TOSHIBA
Leading Innovation

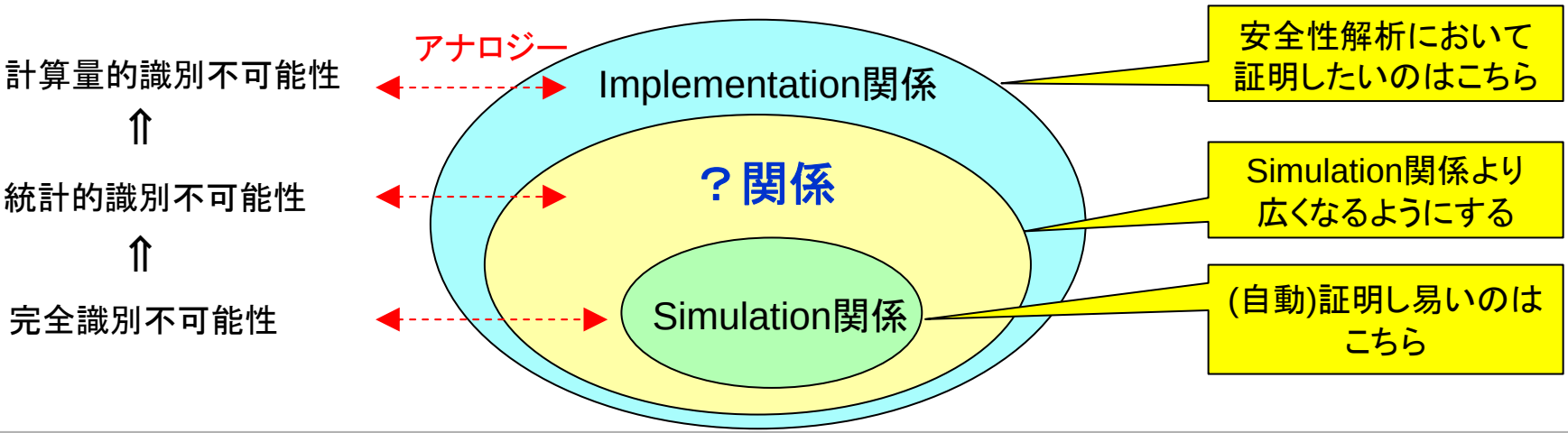
タスクPIOAの統計的Simulation関係に関する考察

日本応用数理学会 2007年度年会
2007年9月15日　北海道大学

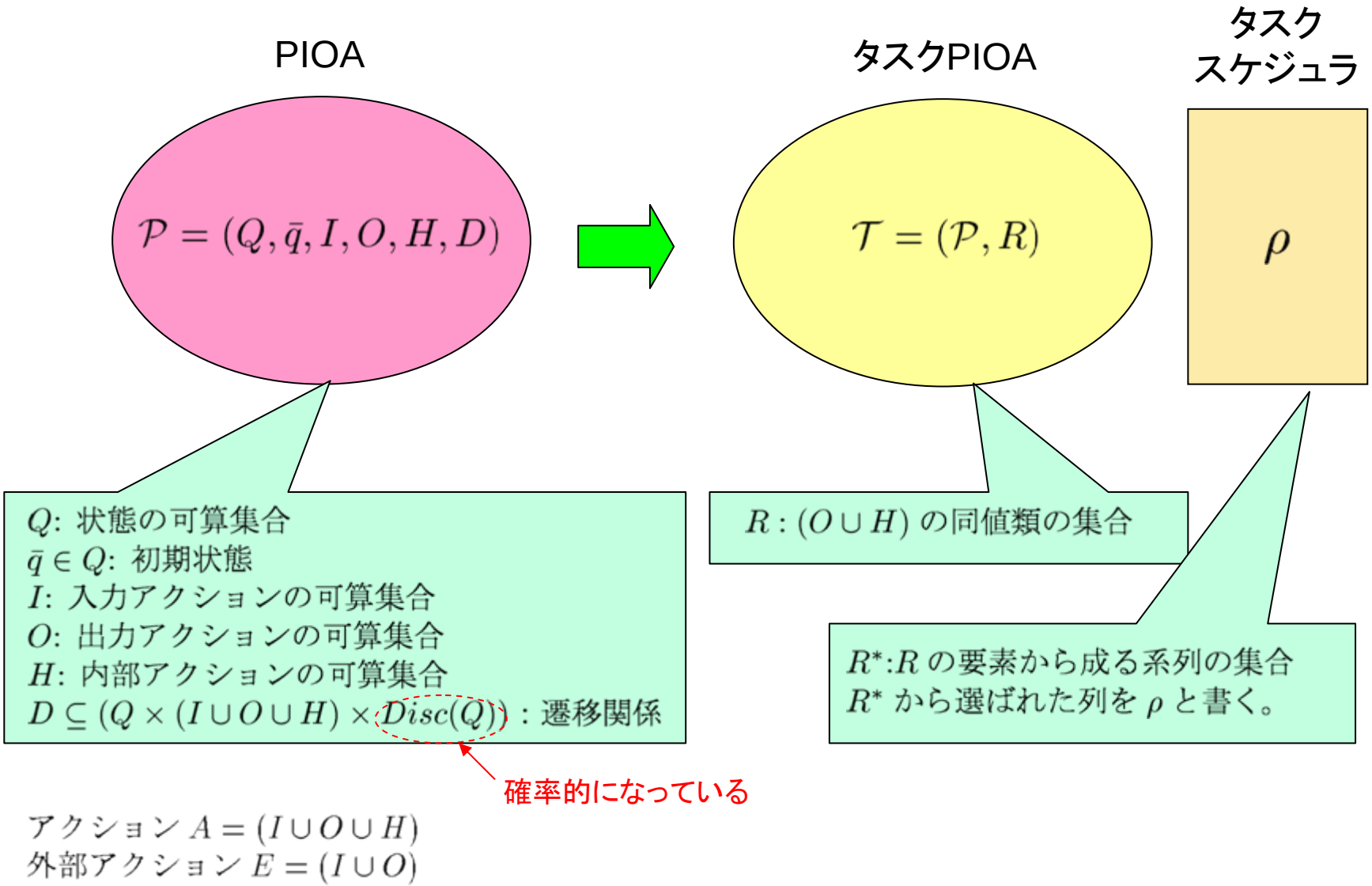
◎古田憲一郎、村谷博文、花谷嘉一（東芝　研究開発センター）

はじめに

- 背景
  - 暗号プロトコルをタスクPIOAで表現し安全性解析[Canetti et al.,2005]
    - 現実／理想プロトコルが識別不可能⇒現実プロトコルは安全
    - Simulation関係⇒Implementation関係
      - 最終的に示したいのはImplementation関係
      - Simulation関係があることを示せばよい
- 目的
  - Simulation関係より広くImplementation関係に含まれるような関係を構築
    - （自動）証明可能なプロトコルの範囲の拡張が期待できる

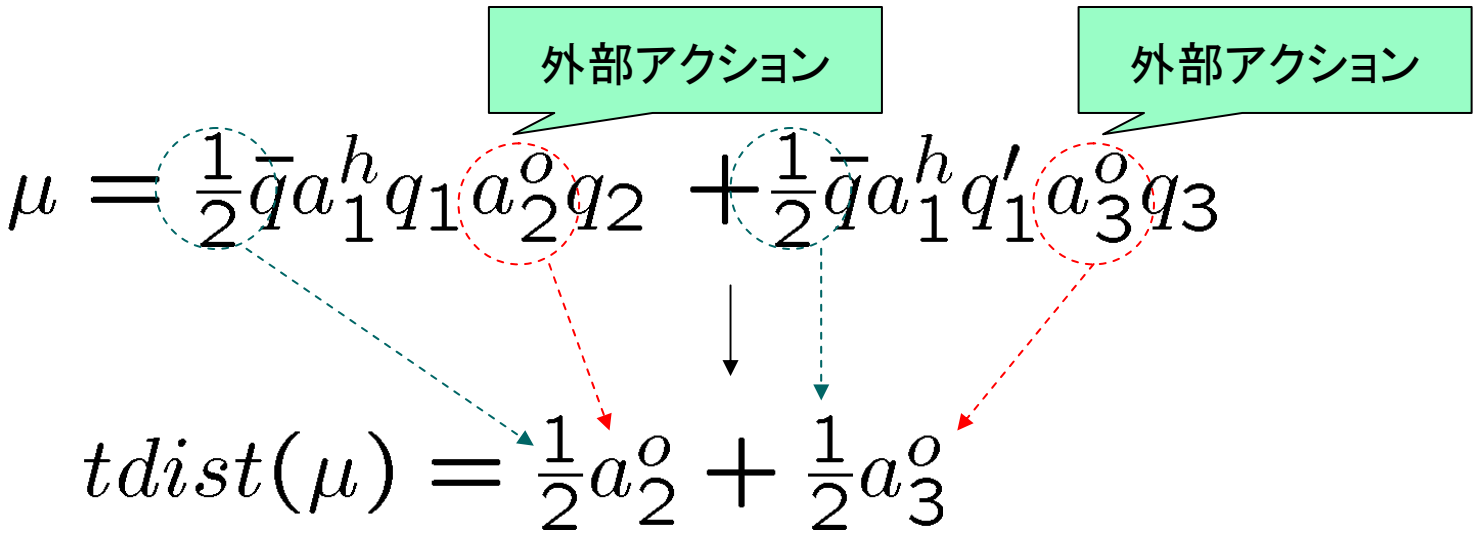


タスクPIOAとタスクスケジュラ



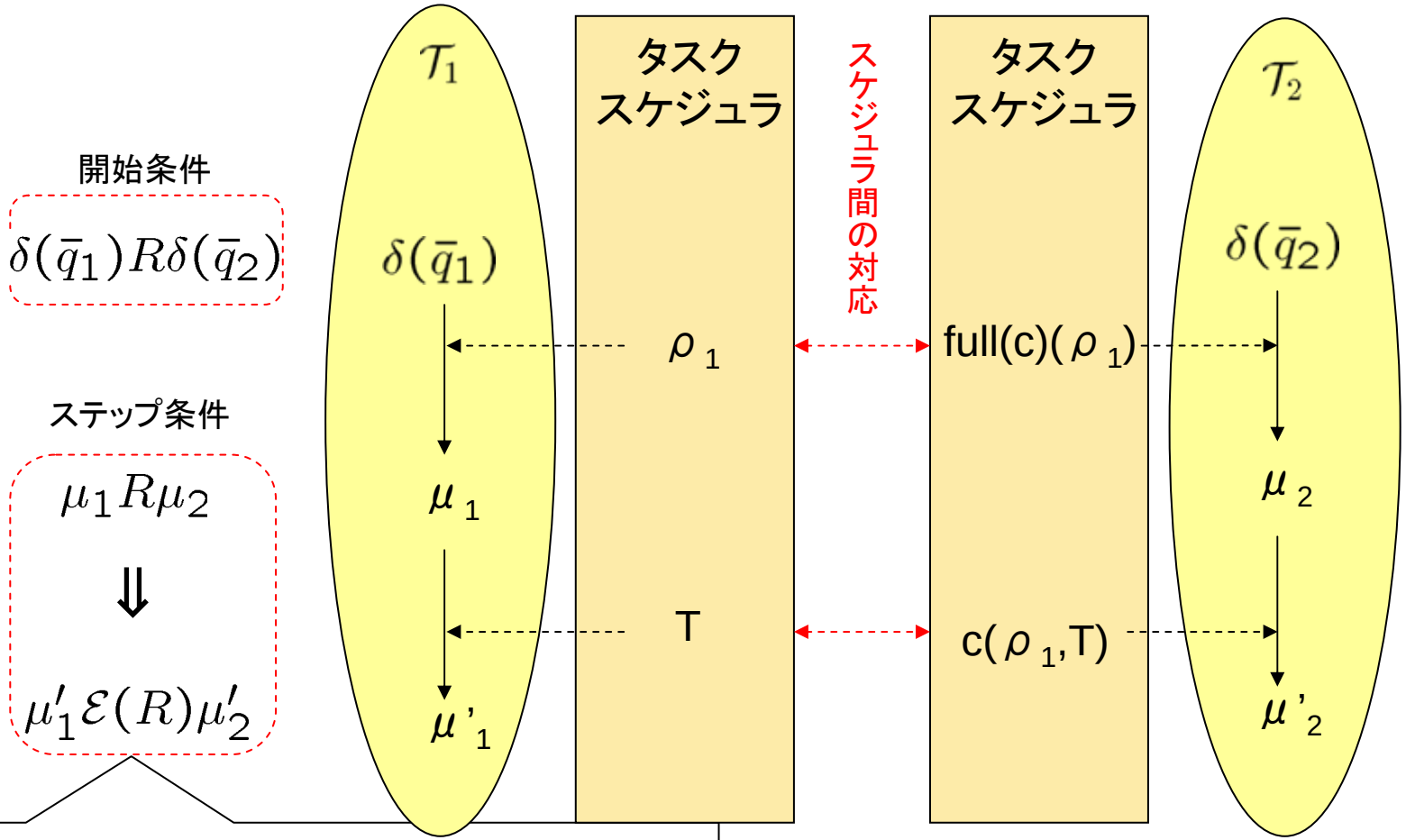
トレース分布

- **実行(Execution)**
  - （初期状態）（アクション）（状態）（アクション）（状態）・・・・
- **トレース**
  - 実行(Execution)を外部アクションに制限して得られる列
- **トレース分布 tdist(μ)**
  - トレース上の確率分布
  - μ は実行(Execution)の上の確率分布を表す



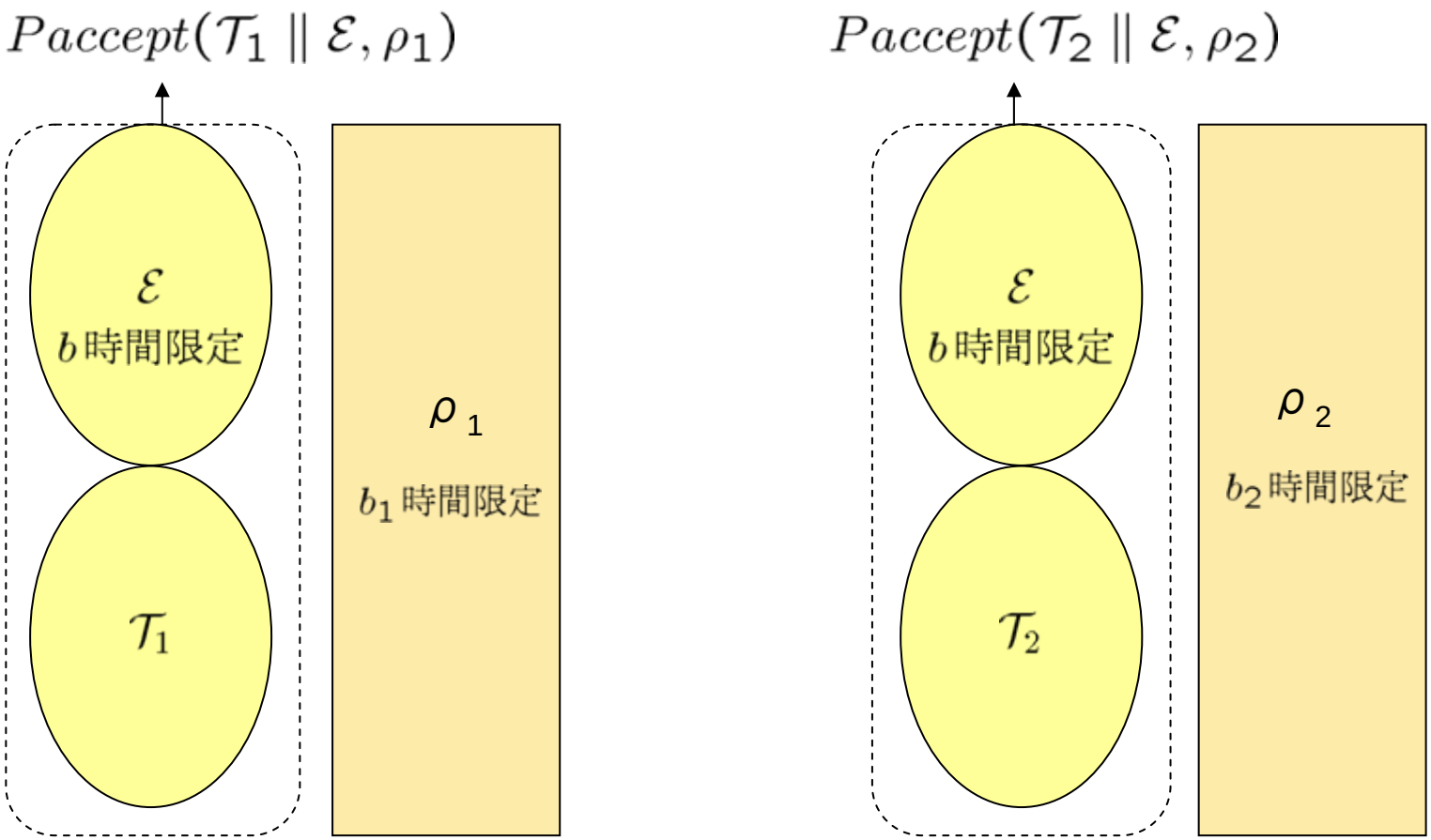
Simulation関係

Let R be a relation such that $\mu_1 R \mu_2 \Rightarrow tdist(\mu_1) = tdist(\mu_2)$



full(c)(λ)= λ,
full(c)(ρ_1)c(ρ_1,T)=full(c) (ρ_1T)

Implementation関係

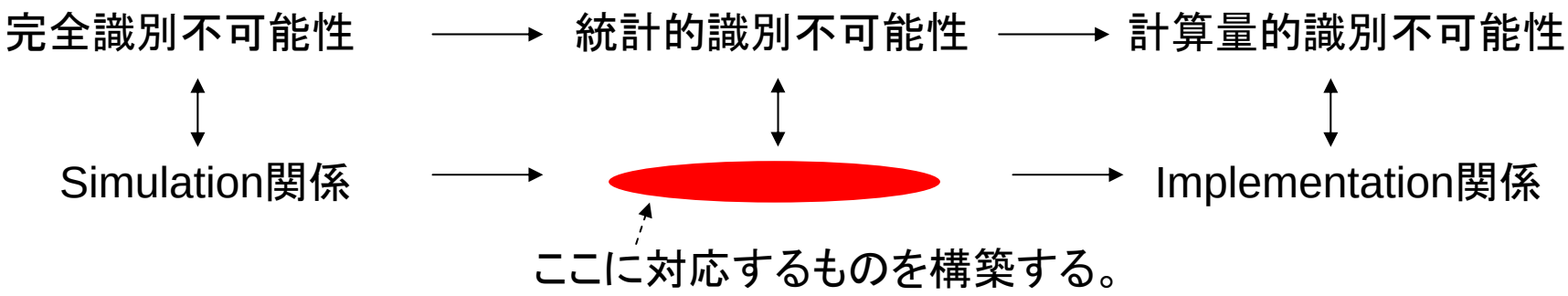


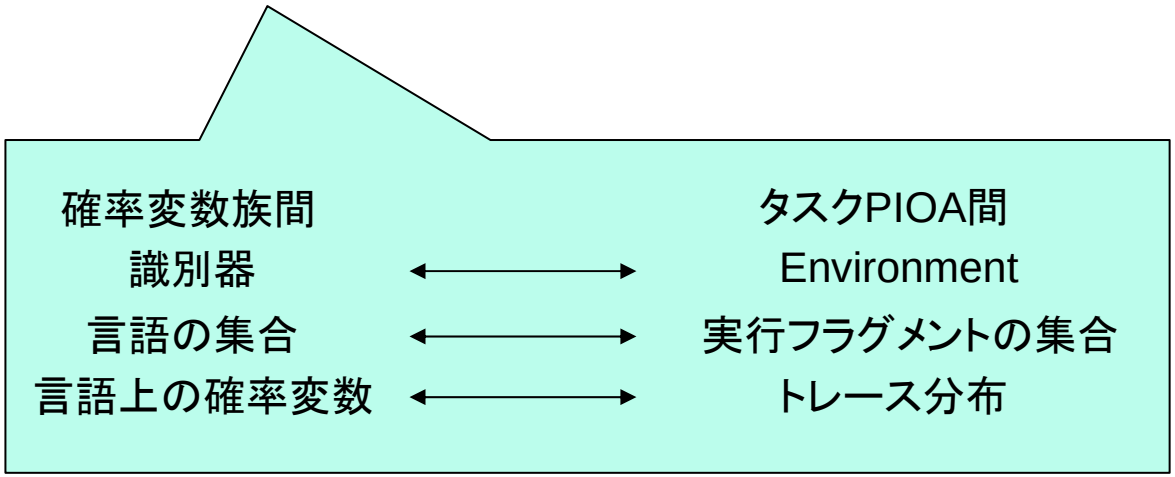
$$\forall \mathcal{E} \forall \rho_1 \exists \rho_2 \ |Paccept(\mathcal{T}_1 \parallel \mathcal{E}, \rho_1) - Paccept(\mathcal{T}_2 \parallel \mathcal{E}, \rho_2)| \leq \epsilon \Rightarrow \mathcal{T}_1 \leq_{\epsilon,b,b_1,b_2} \mathcal{T}_2$$

$$\forall b\text{:多項式}, \forall b_1\text{:多項式}, \exists b_2\text{:多項式}, \ \exists \epsilon\text{:negligible 関数} \Rightarrow \overline{\mathcal{T}}_1 \leq_{neg,pt} \overline{\mathcal{T}}_2$$

対応関係

確率変数族間の識別不可能性概念とタスクPIOA間の
識別概念との間には以下のような対応が見てとれる。





統計的Simulation関係

- 確率変数族間の統計的識別不可能性に対応する概念として定義
- トレース分布間で関係R_εが成立するように拡張
  - トレース分布が一致する必要はない。

$$\mu_{1,k} R_\epsilon \mu_{2,k} \Rightarrow \sum_{\beta \in \bigcup_{i=1,2} supp(tdist(\mu_{i,k}))} |tdist(\mu_{1,k})(\beta) - tdist(\mu_{2,k})(\beta)| < \epsilon.$$

開始条件

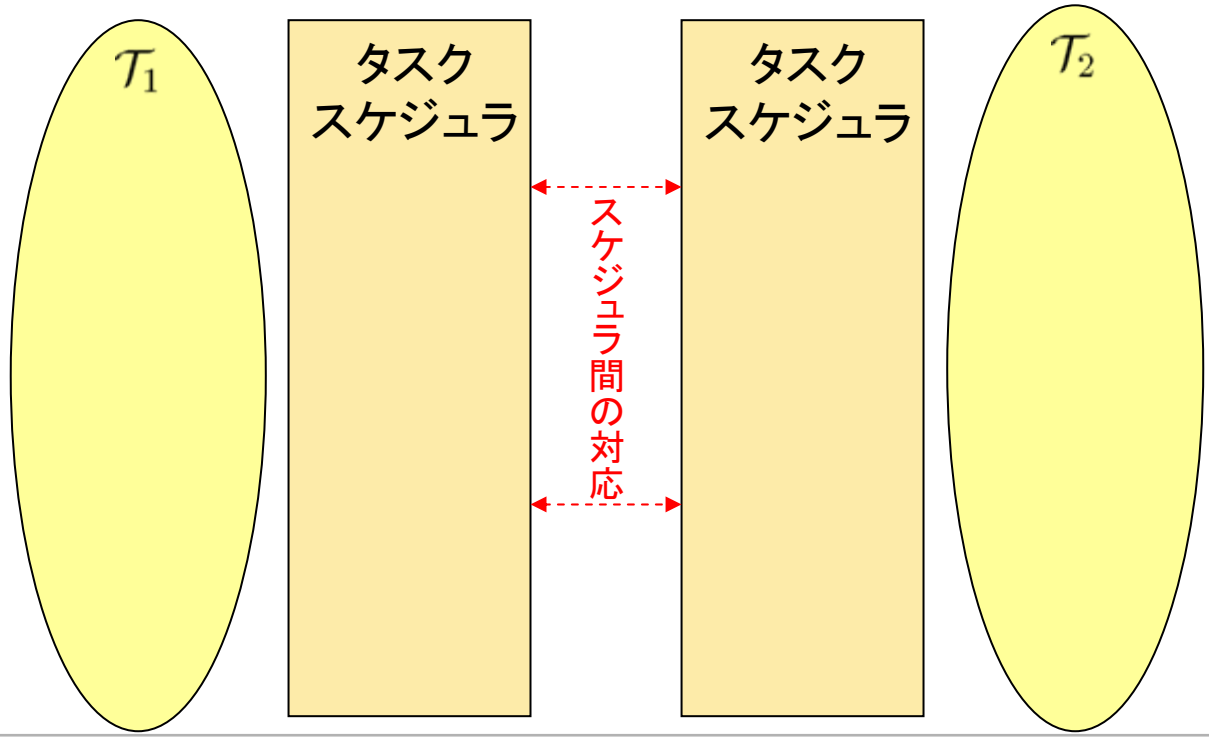
$$\delta(\bar{q}_1) R_{\epsilon(k)} \delta(\bar{q}_2)$$

ステップ条件

$$\mu_1 R_{\epsilon(k)} \mu_2$$

$$\Downarrow$$

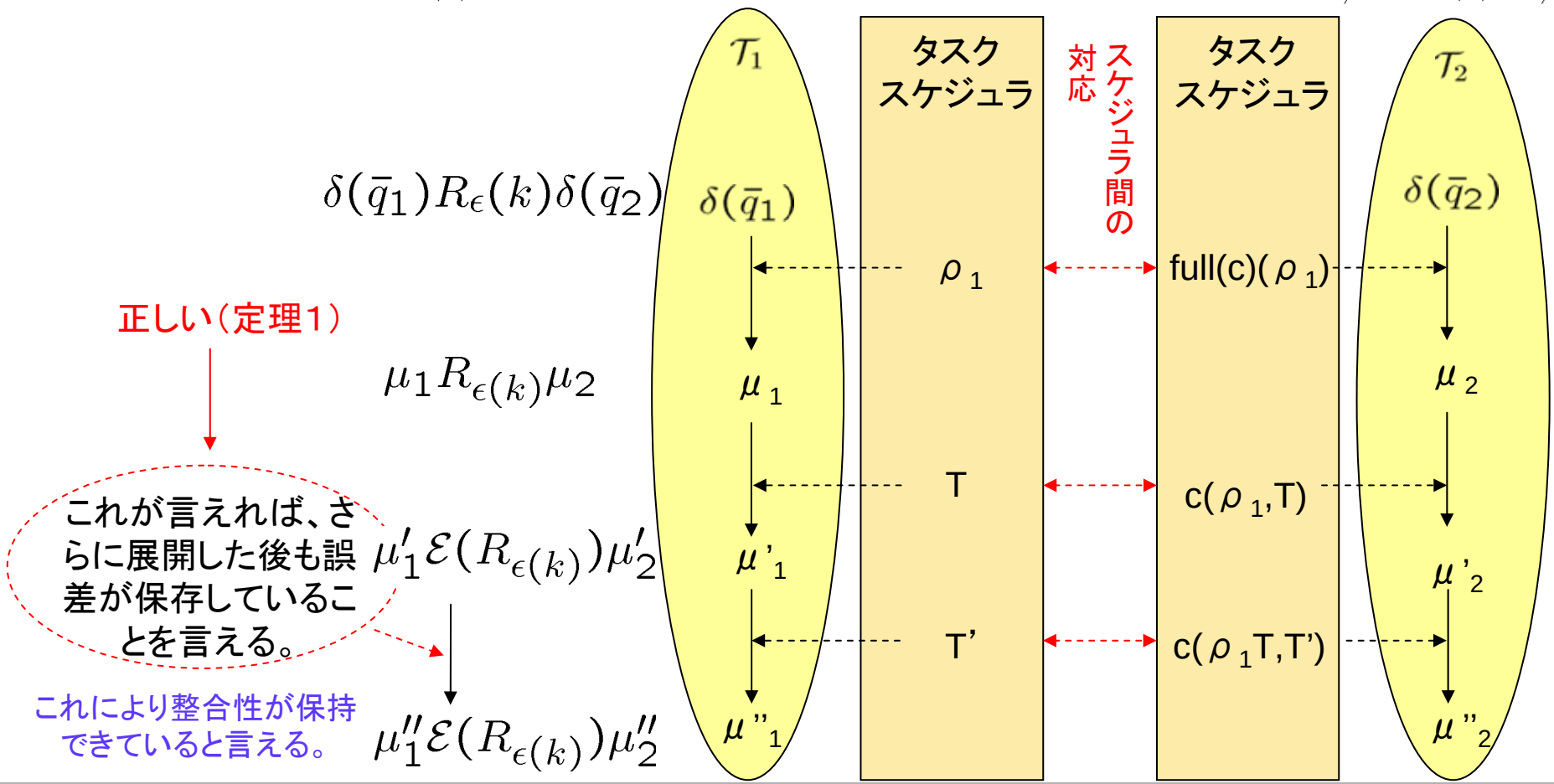
$$\mu_1' \mathcal{E}(R_{\epsilon(k)}) \mu_2'$$



統計的Simulation関係の満たすべき性質

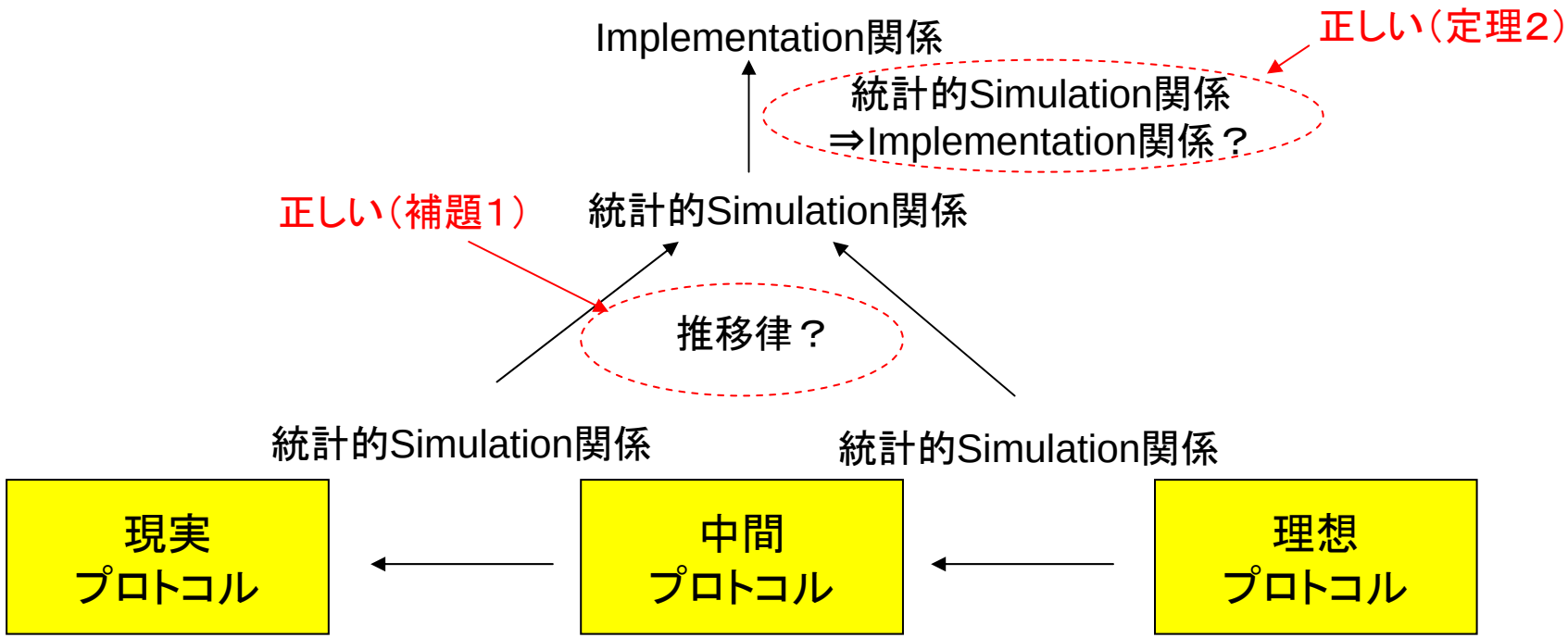
- **定理1**
  - Expansion関係の保存

ある時点で $\epsilon_{1,k}\mathcal{E}(R_{\epsilon(k)})\epsilon_{2,k}$ ならば、consistent なタスクによる展開後にも $\epsilon'_{1,k}\mathcal{E}(R_{\epsilon(k)})\epsilon'_{2,k}$.



統計的Simulation関係の満たすべき性質

- **補題1**
  - 統計的Simulation関係は推移律を満たす。
- **定理2**
  - 統計的Simulation関係 ⇒ Implementation関係



関連する研究

- **ε -Simulation関係[R.Segalaら,2007]**

  2 つの測度 μ_1, μ_2 の間に ϵ-simulation 関係 R_ϵ があるとは、

  $\mu_1 R_\epsilon \mu_2 \Rightarrow \mu_1' R \mu_2'$.

  ただし、$\mu_1 = (1-\epsilon)\mu_1' + \epsilon\mu_1''$, $\mu_2 = (1-\epsilon)\mu_2' + \epsilon\mu_2''$

- **(ε , δ)-Simulation関係[L.Cheungら,2007]**

  ＜開始条件＞

  $\phi(\mu_{10}, \mu_{20}) \leq \epsilon$

  ＜ステップ条件＞

  $\phi(\mu_1, \mu_2) \leq \epsilon \Rightarrow$(consistent なタスクで展開)$\Rightarrow \phi(\mu_1', \mu_2') \leq \epsilon$.

  ＜トレース条件＞

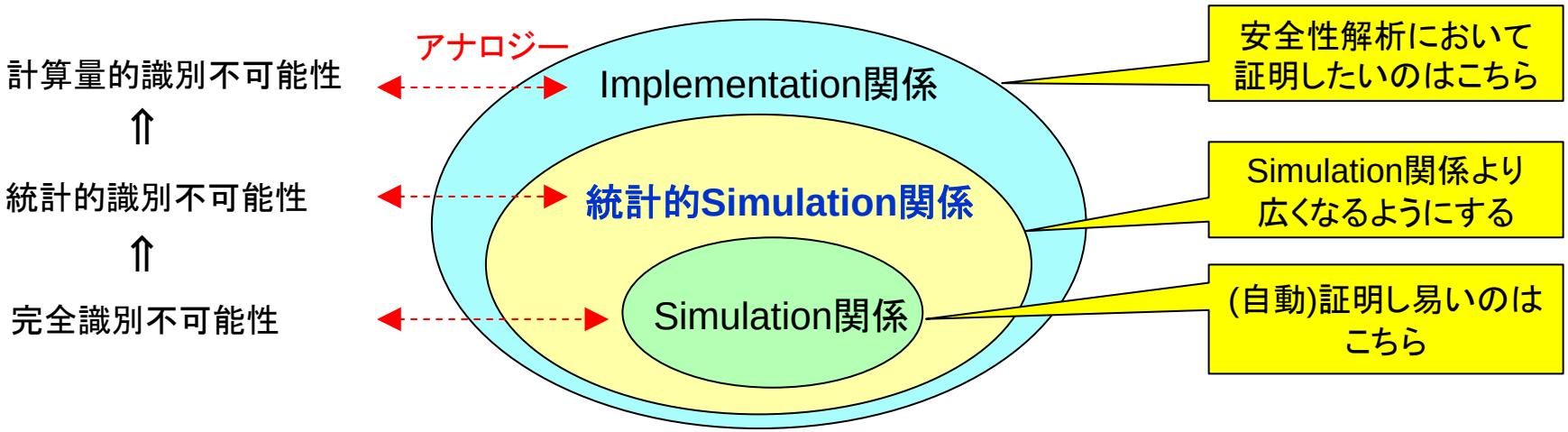
  $\phi(\mu_1, \mu_2) \leq \epsilon \Rightarrow \exists\delta > 0,\ d_u(tdist(\mu_1), tdist(\mu_2)) \leq \delta$.

既存研究との差異

	関係確認の手間	概念の広さ
統計的Simulation関係 [今回提案するもの]	●測度の分解は不要 ●手間は従来のSimulation関係とほぼ同じと推定	●ステップ後の関係はステップ前の関係Rをを Expansion演算 （Simulation関係の性質継承）
ε-Simulation関係 [Segala et al.,2007]	●測度の分解が必要	●開始条件には誤差が入っていない。
(ε, δ)-Simulation関係 [Cheung et al.,2007]	●測度の分解は不要	●関数ϕは抽象的で具体的構成は特殊な場合のみ ●具体的構成の中に統計的Simulation関係は含まれない ●ϕの構成如何によっては良くなる場合も悪くなる場合も ●一般的なϕに対して定理1のような性質を満たす保障なし ●ステップ条件のステップ前後で同じϕを用いており、効果の拡張は要件の拡張を伴う

まとめと今後の課題

- まとめ
  - Simulation関係とImplementation関係の中間に位置する統計的Simulation関係を定義した。
    - 統計的Simulation関係を示せば安全性証明できる
    - （自動）証明が容易なプロトコルの範囲の拡張が期待できる。
  - 統計的Simulation関係の持つ性質について考察した。



- 今後の課題
  - 統計的Simulation関係と他のSimulation関係との詳細な比較を行うこと。
    - 現状は定性的な比較なので、今後は定量的な比較も行いたい。
  - 統計的Simulation関係を用いた場合の形式的証明や自動証明の容易性を詳細に検討すること。