発表番号: 31 LA Symposium (2003.7.18)

π 計算に対する時間拡張と双模倣関係

桑原 寛明* 結縁 祥治† 阿草 清滋‡

1 はじめに

現在実時間システムが広く利用されている。ペースメーカーのように誤動作が人命にかかわるシステムもあり、このようなシステムには高い信頼性が要求される。そのため形式的な検証手法により動作の正しさを示すことが必要である。実時間システムは動作に時間制約を持つ並行システムである [1] ため、並行計算の非決定性と実時間性を形式的に扱える必要がある。

本研究では形式的手法として並行計算モデルである π 計算 [2, 3, 4] を利用する。π 計算ではプロセス間通信に利用するリンク自身の送受信やプロセスの動的生成が表現可能であり高い表現能力を持つ。このことによりソフトウェアにおけるオブジェクトの生成やメッセージ通信の表現に適している。また時間に関する動作を直接的に記述するために π 計算を時間に関して拡張する。検証の一つとしてシステムの設計と実装の間の動作の等価性検証を考えている。そこで時間に関して拡張した π 計算における双模倣関係を定義する。

2 π 計算に対する時間拡張

2.1 構文

π 計算に時間経過アクション t を導入する。タイムアウトまでの時間を $[n]$ と表し、n 単位時間でタイムアウトする時間待ちを $t[n]$ と記述する。

初めにアクションガードつきプロセスを以下のように定義する。

定義 1 $\pi ::= x(\widetilde{y}) \mid \overline{x}\langle\widetilde{y}\rangle \mid \tau$ とする時

- 任意のプロセス P に対し $\pi.P$ はアクションガードつきプロセスである
- P_1, P_2 がアクションガードつきプロセスであるとすると

  $$P_1|P_2,\ P_1+P_2,\ \boldsymbol{\nu} a\, P_1,\ !P_1$$

  はアクションガードつきプロセスである □

$\mathcal{N}ame$ を名前の集合、$\mathcal{I}$ を 0 以上の整数を表す名前の集合とする。$\mathcal{I} = \{0, 1, \ldots\} \subset \mathcal{N}ame$ である。さらに $\mathcal{N} = \mathcal{N}ame - \mathcal{I}$ とする。$\overline{\mathcal{N}} = \{\overline{x} | x \in \mathcal{N}\}$、$\mathcal{L} = \mathcal{N} \cup \overline{\mathcal{N}}$、$a, x \in \mathcal{N}$ とする。$\widetilde{y}$ は名前の並びを表す。また π 計算のプロセス式全体の集合を $\mathcal{P}$ と書き、アクションの集合を $Act = \mathcal{L} \cup \{\tau\}$ と記す。

*名古屋大学大学院情報科学研究科
†名古屋大学大学院情報科学研究科・PRESTO/JST
‡名古屋大学大学院情報科学研究科

定義 2 時間拡張した π 計算のプロセス式 P は以下の構文によって定義される。

$$\begin{aligned} \pi &::= x(\widetilde{y}) \mid \overline{x}\langle\widetilde{y}\rangle \mid \tau \mid t[n] \\ P &::= M \mid P_1|P_2 \mid \boldsymbol{\nu} a\, P \mid !\, P \\ M &::= \mathbf{0} \mid \pi.P \mid M_1 + M_2 \end{aligned}$$

ただし $!\,P$ はアクションガードつきプロセスでなければならない。 □

定義 3 $P = t[x].P'$ に対し、$x \in \mathcal{N}$ かつ x が P を内部に含むプロセスにおいて入力アクションによって束縛されていない場合、P は動作不能であるといい $P\!\uparrow$ と書く。また $P\!\uparrow$ の時、

$$\begin{gathered} (\overline{x}\langle\widetilde{y}\rangle.P)\!\uparrow, (x(\widetilde{y}).P)\!\uparrow, (\tau.P)\!\uparrow, (t[n].P)\!\uparrow, \\ (P+Q)\!\uparrow, (P \mid Q)\!\uparrow, (\boldsymbol{\nu} z\, P)\!\uparrow, (!\, P)\!\uparrow \end{gathered}$$

とする。

プレフィックスが $t[n]$ であるプロセスは n 単位時間待機する。例えばプロセス $t[5].P$ は 5 単位時間後にプロセス P へ遷移する。時間経過アクションと非決定的選択を用いることで、イベントの発生を一定時間待機しイベントが発生したか否かで動作が異なるプロセスを記述することができる。$a.P + t[5].\tau.Q$ というプロセスはアクション a の発生まで 5 単位時間待機する。5 単位時間経過する前に a が発生すればプロセス P へ、発生しなければタイムアウトしプロセス Q へ遷移する。

2.2 時間動作意味

従来の π 計算の動作意味に対し時間経過に関する規則を導入して拡張する。時間は離散時間であるとする。また時間の経過は時間経過規則による遷移によってのみ発生し、他の規則による遷移では時間は経過しないとする。

$\mathcal{P}$ 上の遷移関係 $\{\stackrel{\alpha}{\longrightarrow} \mid \alpha \in Act\} \cup \rightsquigarrow$ は図 1 の遷移規則及び図 2 の時間経過規則によって定義される。ABORT 規則以外のすべての規則において $P\not\downarrow, Q\not\downarrow$ とする。また、図 1、図 2 において $x \in \mathcal{N}, n \in \mathcal{I}, y \in \mathcal{N}ame, z \in \mathcal{N}ame$ とする。

ラベル付き遷移は

- プロセスが他のプロセスとどのように通信するか
- プロセスが単位時間ごとにどのように遷移するか

を示す。$P \stackrel{\alpha}{\longrightarrow} P'$ は入力、出力、内部アクションのいずれかのアクション α により P から P' に遷移することを表し、$P \rightsquigarrow P'$ は P が 1 単位時間の経過により P' に遷移することを表す。

時間はすべてのプロセスにおいて同時に経過する。時間経過によりプレフィックス $t[n]$ は $t[n-1]$ となり、タイムアウトまでの時間が 1 単位時間短くなったことを示す。プレフィックスでない $t[n]$ の n の値は変化しない。$\mathrm{PAR_T}$ 規則と $\mathrm{REP_T}$ 規則において遷移は τ 遷移が発生しない場合にのみ発生する。

3 双模倣関係

定義 4 以下を満たす対称な関係 $\mathcal{S}$ を**時間付き強双模倣関係**と呼び、最大の関係を $\sim_T$ と書く。

$(P, Q) \in \mathcal{S}$ の時、

$$\text{OUT}: \frac{}{\overline{x}\langle\widetilde{y}\rangle.P \xrightarrow{\overline{x}\langle\widetilde{y}\rangle} P} \qquad \text{INPUT}: \frac{}{x(\widetilde{y}).P \xrightarrow{x(\widetilde{z})} P\{\widetilde{z}/\widetilde{y}\}} \qquad \text{TAU}: \frac{}{\tau.P \xrightarrow{\tau} P}$$

$$\text{SUM-L}: \frac{P \xrightarrow{\alpha} P'}{P+Q \xrightarrow{\alpha} P'} \qquad \text{SUM-R}: \frac{Q \xrightarrow{\alpha} Q'}{P+Q \xrightarrow{\alpha} Q'}$$

$$\text{PAR-L}: \frac{P \xrightarrow{\alpha} P'}{P \mid Q \xrightarrow{\alpha} P' \mid Q} \ \mathsf{bn}(\alpha) \cap \mathsf{fn}(Q) = \emptyset$$

$$\text{PAR-R}: \frac{Q \xrightarrow{\alpha} Q'}{P \mid Q \xrightarrow{\alpha} P \mid Q'} \ \mathsf{bn}(\alpha) \cap \mathsf{fn}(P) = \emptyset$$

$$\text{COMM-L}: \frac{P \xrightarrow{\overline{x}\langle\widetilde{y}\rangle} P' \quad Q \xrightarrow{x(\widetilde{y})} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'} \qquad \text{COMM-R}: \frac{P \xrightarrow{x(\widetilde{y})} P' \quad Q \xrightarrow{\overline{x}\langle\widetilde{y}\rangle} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'}$$

$$\text{RES}: \frac{P \xrightarrow{\alpha} P'}{\boldsymbol{\nu} x\, P \xrightarrow{\alpha} \boldsymbol{\nu} x\, P'} \text{ if } \alpha \notin \{x, \overline{x}\}$$

$$\text{REP-ACT}: \frac{P \xrightarrow{\alpha} P'}{!P \xrightarrow{\alpha} P' \mid !P} \qquad \text{REP-COMM}: \frac{P \xrightarrow{\overline{x}\langle\widetilde{y}\rangle} P' \quad P \xrightarrow{x(\widetilde{y})} P''}{!P \xrightarrow{\tau} (P' \mid P'') \mid !P}$$

$$\text{TIMEOUT}: \frac{P \xrightarrow{\alpha} P'}{t[0].P \xrightarrow{\alpha} P'} \qquad \text{ABORT}: \frac{}{P \xrightarrow{abort}} \text{ if } \ P\!\uparrow$$

図 1: 遷移規則

- $P\!\uparrow \ \Rightarrow \ Q\!\uparrow$
- $P \xrightarrow{\alpha} P' \ \Rightarrow \ \exists Q' \,.\, Q \xrightarrow{\alpha} Q' \,.\, (P', Q') \in \mathcal{S}$
- $P \rightsquigarrow^n P \ \Rightarrow \ \exists Q'' \,.\, Q \rightsquigarrow^n Q'' \,.\, (P'', Q'') \in \mathcal{S}$

ただし $n \geq 1$ とする。 □

定理 1 $\sim_{\mathcal{I}}$ は等価関係である。 □

証明： 反射性と対称性については容易に証明できる。ここでは推移性について示す。$\sim_{\mathcal{I}}\sim_{\mathcal{I}} \subseteq \sim_{\mathcal{I}}$ であることを示せばよい。

$(P, R) \in \sim_{\mathcal{I}}\sim_{\mathcal{I}}$ とすると、$(P, Q) \in \sim_{\mathcal{I}}$ かつ $(Q, R) \in \sim_{\mathcal{I}}$ となる Q が存在する。この時 $P \rightsquigarrow^n P''$ とすると、$(P, Q) \in \sim_{\mathcal{I}}$ より $Q \rightsquigarrow^n Q''$ かつ $(P'', Q'') \in \sim_{\mathcal{I}}$ を満たす Q'' が存在し、さらに $(Q, R) \in \sim_{\mathcal{I}}$ ゆえ Q'' に対し $R \rightsquigarrow^n R''$ かつ $(Q'', R'') \in \sim_{\mathcal{I}}$ となる R'' が存在する。よって $P'' \sim_{\mathcal{I}} Q'' \sim_{\mathcal{I}} R''$ であるので $\sim_{\mathcal{I}}\sim_{\mathcal{I}} \subseteq \sim_{\mathcal{I}}$。 □

定義 5 以下を満たす対称な関係 $\mathcal{S}$ を**時間付き弱双模倣関係**と呼び、最大の関係を $\approx_{\mathcal{I}}$ と書く。

$(P, Q) \in \mathcal{S}$ の時、

- $P\!\uparrow \ \Rightarrow \ Q\!\uparrow$
- $P \xrightarrow{\alpha}_{\tau} P' \ \Rightarrow \ \exists Q' \,.\, Q \xrightarrow{\alpha}_{\tau} Q' \,.\, (P', Q') \in \mathcal{S}$
- $P(\rightsquigarrow_{\tau})^n P \ \Rightarrow \ \exists Q'' \,.\, Q(\rightsquigarrow_{\tau})^n Q'' \,.\, (P'', Q'') \in \mathcal{S}$

ただし $\xrightarrow{\alpha}_{\tau} = (\xrightarrow{\tau})^* \xrightarrow{\alpha} (\xrightarrow{\tau})^*$、$\rightsquigarrow_{\tau} = (\xrightarrow{\tau})^* \rightsquigarrow (\xrightarrow{\tau})^*$、$n \geq 1$ とする。 □

$$\text{PASS}_\text{T}: \frac{}{t[n].P \rightsquigarrow t[n-1].P} \text{ if } n > 0$$

$$\text{OUT}_\text{T}: \frac{}{\overline{x}\langle\widetilde{y}\rangle.P \rightsquigarrow \overline{x}\langle\widetilde{y}\rangle.P} \qquad \text{IN}_\text{T}: \frac{}{x(\widetilde{y}).P \rightsquigarrow x(\widetilde{y}).P}$$

$$\text{SUM}_\text{T}: \frac{P \rightsquigarrow P' \quad Q \rightsquigarrow Q'}{P+Q \rightsquigarrow P'+Q'} \qquad \text{PAR}_\text{T}: \frac{P \rightsquigarrow P' \quad Q \rightsquigarrow Q'}{P \mid Q \rightsquigarrow P' \mid Q'} \text{ if } P \mid Q \overset{\tau}{\not\rightarrow}$$

$$\text{RES}_\text{T}: \frac{P \rightsquigarrow P'}{\boldsymbol{\nu} x\, P \rightsquigarrow \boldsymbol{\nu} x\, P'} \qquad \text{REP}_\text{T}: \frac{P \rightsquigarrow P'}{!P \rightsquigarrow !P'} \text{ if } P \mid P \overset{\tau}{\not\rightarrow}$$

$$\text{STRUCT}_\text{T}: \frac{P \rightsquigarrow P'}{Q \rightsquigarrow Q'} \text{ if } P \equiv Q,\ P' \equiv Q' \qquad \text{TIMEOUT}_\text{T}: \frac{P \rightsquigarrow P'}{t[0].P \rightsquigarrow P'}$$

図 2: 時間経過規則

弱双模倣関係の例を以下に示す。

$$\begin{aligned} P &= t[10].\overline{m}.R \\ Q &= \overline{l'}\langle 10\rangle \mid l'(n).t[n].\bar{l} \mid l.\overline{m}.R \end{aligned}$$

とすると、それぞれのプロセスの遷移は以下のようになり、$\rightsquigarrow^{10}$ と $\xrightarrow{\overline{m}}$ に着目すると $P \approx_\mathcal{T} Q$ であることがわかる。

$$\begin{aligned} P &\rightsquigarrow^{10} t[0].\overline{m}.R \\ &\xrightarrow{\overline{m}} R \end{aligned} \qquad \begin{aligned} Q &\xrightarrow{\tau} t[10].\bar{l} \mid l.\overline{m}.R \\ &\rightsquigarrow^{10} t[0].\bar{l} \mid l.\overline{m}.R \\ &\xrightarrow{\tau} \overline{m}.R \\ &\xrightarrow{\overline{m}} R \end{aligned}$$

4 おわりに

本稿では実時間システム開発への適用を目的として π 計算を時間に関して拡張し、さらにその上での双模倣関係を定義した。今後の課題として、双模倣関係の合同性の証明や、実際のシステム開発に適用する具体的な手法の検討などがある。

参考文献

[1] Hassan Gomma. *Designing Concurrent, Distributed, and Real-Time Applications with UML*. Addison Wesley, 2000.

[2] Robin Milner, Joachim Parrow, and David Walker. A calculus of mobile processes, part I/II. *Information and Computation*, 100:1–77, 1992.

[3] Robin Milner. *Communicating and Mobile Systems: the π-Calculus*. Cambridge University Press, 1999.

[4] Davide Sangiorgi and David Walker. *The π-calculus: A Theory of Mobile Processes*. Cambridge University Press, 2001.