TOSHIBA
Leading Innovation

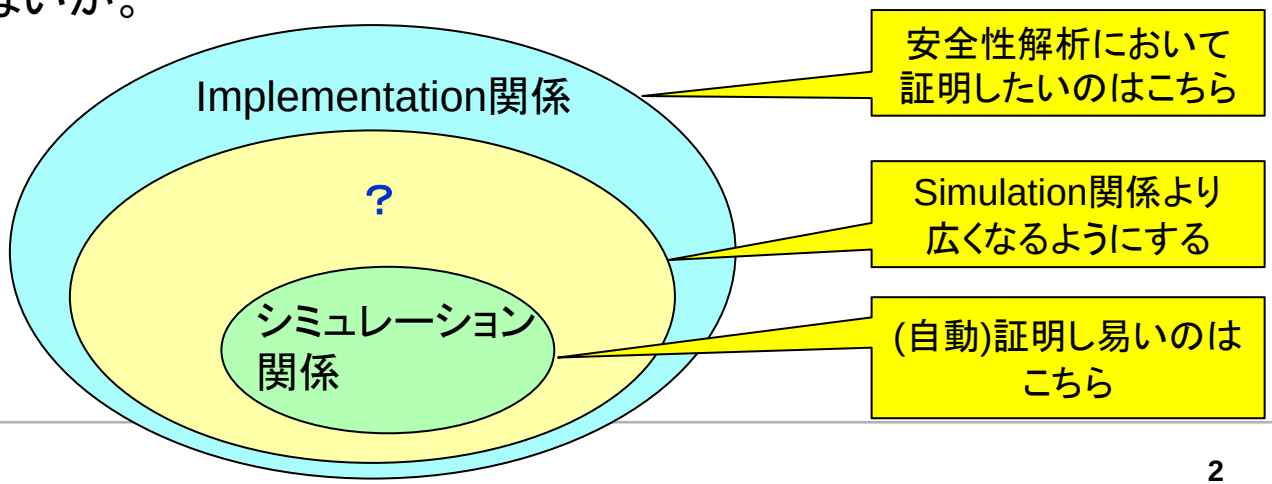
統計的シミュレーション関係の証明能力について

日本応用数理学会 2008年度年会
2008年9月18日　東京大学柏キャンパス

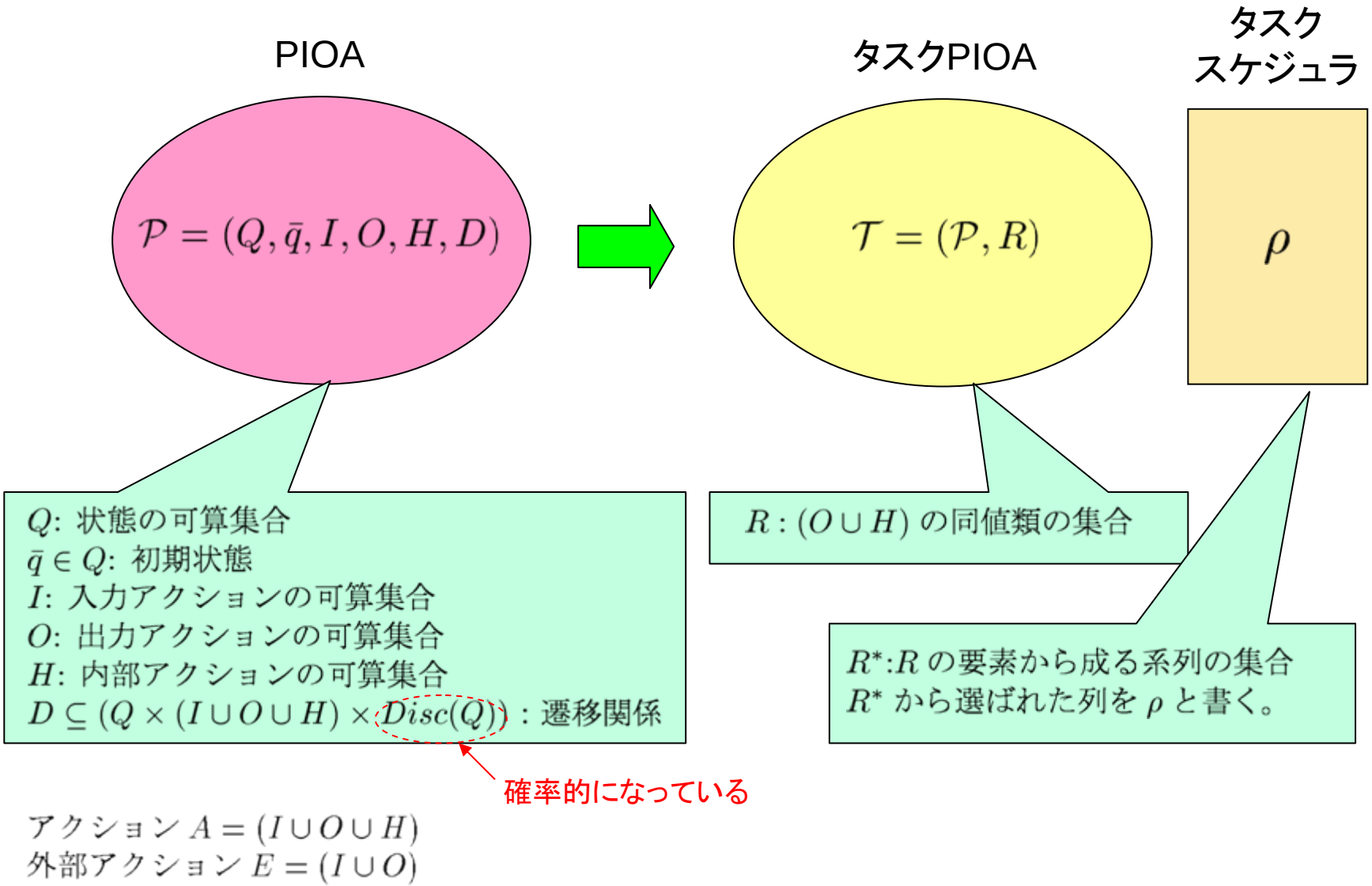
◎古田憲一郎、花谷嘉一、大熊建司、村谷博文（東芝　研究開発センター）

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[R.Canetti2005]
    - 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
    - シミュレーション関係⇒Implementation関係
    - シミュレーション関係より広く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
- 目的
  - 証明範囲拡張のために構築された、統計的シミュレーション関係（統計的関係）と近似的シミュレーション関係（近似的関係）とを比較する。
  - 各種関係の改良の指針となりうる有用な指標を考えることはできないか。
    - 指標の値を変化させるように改善することで、証明できるプロトコル範囲を改善するようにできないか。

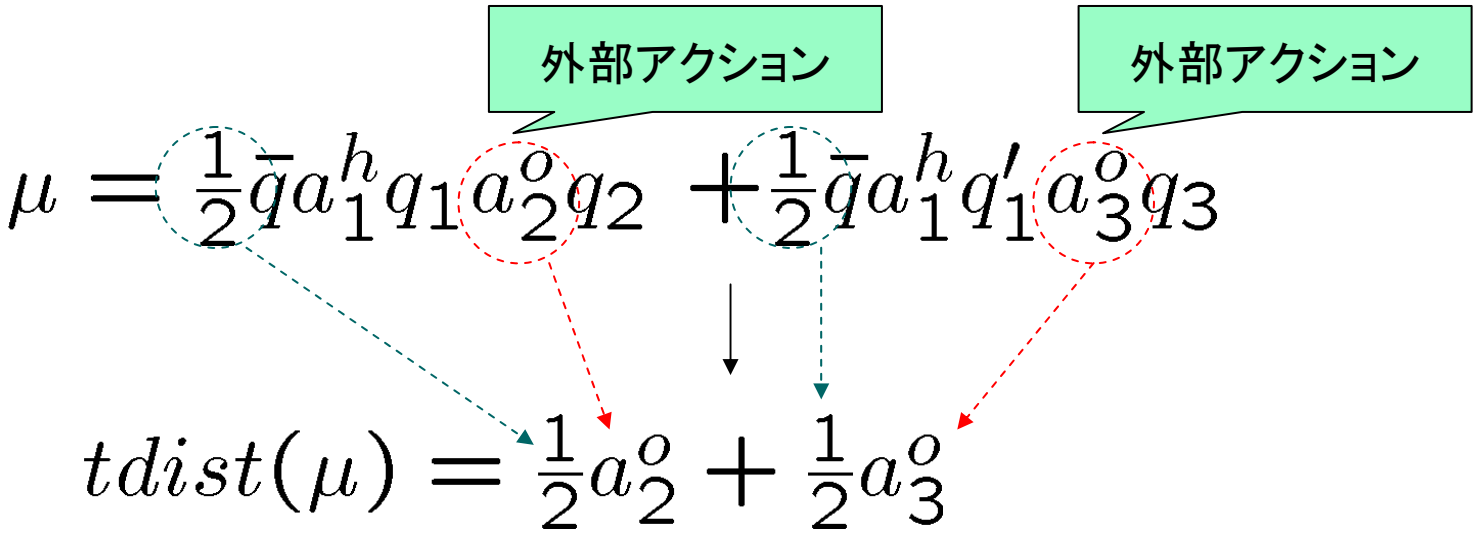


タスクPIOAとタスクスケジュラ[R.Canetti2006]



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）・・・・
  - オートマトンPの実行の集合を**Execs(P)**で表す
  - Execs(P)の上の離散確率分布の集合を**Disc(Execs(P))**で表す。
- **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Disc(Execs(P))を表す



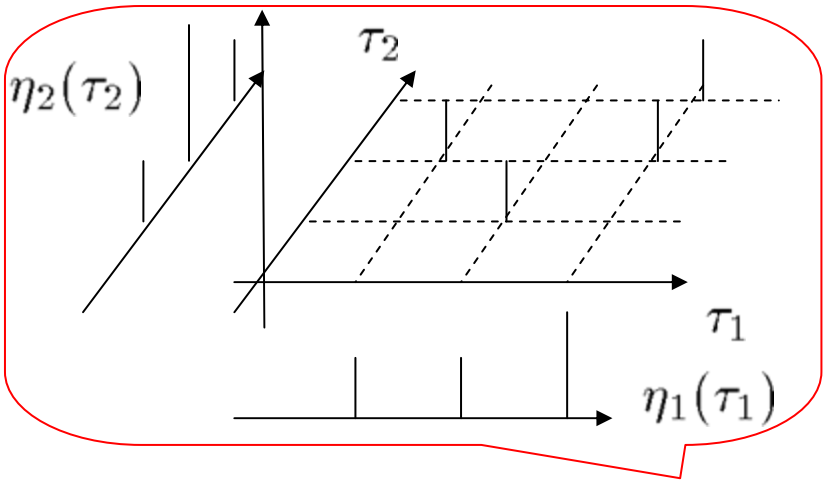
シミュレーション関係と拡張された2つの関係

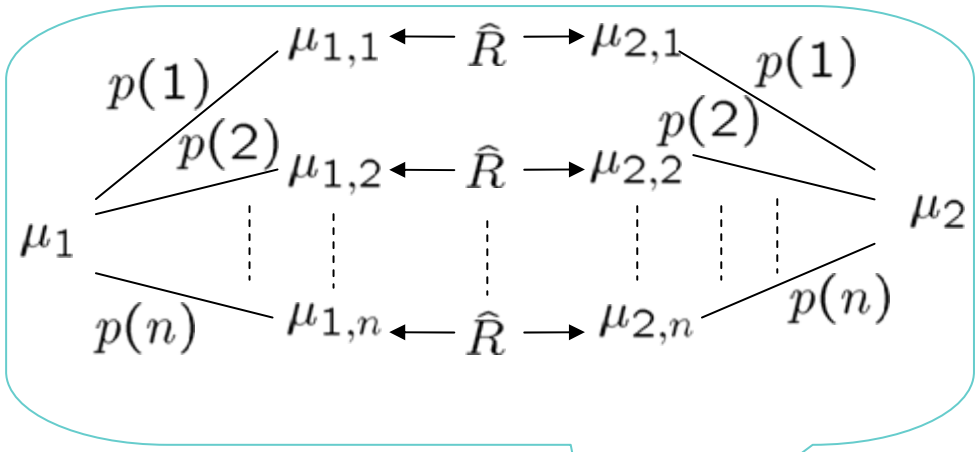
	シミュレーション関係 [R.Canetti2005]	統計的関係 [古田,村谷,花谷2007]	近似的関係 [R.Segala2007]
開始条件	$\delta(\bar{q}_1)\hat{R}\delta(\bar{q}_2)$	$\delta(\bar{q}_1)R_{\epsilon(k)}\delta(\bar{q}_2)$	$\bar{q}_1 R \bar{q}_2$
ステップ条件	$\mu_1 \hat{R} \mu_2$ $\Downarrow$ $\mu'_1 \mathcal{E}(\hat{R}) \mu'_2$	$\mu_1 R_{\epsilon(k)} \mu_2$ $\Downarrow$ $\mu'_1 \mathcal{E}(R_{\epsilon(k)}) \mu'_2$	$\mu_1 \mathcal{L}(R,\gamma) \mu_2$ $\Downarrow$ $\mu'_1 \mathcal{L}(R, \gamma + k^{-c}) \mu'_2$
Rの性質	$\mu_1 \hat{R} \mu_2$ ならば $tdist(\mu_1)$ $= tdist(\mu_2)$	$\mu_{1,k} R_\epsilon \mu_{2,k}$ ならば $\sum_\beta \lvert tdist(\mu_{1,k})(\beta)$ $- tdist(\mu_{2,k})(\beta) \rvert < \epsilon$	R は $Execs(P)$ 上の恒等的関係

μ'_1, μ'_2 が、$\mu'_{1,i}, \mu'_{2,i}$ の和に分解でき、
各部分について $\mu'_{1,i} \hat{R} \mu'_{2,i}$.

定義には書かれていないが、証明を行う際には用いられている条件

関係の演算[R.Canetti2005]





$< \hat{R}\text{の Lifting} >$

$$\eta_1(\tau_1)\mathcal{L}(\hat{R})\eta_2(\tau_2)$$

$$\sum_{\tau_2} \omega(\tau_1,\tau_2) = \eta_1(\tau_1)$$

$$\sum_{\tau_1} \omega(\tau_1,\tau_2) = \eta_2(\tau_2)$$

$$\omega(\tau_1,\tau_2) > 0 \rightarrow \tau_1 \hat{R} \tau_2$$

$$\eta_1(\tau_1), \eta_2(\tau_2) \in Disc(Disc(Execs(P)))$$

$$\tau_1 \hat{R} \tau_2$$

$$\tau_1, \tau_2 \in Disc(Execs(P))$$

$< \hat{R}\text{の Expansion} >$

$$\mu_1 \mathcal{E}(\hat{R}) \mu_2$$

$$\mu_1 = flatten(\eta_1)$$

$$\mu_2 = flatten(\eta_2)$$

$$flatten(\eta_i) = \sum \eta_i(\tau_i)\tau_i$$

$$\mu_1, \mu_2 \in Disc(Execs(P))$$

近似的な演算[R.Segala2007]

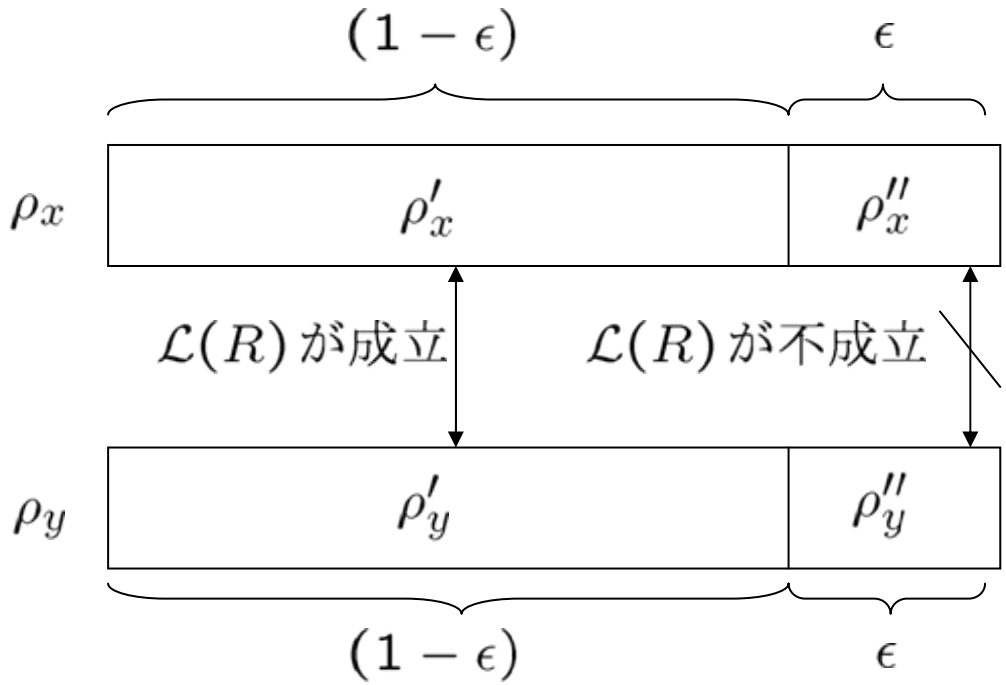
関係 R を Lifting 演算して生成される関係 $\mathcal{L}(R)$ に対して、
近似的な Lifting 関係が以下のように定義できる。

$< \rho_x \mathcal{L}(R, \epsilon) \rho_y$ の意味$>$

数式で表すと

$$\rho_x = (1-\epsilon)\rho'_x + \epsilon\rho''_x,$$
$$\rho_y = (1-\epsilon)\rho'_y + \epsilon\rho''_y,$$
$$\rho'_x \mathcal{L}(R) \rho'_y$$

図で表すと



2つの関係の比較

- 目的
  - 統計的関係と近似的関係とで、証明を行う能力について比較する。
- 比較に用いる量
  - ステップ後に許容される分布間の差（以下、許容誤差）からステップ前の許容誤差をひいた量（後述の証明では ε に対応）。以下では、許容誤差の変化分と記す。
    - この量は、認証プロトコルの1種であるMAP1プロトコルの証明において重要な役割を果たす。
- 結果
  - 改良された統計的関係、および恒等関係という条件を付した近似的関係とで、許容誤差の変化分は、ともにnegligible関数となる。

ステップ条件

$$\mu_1 F(R) \mu_2$$
$$\Downarrow$$
$$\mu'_1 F'(R) \mu'_2$$

ここで$F(R), F'(R)$は関係RにLiftingやExpansionなどの演算を施したものを表している。

トレース分布による表現では、

$$\sum_{\beta} |tdist(\mu'_1)(\beta) - tdist(\mu'_2)(\beta)| - \sum_{\beta} |tdist(\mu_1)(\beta) - tdist(\mu_2)(\beta)|$$

が許容誤差の変化分に相当する。

ここでβは各トレースを表す。

近似的関係によるMAP1の証明[R.Segala2007]

＜現実プロトコルと中間プロトコルとの間の関係＞

近似的関係におけるステップ条件が成立しないと仮定する。

↓

ステップによる許容誤差の変化分を ϵ とするとき、$\epsilon > k^{-c}$

↓

ϵ は繰り返しNonceの生成確率に対応

↓

繰り返しNonceの生成確率が少なくとも k^{-c} となる。

↓

このことは N_R がReal-NGであることに矛盾する。なぜなら、上記の事実はClaim1(NGの定義)により得られる事実を無視することになるからである。

近似的関係の変換の過程

- 比較の方法
  - 許容誤差をトレース分布として表現した上で比較する。近似的関係では、トレース分布による誤差が明確でないため、近似的関係の変換がメインになる。
  - 近似的関係が恒等関係であるという条件を加えて比較する。

ステップ条件のステップ前には、$\mathcal{L}(R,\gamma)$、つまり $\nu_1 = (1-\gamma)\nu_1^* + \gamma\nu_1^{**}$, $\nu_2 = (1-\gamma)\nu_2^* + \gamma\nu_2^{**}$, $\nu_1^*\mathcal{L}(R)\nu_2^*$ が成り立つので、ν_1^*, ν_2^* の部分の Expansion 演算への変換を試みる。

↓

すると、$flatten(\nu_1^*)\mathcal{E}(R)flatten(\nu_2^*)$ が成立する。

↓ 補題1

$\nu_1^*\mathcal{E}(R)\nu_2^*$ が成立する。

↓ 補題2

$\nu_1^*\mathcal{E}(R)\nu_2^* \rightarrow tdist(\nu_1^*) = tdist(\nu_2^*)$

↓

トレース分布が一致しない部分の割合は γ 以下になる。

導出過程における特殊性

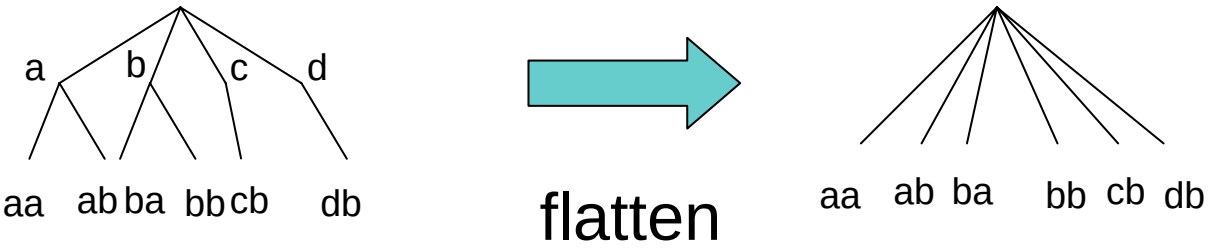
- **2つの補題を用いて変換する。**
  - 今回の導出の特殊性：近似的関係においては、関係RがExecs(P_1) からExecs(P_2)への関係であって、Disc(Execs(P_1)) からDisc(Execs(P_2))への関係ではない。
  - このような場合の各種演算間の関係を導出することにより変換が可能になる。

- **補題1**
  - Flatten演算の入力がDisc(Execs(P))である場合、Flatten演算は恒等写像となり、出力もDisc(Execs(P))となる。

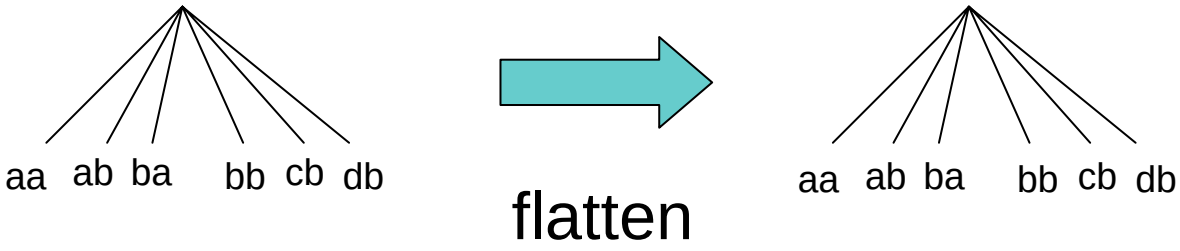
- **補題2**
  - RをExecs(P_1)からExecs(P_2)への恒等関係とする。このとき$\nu_x^* \mathcal{E}(R) \nu_y^*$ が成立するならば、$tdist(\nu_x^*) = tdist(\nu_y^*)$ が成立する。

補題1の証明

Flatten演算の入力がDisc(Disc(Execs(P)))の場合

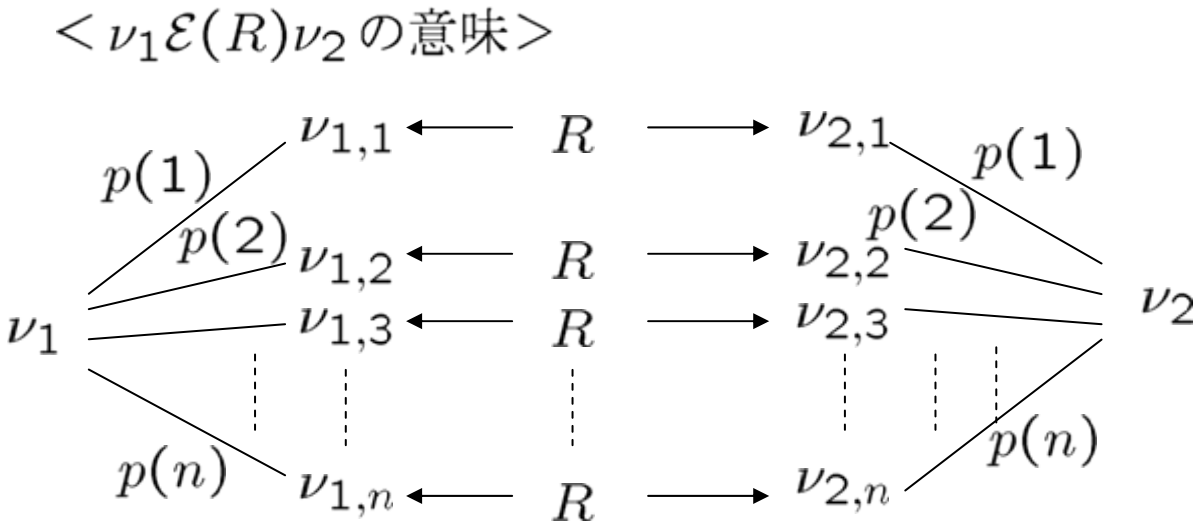


Flatten演算の入力がDisc(Execs(P))の場合



$$flatten(\eta_i) = \sum \eta_i(\tau_i)\tau_i$$

補題2の証明



$\nu_{1,i}, \nu_{2,i}$ として ν_1, ν_2 を構成する $Execs(P)$ の要素をとる。
つまり、$\forall i, \nu_{1,i}, \nu_{2,i} \in Execs(P)$ として、上の図式を使う。

↓

次に、R が恒等関係であることを用いると、
上の図式から $tdist(\nu_1) = tdist(\nu_2)$ であることが分かる。

近似的関係について

以上より、近似的なLifting演算におけるパラメータγが、そのまま分布間の許容誤差のトレース分布による表現になることが分かった。

ステップ前　$\mu_1 \mathcal{L}(R, \gamma)\mu_2$　トレース分布による表現での許容誤差は、γとなる。

⇓

ステップ後　$\mu_1' \mathcal{L}(R, \gamma + k^{-c})\mu_2'$　トレース分布による表現での許容誤差は、$\gamma + k^{-c}$となる。

よって、許容誤差の変化分は$(\gamma + k^{-c}) - \gamma = k^{-c}$で、negligible関数となる。

統計的関係について

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

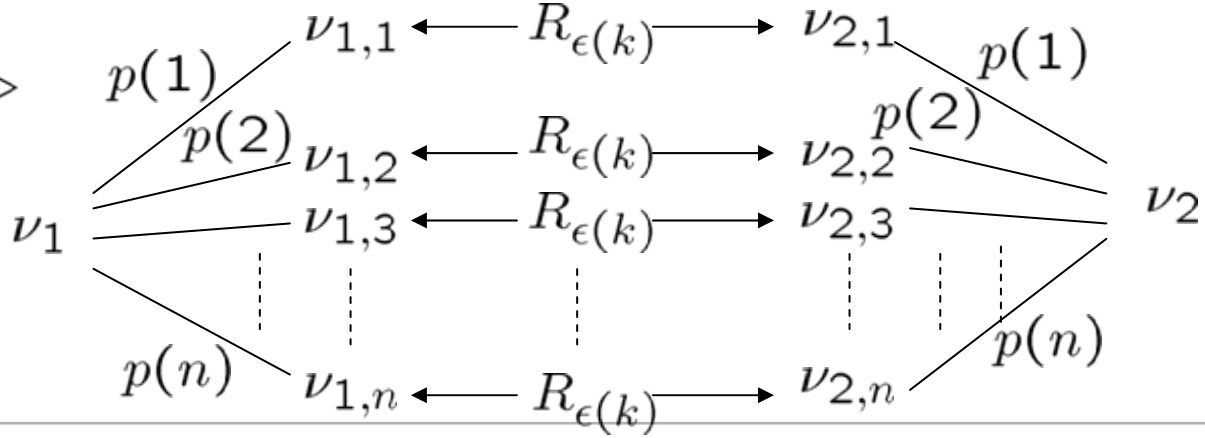
この関係式を用いてステップ条件における許容誤差を算出

ステップ前　$\mu_1 R_{\epsilon(k)} \mu_2$ ←　許容誤差は ε (k)

⇓　　↕　この差は0

ステップ後　$\mu_1' \mathcal{E}(R_{\epsilon(k)}) \mu_2'$ ←　許容誤差は ε (k)

$<\nu_1 \mathcal{E}(R_{\epsilon(k)}) \nu_2$ の意味>



統計的関係に対する改良と改良後の評価

次に、ステップ条件の前後で、異なる ε を取れるように改良してみる。

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

ステップ前 $\mu_1 R_{\epsilon 1(k)} \mu_2$ ← 許容誤差はnegligible関数 ε 1(k)

⇓

この差はnegligible関数 ε 2(k)- ε 1(k)

ステップ後 $\mu'_1 \mathcal{E}(R_{\epsilon 2(k)}) \mu'_2$ ← 許容誤差はnegligible関数 ε 2(k)

考察

- 近似的関係においても、統計的関係（改良後）においても、ステップ条件が成立するならば、許容誤差の変化分はnegligible関数となる。

- 2つの関係では共に、ステップ条件が成立しないと仮定したときに、許容誤差の変化分がnegligible関数でなくなる。
- MAP1プロトコルの証明に類似する証明を行う能力が等しくなると考えられる。
  - 背理法における仮定から導かれる命題として、許容誤差の変化分がnegligible関数でなくなるという命題を用いる証明。

- 許容誤差は、negligible関数になるときに、MAP1プロトコルの証明に類似する証明が可能であることを表す指標として使えると考えられる。

まとめ

- **結果**
  - 2つの関係では、MAP1プロトコルの証明に類似する証明を行う能力が等しくなると考えられる。
    - 背理法における仮定から導かれる命題として、許容誤差の変化分がnegligible関数でなくなるという命題を用いる証明。
  - 許容誤差の変化分は、negligible関数になるときに、MAP1プロトコルの証明に類似する証明が可能であることを表す指標として使えると考えられる。

- **今後の課題**
  - 許容誤差の変化分以外の指標によってもシミュレーション関係を比較すること。
    - 比較すべき指標を体系的にリストアップすること。
  - 指標と証明できるプロトコル範囲との関係を体系的に示すこと。

- ご清聴ありがとうございました。