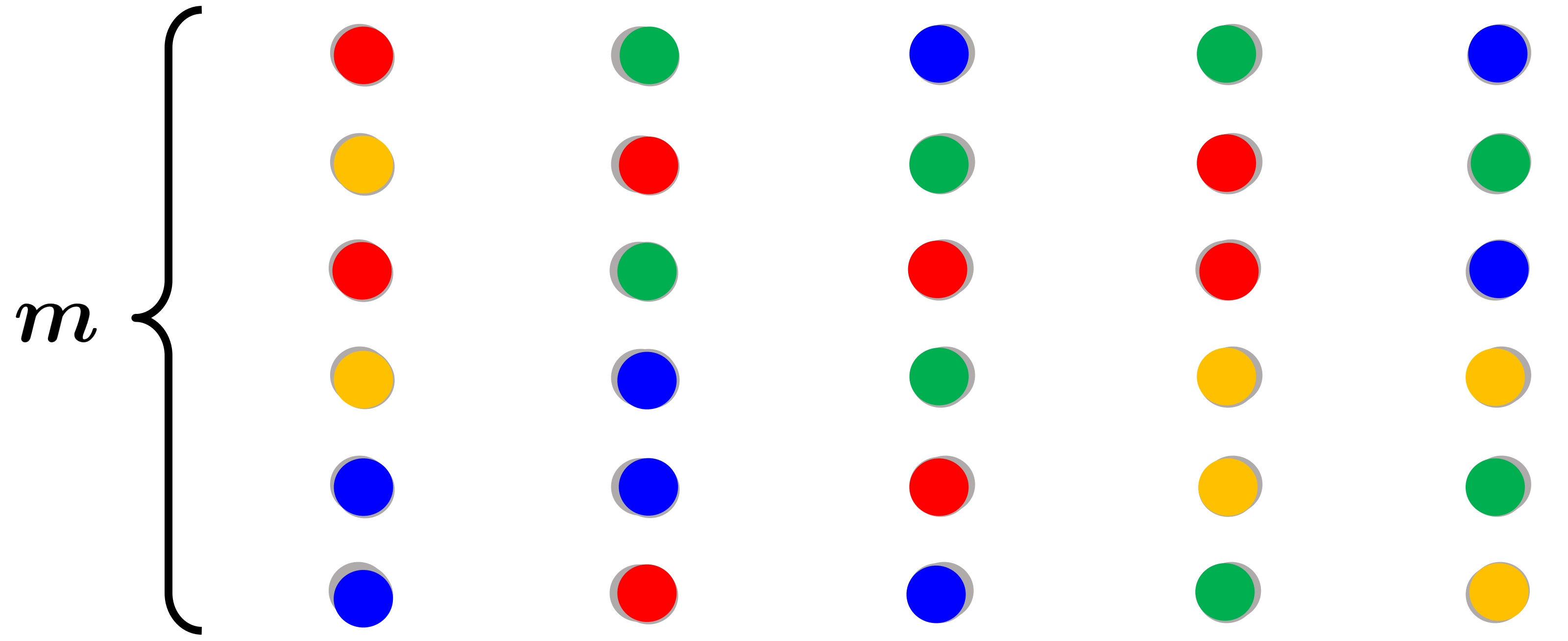
Alice: $x_1, x_2, x_3, x_4, x_5 \in [m]$

Bob: $y_1, y_2, y_3, y_4, y_5 \in [k-1]^m$



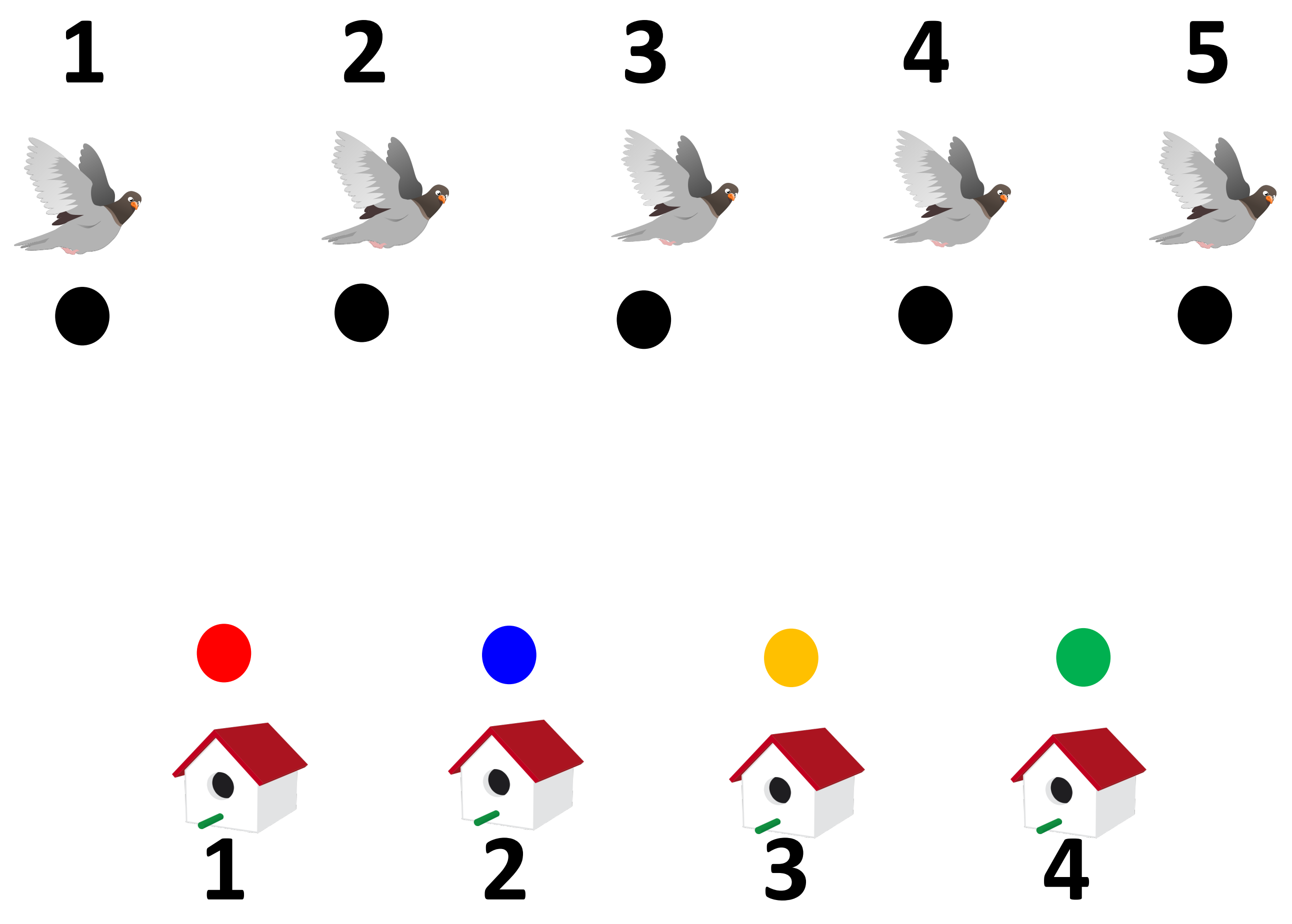
find $i \neq j$ s.t. x_i and x_j point to same number





Includes all edges between vertices of $\neq$ colours

$\text{Find-collision}_k \circ \text{Ind}_m \preccurlyeq \text{mKW}(\text{Clique-Col}_{k,n=mk})$

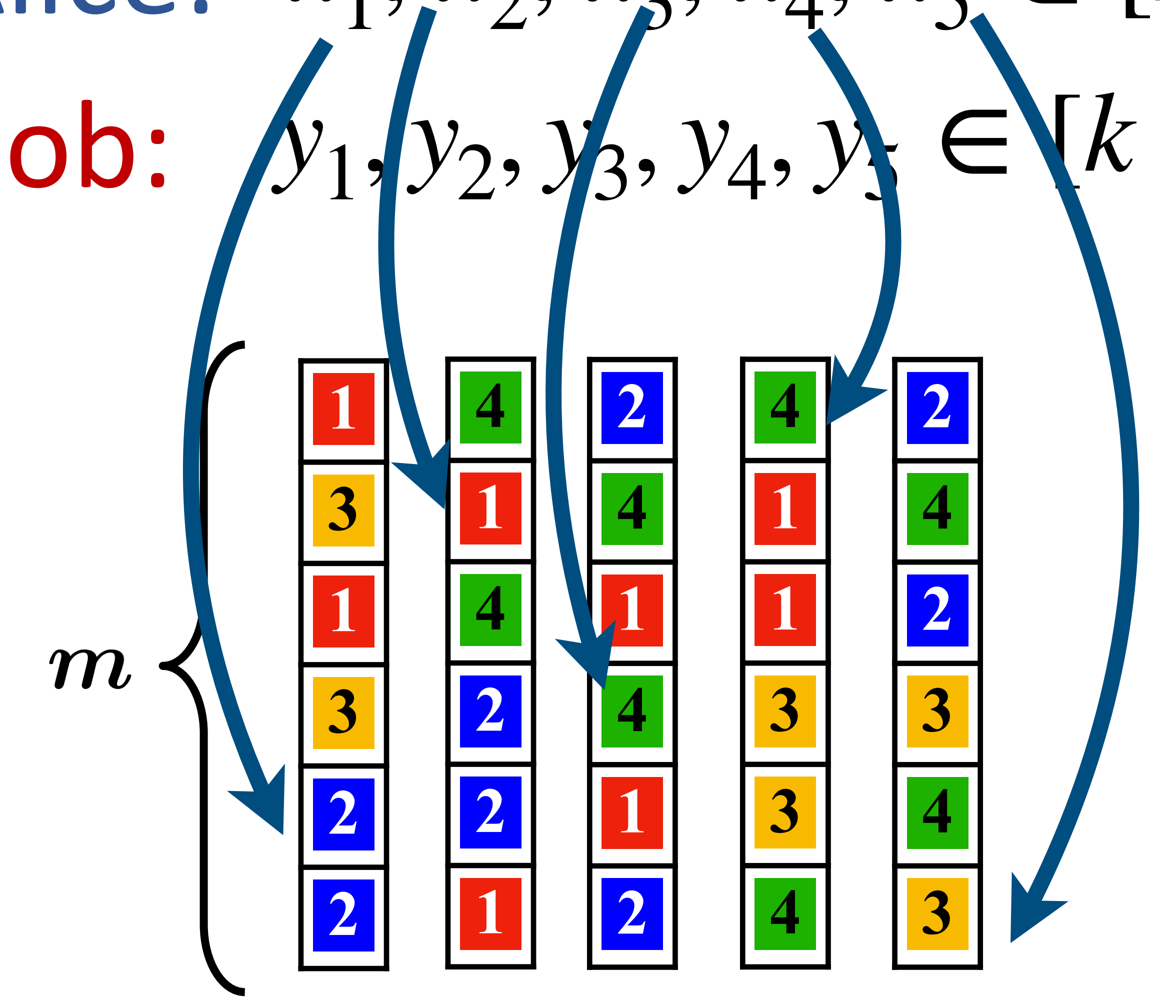


$z_i \in [k-1], \ \forall i \in n$

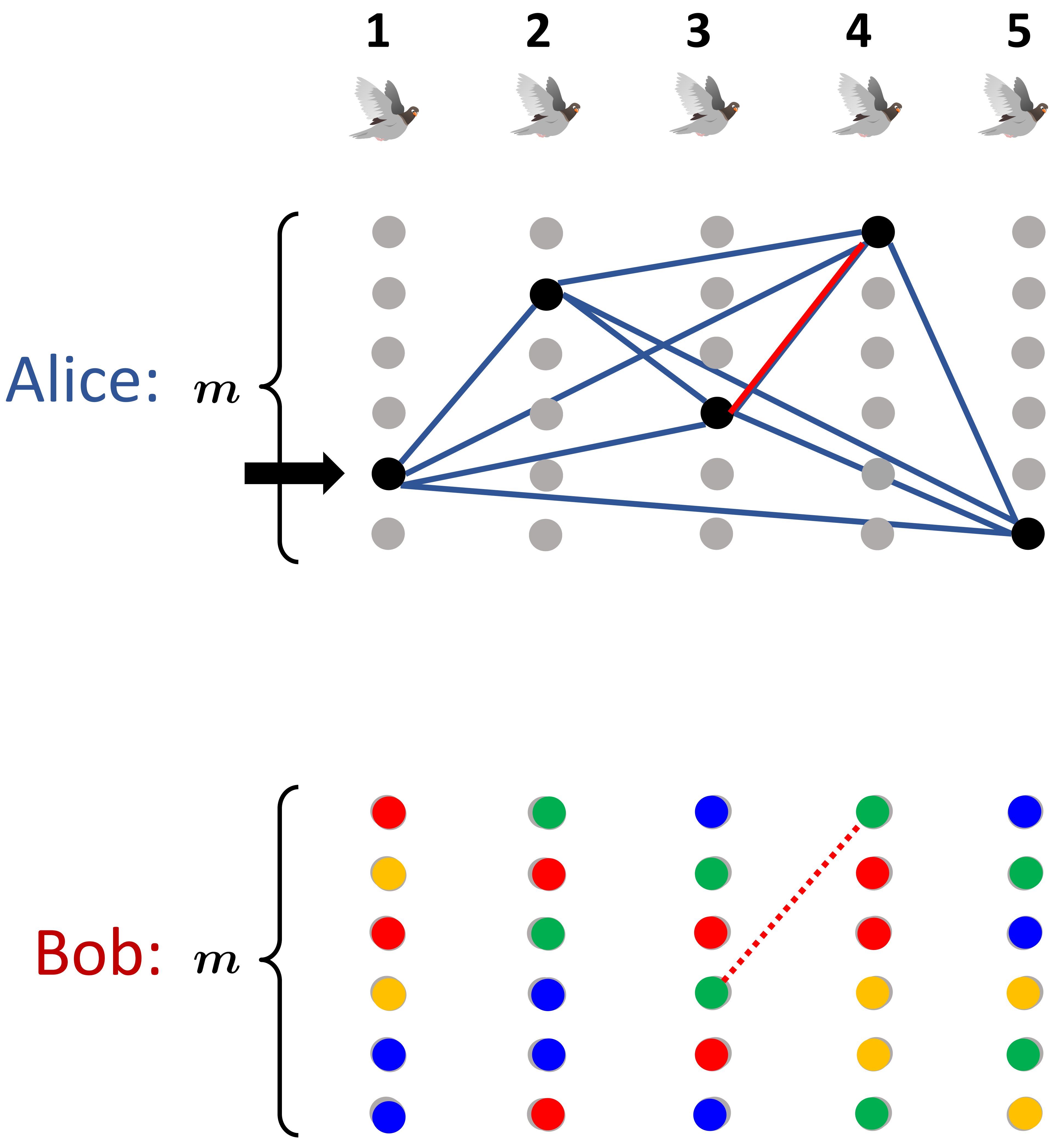
find $i \neq j$ s.t. $z_i = z_j$

Alice: $x_1, x_2, x_3, x_4, x_5 \in [m]$

Bob: $y_1, y_2, y_3, y_4, y_5 \in [k-1]^m$

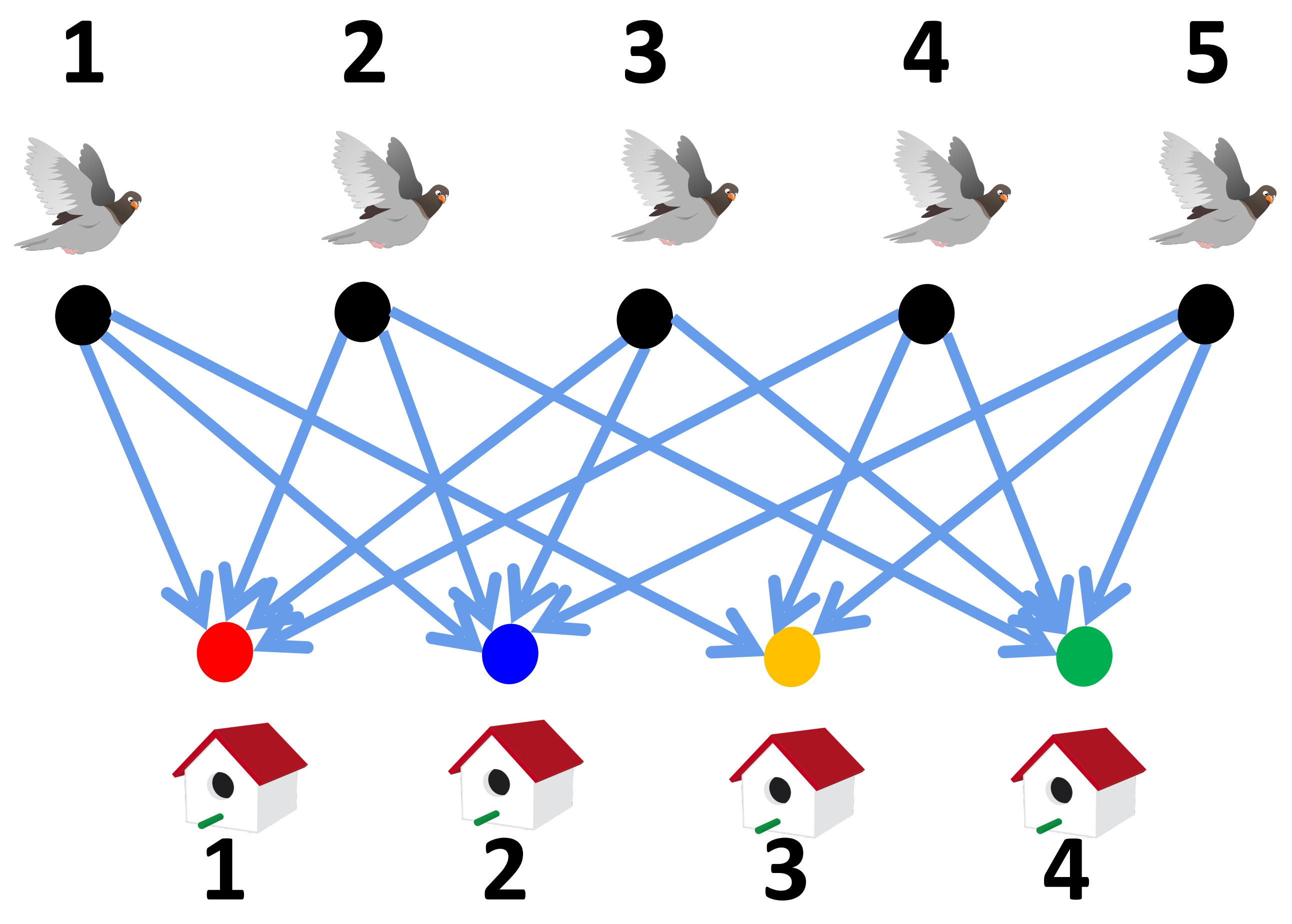


find $i \neq j$ s.t. x_i and x_j point to same number



Includes all edges between vertices of $\neq$ colours

Find-collision$_k \circ \mathrm{Ind}_m \preccurlyeq$ mKW(Clique-Col$_{k,n=mk}$)

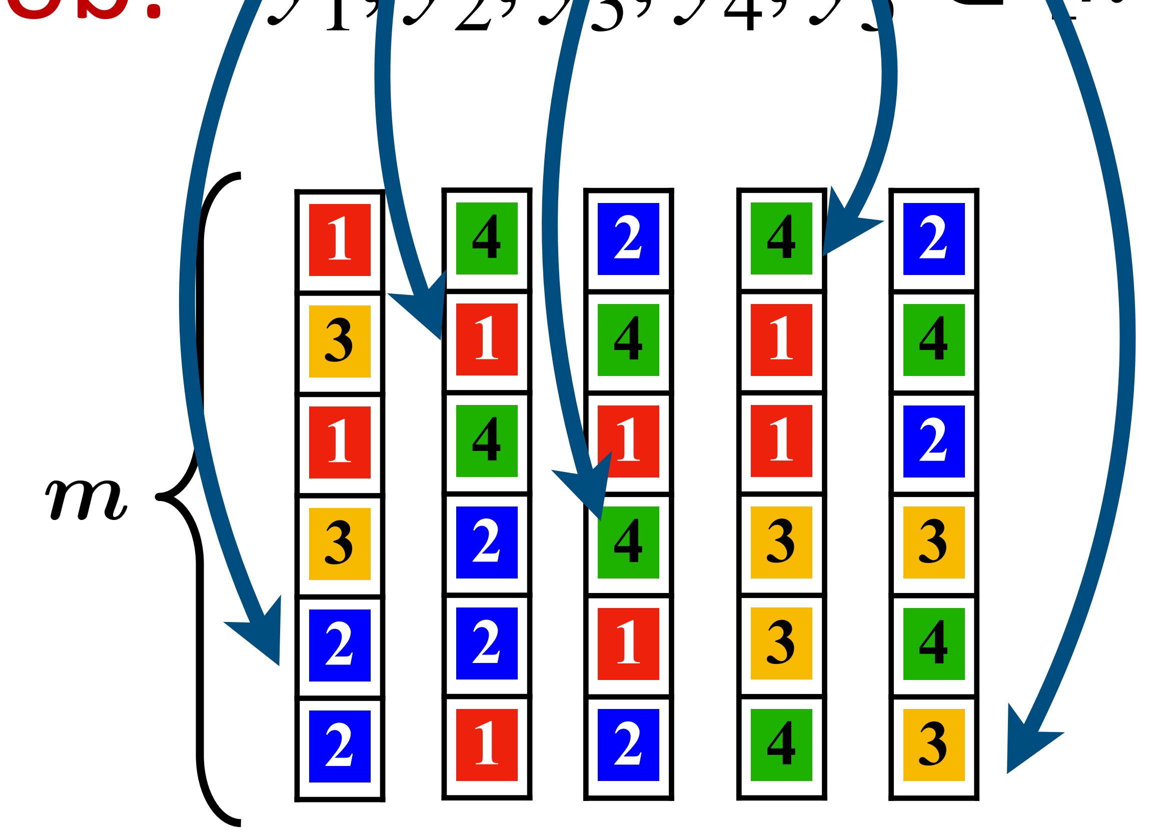


$z_i \in [k-1], \ \forall i \in n$

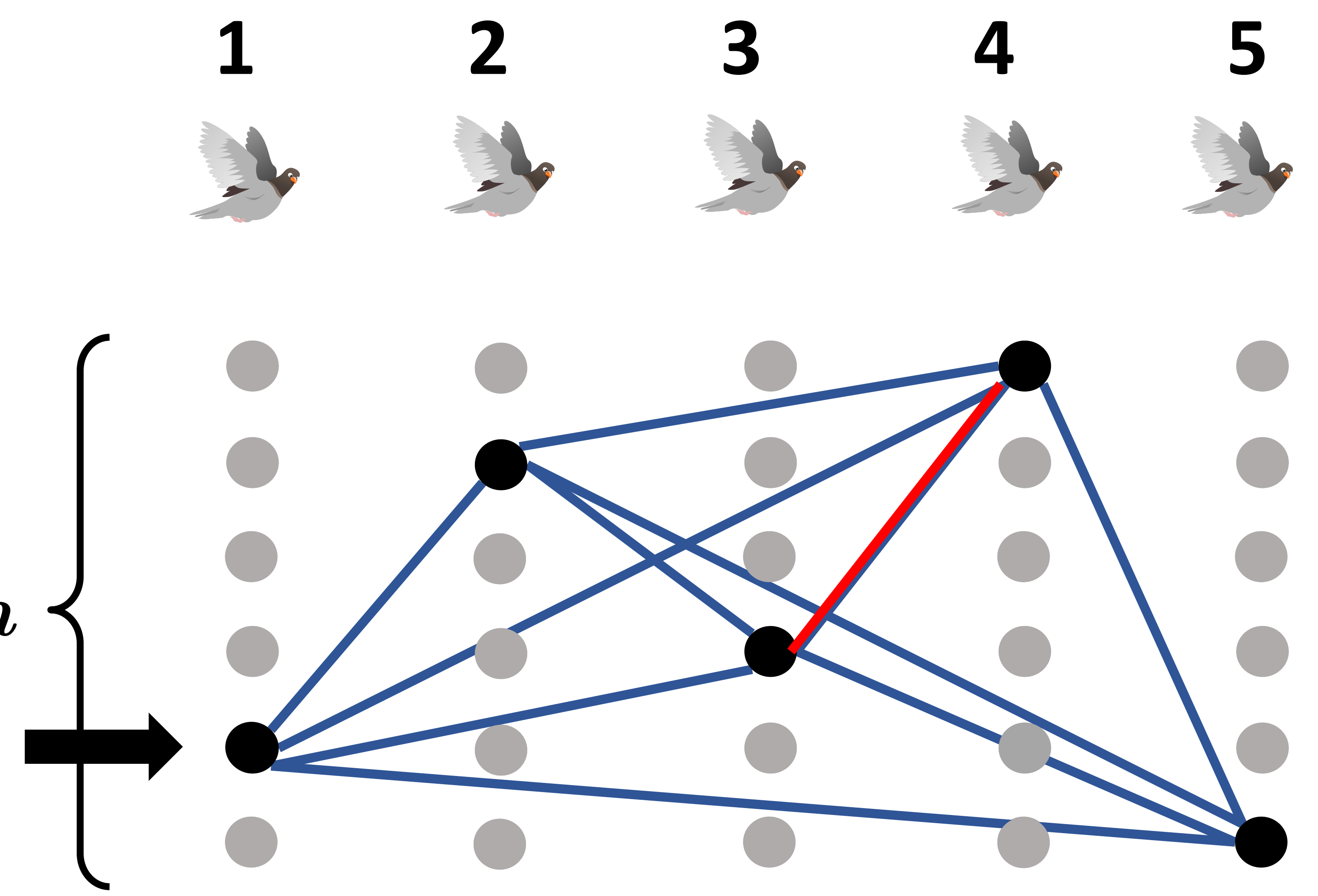
find $i \neq j$ s.t. $z_i = z_j$

Alice: $x_1, x_2, x_3, x_4, x_5 \in [m]$

Bob: $y_1, y_2, y_3, y_4, y_5 \in [k-1]^m$

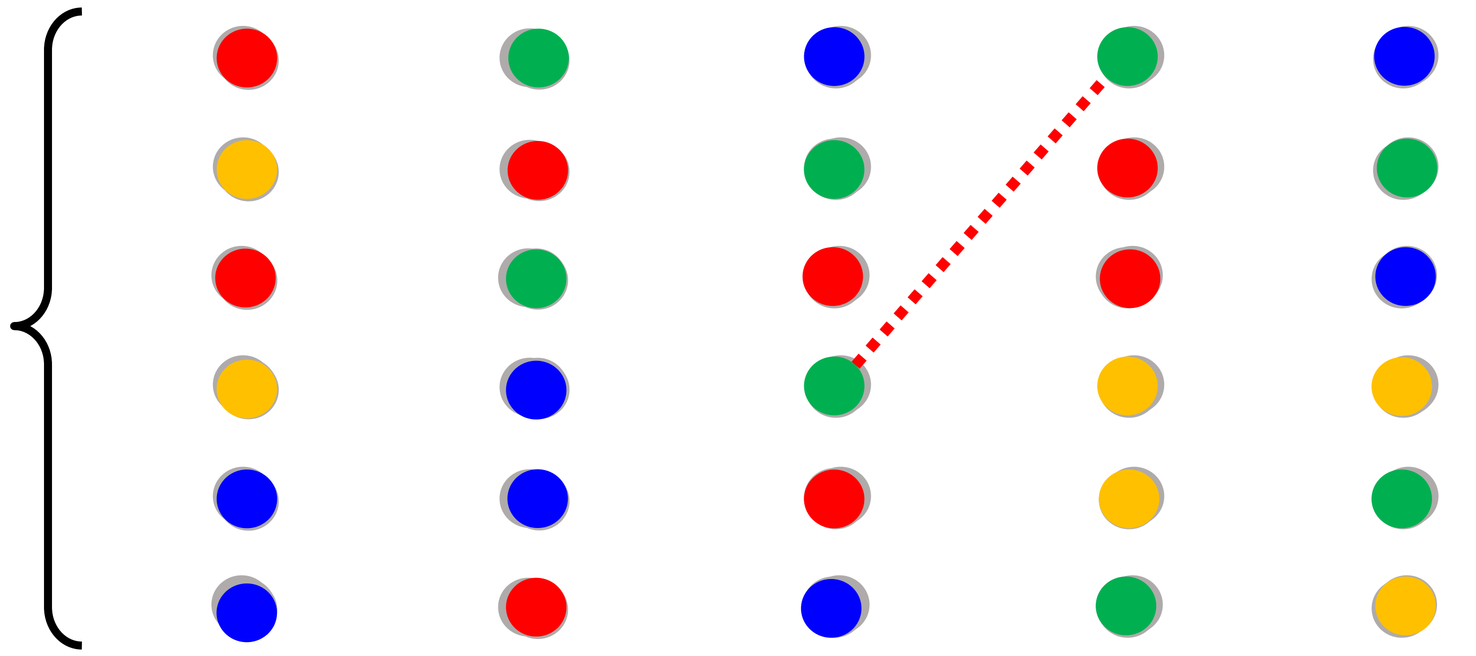


find $i \neq j$ s.t. x_i and x_j point to same number



Alice: m

Bob: m



Includes all edges between vertices of $\neq$ colours

New results using approximation method

Improved on [Andreev '87, Harnik, Raz '00] $\exp(\tilde{\Omega}(n^{1/3}))$-size lower bound for f in NP

- $\exp(\tilde{\Omega}(n^{1/2}))$ lower bound for f in NP
- $n^{\Omega(k)}$-size lower bound for k-clique for any $k \leq n^{1/3-o(1)}$

[Cavalar, Kumar, Rossman '20]

- $n^{\Omega(k)}$-size lower bound for k-clique for any $k \leq n^{1/2-o(1)}$ [Błasiok, Meierhöfer '25]

- Clique lower bounds not for clique-colouring

- *Key tool:* improved sunflower lemmas [Alweiss, Lovett, Wu, Zhang '19] and further improvements [Rao '19], [Bell, Chueluecha, Warnke '20]

Very recent result for monotone circuits

> The difficulty in proving that a given boolean function has high complexity lies in the nature of our adversary: the circuit. Small circuits may work in a counterintuitive fashion, using deep, devious, and fiendishly clever ideas. How can one prove that there is no clever way to quickly compute the function? [Jukna '12]

- How deep must we go? Are circuits of depth $> n$ stronger?

- $\exists f$ computable by monotone circuits of size $s = n^{O(1)}$ [dR, Fleming, Janett, Nordström, Pang '25]
  - any monotone circuit of depth-n^2 requires size $s^{1.4}$

- $\exists f$ computable by size-$n^{O(\log n)}$ monotone circuits [Göös, Maystre, Risse, Sokolov '25]
  - any monotone circuit of depth-$n^{O(1)}$ requires size $\exp(\Omega(n^{\epsilon}))$

Some open problems

- Truly exponential size lower bound for f in NP (and in P)
  - Best known $\sim \exp(n^{1/2})$ and $\exp(n^{1/3})$, respectively
- Super-poly lower bound for f in AC^0 [Grigni, Sipser '92] (or even in NC^1)
  - Best known for f in NC^2 [GKRS '19] and for f in $\mathrm{AC}^0[\oplus]$ [Cavalar, Oliveira '23]
- Exhibit function f that has poly-size monotone circuits s.t. any monotone circuit computing f in depth $\leq n$ requires super-poly size

Some more open problems

- Prove $\Omega(n^3)$ lower bound for st-connectivity [Jukna '12]
- Prove $n^{O(\log n)}$ upper bound for matching or prove better lower bound
  - Or explain why it's hard to prove exponential lower bounds
- Prove $n^{\Omega(k)}$ lower bound for k-clique for $k > \sqrt{n}$

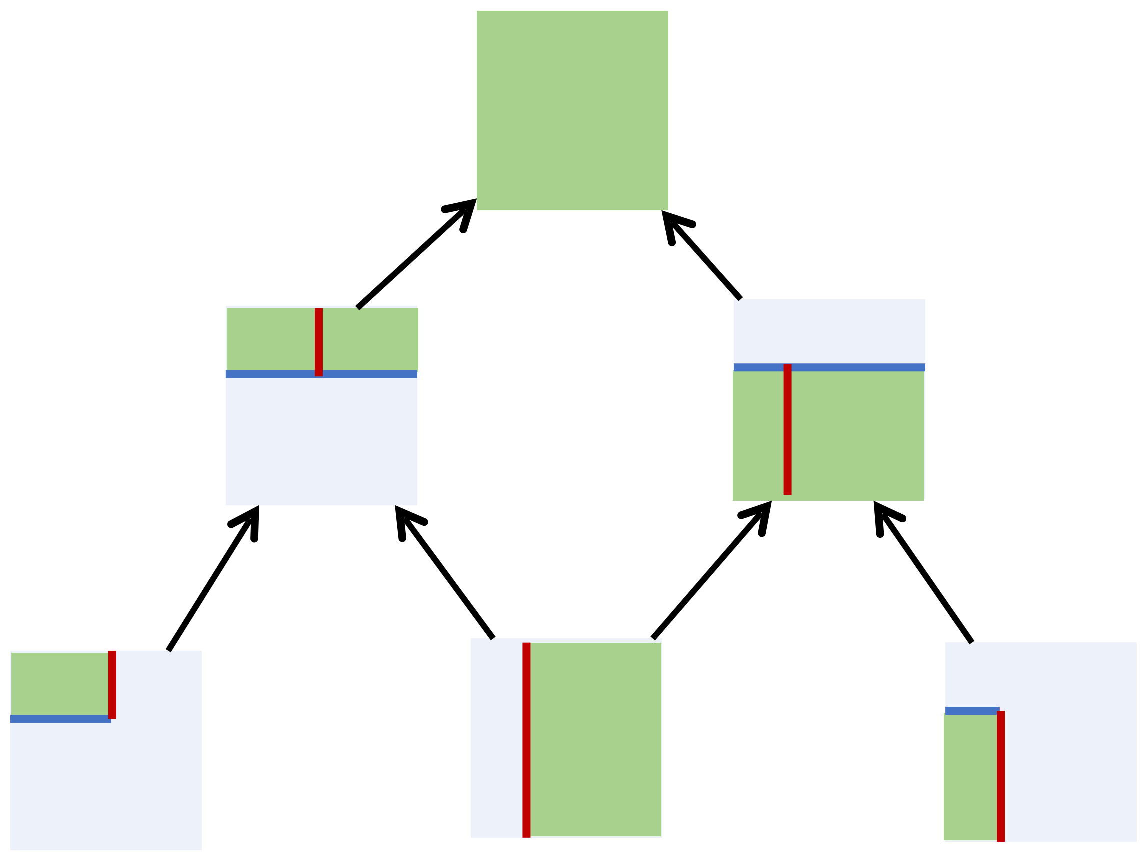
Thank you!

Thoughts on methods

- Methods to obtain monotone circuit lower bounds
  - Approximation method
  - Bottle-neck counting
  - DAG-like lifting

  } Specialised per problem (Approximation method, Bottle-neck counting)

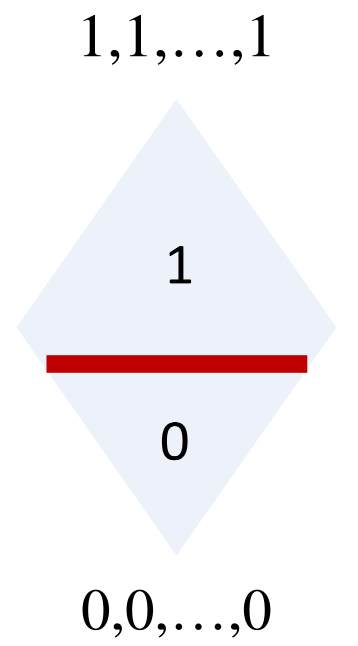
  Generalised method (DAG-like lifting)



- Generalised method: black-box, main argument done once
- Specialised method: can perhaps get better bounds
- Common flavour: is lifting a special case of approximation method?
- Also common: use of sunflowers

Thoughts: challenges for slice functions

- All(?) size lower bounds for monotone circuits hold for monotone ***real*** circuits
  - Linear size monotone real formulas can compute slice functions
  - Current lower bound methods don't work for slice functions



- Monotone real circuits introduced to study cutting planes in proof complexity
  - Corresponding "communication" model: triangle-DAGs
  - Only way we know of proving lower bounds for cutting planes
  - Gives important insight on the methods

Some more open problems

- Prove lower bounds with limited number of negations $\gg \log \log n$ [Jukna '12]
  - Methods work only to $\leq \log \log n$ [Amanoand, Maruoka '05]
  - $\lceil \log(n+1) \rceil$ negation gates are enough [Markov '57]
- Can all (monotone) circuit lower/upper bounds be seen naturally as communication lower/upper bounds for $(\mathrm{m})\mathrm{KW}$? (Majority?) [Karchmer '89]
- Understand power and limitations of lifting? [Cavalar, Oliveira '23]
- General TFNP framework: other lifting theorems & communication l.b.?