# 天秤を用いるゼロ知識証明

金子　尚平
電気通信大学

# 目次

# 研究背景



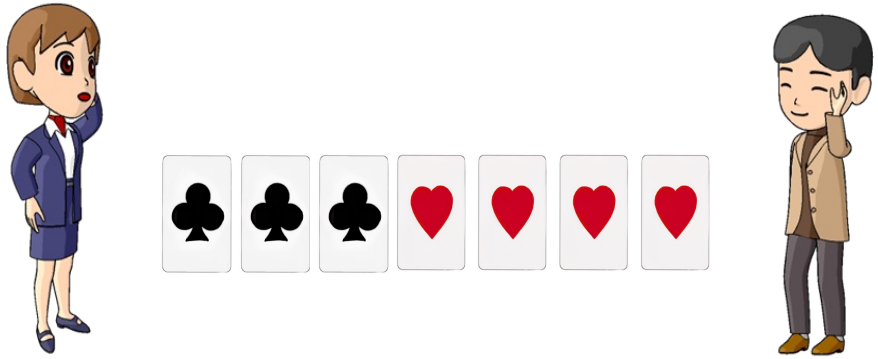
- パズルの答えに対するゼロ知識証明
  - ➢答えを知っていることだけを証明


| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 8 | | | | | 5 | 1 | | |
| | | 1 | | | | 8 | | |
| | 4 | | 2 | | | | 9 | |
| | | | | 3 | | | | 2 |
| 1 | 2 | 3 | 4 | | 6 | 7 | 8 | 9 |
| 6 | | | | 1 | | | | 3 |
| | 8 | | | | 9 | 5 | | |
| | | 2 | | | | 4 | | |
| | | 7 | 6 | | | | | |

# カード組を用いた暗号プロトコルの実現

崎山·李·宮原 研究室

- ゼロ知識証明
  - 数独に対するゼロ知識証明[1]
  - シャッフル回数とカード枚数の削減[2,3]
- マルチパーティ計算
  - 投票プロトコルに用いるカード枚数の削減[4]
  - カード以外の物理道具の利用[5]

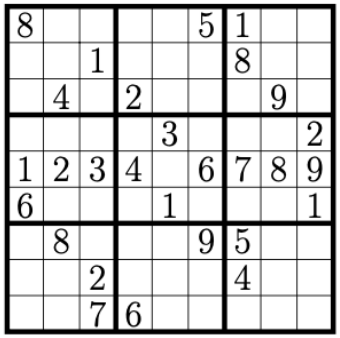



[1] Gradwohl, R. et al.: Cryptographic and physical zero-knowledge proof systems for solutions of Sudoku puzzles. ToCS (2009)
[2] Ruangwises, S.: Two standard decks of playing cards are sufficient for a ZKP for Sudoku. New Gener. Comput. (2022)
[3] Sasaki, T., Miyahara, D., Mizuki, T., Sone, H.: Efficient card-based zero-knowledge proof for Sudoku. Theor. Comput. Sci. (2020)
[4] Mizuki, T. et al.: Voting with a logarithmic number of cards. Unconventional Computation and Natural Computation. (2013)
[5] Murata, S., Miyahara, D., Mizuki, T., Sone, H.: Public-PEZ cryptography. ISC. (2020)

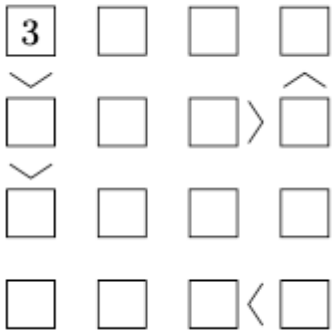
# 天秤を用いたゼロ知識証明

崎山·李·宮原 研究室

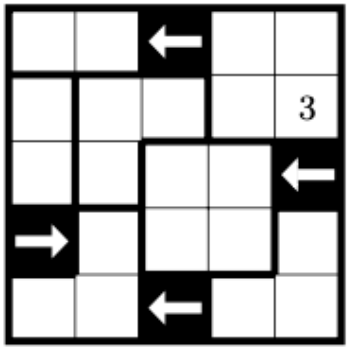
- ISC 2024[6]で天秤を用いたゼロ知識証明を発表
  - ➢数独を含む４つのパズルに対するプロトコルを構築
  - ➢セキュリティ証明を与え、効率性を評価
- SCIS 2025[7]で数独のプロトコルの効率化
  - ➢比較順序を工夫し比較回数を削減



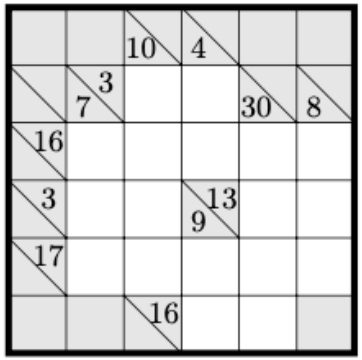
数独



不等式



マカロ



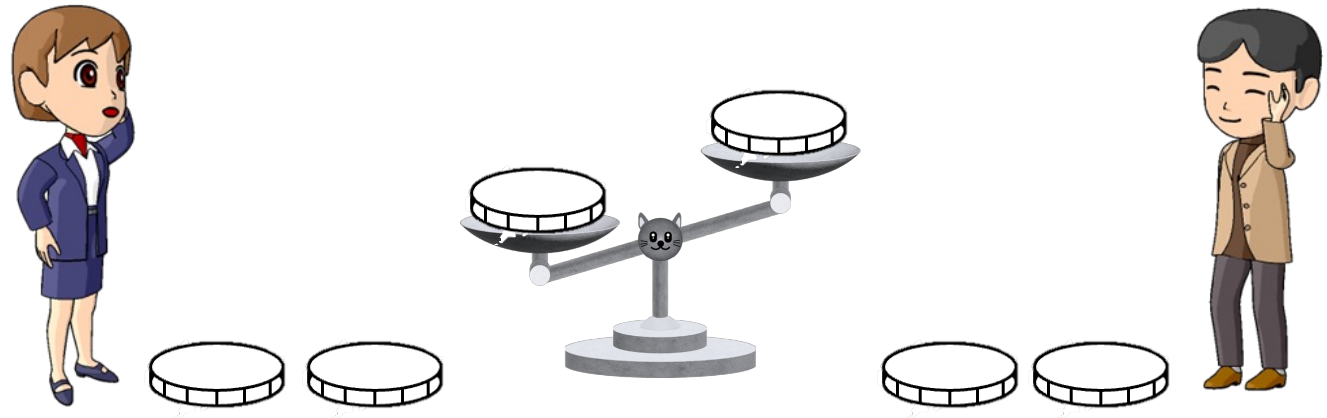
カックロ


[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)
[7] 金子尚平, 崎山一男, 宮原大輝, “天秤ベースゼロ知識証明の推進,”暗号と情報セキュリティシンポジウム(SCIS),(2025).

# 秘密計算

崎山·李·宮原 研究室

- DICOMO2023[8]で天秤ベース秘密計算を発表
  - 2入力ANDプロトコルとしきい値関数プロトコル
  - 計算モデルの作成
- Suthee Ruangwises[9]による研究
  - AND、しきい値関数、対象関数、任意のブール関数
  - 袋やペンを必要とするものがある

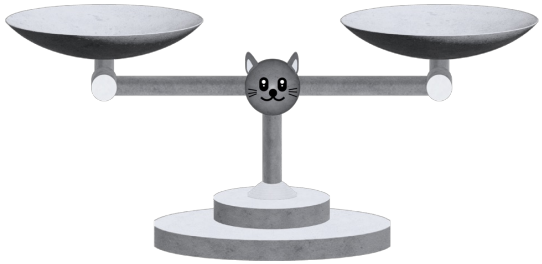


[8] 金子尚平, 李陽, 崎山一男, 宮原大輝, “天秤ベース秘密計算に対する計算モデルの構築,” DICOMO2023, (2023).
[9] Suthee Ruangwises.: Balance-Based Cryptography: Physically Computing Any Boolean Function. arXiv.(2025)

# 貢献

崎山·李·宮原 研究室

- 既存プロトコル[6]における比較回数の効率化
  - ➢トーナメント表を用いた比較順序の工夫
  - ➢カードベース暗号に現れない独自の改良
- 新しいソーティングアルゴリズムの提案
  - ➢ソートされていない2つの数列を同時にソート
  - ➢新しいアルゴリズムの設計と解析につながる



[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 対象とする問題の種類

崎山·李·宮原 研究室

- 本発表は数独の判定問題に対するZKPを扱う
- 解の一意性（一つしか存在しない）について：
  - ➢別解が存在することのZKPは大抵可能
  - ➢別解が存在しないことのZKPは不可能（と予想される）

NP問題
この数独は解けます

co-NP問題
この数独は解けません

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 8 | | | | | 5 | 1 | | |
| | | 1 | | | | 8 | | |
| | 4 | | 2 | | | | 9 | |
| | | | | 3 | | | | 2 |
| 1 | 2 | 3 | 4 | | 6 | 7 | 8 | 9 |
| 6 | | | | 1 | | | | 1 |
| | 8 | | | | 9 | 5 | | |
| | | 2 | | | | 4 | | |
| | | 7 | 6 | | | | | |

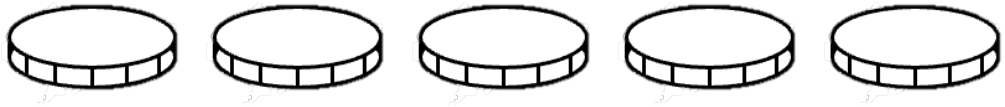
ASP問題
別解があります

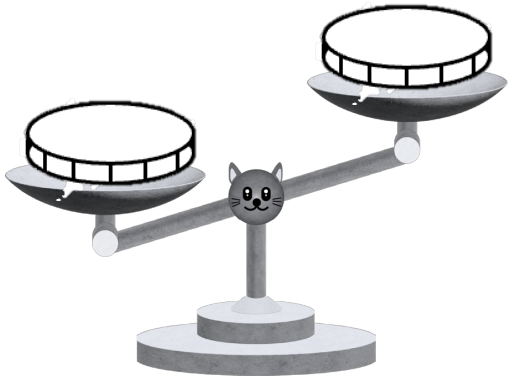
co-ASP問題
別解はありません

# 目次

# モデル

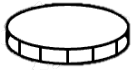
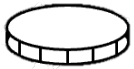
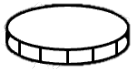
- 天秤とコインのシャッフルを利用
  - ➢コインの重さは見た目から区別できない
  - ➢コインの重さがそのマスの数字を表す
  - ➢一定の角度とスピードで傾く理想的な天秤を仮定

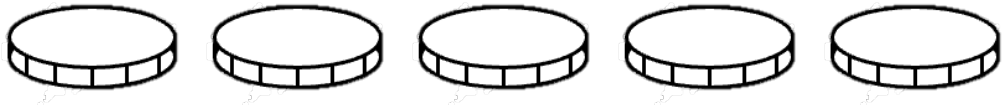


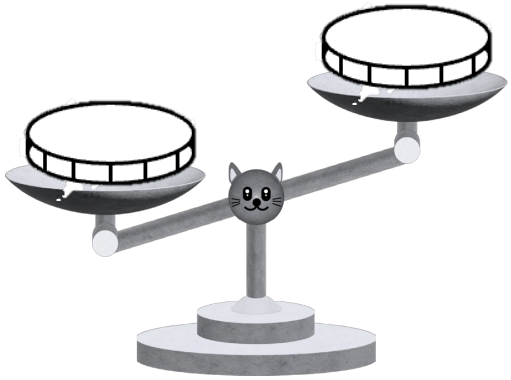


# モデル

崎山·李·宮原 研究室

- 天秤とコインのシャッフルを利用
  - コインの重さは見た目から区別できない
  - コインの重さがそのマスの数字を表す
  - 一定の角度とスピードで傾く理想的な天秤を仮定
- コインと天秤の利用
  - コインを  で表す
  - 2枚のコインの比較:  | 
  - シャッフルはコイン列を完全ランダムに並び替える





# 計算モデル

- DICOMO[8]でのコインの定式化
  - コインを$\textcircled{w}$で表し、$w > 0$ がコインの重さを表す
  - コインの集合を$C$ とする
  - 天秤は$C_1\ ops\ C_2$のように表し、$ops \in \{-,\ /,\ \backslash\}$は傾き

- 品川ら[10]による計算モデル
  - コインを$w$で表し、 $w > 0$ はコインの重さを表す
  - 比較操作を$f(C_1, C_2)$と表し、1, 2, 3を傾きとして出力

[8] 金子尚平, 李陽, 崎山一男, 宮原大輝, “天秤ベース秘密計算に対する計算モデルの構築,” DICOMO2023, (2023).
[10] 品川和雅, 縫田光司, “Mizuki-Shizuyaモデルとその周辺,”暗号と情報セキュリティシンポジウム(SCIS),(2025).

# 目次

# 既存プロトコル[6](準備)

崎山·李·宮原 研究室

- 1から9までの数字が1つずつ現れることを証明

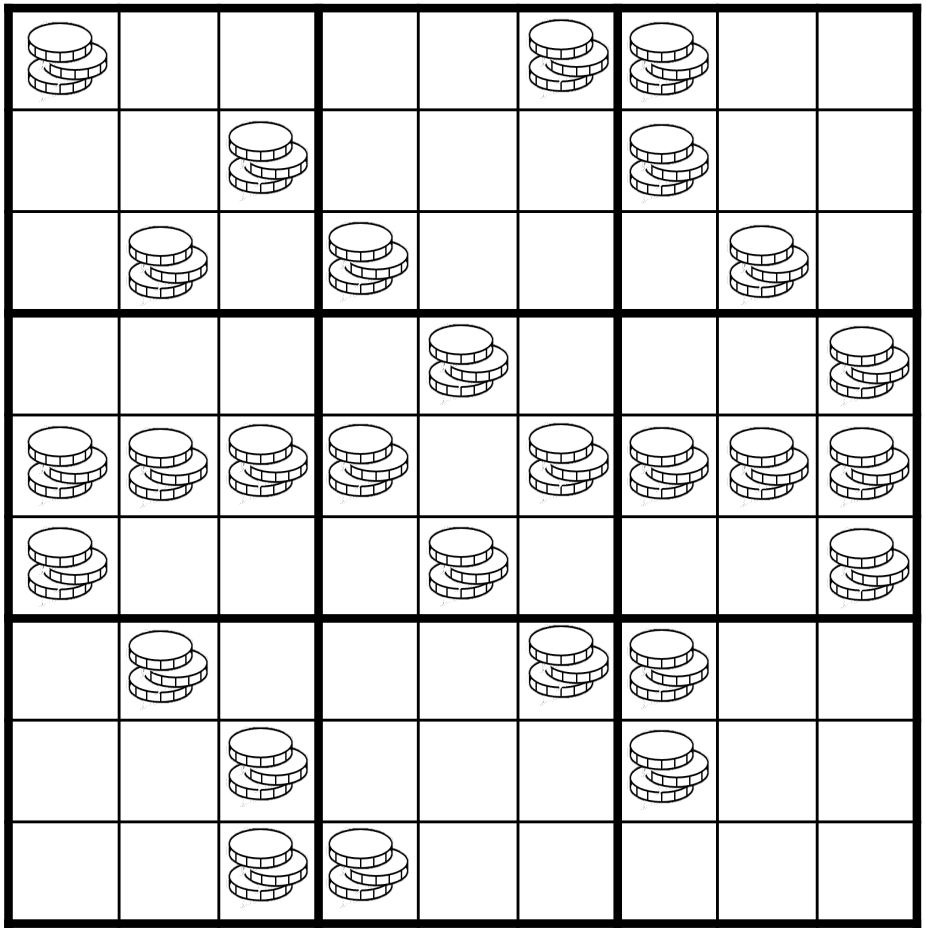
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 8 | | | | | 5 | 1 | | |
| | | 1 | | | | 8 | | |
| | 4 | | 2 | | | | 9 | |
| | | | | 3 | | | | 2 |
| 1 | 2 | 3 | 4 | | 6 | 7 | 8 | 9 |
| 6 | | | | 1 | | | | 3 |
| | 8 | | | | 9 | 5 | | |
| | | 2 | | | | 4 | | |
| | | 7 | 6 | | | | | |

[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 既存プロトコル[6](準備)

崎山·李·宮原 研究室

- 証明者は各セルに同じ重さのコインを3枚ずつ置く



[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 既存プロトコル[6](準備)

崎山·李·宮原 研究室

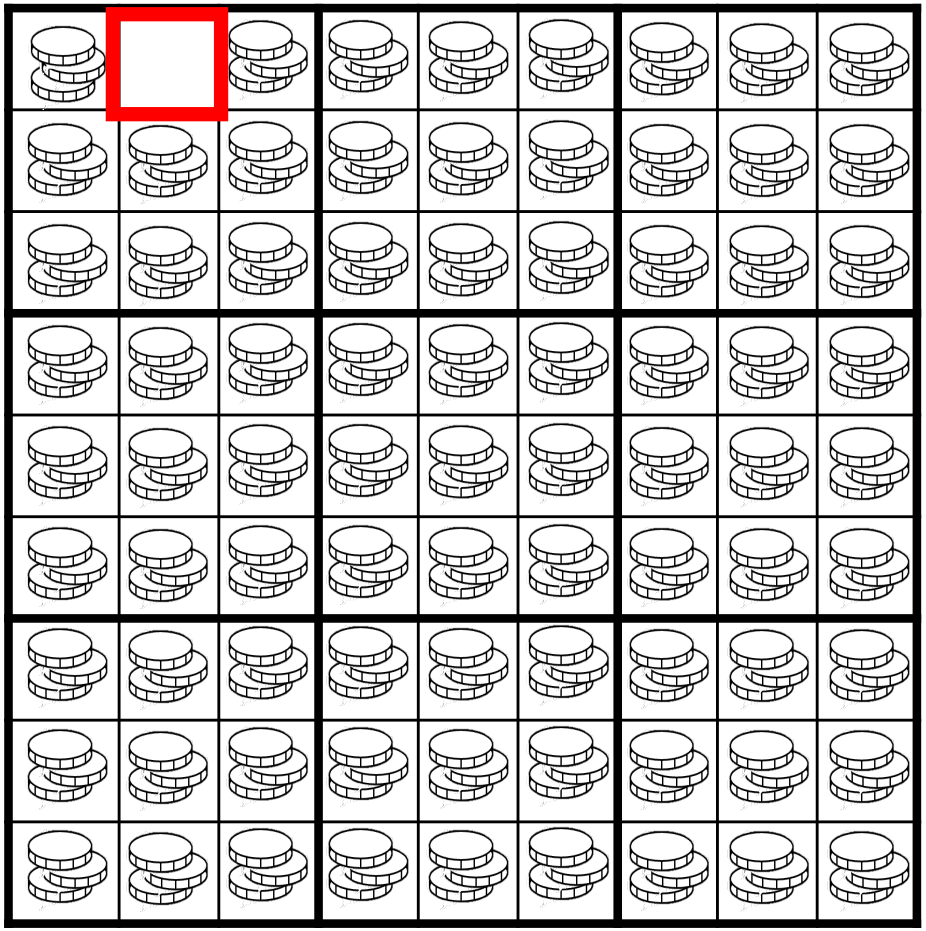
- 各セルに同じ重さのコインを3枚ずつ置く

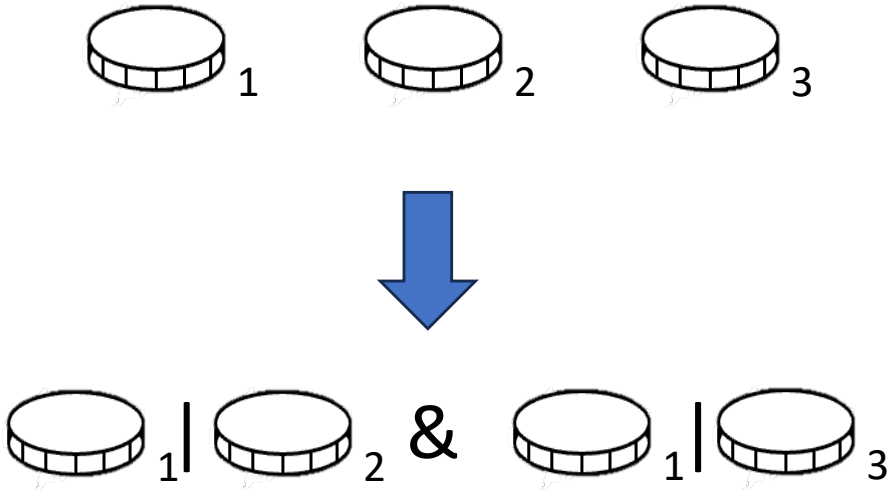
[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 既存プロトコル[6](準備)



- 各セルに同じ重さのコインを3枚ずつ置く
  - ➢空きマスに置かれた3枚の重さが等しいことを確認






[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 既存プロトコル[6](検証)

崎山·李·宮原 研究室

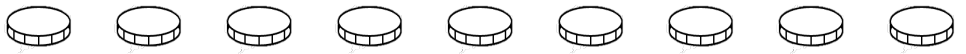
- 9枚のコインに1から9の重さが含まれることを証明

[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 既存プロトコル[6](検証)

崎山·李·宮原 研究室

- $R_1$の重さが全て違うことを検証

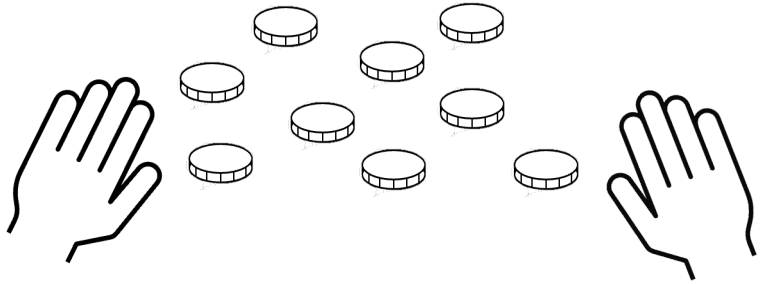


[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 既存プロトコル[6](検証)



- $R_1$の重さが全て違うことを検証

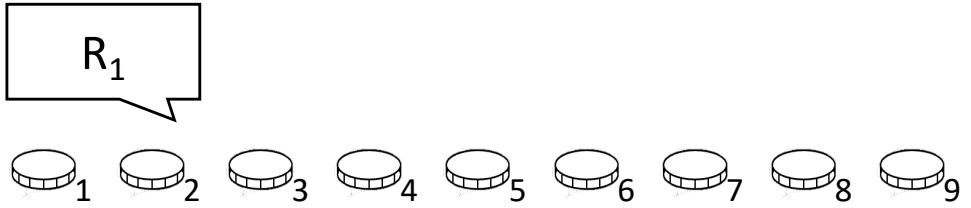


[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 既存プロトコル[6](検証)



- $R_1$の重さが全て違うことを検証

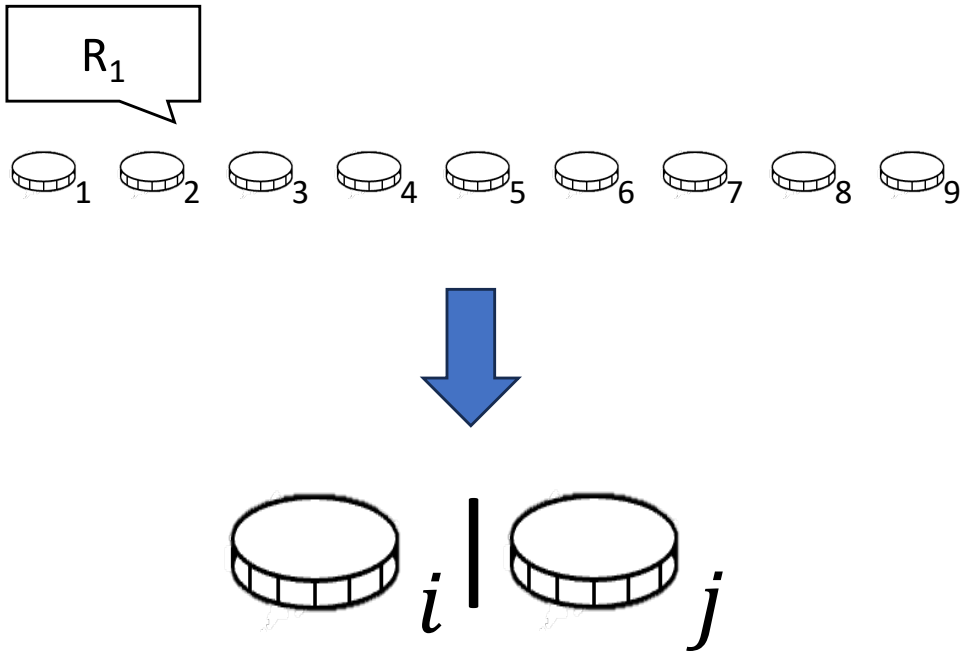



[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 既存プロトコル[6](検証)



- $R_1$の重さが全て違うことを検証



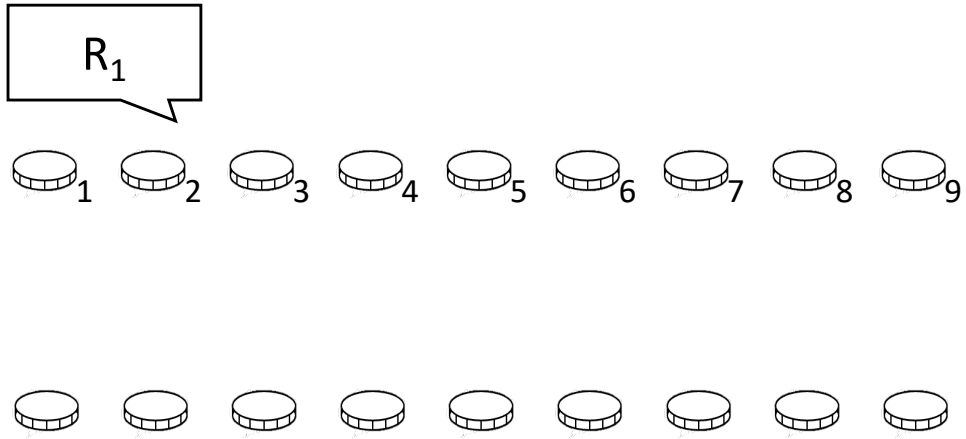

for all $i$ and $j$ such that $1 \leq i < j \leq 9$

[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 既存プロトコル[6](検証)



- $R_1$=$R_2$を検証し、$R_2$にも同じコインがあることを確認

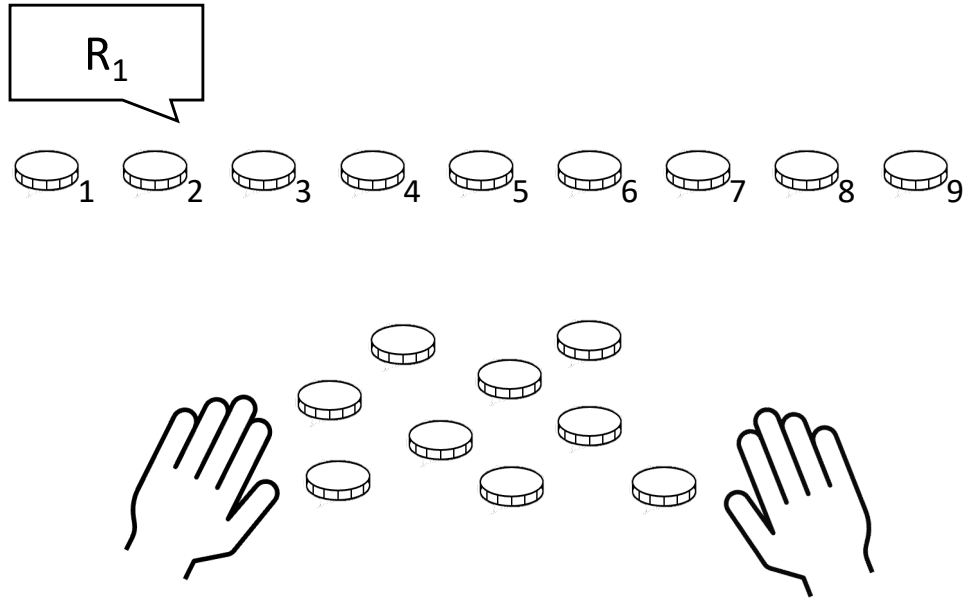



[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 既存プロトコル[6](検証)



- $R_1$=$R_2$を検証し、$R_2$にも同じコインがあることを確認



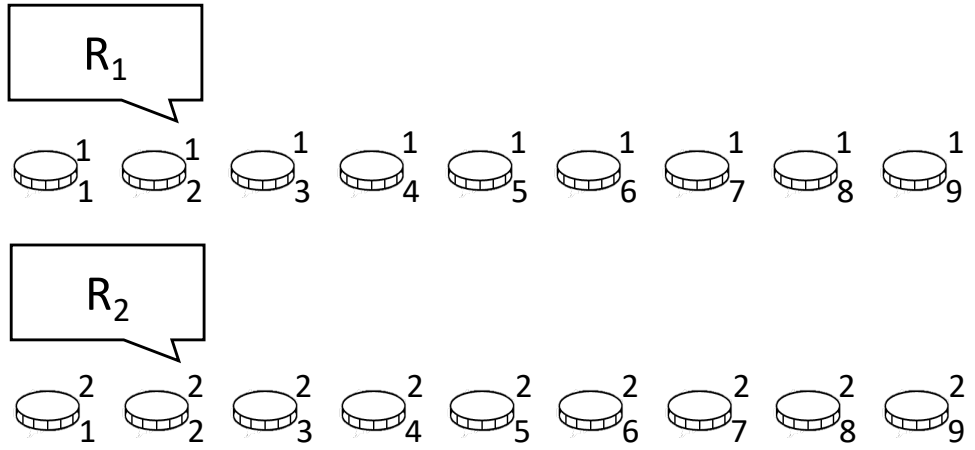



[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 既存プロトコル[6](検証)



- $R_1$=$R_2$を検証し、$R_2$にも同じコインがあることを確認

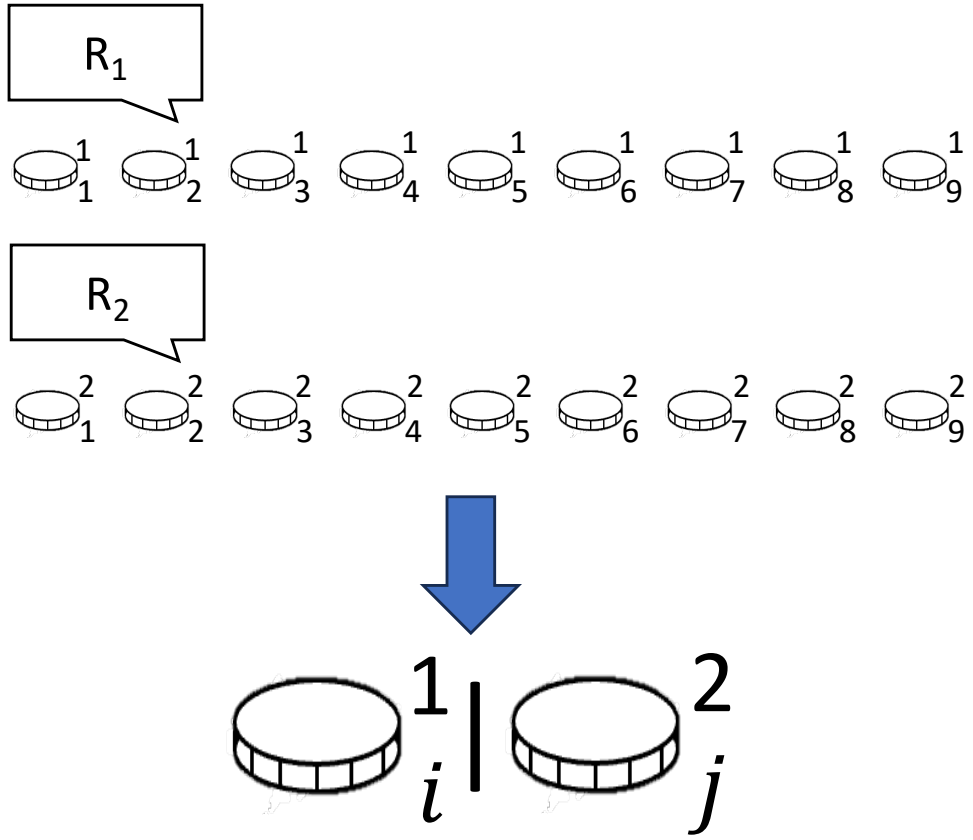



[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 既存プロトコル[6](検証)



- $R_1$=$R_2$を検証し、$R_2$にも同じコインがあることを確認



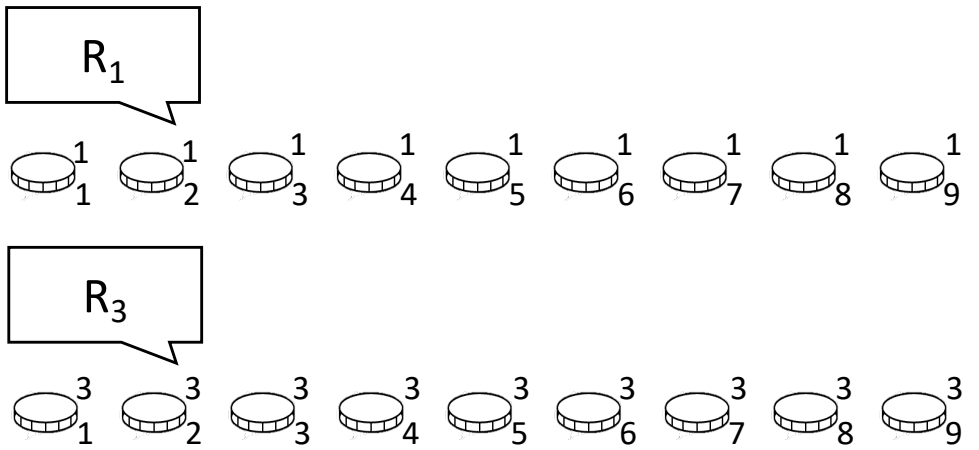

for all $i$ and $j$ such that $1 \leq i, j \leq 9$

[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 既存プロトコル[6](検証)

崎山·李·宮原 研究室

- $R_3$から$R_{27}$も同様に検証
  - ➢列が$R_{10}$～$R_{18}$、ブロックが$R_{19}$～$R_{27}$に対応

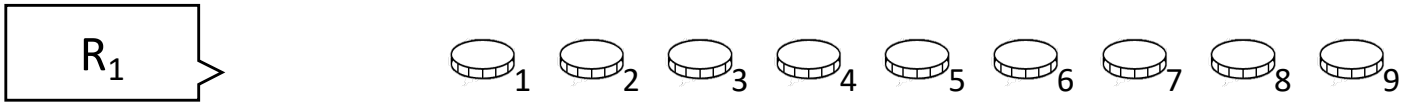



[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# クイックソートを用いた効率化[6]



- 1列目の検証にクイックソートを用いる
  - ソートしながら天秤が釣り合わないことを確認

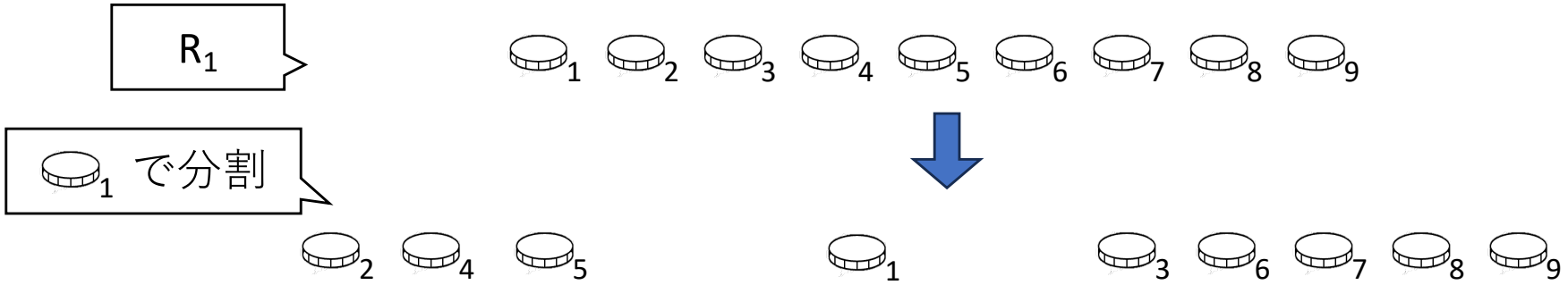



[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# クイックソートを用いた効率化[6]

崎山·李·宮原 研究室

- 1列目の検証にクイックソートを用いる
  - ➢ソートしながら天秤が釣り合わないことを確認

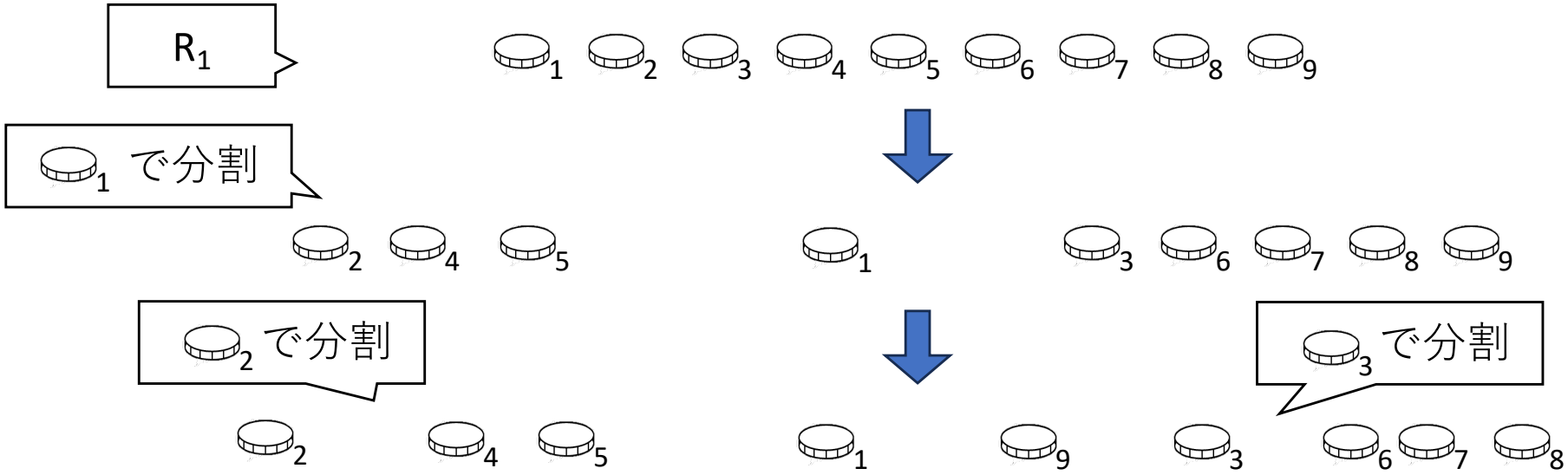



[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# クイックソートを用いた効率化[6]



- 1列目の検証にクイックソートを用いる
  - ➢ソートしながら天秤が釣り合わないことを確認

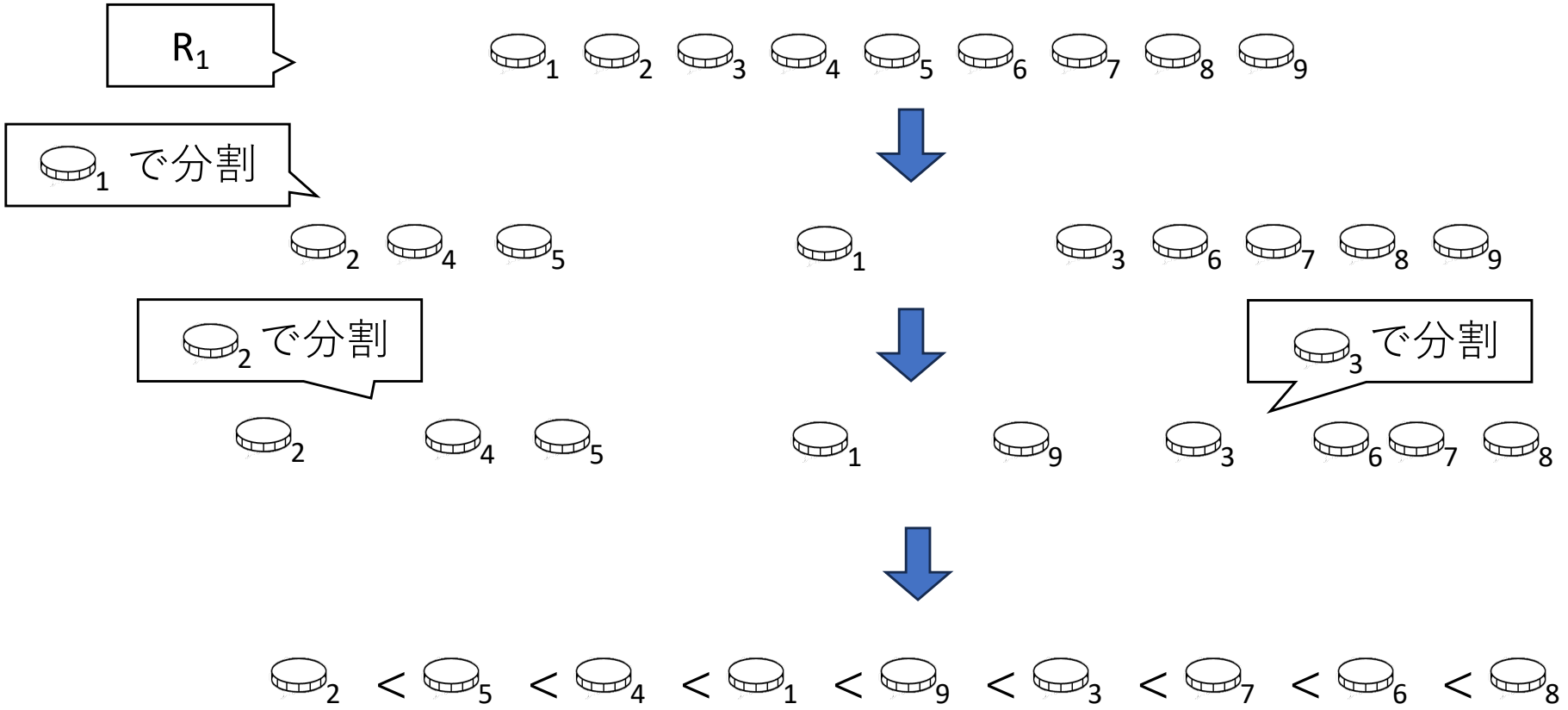



[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# クイックソートを用いた効率化[6]

崎山·李·宮原 研究室

- 1列目の検証にクイックソートを用いる
  - ➢ソートしながら天秤が釣り合わないことを確認

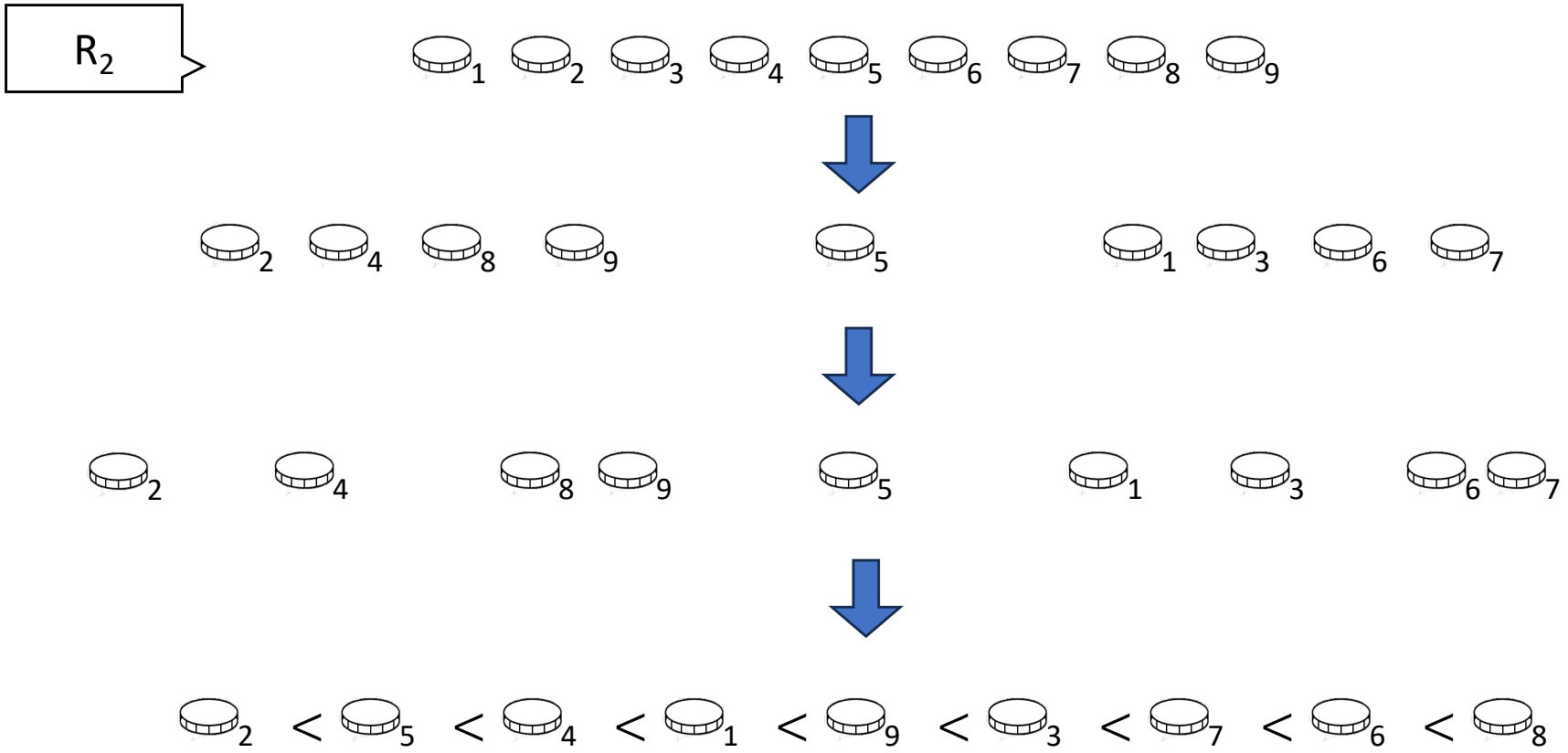



[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# クイックソートを用いた効率化[6]

崎山·李·宮原 研究室

- 残りの検証では最速クイックソートが可能
  - ソートされた$R_1$から最適なピボットを選択
  - 比較回数は25回（全比較の36回より効率的）

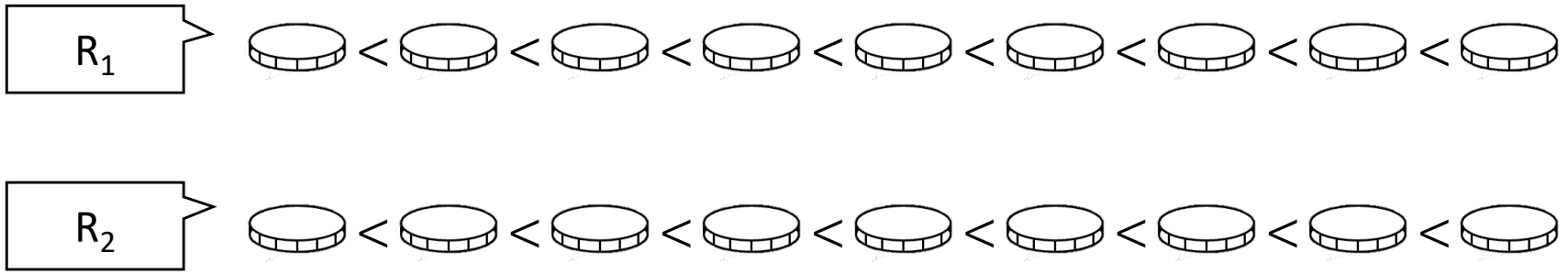



[6] Kaneko, S. et al.: Balance-based ZKP protocols for pencil-and-paper puzzles. ISC. (2024)

# 目次

# アイデア

- ソートされた２列の同一検証は簡単
  - ➢軽い方のコインから順に比較する（合計9回）



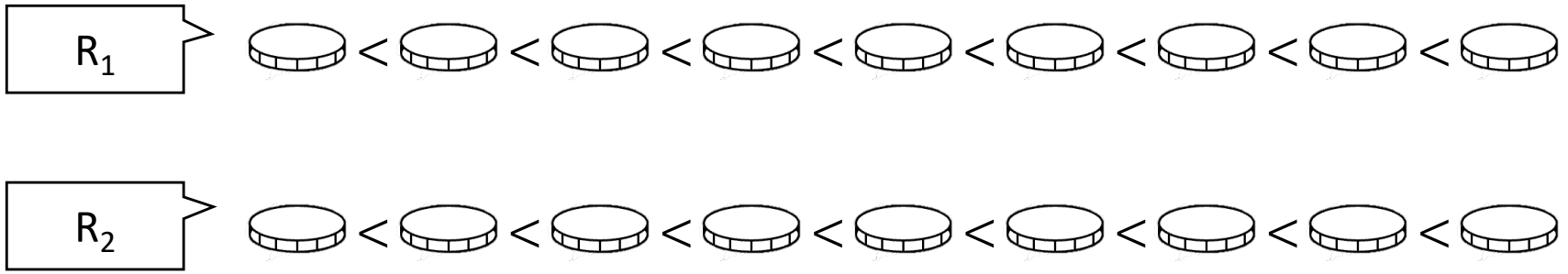
# アイデア



- ソートされた２列の同一検証は簡単
  - ➢軽い方のコインから順に比較する（合計9回）
- 検証の順番を工夫することによる効率化
  - ➢既存：$R_1=R_2$, $R_1=R_3$, …, $R_1=R_{27}$のように順番に検証
  - ➢提案：$R_1=R_2$, $R_3=R_4$, $R_1=R_3$ ,…のようにトーナメント検証

２列同時ソート

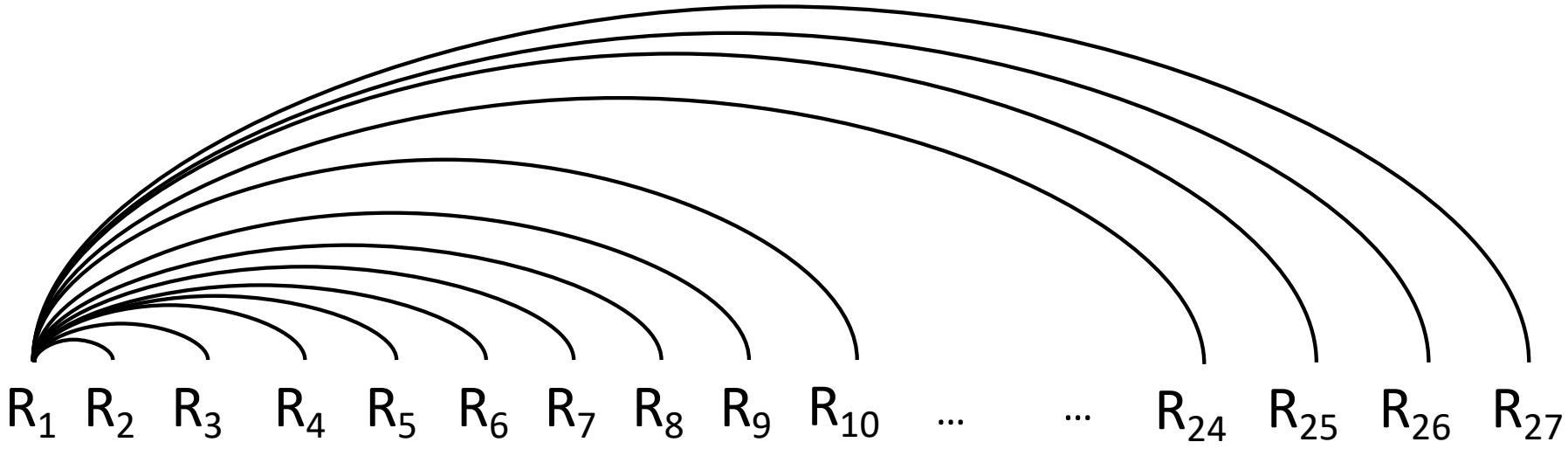
9回



# 提案プロトコル

崎山·李·宮原 研究室

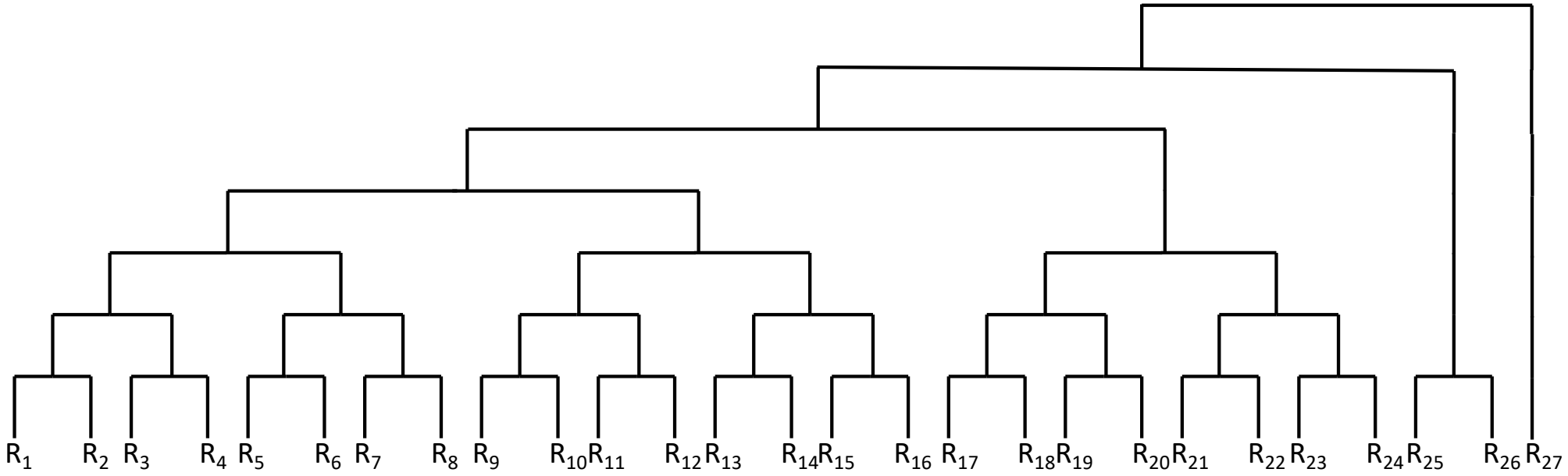
- 既存プロトコルの比較の順序



# 提案プロトコル

崎山·李·宮原 研究室

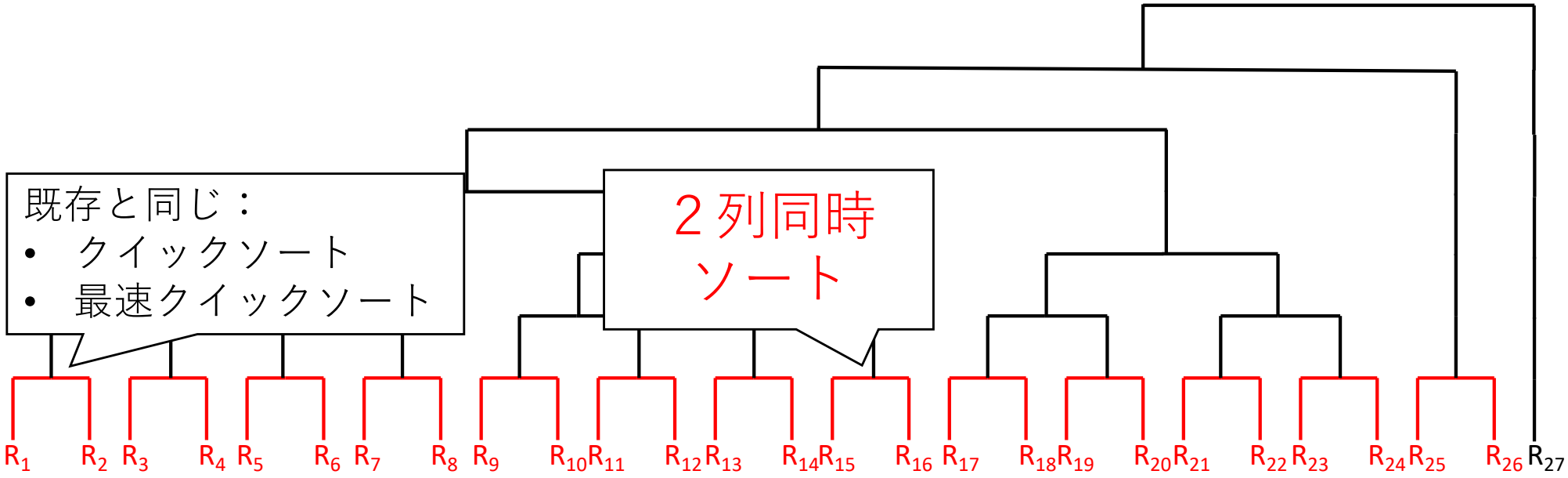
- トーナメントの表を用いて比較



# 提案プロトコル

崎山·李·宮原 研究室

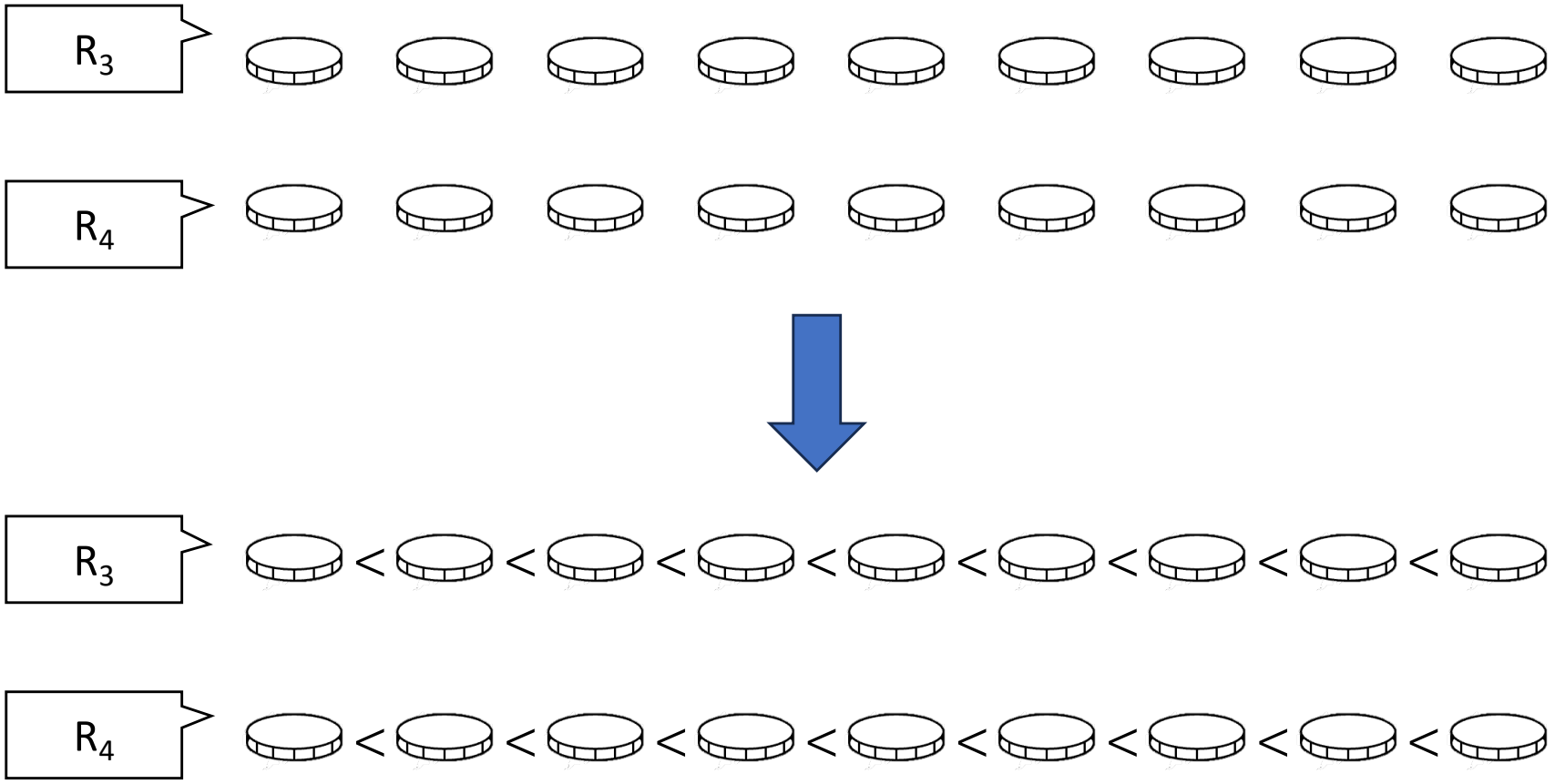
- トーナメントの表を用いて比較
  1. コイン列ごとのペアを作成
  2. 各ペアが等しいことをソートしながら検証（1回戦）
  3. ペアから1列ずつ選んで検証（2回戦以降）
  4. 1つだけソートされてないペアとの検証（決勝戦）



# 2列同時ソート



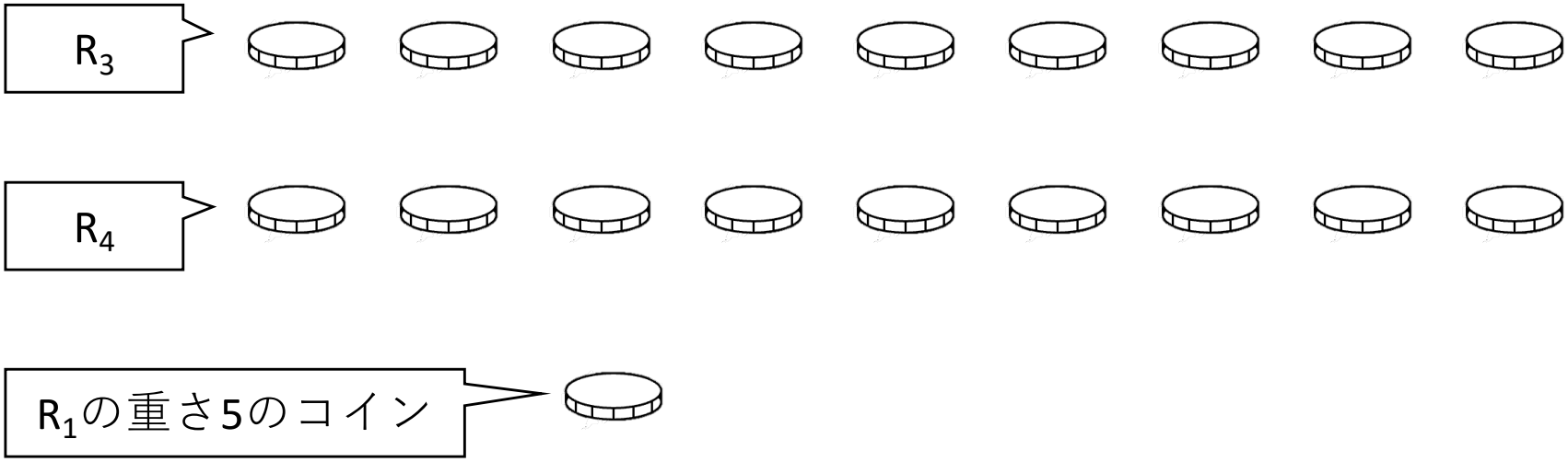
- 9枚のソートされていないコインを同時にソート



# 2列同時ソート



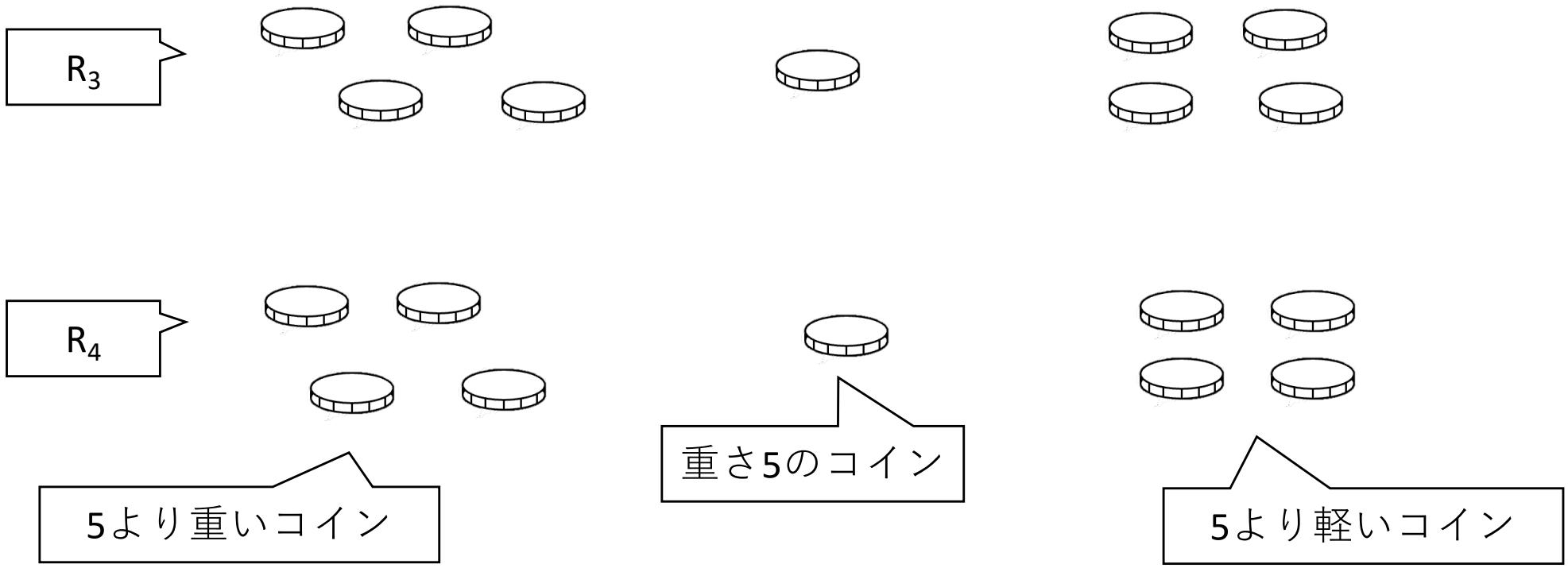
- 2列を半分に分ける
  - ➢全てのコインを重さ5のコインと比較



# 2列同時ソート



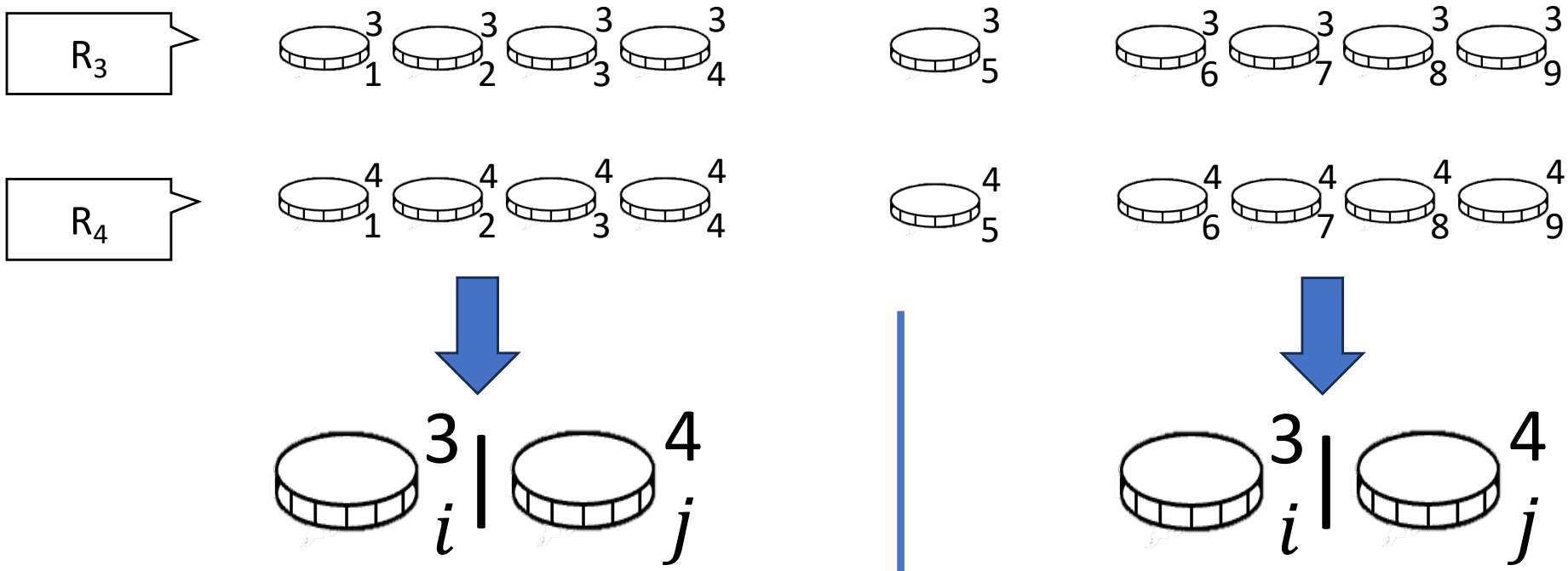
- 2列を3つに分ける



# 2列同時ソート



- 各グループのコインをすべて比較




for all $i$ and $j$ such that $1 \leq i, j \leq 4$

for all $i$ and $j$ such that $6 \leq i, j \leq 9$

# 目次

# 性能比較



- 既存プロトコル
  - $N_q$:クイックソートに必要な比較回数
  - 最適クイックソートに必要な比較回数は25回

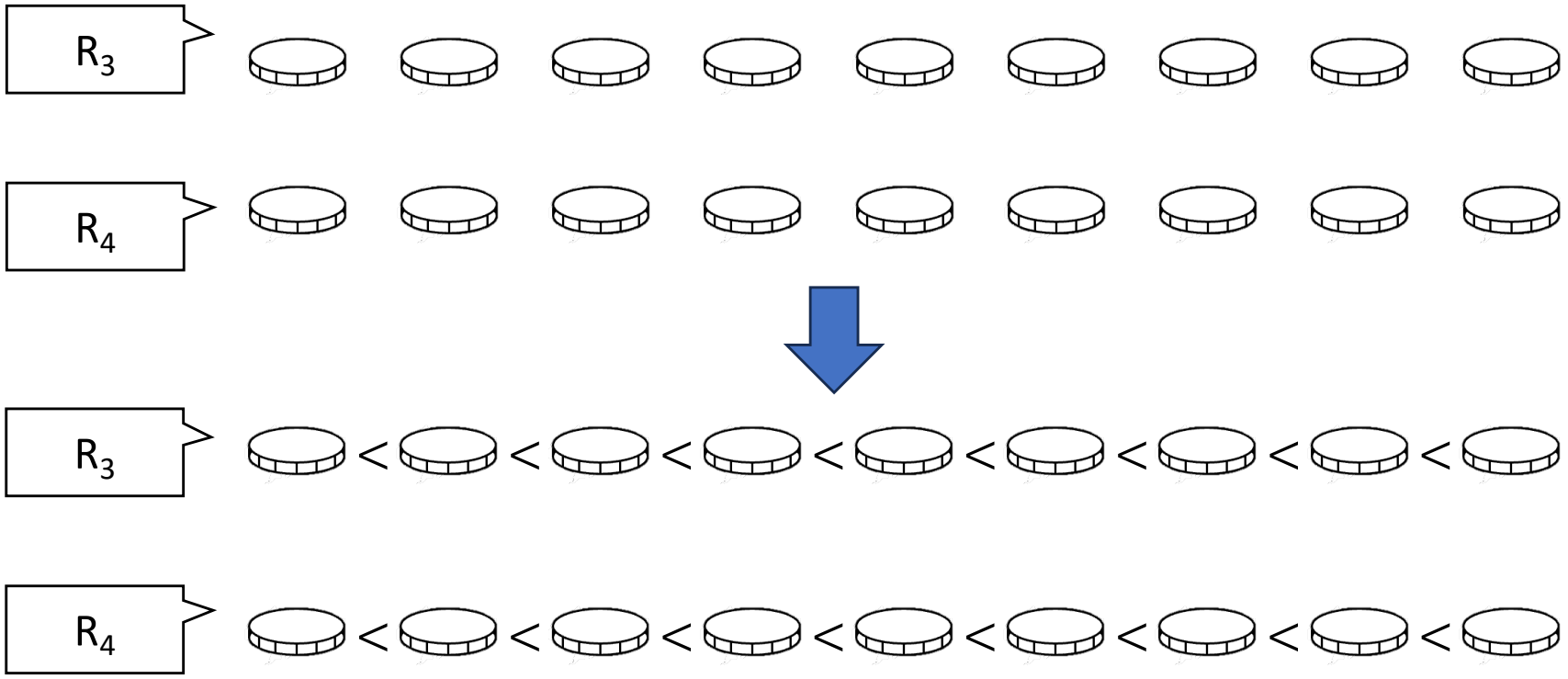
$$N_q + 25{\times}26 = N_q + 650$$

- 提案プロトコル
  - $N_p$:2列同時ソートに必要な比較回数

$$N_q + 25 + 12N_p + 12{\times}9 + 25 = N_q + 12N_p + 125$$

# 性能比較

- 2列同時ソートの比較回数を削減
  - ➢$N_p$を40回以下に抑えたい
  - ➢2列同時ソートの最悪の比較回数は38回

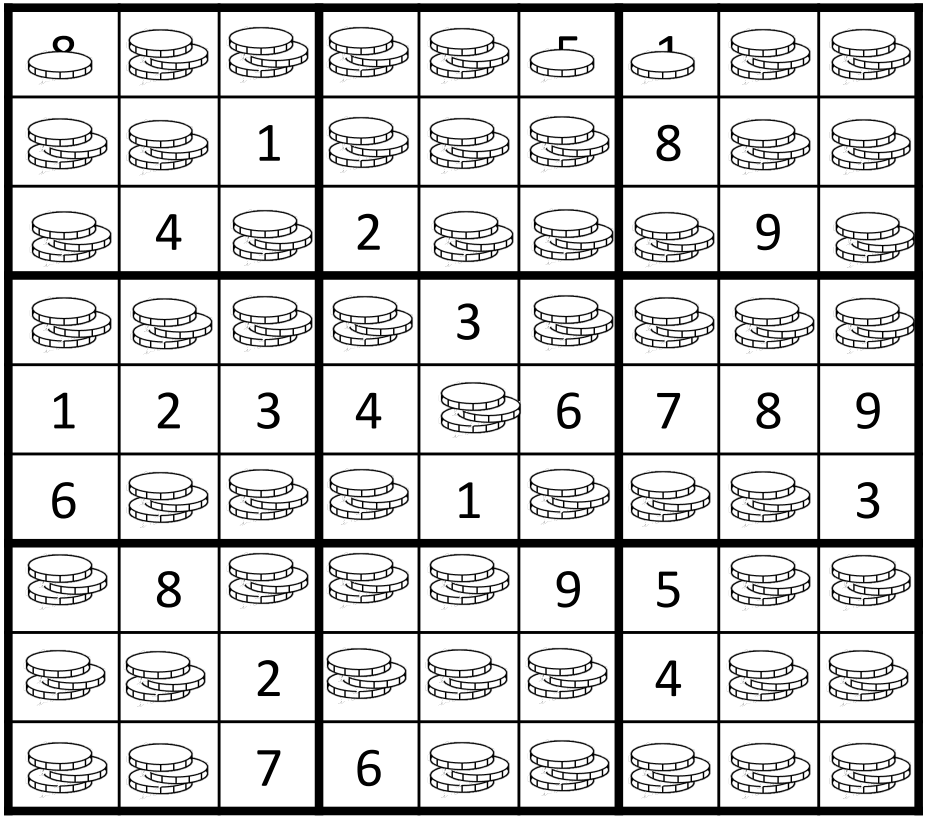


# 目次

# コインを削減したプロトコル



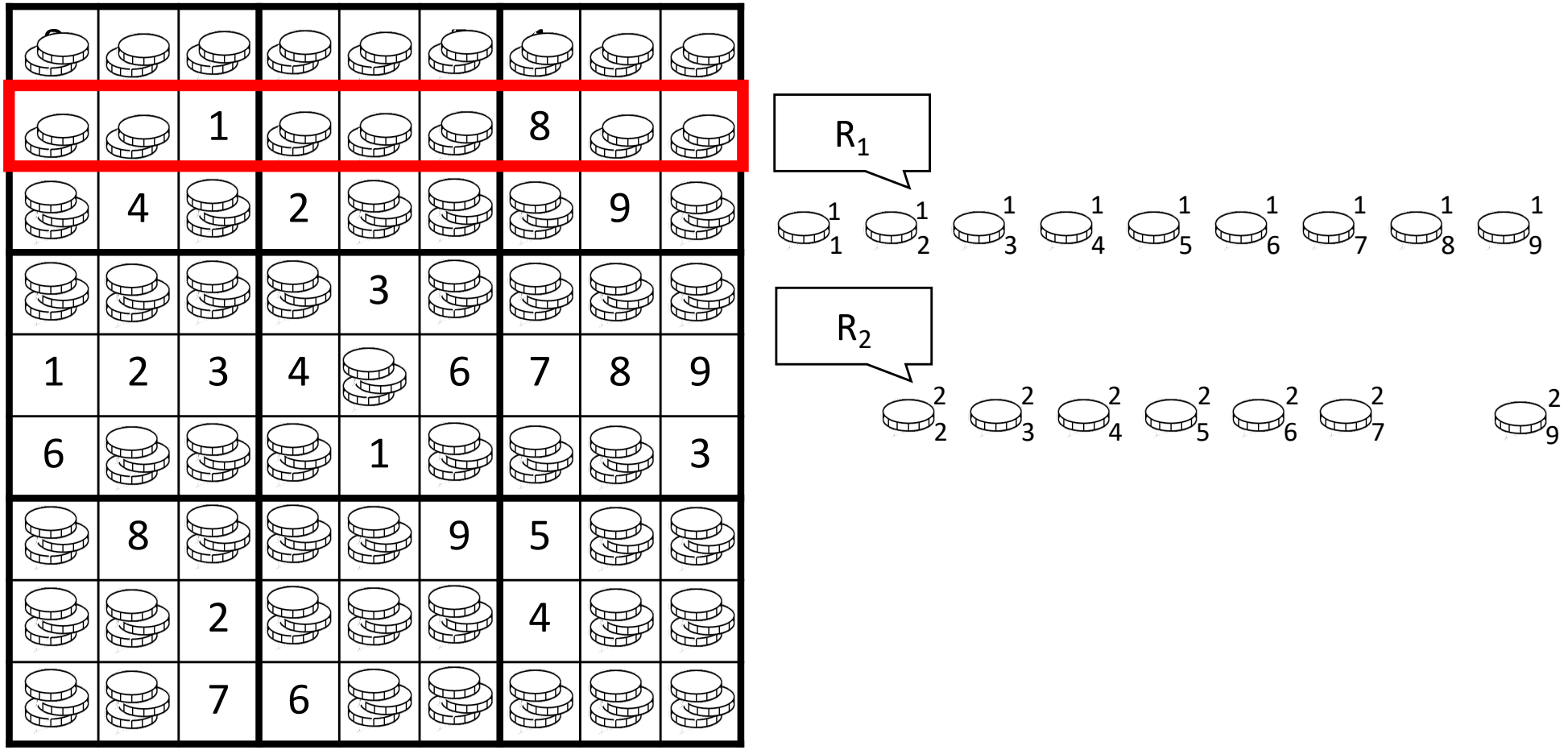
- コインの枚数と天秤の利用回数を削減する
  - ➢すでに数字が書かれたマスにはコインを置かない プロトコルをSSSSで発表予定



# コインを削減したプロトコル



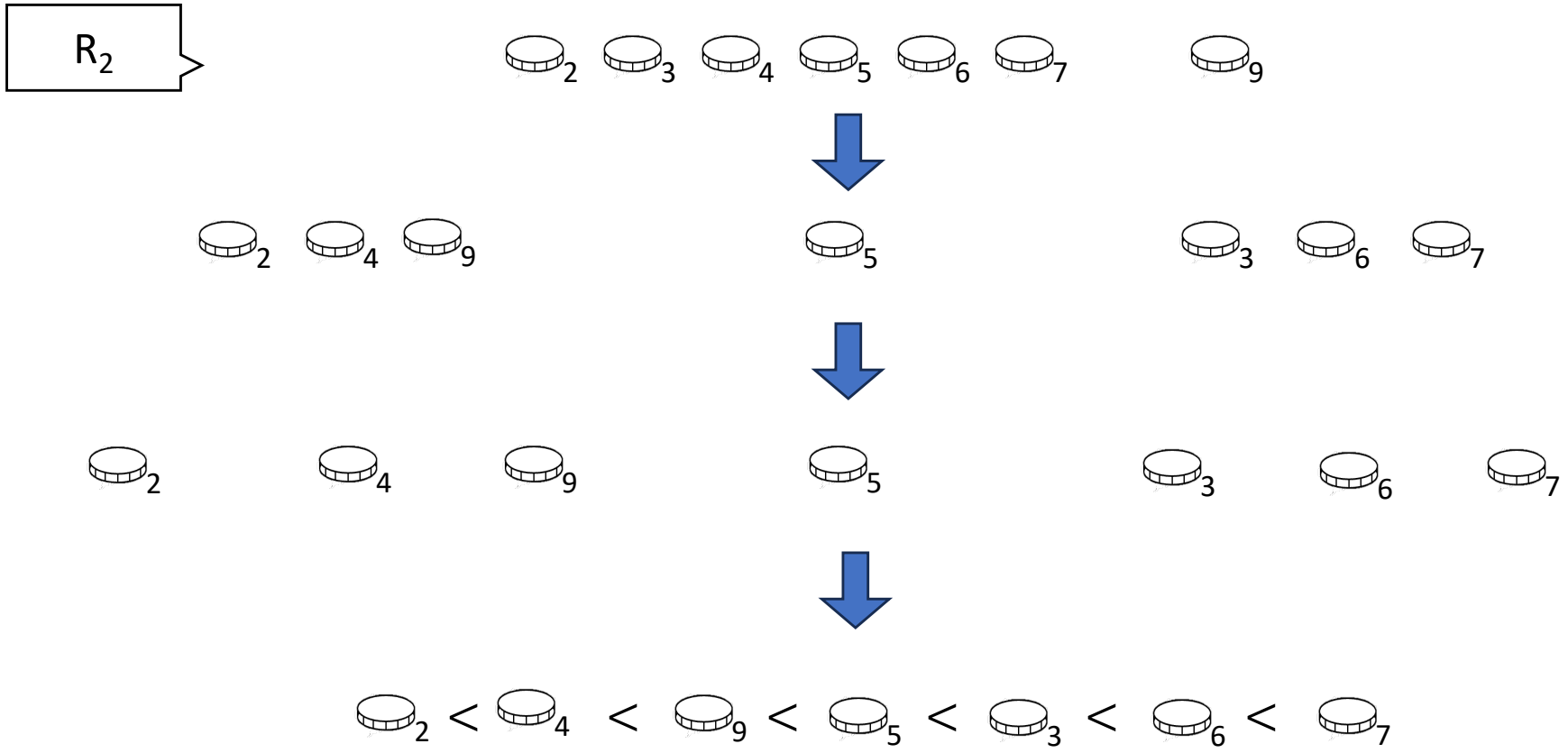
- 7枚だけ一致することを確認



# 最速クイックソート

崎山·李·宮原 研究室

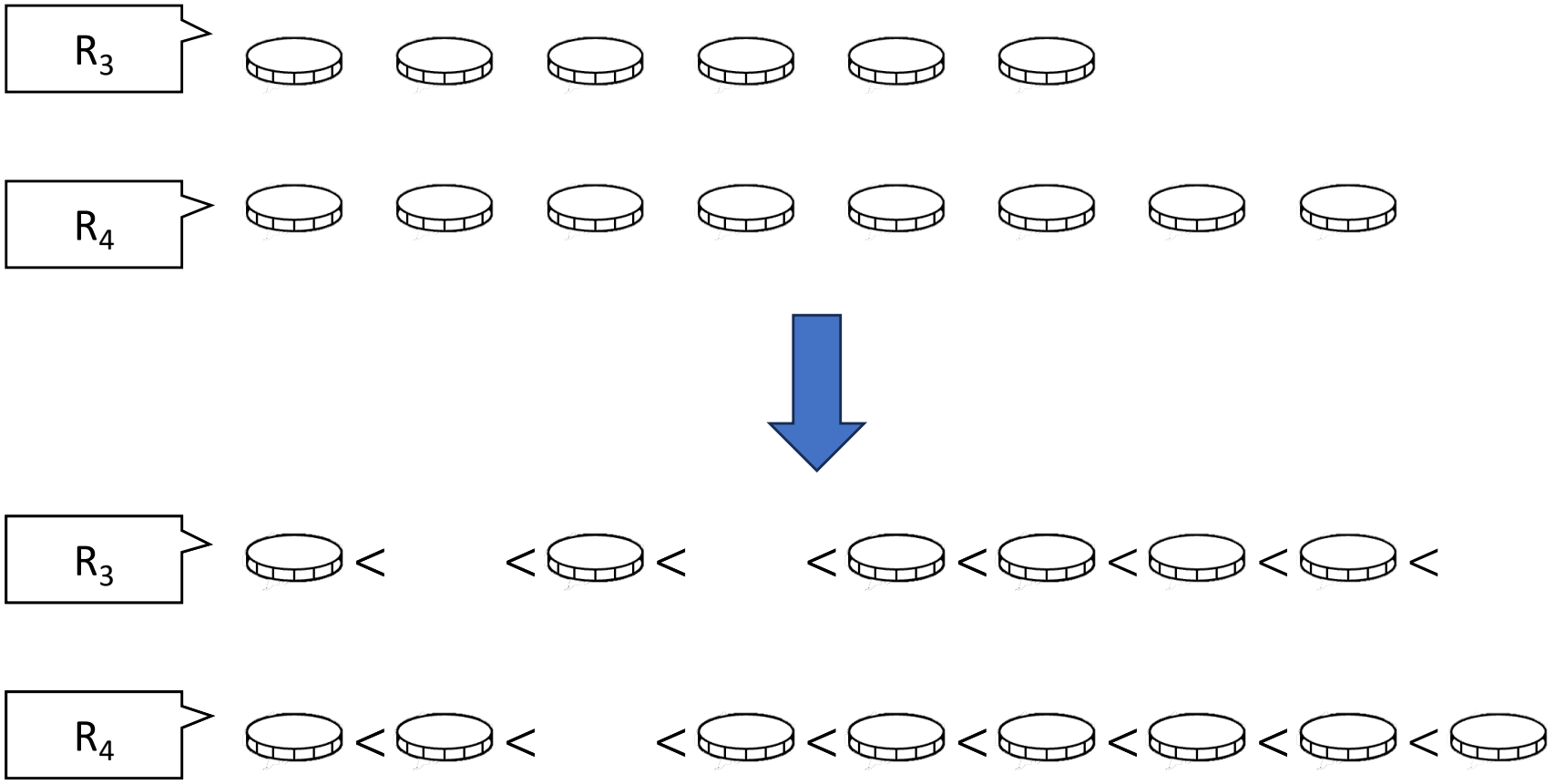
- コインが抜けたまま最速クイックソート



# トーナメント方式



- コインが少ないままソート
  - ➢穴の数や場所によって比較回数が変わる



# トーナメント方式



- 穴あきの状態でトーナメント
  - ➢穴を埋めながら次の比較をする