ソフトウェア基礎論配布資料 (9)
プロセスの等しさ

五十嵐 淳
京都大学 大学院情報学研究科知能情報学専攻
e-mail: `igarashi@kuis.kyoto-u.ac.jp`

平成 19 年 1 月 30 日

1 プロセスが「等しい」とは？

お互いに相手の挙動の真似・模倣ができること:

- プロセスの状態同士の対応関係
- 各状態で観測できる挙動が同じ

2 強有刺双模倣性，強有刺同値性，強有刺合同性

プロセスのある瞬間の挙動を捉えるために，P は μ が観測可能であることを表す観測可能性 $P \searrow \mu$ という概念を導入する．ここで μ は $\#^i x!$ か $\#^i x?$ のいずれかで，$\#^i x$ に対して出力 (入力) が観測できることを示す．

$$\frac{\Gamma \vdash P \cong (\boldsymbol{\nu} x_1)\cdots(\boldsymbol{\nu} x_n)((\#^i x![\#^j z].Q + R_1) \parallel R_2) \qquad \Gamma \vdash \#^i x \downarrow_{x_n} \cdots \downarrow_{x_1} \in \mathbf{Ch}}{\Gamma \vdash P \searrow \#^i x!}$$

$$\frac{\Gamma \vdash P \cong (\boldsymbol{\nu} x_1)\cdots(\boldsymbol{\nu} x_n)((\#^i x?[y].Q + R_1) \parallel R_2) \qquad \Gamma \vdash \#^i x \downarrow_{x_n} \cdots \downarrow_{x_1} \in \mathbf{Ch}}{\Gamma \vdash P \searrow \#^i x?}$$

(ちなみに，多くの文献では，$\searrow$ の代わりに $\downarrow$ が使われる．)

この観測可能であることと，プロセスの状態が簡約を通じて対応していることを強有刺双模倣的関係として定式化する．ここで「強」というのは，片方のプロセスの 1 ステップがもう一方のきっちり 1 ステップで模倣されることを示している．「有刺」は barbed の訳[1] で観

[1]余り一般的ではないかもしれません．

測可能な挙動を barb と呼んでいることに由来する．以下，環境で添字付けされた関係の族 $\mathcal{R}$ に対し，$\Gamma \vdash P, Q \in \mathbf{Pr}$ かつ $P \mathcal{R}_\Gamma Q$ であることを，$\Gamma \vdash P \mathcal{R} Q$ と書く．ある Γ について $\Gamma \vdash P \mathcal{R} Q$ であることを単に $P \mathcal{R} Q$ と書く．

2.1 定義 [**強有刺双模倣的関係，強有刺双模倣性**]: 環境で添字付けされた関係の族 $\mathcal{S}$ が**強有刺双模倣的関係**(*strong barbed bisimulation*) であるとは，任意の $\Gamma \vdash P \mathcal{S} Q$ に対し，

- $\Gamma \vdash P \searrow \mu \iff \Gamma \vdash Q \searrow \mu$
- $\Gamma \vdash P \longrightarrow P'$ ならば，ある $\Gamma \vdash Q' \in \mathbf{Pr}$ に対し $\Gamma \vdash Q \longrightarrow Q'$ かつ $\Gamma \vdash P' \mathcal{S} Q'$
- $\Gamma \vdash Q \longrightarrow Q'$ ならば，ある $\Gamma \vdash P' \in \mathbf{Pr}$ に対し $\Gamma \vdash P \longrightarrow P'$ かつ $\Gamma \vdash P' \mathcal{S} Q'$

が成立することである．プロセス P, Q が**強有刺双模倣的**(*strong barbed bisimilar*) である ($\Gamma \vdash P \dot{\sim} Q$ と書く) とは，ある強有刺双模倣的関係 $\mathcal{S}$ に対し，$\Gamma \vdash P \mathcal{S} Q$ であることと定義する．

2.2 例:

- $\tau.P \dot{\sim} (\boldsymbol{\nu} x)(x![a].P{\uparrow_x} \parallel x?[y].\mathbf{0})$
- $\tau.P \not\dot{\sim} x![a].P{\uparrow_x} \parallel x?[y].\mathbf{0}$
- $(x?[z].\mathbf{0} + y?[z].\mathbf{0}) \parallel x![a].\mathbf{0} \parallel y![b].\mathbf{0} \not\dot{\sim} x?[z].\mathbf{0} \parallel y?[z].\mathbf{0} \parallel x![a].\mathbf{0} \parallel y![b].\mathbf{0}$
- $\tau.(\tau.x![a].\mathbf{0} + \tau.y![b].\mathbf{0}) \not\dot{\sim} \tau.\tau.x![a].\mathbf{0} + \tau.\tau.y![b].\mathbf{0}$
- $x![z].\mathbf{0} \parallel y?[v].\mathbf{0} \dot{\sim} x![z].y?[v].\mathbf{0} + y?[v].x![z].\mathbf{0}$
- $x![y].z![y].\mathbf{0} \dot{\sim} x![y].y![z].\mathbf{0}$
- $x![y].\mathbf{0} \dot{\sim} x![z].\mathbf{0}$

強有刺双模倣性 $\dot{\sim}$ は同値関係ではあるが，プロセスの等しさとしては，かなり粗い関係である．つまり，最後から二番目の例のように，この時点では発生しない x 上での通信の後の挙動が全く違ったり，最後の例のように，送信に使うチャネルが同一でも送られる名前が異なるようなプロセスをも関係づけてしまう．

これらのプロセスを区別するためには，例えば，それぞれ $R_1 = x?[w].\mathbf{0}$ や $R_2 = x?[w].w![z].\mathbf{0}$ というプロセスと並列に実行させてみればよい．その結果は強有刺双模倣ではない，つまり，$x, y, z \vdash x![y].\mathbf{0} \parallel R_2 \not\dot{\sim} x![z].\mathbf{0} \parallel R_2$ である．この R_i は，プロセスの等しさを判定するテストをしているプロセスと考えることができる．一方，上の五番目のプロセスは，$R = x?[w].\mathbf{0} \parallel y![z].\mathbf{0}$ と並列実行させても $\dot{\sim}$ の関係にある．実際，任意のプロセス R と並列実行させても，$\dot{\sim}$ の関係を保存する．このようなプロセス同士は強有刺同値であるという．

2.3 定義 [**強有刺同値性**]: $\Gamma \vdash P \simeq Q$ を，任意の $\Gamma \vdash R$ に対し $\Gamma \vdash P \parallel R \dot{\sim} Q \parallel R$ であること，と定義する．$\simeq$ を**強有刺同値性**(*strong barbed equivalence*) と呼ぶ.

2.4 例:

- $x![a].(y![a].\mathbf{0} + z![a].\mathbf{0}) \not\simeq x![a].y![a].\mathbf{0} + x![a].z![a].\mathbf{0}$
- $x![z].\mathbf{0} \parallel y?[v].\mathbf{0} \simeq x![z].y?[v].\mathbf{0} + y?[v].x![z].\mathbf{0}$
- $x![z].\mathbf{0} \parallel x?[v].\mathbf{0} \not\simeq x![z].x?[v].\mathbf{0} + x?[v].x![z].\mathbf{0}$
- $x![y].z![y].\mathbf{0} \not\simeq x![y].y![z].\mathbf{0}$
- $x![y].\mathbf{0} \not\simeq x![z].\mathbf{0}$

残念ながら，強有刺同値は合同関係ではない．それは，異なる変数が同じ名前を示す場合に挙動が変わってしまうためである．例えば，上の二番目のプロセスで，x と y が同じ名前を指しているとしたら，左辺は $\mathbf{0}$ に簡約される一方で，右辺は簡約できないため，$\dot{\sim}$ の関係にはない．ふたつの変数が同じ名前を指すような状況はプロセスを入力動作の元に置くことで発生させることができる．つまり，文脈 $C = z![y]. \parallel z?[x].[\,]$ に埋めこむことで,

$$C[x![z].\mathbf{0} \parallel y?[v].\mathbf{0}] \not\dot{\sim} C[x![z].y?[v].\mathbf{0} + y?[v].x![z].\mathbf{0}]$$

となる．強有刺同値をさらに強めて，合同関係である強有刺双模倣的関係を考えたのが強有刺合同性であり，プロセスの等しさの，ひとつの標準的定義と考えられる．

2.5 定義 [**強有刺合同性**]: $\Gamma \vdash P \simeq^c Q$ を，任意の $\Gamma' \vdash C \in \mathbf{Ctx}[\Gamma]$ に対し $\Gamma' \vdash C[P] \dot{\sim} C[Q]$ であること，と定義する．$\simeq^c$ を **強有刺合同性**(*strong barbed congruence*) と呼ぶ.

3　ラベル付遷移システムと強双模倣性

あるプロセスが強有刺等価・合同であることを示すためには，全ての並列実行されるプロセス・文脈について $\dot{\sim}$ であることを示すわけだが，これはたいてい困難 (文脈の構造に関する帰納法を使っても証明がうまくいかない) である．そのため，別の等価な定義 (特徴付け) を示す.

この特徴付けは**ラベル付き遷移システム**(*labelled transition system*) を使って行われる．ラベル付き遷移システムは，状態遷移に遷移の動作内容を表すラベルが付与されたもので，有限オートマトンは，アルファベットの入力を動作と考えたラベル付き遷移システムの一種と考えることができる．同様に，プロセスに対するラベル付き遷移システムは，プロセスの**外部と**どのような送受信行うかをラベルとして記述される．このラベルを**アクション**(*action*) と呼ぶ．簡約もプロセスの状態遷移を記述したものだが，プロセス内部での通信の発生による状態遷移しか考慮しない点が大きく異なる.

3.1 定義 [アクション]: アクション α を以下の構文で定義する．

$$\alpha ::= \tau \mid \#^i x![\#^j y] \mid \#^i x?[\#^j y]$$

また，アクションの**主体**(*subject*) $subj(\alpha)$ を $subj(\tau) = \tau$, $subj(\#^i x![\#^j y]) = subj(\#^i x?[\#^j y]) = \#^i x$ で定義する．

3.2 定義 [ラベル付き遷移関係]: 環境 Γ の下でのプロセス P が動作 α を行い，環境 Γ' の下でのプロセス Q に遷移することを

$$\Gamma \vdash P \xrightarrow{\alpha} Q \dashv \Gamma'$$

と書き，以下の規則で定義される．

$$\frac{\Gamma \vdash \#^i x![\#^j z].P \in \mathbf{Pr}}{\Gamma \vdash \#^i x![\#^j z].P \xrightarrow{\#^i x![\#^j z]} P \dashv \Gamma} \qquad (\textsc{Tr-Out})$$

$$\frac{\Gamma \vdash \#^i x?[y].P \in \mathbf{Pr} \qquad \Gamma, z^n \vdash \#^j v \in \mathbf{Ch} \quad \Gamma, z^n, y = \#^j v \vdash (P \uparrow_z \cdots \uparrow_z)[y] \Rightarrow P'}{\Gamma \vdash \#^i x?[y].P \xrightarrow{\#^i x?[\#^j z]} P' \downarrow_y \dashv \Gamma, z^n} \qquad (\textsc{Tr-In})$$

$$\frac{\Gamma \vdash \tau.P \in \mathbf{Pr}}{\Gamma \vdash \tau.P \xrightarrow{\tau} P \dashv \Gamma} \qquad (\textsc{Tr-Tau})$$

$$\frac{\Gamma \vdash P \xrightarrow{\alpha} P' \dashv \Gamma'}{\Gamma \vdash P + Q \xrightarrow{\alpha} P' \dashv \Gamma'} \qquad (\textsc{Tr-SumL})$$

$$\frac{\Gamma \vdash P \xrightarrow{\alpha} P' \dashv \Gamma, x^n \qquad \Gamma \vdash Q \in \mathbf{Pr}}{\Gamma \vdash P \parallel Q \xrightarrow{\alpha} P \parallel (Q \uparrow_x \cdots \uparrow_x) \dashv \Gamma, x^n} \qquad (\textsc{Tr-ParL})$$

$$\frac{\Gamma \vdash P \xrightarrow{\#^i x![\#^j y]} P' \dashv \Gamma, z^n \qquad \Gamma \vdash Q \xrightarrow{\#^i x?[\#^j y]} Q' \dashv \Gamma, z^n}{\Gamma \vdash P \parallel Q \xrightarrow{\tau} \underbrace{(\boldsymbol{\nu} z) \cdots (\boldsymbol{\nu} z)}_{n}(P' \parallel Q') \dashv \Gamma} \qquad (\textsc{Tr-CommL})$$

$$\frac{\Gamma, x \vdash P \xrightarrow{\alpha} P' \dashv \Gamma, x, z^n \qquad (x \notin \{z, subj(\alpha)\})}{\Gamma \vdash (\boldsymbol{\nu} x)P \xrightarrow{\alpha \downarrow_x} (\boldsymbol{\nu} x)P' \dashv \Gamma, z^n} \qquad (\textsc{Tr-New})$$

$$\frac{\Gamma, x \vdash P \xrightarrow{\alpha} P' \dashv \Gamma, x, x^n \qquad (x \neq subj(\alpha))}{\Gamma \vdash (\boldsymbol{\nu} x)P \xrightarrow{\alpha \downarrow_x} P' \dashv \Gamma, x^{n+1}} \qquad (\textsc{Tr-NewEx})$$

$$\frac{\Gamma \vdash P \xrightarrow{\alpha} P' \dashv \Gamma, x^n}{\Gamma \vdash *P \xrightarrow{\alpha} P' \parallel (*P\uparrow_x \cdots \uparrow_x) \dashv \Gamma, x^n} \qquad (\textsc{Tr-RepAct})$$

$$\frac{\Gamma \vdash P \xrightarrow{\#^i x![\#^j y]} P' \dashv \Gamma, z^n \qquad \Gamma \vdash P \xrightarrow{\#^i x?[\#^j y]} P'' \dashv \Gamma, z^n}{\Gamma \vdash *P \xrightarrow{\tau} \underbrace{(\boldsymbol{\nu} z)\cdots(\boldsymbol{\nu} z)}_{n}(P' \parallel P'') \parallel *P \dashv \Gamma} \quad (\textsc{Tr-RepComm})$$

(ただし，Tr-SumL, Tr-ParL, Tr-CommL と対称的な規則 Tr-SumR, Tr-ParR, Tr-CommR は省略している．)

3.3 例: 以下の遷移関係が成り立つ．

- $x, y \vdash x![y].\mathbf{0} \xrightarrow{x![y]} \mathbf{0} \dashv x, y$
- $x \vdash (\boldsymbol{\nu} y)x![y].\mathbf{0} \xrightarrow{x![y]} \mathbf{0} \dashv x, y$
- $x \vdash x?[z].z![x].\mathbf{0} \xrightarrow{x?[y]} y![x].\mathbf{0} \dashv x, y$
- $x \vdash ((\boldsymbol{\nu} y)x![y].\mathbf{0}) \parallel x?[z].z![x].\mathbf{0} \xrightarrow{\tau} (\boldsymbol{\nu} y)(\mathbf{0} \parallel y![z].\mathbf{0}) \dashv x$

3.4 定理: $(\Gamma \vdash P \xrightarrow{\tau} P' \dashv \Gamma \;\&\; \Gamma \vdash P' \cong P'') \iff \Gamma \vdash P \longrightarrow P''$.

3.5 定義 [強双模倣的関係，強双模倣性]: 環境で添字付けされた関係の族 $\mathcal{S}$ が**強双模倣的関係**(*strong bisimulation*) であるとは，任意の $\Gamma \vdash P \;\mathcal{S}\; Q$ に対し，

- $\Gamma \vdash P \xrightarrow{\alpha} P' \dashv \Gamma'$ ならば，ある $\Gamma' \vdash Q' \in \mathbf{Pr}$ に対し $\Gamma \vdash Q \xrightarrow{\alpha} Q' \dashv \Gamma'$ かつ $\Gamma' \vdash P' \;\mathcal{S}\; Q'$
- $\Gamma \vdash Q \xrightarrow{\alpha} Q' \dashv \Gamma'$ ならば，ある $\Gamma' \vdash P' \in \mathbf{Pr}$ に対し $\Gamma \vdash P \xrightarrow{\alpha} P' \dashv \Gamma'$ かつ $\Gamma' \vdash P' \;\mathcal{S}\; Q'$

が成立することである．プロセス P, Q が**強双模倣的**(*strong bisimilar*) である ($\Gamma \vdash P \sim Q$ と書く) とは，ある強双模倣的関係 $\mathcal{S}$ に対し，$\Gamma \vdash P \;\mathcal{S}\; Q$ であることと定義する．

3.6 定理: $\sim$ は，(各 Γ について) 最大の強双模倣的関係である．

3.7 予想:

1. $P \simeq Q \iff P \sim Q$
2. $P \simeq^c Q \iff \forall \sigma. \sigma P \sim \sigma Q$

σ はプロセス中の名前の置き換え操作を示す．