動的認識論理を用いた分散計算タスクの不可解性証明について

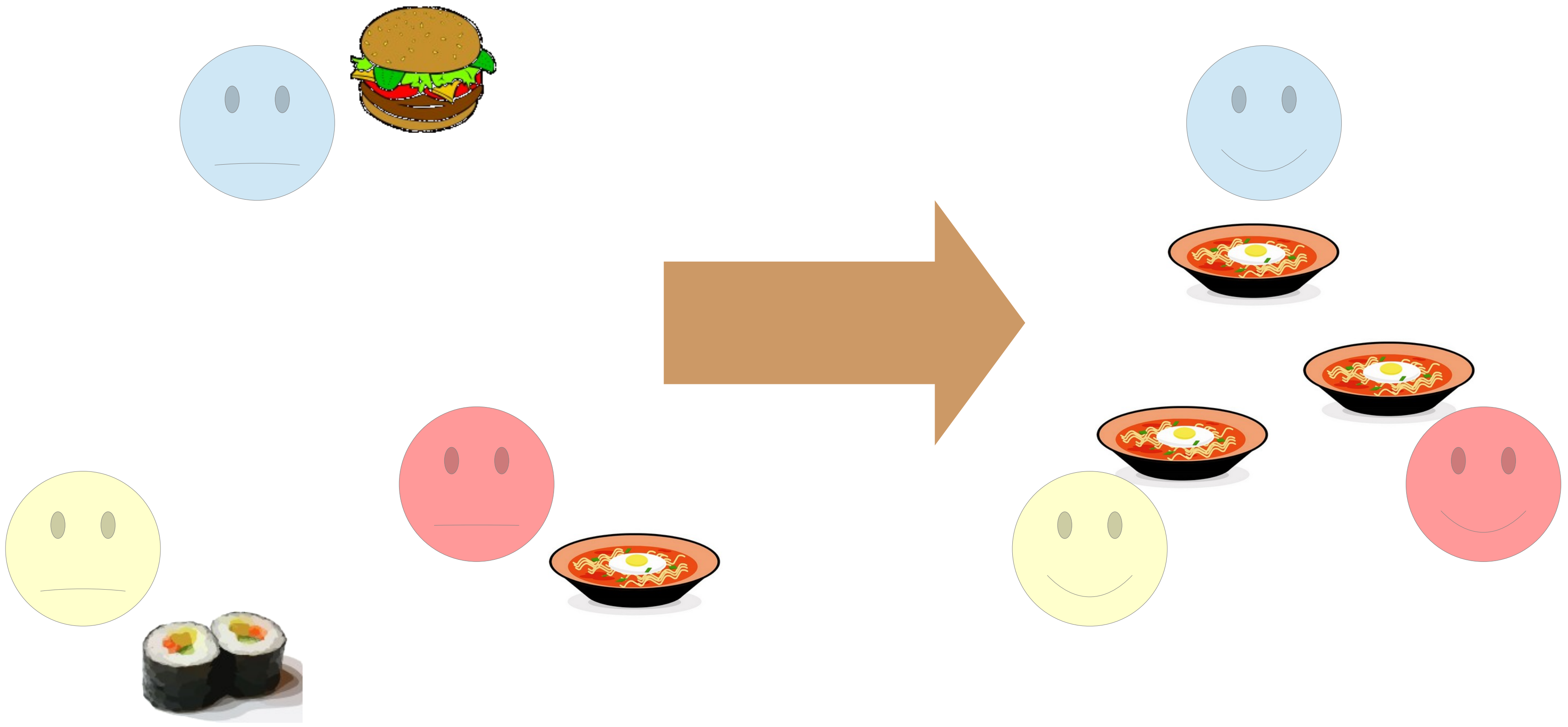
西村進　(M2 八木混希 との共同研究)

susumu@math.kyoto-u.ac.jp

京都大学理学研究科

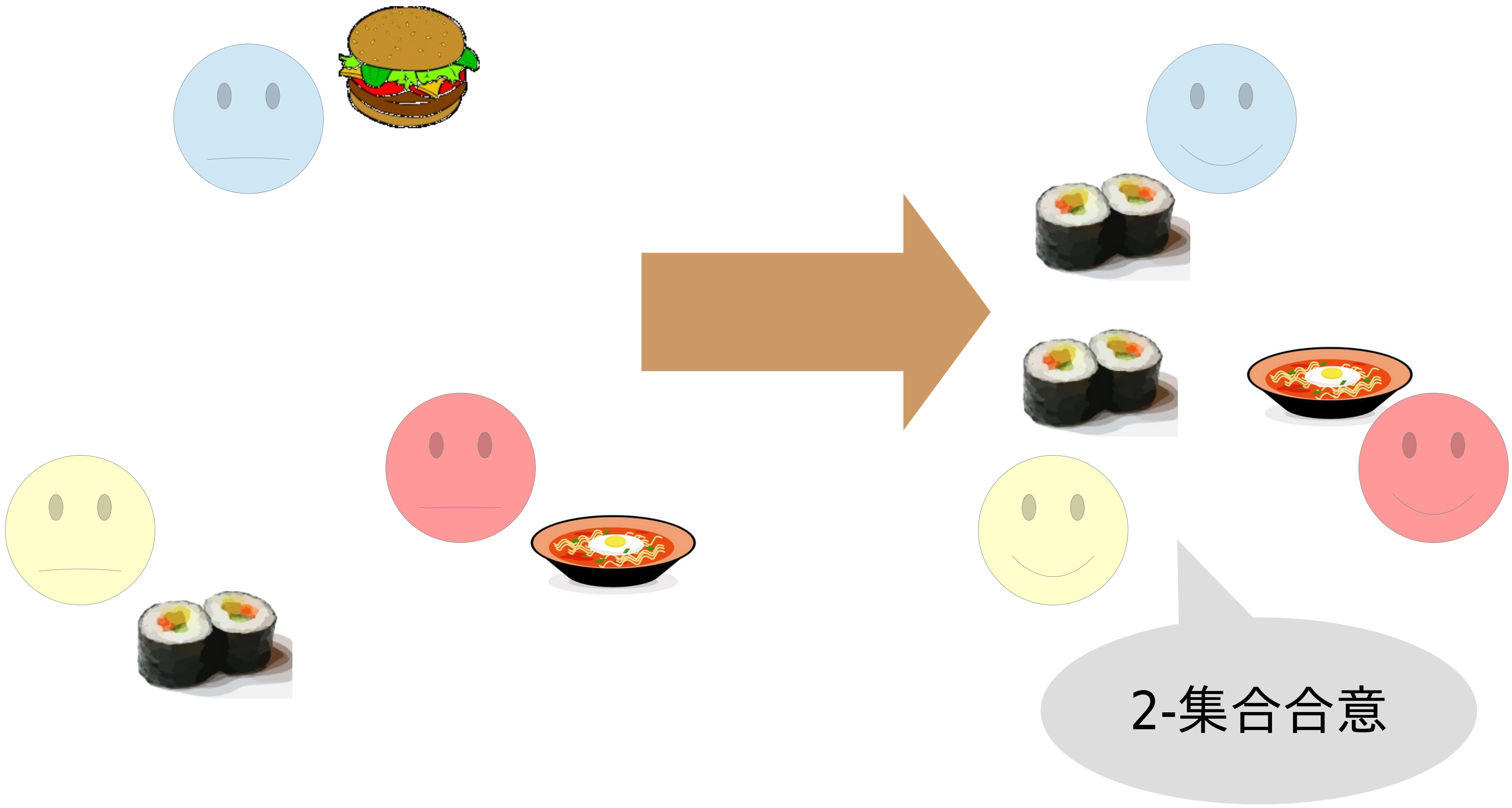
分散コンセンサス問題

- 各プロセスに初期値が入力された時、そのどれかひとつに合意する。



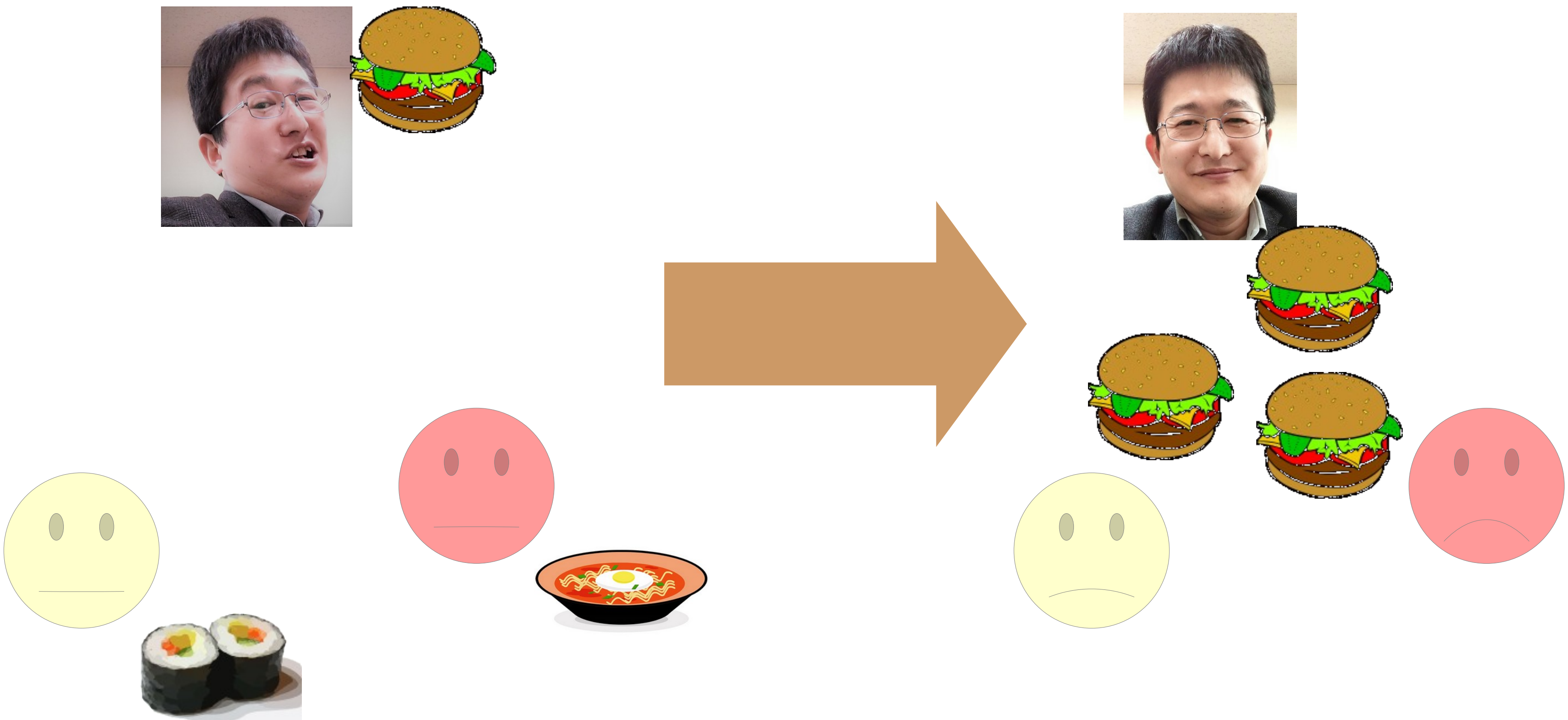
分散 k-集合合意問題 (1-集合合意=コンセンサス)

- 各プロセスに初期値が入力された時、そのうち高々 k種類で合意する。



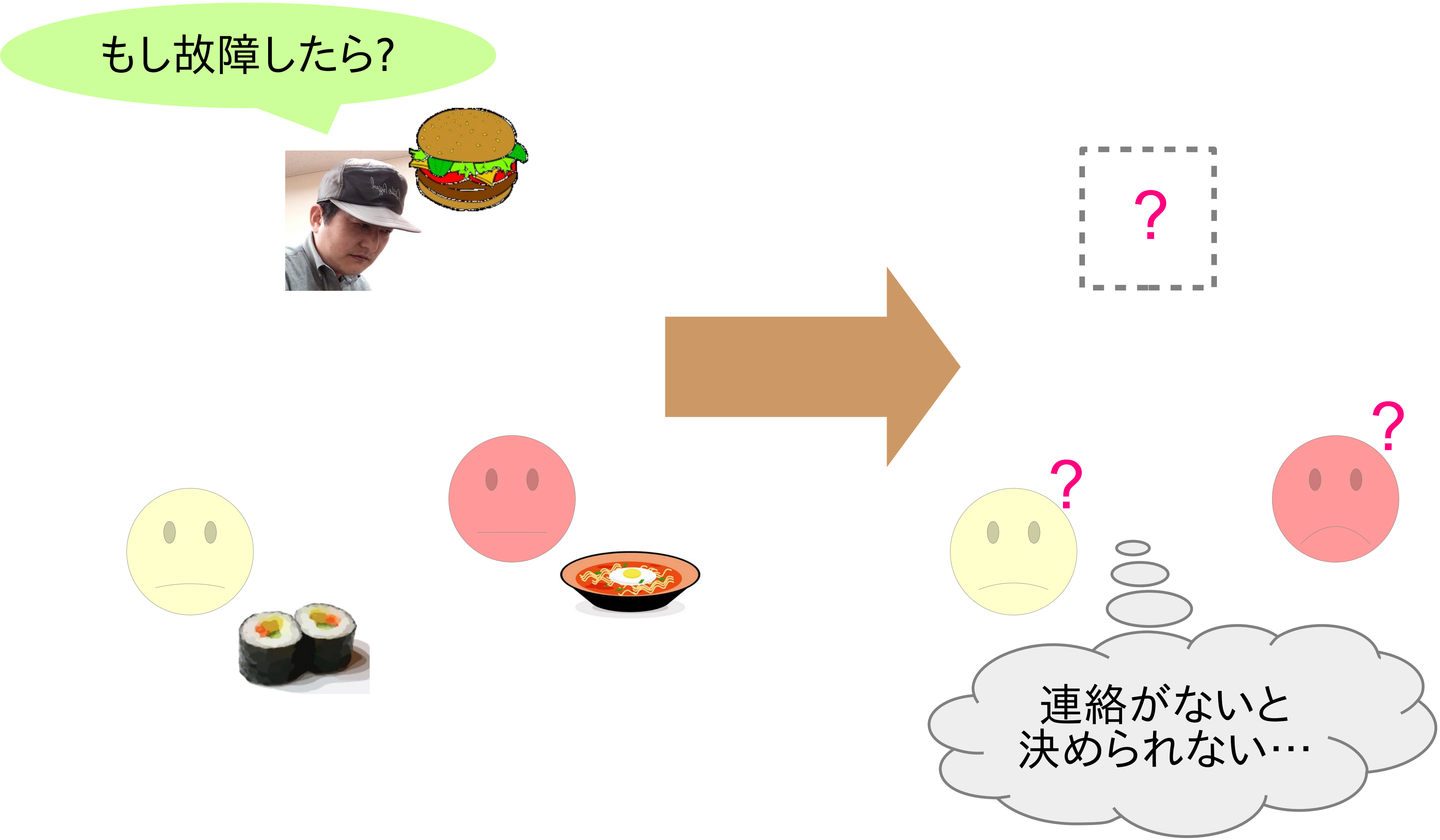
望ましくない分散コンセンサスの解法プロトコル

- プロトコル: 予め決めておいた代表プロセスが決定する



こんなとき困る

- プロトコル: 予め決めておいた代表プロセスが決定する



分散計算システム

- 分散システム　＝　Concurrency ＋ Failure
  　　　　　　　　　並行　　　　　故障
  - 並行システム: n個の異なるプロセスが並行して計算を実行
    - 同期モデル: 非同期実行
    - プロセス間通信: Read-Write共有メモリによる
  - 耐故障性
    - いくつかのプロセスが故障したとしても、残ったプロセスは各々有限ステップ内で計算結果を出力する
      ＝他プロセス(←故障しているかも!)の応答を永遠には待たない

どのように故障が起こる?

故障モデル

- Wait-free
  - すべてのプロセスは故障する可能性がある
- Super-set closed Adversary

本発表

  - (故障しない)正常プロセスの集合のクラス$\mathcal{A}$がsuperset-closed (i.e., $A \in \mathcal{A} \wedge A \subseteq B \Rightarrow B \in \mathcal{A}$)
    - $\mathcal{A} = \{S \mid S \neq \emptyset\}$ のとき、wait-free

プロセスの「生き残り方」のすべてのパターン

- *t*-resilient
- Byzantine failure
- …

分散合意タスクの不可解性(実現不可能性)

- nプロセス分散システムにおいて以下の結果が知られている
  - 故障モデル Wait-free の場合
    - n>1のとき、コンセンサス問題は解けない
    - n>kのとき、k-集合合意問題は解けない
  - 故障モデル Super-set closed adversary $\mathcal{A}$ の場合
    - k<csize($\mathcal{A}$) のとき、k-集合合意問題は解けない

csize($\mathcal{A}$): $\mathcal{A}$ の最小コアサイズ

- csize($\mathcal{A}$) = $\min \{ \#C \mid C$ は $\mathcal{A}$ のコア集合 $\}$
- C が $\mathcal{A}$ のコア集合
  $\Leftrightarrow$ C は $\forall A \in \mathcal{A}. C \cap A \neq \emptyset$ なるCで極小のもの

- 組み合わせトポロジーによる証明 [Herlihy&Shavit1999, Herlihy&Rajsbaum2010]がエレガント。

不可解性証明 = Obstructionの発見

組み合わせトポロジー

- Topological obstruction
  - 可解性を仮定すると、トポロジカルな不変量 (e.g., 連結性)と矛盾する

長所: 不変量概念の堅牢性

短所: 非初等的な定理の適用 (e.g., Nerve補題)

動的認識論理

- Logical obstruction
  - 可解性を仮定すると、論理命題の妥当性と矛盾する [Goubault他2018]

長所: 初等的(帰納法) 証明

短所: 実例の不足
不変量ほど堅牢でない

本研究の主結果

- 以下の不可解性を導くlogical obstructionを具体的な認識論理式として与えた。

定理 $\mathcal{A}$: super-set closed adversary, k<csize($\mathcal{A}$) のとき、k-集合合意問題は不可解

- 先行研究
  - Topological obstruction による証明 [Herlihy&Rajsbaum2010]
  - 動的認識論理を用いたlogical obstructionの枠組み (具体例少) [Goubault,Ledent,Rajsbaum2018]
  - Wait-free故障モデルに対する logical obstruction による証明 [西田2020]
- 本研究は西田のlogical obstruction をsuperset-closed adversaryに一般化し、証明も簡潔にした

概 要

- 背景と目的
- 分散計算の組合せトポロジー論
- 組合せトポロジーから認識論理へ
- Adversaryモデルでのlogical obstruction
- まとめと将来課題

分散計算の組合せトポロジー論

システム状態 = 単体(simplex)

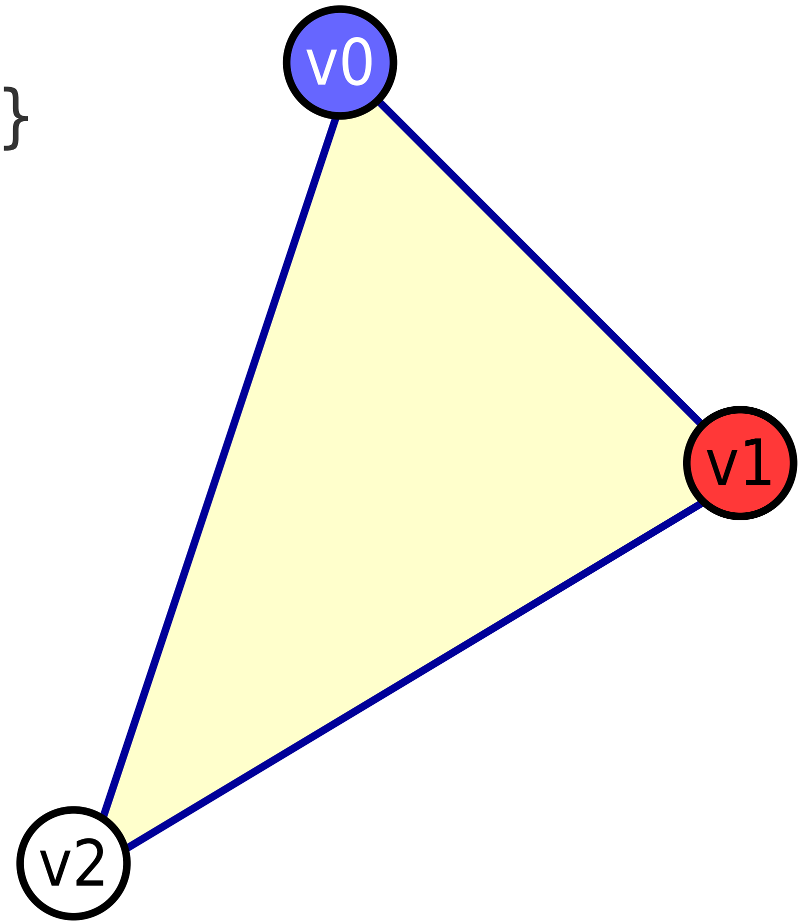
- プロセスの状態 = (プロセスID, 局所状態)
- システムの状態 = プロセス状態の集合

頂点

単体=頂点集合

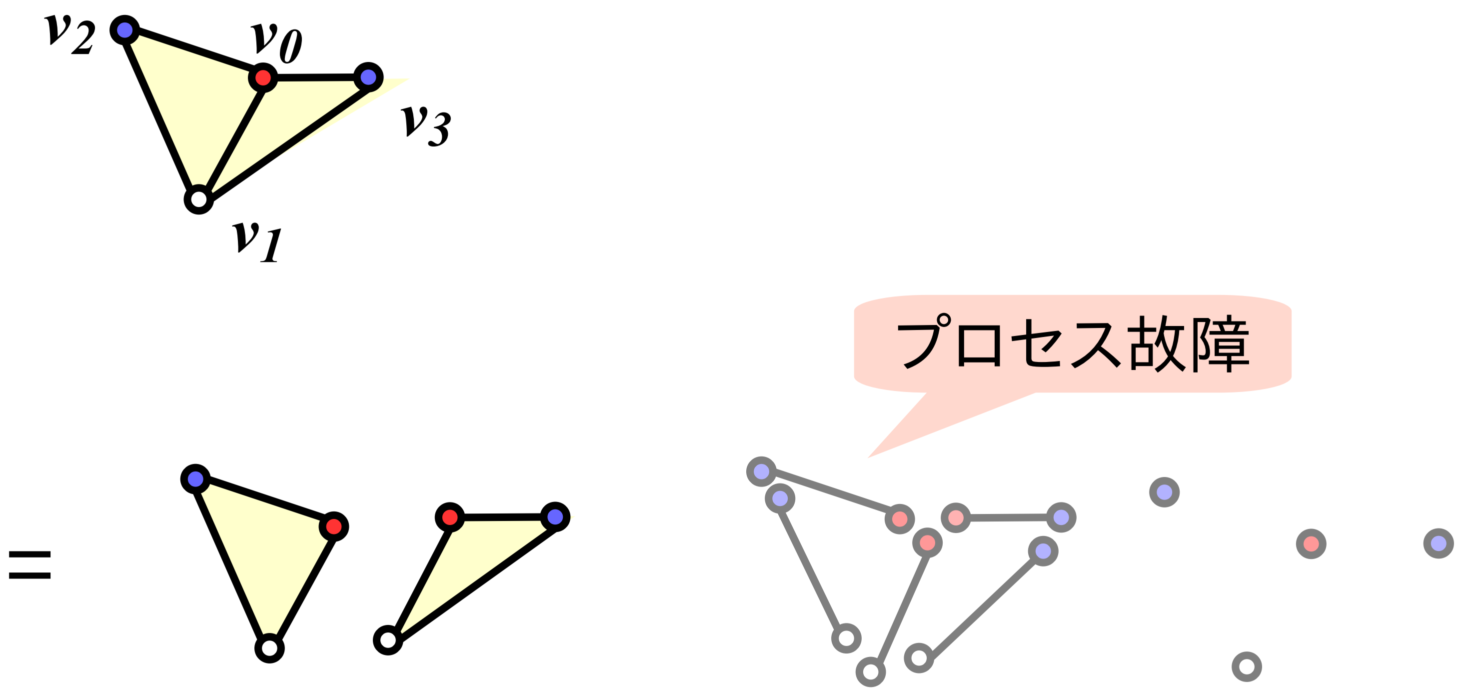
σ={(p0,v0),(p1,v1),(p2,v2)}

青　赤　白



非決定的状態 = 単体的複体(simplical complex)

- 単体的複体 = (集合の包含関係について閉じた)単体の集合



関数による分散タスク定義

- Carrier map

$$\Phi : \; I \rightarrow 2^{O}$$

$$\sigma \;\mapsto\; \Phi(\sigma)$$

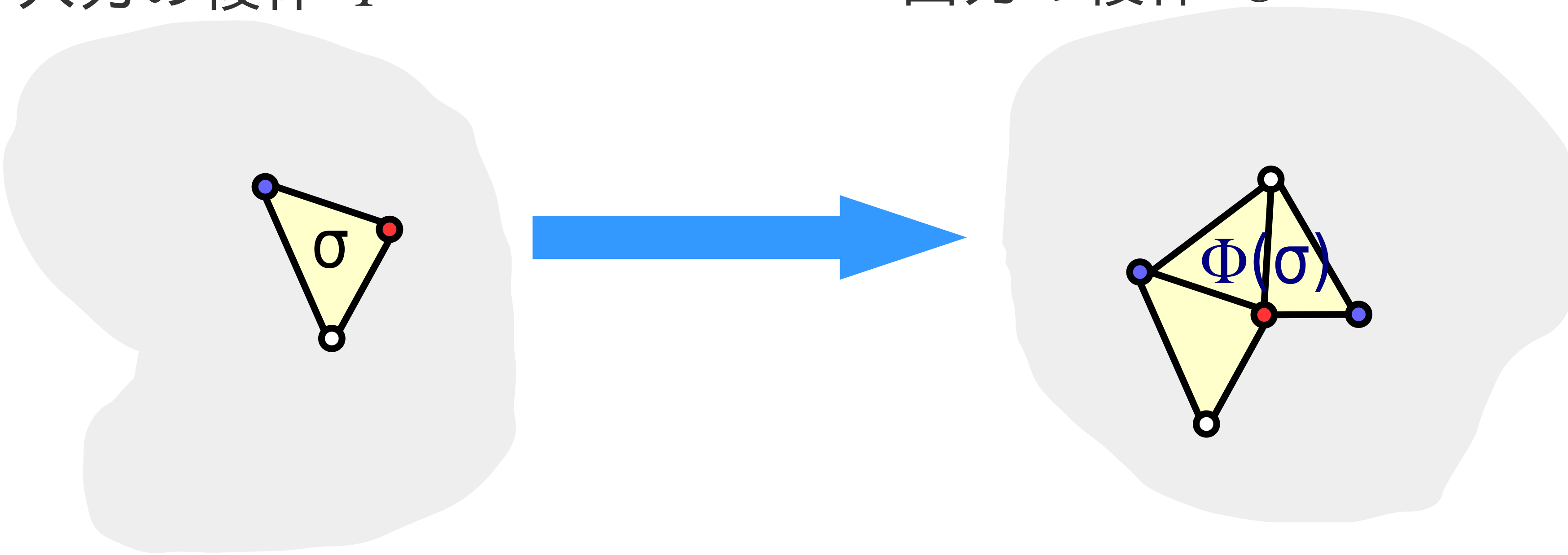
input

output

- 単体を部分複体に写す関数
  - 単調かつ色を保存

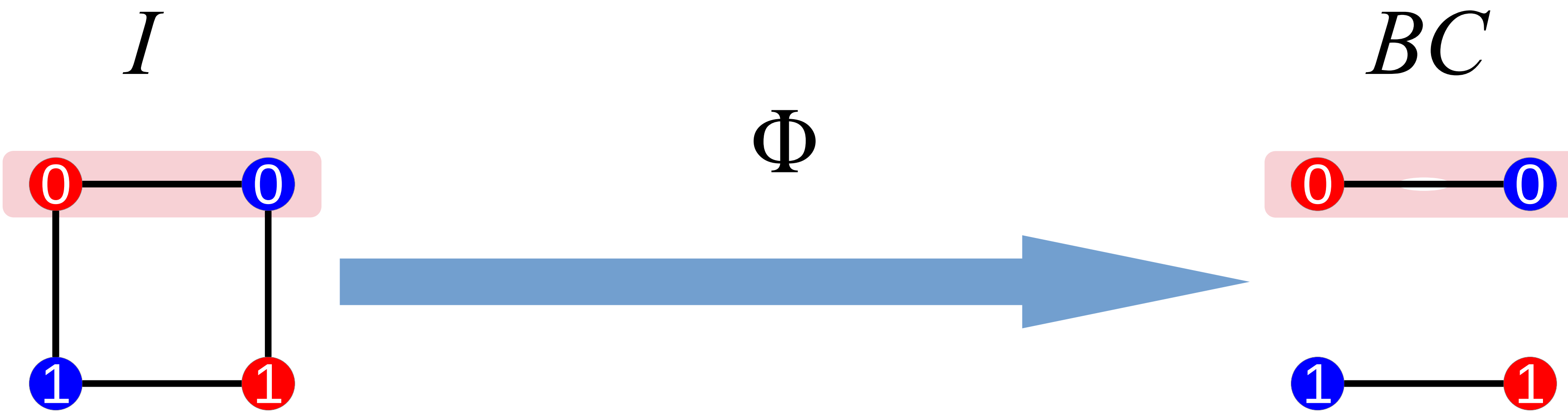
入力の複体 I

出力の複体 O



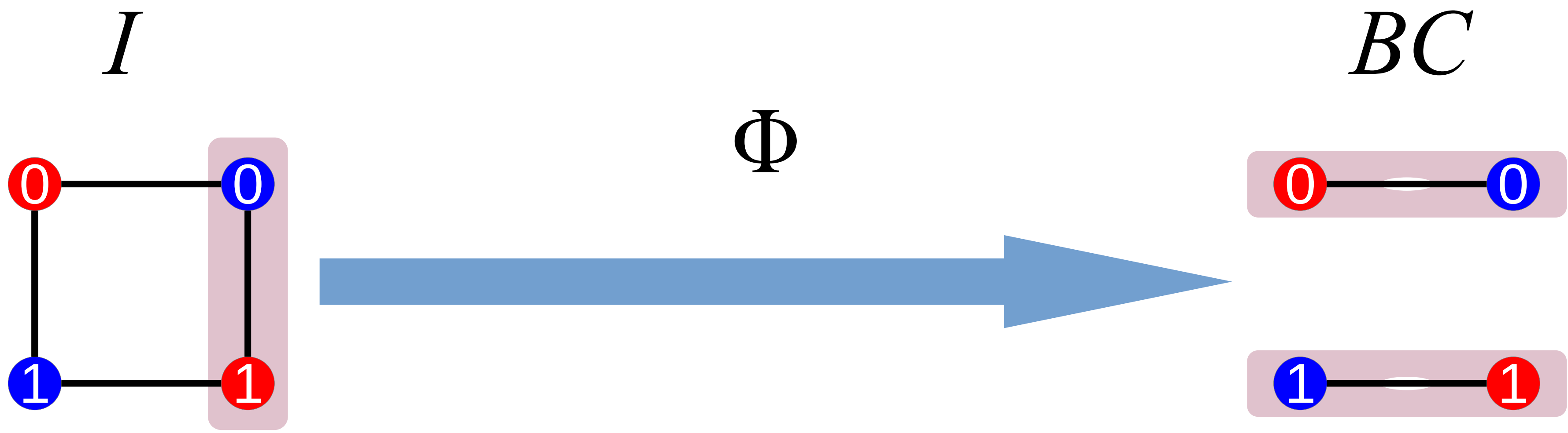
例: 2プロセスによる2値コンセンサス

入力値: 0 または 1
出力値: 両プロセスの入力値のどちらか一つのみを出力とする



例: 2プロセスによる2値コンセンサス

入力値: 0 または 1
出力値: 両プロセスの入力値のどちらか一つのみを出力とする



Wait-free分散計算 = 複体の細分

READ-WRITE共有メモリモデル

≅ 即時スナップショット(Immediate snapshot)モデル
[Herlihy&Shavit1999]

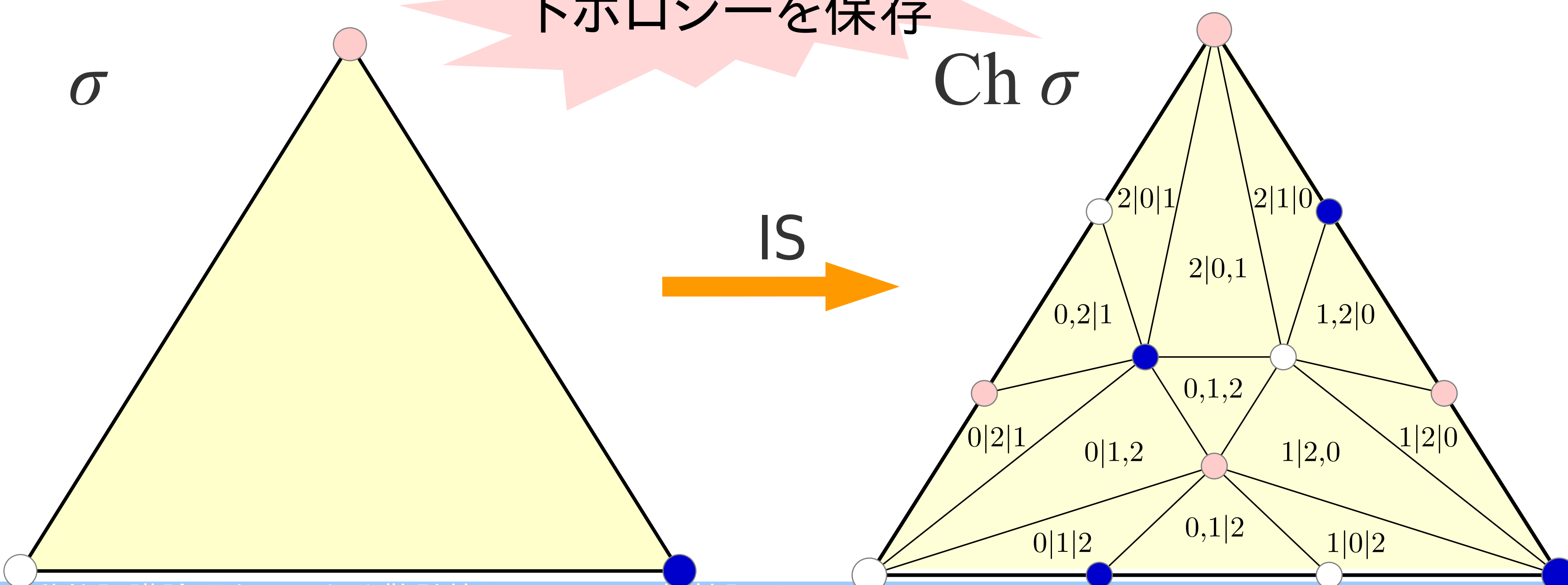
≅ Ordered set partition

組合せ構造

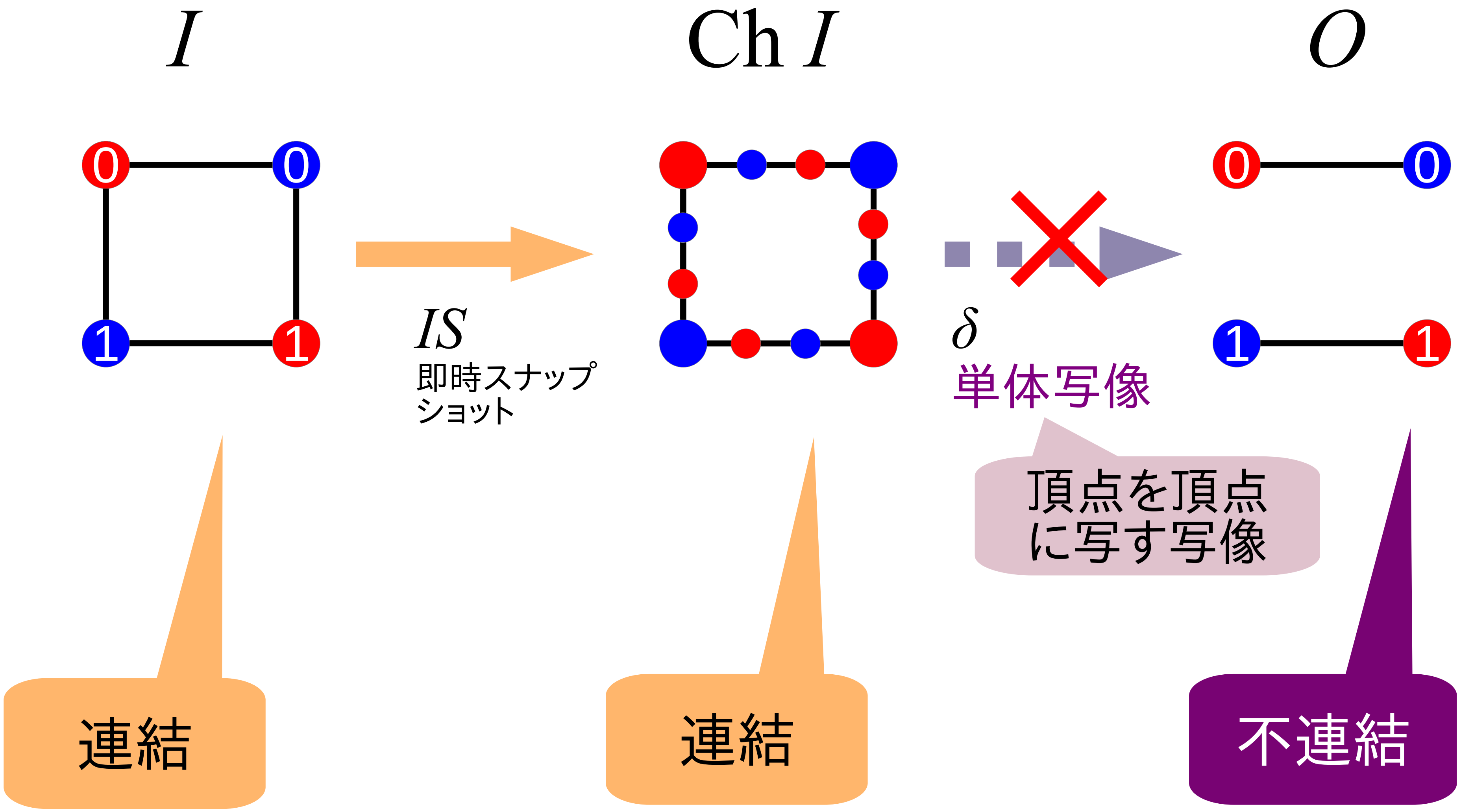
≅ 標準色付き細分
[Kozlov2012]

複体の細分

細分は
トポロジーを保存



例: 2プロセス コンセンサス のwait-free不可解性



組合せトポロジーから認識論理へ

認識論理 (Epistemic logic)

Knowledge

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

プロセス a の入力値が i

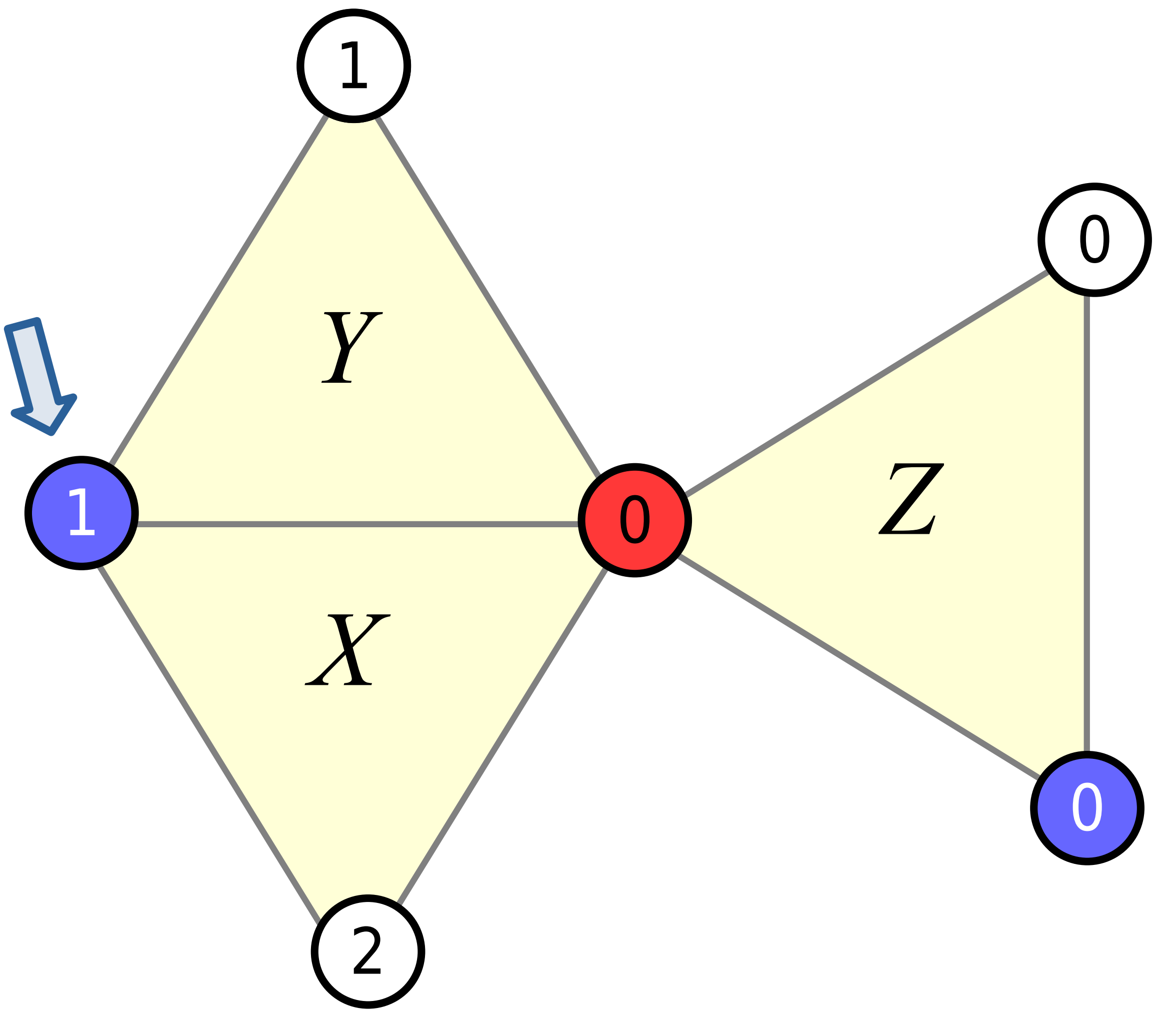
Distributed knowledge

- 認識論理式 φ がpositive
  ⇔ φ の任意の否定部分式 $\neg\psi$が様相記号を含まない

単体的複体 ≒ Kripkeモデル [Goubault他2018]

- 複体のファセット(極大単体) X, Y, Z → Kripkeモデルのworld
- $X \sim_a Y$ ⇔ 色aの頂点がX∩Yに属する

S5 + Local



Z ~●Z Z ~●Z Z~○Z

X ~●X X ~●X X~○X

Y ~●Y Y ~●Y Y~○Y

X ~●Y

X ~● Y X ~● Z Y ~● Z

※対称性から導かれる関係は省略した

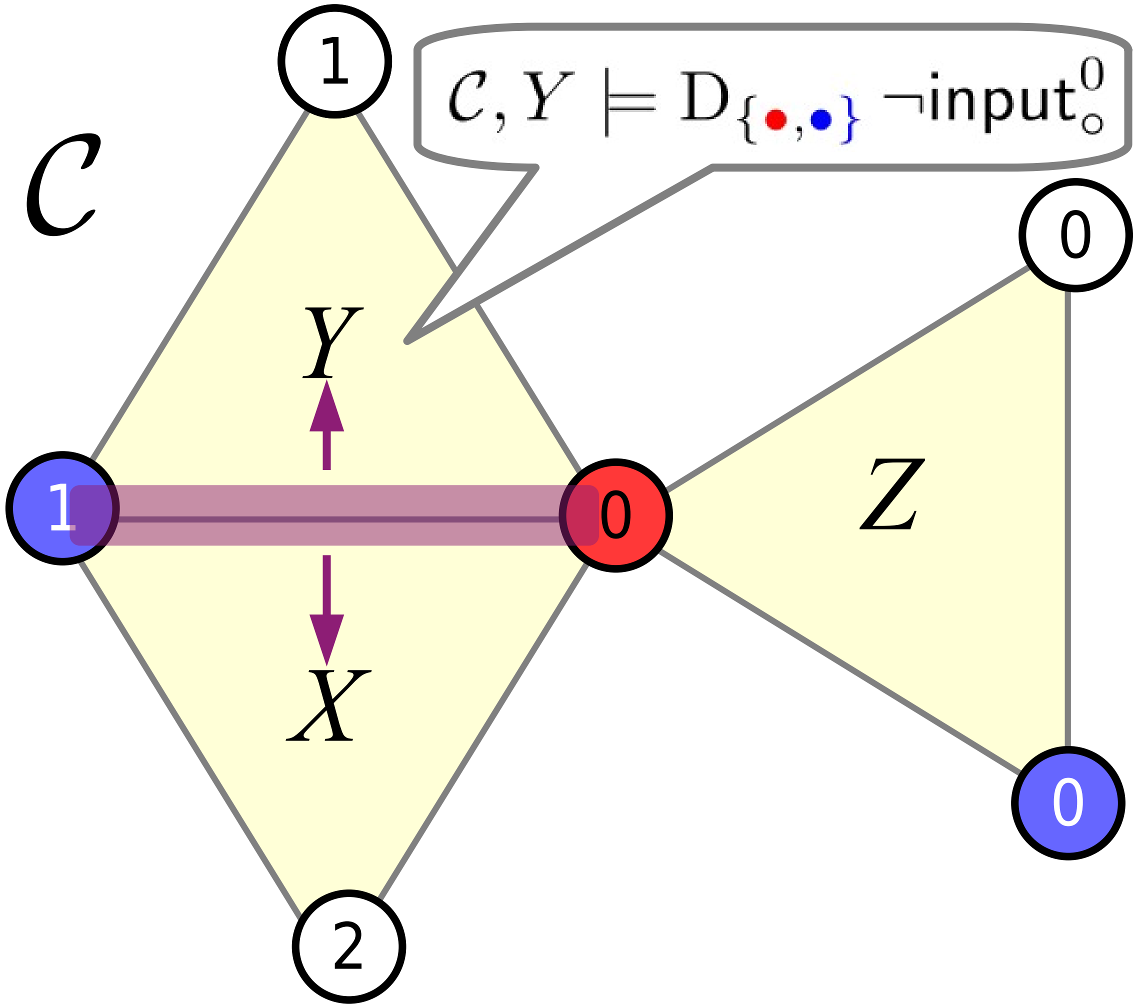
様相 (Distributed Knowledge)

A に属するプロセスの知識を合わせれば φ がわかる

様相 ≒ 局地的な連結性

$$\mathcal{C}, X \models \mathrm{D}_A\,\varphi \iff \text{すべての } X \sim_{D_A} W \text{ なる } W \text{ について } \mathcal{C}, W \models \varphi$$

ただし、$\sim_{D_A} = \bigcap_{a \in A} \sim_a$



様相(Knowledge)

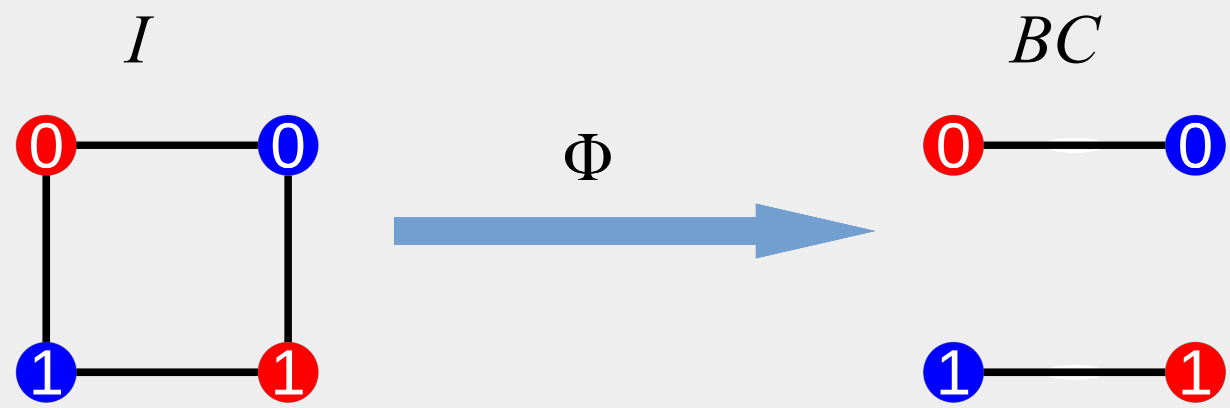
プロセス a は φ を知っている

$$\mathrm{K}_a\varphi \equiv \mathrm{D}_{\{a\}}\varphi$$

Product update

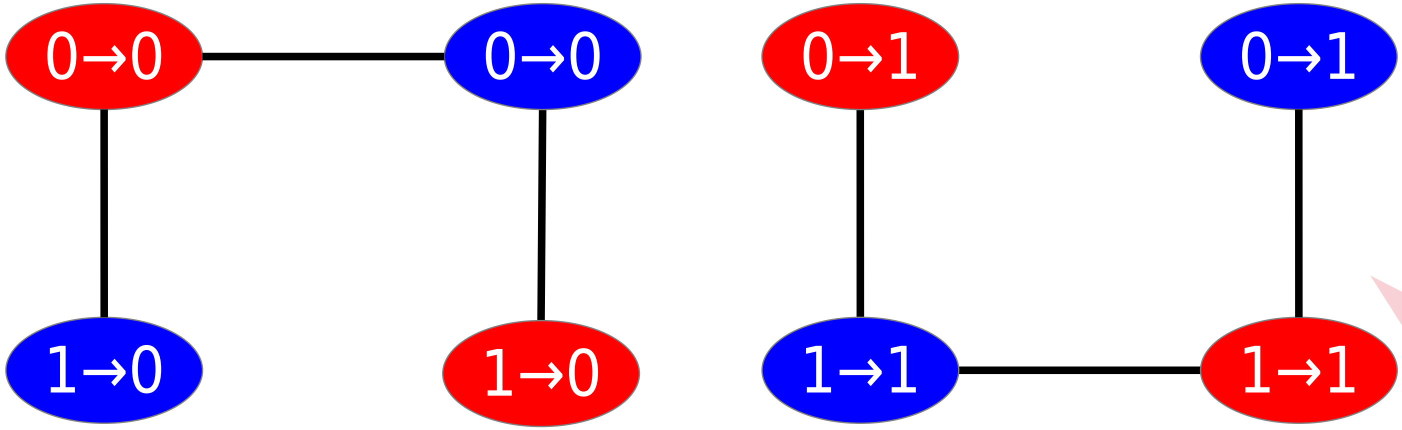
Kripkeモデルの動的更新を
表すための手法を応用

2値コンセンサス
のCarrier map



関数を二項関係として
エンコード

- Product update $I\,[BC]$



複体から複体へ
の関数を単一の
複体で表現

Logical obstructionによる不可解性証明

定理[Goubault他2018] 以下のようなpositiveなlogical obstruction φ が存在するとき、分散タスク $\Phi : I \rightarrow 2^O$ は分散プロトコル $\Psi : I \rightarrow 2^P$ で不可解

計算したいこと

システムの計算能力

- $I[O] \models \varphi$

$I[O], X \models \varphi$
for every world X of $I[O]$

- $I[P] \not\models \varphi$

$I[P], X \not\models \varphi$
for some world X of $I[P]$

より連結性が高い

Adversaryモデルでのlogical obstruction

Adversaryの下での不可解性証明

定理. Super-set closed adversary $\mathcal{A}$ の下で、k<csize($\mathcal{A}$) ならば k-集合合意問題は解けない

?

▶ 認識論理のlogical obstruction Φ による証明

k-集合合意問題のproduct update

- k< csize($\mathcal{A}$) のとき、$I\,[SA\text{k}] \models \Phi$

Adversary $\mathcal{A}$ のproduct update

- $I[\mathscr{R}_{\mathcal{A}}] \not\models \Phi$

Round operator $\mathscr{R}_{\mathcal{A}}$:
Adversaryモデル$\mathcal{A}$に対応する複体

k-集合合意問題に対するlogical obstruction Φ

Π：全プロセス集合，(入力値の集合)=Π，　$c = \mathrm{csize}(\mathcal{A})$

$$\Phi = \bigvee_{a \in \Pi} \neg \mathrm{input}_a^a \vee \bigvee_{A \subseteq \Pi, |A| < c} \Psi_A$$

$$\Psi_A = \begin{cases} \mathsf{false} & C \cap (\Pi \setminus A) = \emptyset \text{ for some core set } C; \\ \mathrm{D}_A\, \psi_A & \text{otherwise} \end{cases}$$

$$\psi_A = \bigvee_{a \in \Pi \setminus A} \neg \mathsf{input}_a^a \vee \bigvee_{a \in \Pi \setminus A} \mathrm{K}_a \left(\bigvee_{j \in A} \bigvee_{a' \in \Pi} \mathsf{input}_{a'}^j \right) \vee \bigvee_{B \supsetneq A} \Psi_B$$

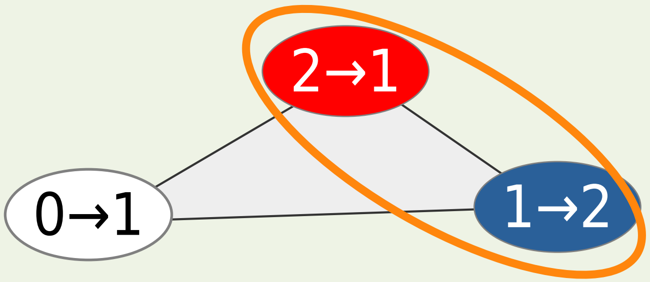
A に関する相互帰納的定義 (A=Πが帰納法の基礎)

証明の概略　$I\,[SA_k] \vDash \Phi$

$$\bigvee_{a\in\Pi} \neg \mathrm{input}_a^a \;\vee \bigvee_{A\subseteq\Pi,|A|<c} \Psi_A$$

- $\bigwedge_{a\in\Pi} \mathrm{input}_a^a$ をみたす任意の world X について、permutation subset A が必ず存在する。

$A\ (\subseteq \Pi)$ が$f:\Pi\to\Pi$の permutation subset
$\Leftrightarrow f(A)=A\ (\neq\emptyset)$



- $\#A$=k のとき(帰納法の基礎)　Ψ_A は成立
- $\#A$<k のとき
  permutation subset A' $(\supsetneq A)$ が存在する。よって

$$\Psi_A = \cdots \vee \bigvee_{B\supsetneq A} \Psi_B$$ は成立(帰納法の仮定)

まとめと将来課題

本研究の成果と展望

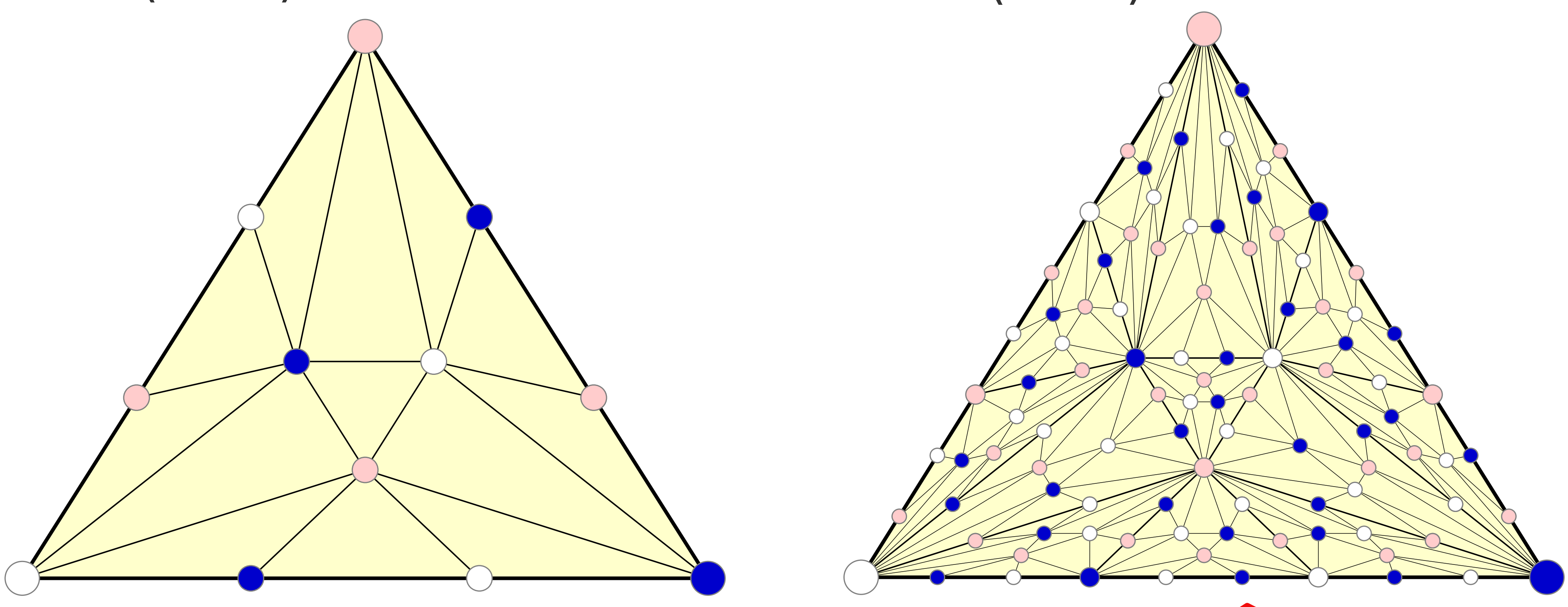
- 一般のsuperset-closed adversaryのもとでのk-集合合意問題の不可解性を示すlogical obstructionを具体的に与えた
  - 認識論理による具体的かつ厳密なobstructionの表記
  - 帰納法による初等的な証明

組合せトポロジーを
代替/補完する新た
な手法になる?

現状の枠組みの限界

- Multi-round プロトコルへの対応が難しい

Ch σ (IS×1)　　　$\mathrm{Ch}^2\sigma$ (IS×2)



Topologyは変わらない(細分が細かくなるだけ)が、
Kripkeモデルの変異のため異なるobstructionが必要

Epistemic μ-calculus ?

- 認識論理 + 不動点演算子 $\nu X.\psi,\ \mu X.\psi$

Common knowledge

- 例: $\mathrm{C}_A P \quad \equiv \quad \nu X.\Big(P \wedge \bigwedge_{a \in A} \mathrm{K}_a X\Big)$

「連結性」を表す論理式

Round数に依存しないobstructionが書けるかも

References

- M. Herlihy & N. Shavit: *"The topological structure of asynchronous computability"* (JACM 1999)
  Wait-free impossibility by topological method
- M. Herlihy & S. Rajsbaum: *"The topology of shared-memory adversaries"* (PODC 2010)
  Adversarial impossibility by topological method
- E. Goubault, J. Ledent, & S. Rajsbaum: *“A simplicial complex model for dynamic epistemic logic to study distributed task computability”* (GandALF 2018) The logical obstruction framework
- 西田悠太郎: *“動的認識論理によるk-合意問題の不可解性”* (修士論文, 2020) Wait-free impossibility by logical obstruction
- K. Yagi & S. Nishimura: *“Logical obstruction to set agreement tasks for superset-closed adversaries”* (2020)
  https://arxiv.org/abs/2011.13630