障害論理式による
集合合意問題の不可解性証明について

八木 滉希　　京都大学 理学研究科・M2

西村 進　　京都大学 理学研究科

GRADUATE SCHOOL OF FACULTY OF SCIENCE
KYOTO UNIVERSITY

背景

- Topological method [Herlihy&Shavit 1999]
  - **入出力を幾何 (単体的複体) の変形ととらえる**
  - **幾何的障害 (矛盾) により分散タスクの不可解性を示す**

- Logical method [Goubault, et al. 2018]
  - **論理的障害 (障害論理式) により分散タスクの不可解性を示す**
    - **障害論理式の具体例はほとんどなし**

- [**西田** 2020] wait-free **集合合意に対する障害論理式を構成**

本研究

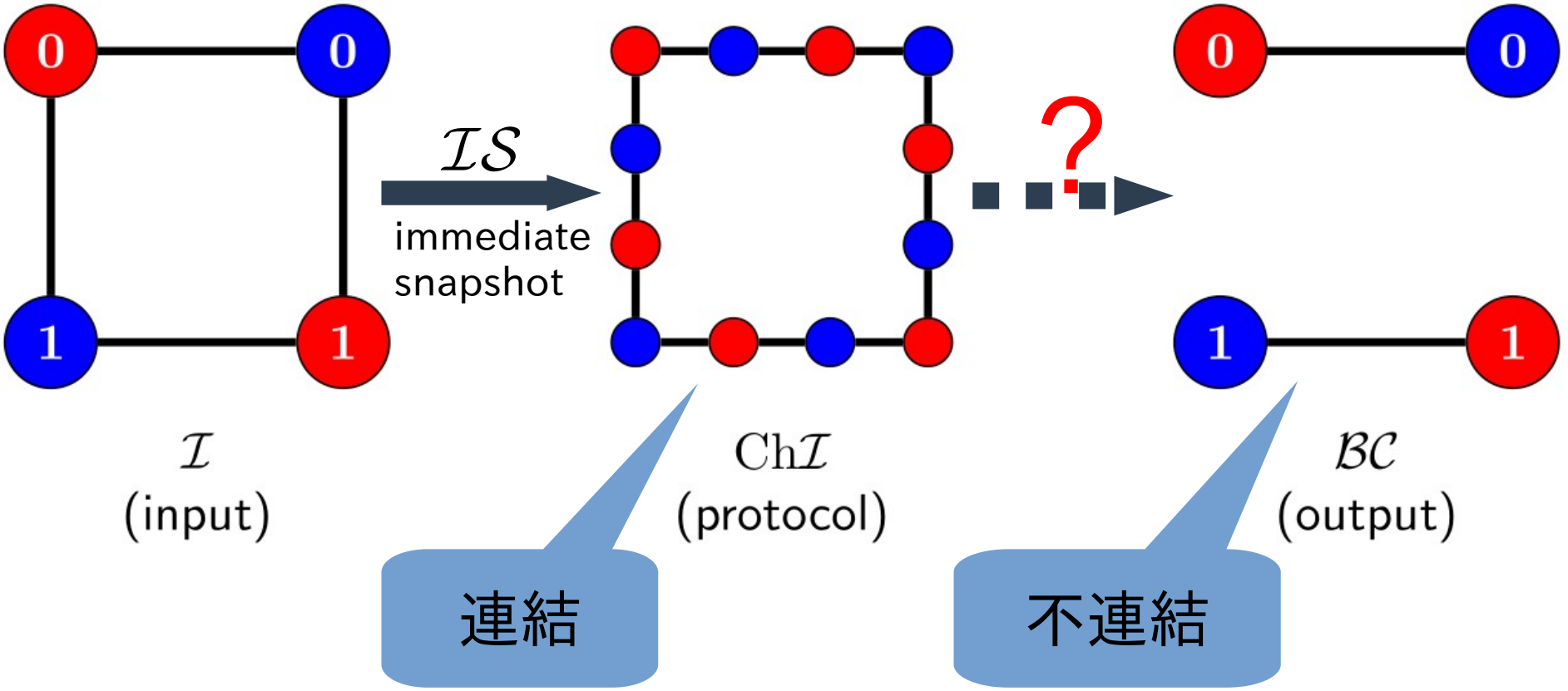
- Logical method により adversary のもとでの集合合意の不可解性を示す
  - Adversary に対しても適用可能な障害論理式を構成
  - [西田 2020] の結果の一般化 (wait-free を adversary に一般化)

問題設定

- 分散システム
  - $n\ (\geq 1)$ プロセス，非同期，共有メモリ
- 耐故障性
  - Adversary (wait-free を特殊例として含む)
- k- 集合合意 $(k < n)$
  - 出力値は入力値のいずれか
  - 異なる出力値は高々 k 個

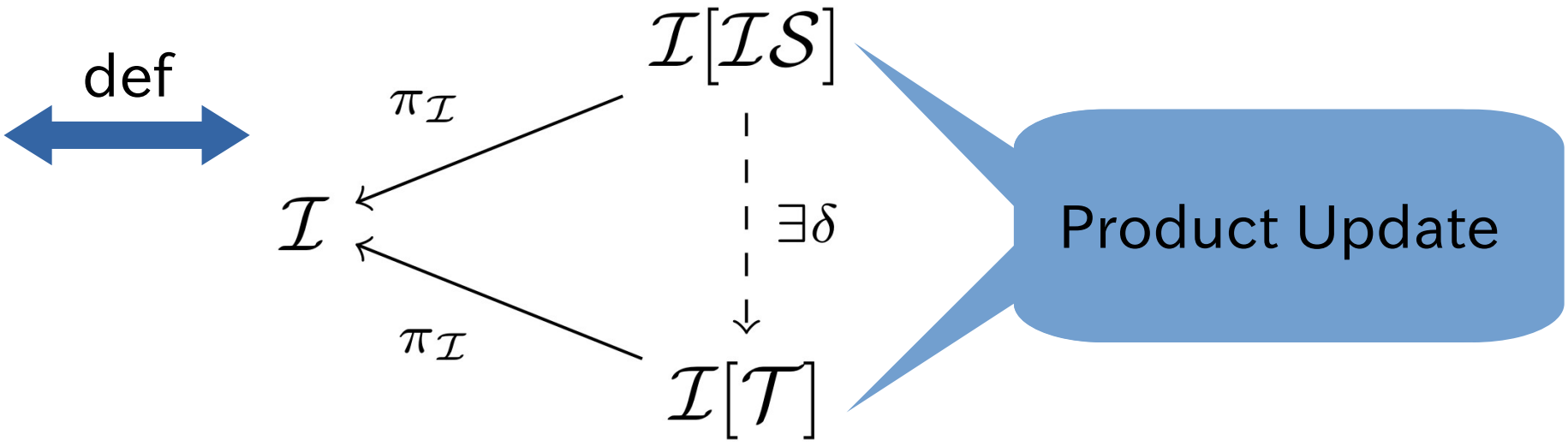
Topological method

例 : wait-free binary consensus (1-**集合合意**)



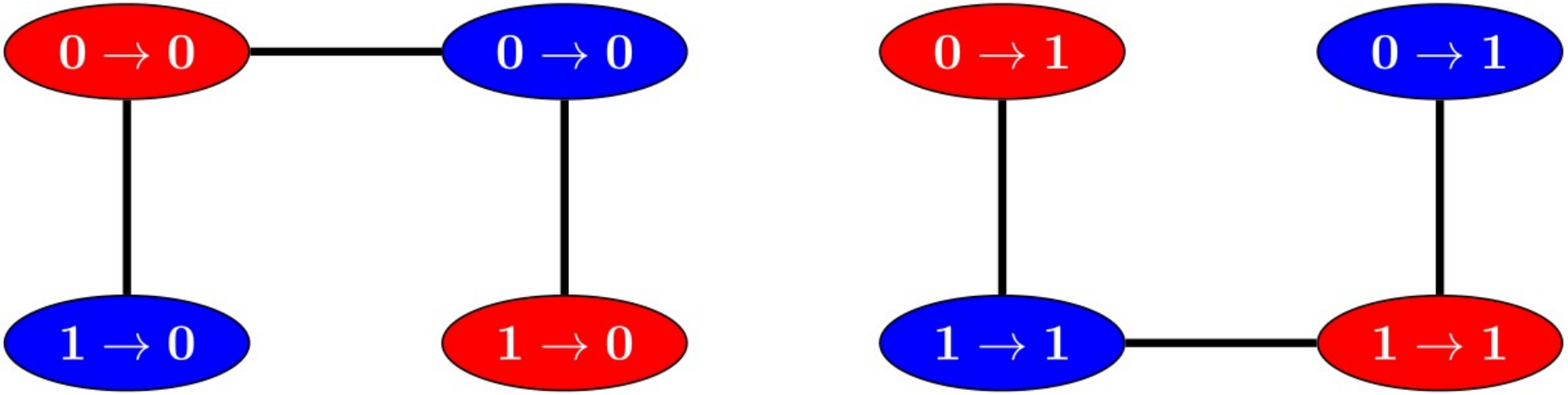
Logical method におけるタスク可解性 [Goubault, et al.]

タスク $\mathcal{T}$ が即時スナップショット $\mathcal{IS}$ で解ける



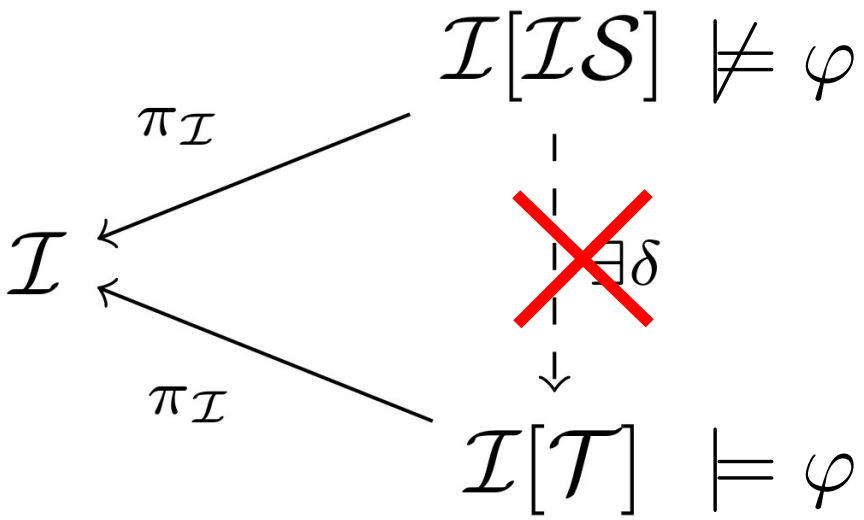
Product Update

入力 / 出力の関数 ＝ 二項関係



$\mathcal{I}[\mathcal{BC}]$
(input/output)

障害論理式による不可解性証明 [Goubault, et al.]



このような φ を
障害論理式と呼ぶ

論理式 (認識論理)

$$\varphi ::= \mathrm{input}_a^i \mid \neg\varphi \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \mathrm{K}_a\varphi \mid \mathrm{D}_A\varphi$$

プロセス a の入力値が i

プロセス a は φ であると知っている

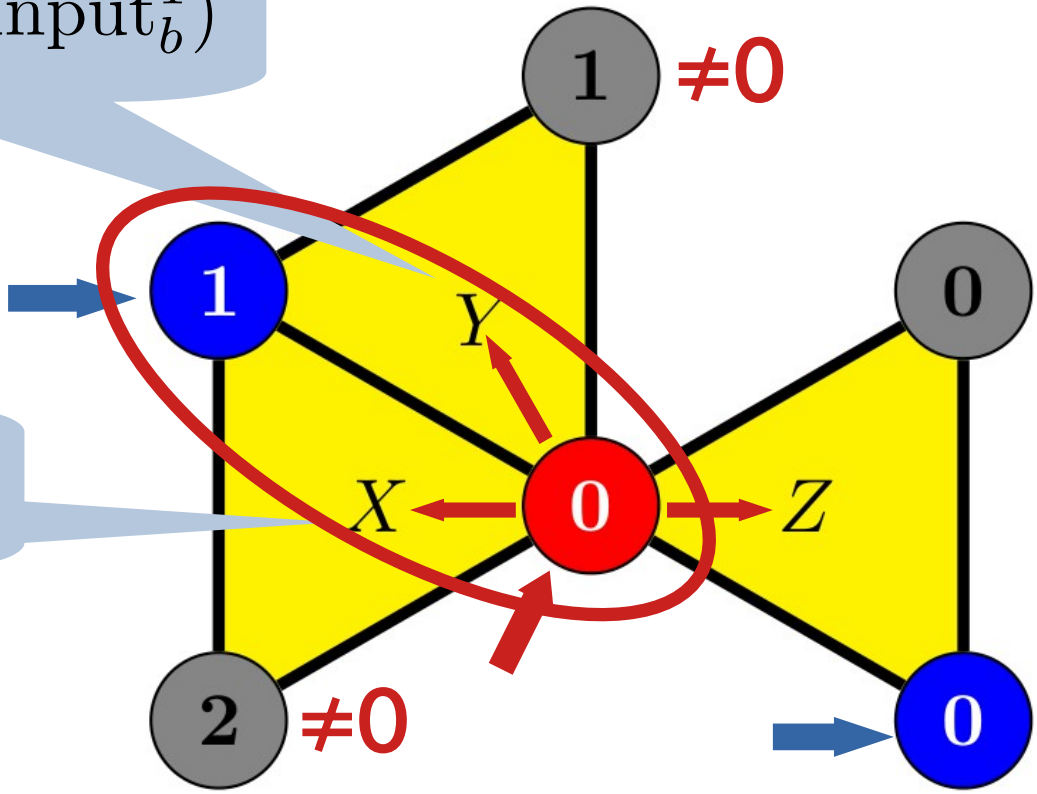
A に属するプロセスの知識を合わせれば φ であるとわかる

認識論理式の例

例 . 3 プロセス : r, b, g

$$Y \models \mathrm{K}_r(\mathrm{input}_b^0 \vee \mathrm{input}_b^1)$$

$$X \models \mathrm{D}_{r,b}\neg\mathrm{input}_g^0$$



Adversary

- Adversary $\mathcal{A} \subseteq 2^{\Pi}$ （Πはプロセス全体の集合）
  - 故障しないプロセスの集合（の集合）
  - Superset-closed を仮定 ($B \supseteq A \wedge A \in \mathcal{A} \Rightarrow B \in \mathcal{A}$)

- $\mathcal{A}$のコア集合：以下を満たす極小な$C \subseteq \Pi$

$$\forall A \in \mathcal{A}. C \cap A \neq \emptyset$$

- Round operator $\mathcal{R}_{\mathcal{A}}$ [Herlihy&Rajsbaum 2010]
  - Wait-free のときの$\mathcal{IS}$に対応

集合合意問題の障害論理式 (adversary ver.)

$$\bigvee_{i \in \Pi} \neg \mathrm{input}_i^i \vee \bigvee_{A \subseteq \Pi, |A| < c} \Psi_A$$

※ c は $\mathcal{A}$ のコア集合の最小サイズ

$$\Psi_A = \begin{cases} \text{false} & \text{if some core set does not intersects with } \Pi \setminus A \\ \mathrm{D}_A \psi_A & \text{otherwise} \end{cases}$$

$$\psi_A = \bigvee_{i \in \Pi \setminus A} \neg \mathrm{input}_i^i \vee \bigvee_{i \in \Pi \setminus A} \mathrm{K}_i \left(\bigvee_{j \in A} \bigvee_{k \in \Pi} \mathrm{input}_j^k \right) \vee \bigvee_{B \supsetneq A} \Psi_B$$

- [西田 2020] の障害論理式の一般化

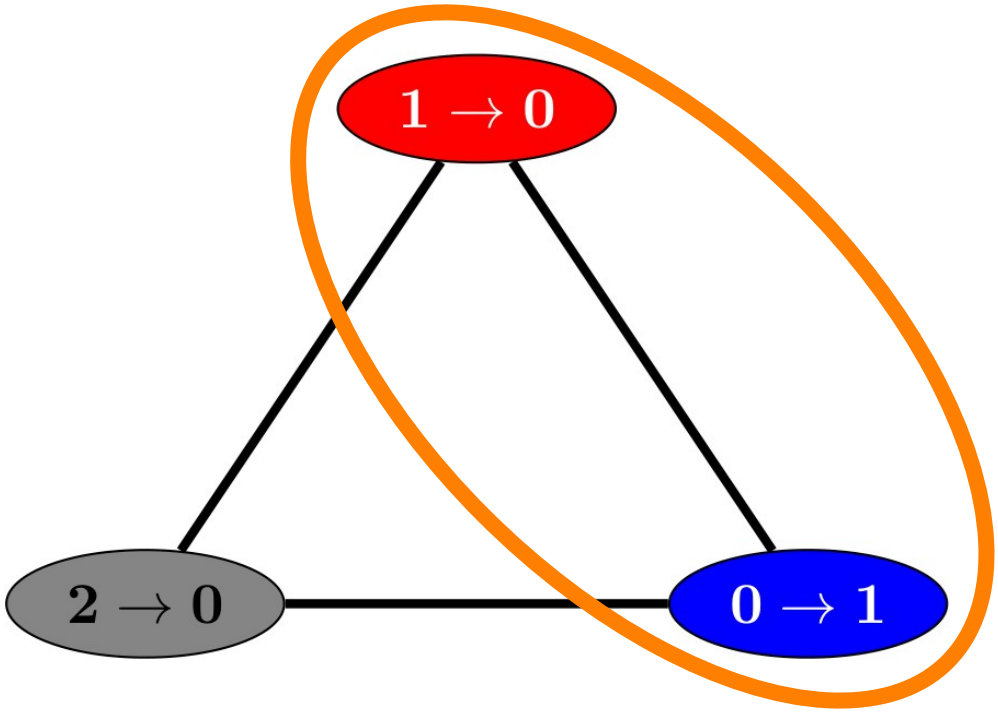
集合合意の不可解性 (adversary ver.)

定理 . Adversary $\mathcal{A}$ のコア集合の最小サイズが c のとき , $k < c$ ならば k- 集合合意は不可解である .

- **この結果自体は既知**
  - Nerve **補題を用いた証明** [Herlihy&Rajsbaum 2010]
- **今回の証明は初等的な帰納法による**
  - Permutation subset A **を添字とする** Ψ_A **の成立を** , A **の大きさに関する帰納法により示す**

Permutation Subset

入力値→出力値が置換になる部分集合



まとめと将来課題

- Adversary のもとでの集合合意に対して，その不可解性を示す障害論理式を具体的に構成した
- 幾何学の大掛かりな道具を使わない初等的な証明を与えた

- Multi-round プロトコルに対する障害論理式を構成できるか
  - 本研究は 1 ラウンドのプロトコルについてのみ適用可能

参考文献

• E. Goubault, J. Ledent & S. Rajsbaum. “A simplicial complex model for dynamic epistemic logic to study distributed task computability”(GandALF 2018)

• **西田 悠太郎 . “ 動的認識論理による k- 合意問題の不可解性” (京都大学理学研究科修士論文** 2020)

• M. Herlihy & S. Rajsbaum. “The topology of shared-memory adversaries”(PODC 2010)