

# A $\pi$ 計算の Coq による形式化

安武 祥平 渡部 卓雄

アクターモデルは並行計算のモデルのひとつであり、互いに非同期メッセージをやりとりするアクターと呼ばれる計算主体によって計算システムを表現する。アクターモデルのもつ性質には、アクターの名前の一意性と新鮮性、およびアクターの永続性が含まれる。これらの性質を  $\pi$  計算の型システムとして導入し、アクターモデルを形式化した A $\pi$  計算が Agha らによって提案されている。A $\pi$  計算の型システムにおける健全性とは、型付けされた項はアクターモデルとしてのふるまいを示すということであるが、その証明は形式的に与えられていない。本研究では、A $\pi$  計算およびその型システムの定義をみなおすことで、型システムの健全性について定理証明支援系 Coq を用いた形式的な証明を与える。

The Actor model is a model of concurrent computation based on autonomous computing entities called actors that communicate through asynchronous message passing. The properties of the Actor model include uniqueness and freshness of actor names and persistency of actors. Agha et al. proposed a typed asynchronous variant of  $\pi$ -calculus called A $\pi$ -calculus whose type system imposes these three properties. In A $\pi$ -calculus, the soundness of the type system means that a typed term certainly behaves as an actor configuration. In this paper, by reconsidering the definitions of the terms and types of A $\pi$ -calculus, we give a formal proof of the soundness using Coq.

## 1 はじめに

アクターモデル [1] は並行計算のモデルのひとつであり、互いに非同期メッセージをやりとりするアクターと呼ばれる計算主体 (computing entity) によって計算システムを表現する。他の並行計算モデル、例えば  $\pi$  計算などと比較すると、アクターモデルは実装しやすく、またプログラミングも比較的容易であると考えられる。実際、アクターモデルやその発展形である並行オブジェクト計算モデル [12] にもとづく言語は多数提案・実装されてきており、それらの研究成果をもとに現在 Scala や Erlang, Akka 等、アクターモデルを並行計算の基盤としたプログラミング言語やライブラリが実用に供されている。そのため、アクターモデルによって構成されたシステムの形式的検証

は喫緊の課題であると考えられる。

形式的検証の研究に先立ち、アクターモデルの形式的意味論については古くから研究が行われてきた。例えば Clinger による Powerdomain を用いた表示の意味 [5] や、Agha による操作的意味 [1] とその発展 [2] がある。これらの研究では、公平性やいくつかの等価性についての成果があるものの、プロセス代数を元に発展してきた  $\pi$  計算等に比べると発展途上であると言わざるを得ない。

一方、形式的検証についてはアクターで記述されたシステムのモデル検査を可能にするモデル記述言語 Rebeca [11]、証明支援系を含むプログラミング言語 Athena を用いた検証例 [10]、および Coq を用いたアクターモデルの定式化と検証例 [7] など、最近になっていくつかの研究成果が出ている。本研究はアクターで構成されたシステムの Coq による形式的検証のための枠組みを提供することを目的としている。

アクターモデルのもつ性質には、アクターの名前は一意であるという性質 (名前の一意性)、メッセージ

A formalization of A $\pi$ -calculus using Coq  
Shohei Yasutake, 東京工業大学大学院情報理工学研究  
科, Dept. of Computer Science, Tokyo Institute of  
Technology.

として送られてきた名前でアクターを作ることはできないという性質 (名前の新鮮性), アクターにはいつでもメッセージを送ることができるという性質 (アクターの永続性) が含まれる。これらの性質をみたす項を構成するよう  $\pi$  計算に型システムを導入し, アクターモデルを形式化した  $A\pi$  計算が Agha らによって提案されている [3]。

$A\pi$  計算の型システムにおける健全性とは, 型付けされた項はアクターモデルとしての振る舞いを示すということであるが, その証明は形式的に与えられていない。本研究では,  $A\pi$  計算およびその型システムの定義を見直すことで, 型システムの健全性について定理証明支援系 Coq を用いた形式的な証明を与える。

## 2 背景知識

### 2.1 アクターモデル

アクターモデルは非同期メッセージ通信に基づいた並行計算のモデルである。アクターと呼ばれる計算主体があり, それらは名前 (またはアドレス) と内部状態をもっている。各アクターは並列に動作し, 非同期にメッセージを送り合うことでコミュニケーションをとる。

アクターは, メッセージの内容に応じて一定の動作を行う。これを振る舞い (behavior) という。振る舞いには以下の様なものがある。

- 他のアクターにメッセージを送信する。
- 新しいアクターを作る。
- 自らの振る舞いを変える。

#### 2.1.1 配置

アクターモデルにおける配置 (configuration) とは, アクターモデルの世界におけるその時点での状態を切り取ったものを表すための概念である。配置はアクターとその振る舞い, まだ受け取られていないメッセージの集合から表される。

配置外からのメッセージを受け取ることでできる配置内のアクターを, 窓口 (receptionist) という。アクターは, 送り先の名前 (アドレス) を知ることで, その名前のアクターにメッセージを送れるようになる。よって窓口は外部のアクターに自身の名前を知られているアクターと言い換えることができる。また, 窓口

の集合のことを窓口集合 (receptionist set) という。

#### 2.1.2 アクターモデルの性質

アクターモデルが満たすべき性質として, 以下がある。

一意性 (uniqueness property)

アクターの名前は一意である。

新鮮性 (freshness property)

アクターが作られるとき, 作られるアクターの名前はまだどのアクターの名前でもない。アクターは, メッセージとして送られてきた名前でアクターを作ることはできない。

永続性 (persistence property)

アクターは消えない。一旦アクターが作られると, いつでもそのアクターにメッセージを送ることができる。

### 2.2 $\pi$ 計算

$\pi$  計算は, Milner らによって提唱された並行計算のモデルである [9]。プロセスと呼ばれるオブジェクト同士が通信しデータを受け渡していくことで計算を進める。また, アクターモデルとは異なり, メッセージを送受信する際にはプロセス間で同期をとる必要がある。

$\pi$  計算の抽象構文は 図 1 のようになっている。ここで,  $P, P_1, P_2, \dots$  はプロセスの式,  $x, y, \dots$  は名前である。

$P ::= 0$	何もしない
$  x(y).P$	$x$ から値を受け取り $P$ 中の $y$ に束縛する
$  \bar{x}(y).P$	$x \rightarrow y$ を送る
$  P_1   P_2$	$P_1, P_2$ を並列に実行させる
$  (\nu x)P$	$P$ 中に現れる $x$ を束縛する
$  !P$	$P$ を繰り返す

図 1:  $\pi$  計算の文法

### 2.3 定理証明支援系 Coq

Coq はフランス国立情報学自動制御研究所で開発されている定理証明支援系である [6]。Coq を用いる

表 1: カリー・ハワード同型対応

論理	コンピュータプログラム
命題 $P$	型 $P$
命題 $P$ の証明	型 $P$ を持つ項
命題 $P \Rightarrow Q$	型 $P \rightarrow Q$ ( $P$ から $Q$ への関数)
命題 $P \wedge Q$	$P, Q$ の直和型
命題 $P \vee Q$	$P, Q$ の直積型

ことで、プログラムがある仕様を満たすということや、数学的な定理などに対して形式的かつ厳密な証明を与えることができる。Coq によって証明されたものとしては、四色定理が有名である [8]。

### 2.3.1 カリー・ハワード同型対応

Coq における定理証明は、カリー・ハワード同型対応という理論に基づいている。カリー・ハワード同型とは、論理における命題と証明という構造と、コンピュータプログラムにおける型と項という構造が直接的に対応しているという理論である。これにより、ある命題を証明することが、命題に対応する型と、その型を持つ項を作ることに帰着される。

カリー・ハワード同型対応では、表 1 に示すような対応関係がある。

## 3 $A\pi$ 計算

本節では、アクターモデルの振る舞いを強制するために非同期  $\pi$  計算に型を付けた  $A\pi$  計算について説明する。まず  $A\pi$  計算における配置の定義をする。次に型システムを導入するが、その際に仮名関数という関数を導入し、型付け規則を定義する。最後にこの型システムにおける健全性について述べる。また、 $A\pi$  計算の定義および使われている記号は、文献 [3] で用いられているものを用いる。

### 3.1 配置

$A\pi$  計算における配置の文法は、図 2 のようになっている。

通常の  $\pi$  計算と異なる点は、他のアクター（プロセス）にメッセージを送ったあとにさらに何かを実行できないこと、名前の場合分けが書けること、振る舞

$$\begin{aligned}
 P ::= & 0 \mid x(y).P \mid \bar{x}y \mid (\nu x)P \mid P_1 \mid P_2 \\
 & \mid \text{case } x \text{ of } (y_1 : P_1, \dots, y_n : P_n) \\
 & \mid ((\tilde{u}, \tilde{v})u_1(z).P)(\tilde{x}, \tilde{y})
 \end{aligned}$$

図 2:  $A\pi$  計算の配置の文法

いの雛形からアクターを作るための文法があること、の 3 つである。

### 3.2 型システムの導入

$A\pi$  計算の文法のみでは、アクターモデルの性質は満たさないような配置も書けてしまう。例えば、 $x(u).P \mid x(v).Q$  は  $A\pi$  計算の文法で書けるが、 $x$  という名前のアクターが 2 つ作られるので、一意性を満たしていない。また、 $x(u).(u(v).P \mid x(v).Q)$  も  $A\pi$  計算の文法で書けるが、メッセージとして送られてきた名前でアクターが作られているので、新鮮性に反する。

また、アクターモデルでは、1 回の通信で複数の名前を送信することができるが、 $A\pi$  計算では 1 回の通信で一つの名前しか送ることはできない。複数の名前を送信するには、その数だけ連続して通信する必要がある。しかし、アクターモデルではこのような複数の名前を含むメッセージの受け渡しはアトミックに行なわれ、即座に次のメッセージを受け取れる状態にならなければならない。そこで、いつでもメッセージを送信できるという永続性を弱め、アクターはメッセージの送信先のアクターの処理が終わるまで待てるようにする（いつかは必ず送れる）。そしてアトミックに行うことのできない処理の最中はメッセージを送れないということを、正規の名前を隠して一時的な名前を使って処理を行うことで実現させる。ここで、仮の名前をとった後、元の名前とは異なる名前になってしまうと、そのアクターにメッセージを送ろうとしているアクターはメッセージを送れなくなってしまい、永続性に反する。仮の名前をとったときには必ず元の名前に戻るという制約が必要である。

以上のような性質を満たすようにするため、型システムを導入し、 $A\pi$  計算に制約を与える。

### 3.2.1 仮名関数

仮の名前は必ず正規の名前に戻するという制約を型システムを用いて与えるためには、仮の名前をとったときに正規の名前を覚えておく必要がある。そこで仮の名前から元の正規の名前にマッピングする関数を導入する。これを 仮名関数 (temporary name mapping function) と呼ぶ。

**定義 3.1** (仮名関数). 仮名関数  $f$  は、集合  $X$  から集合  $X^*$  への写像である。ただし、 $\mathcal{N}$  を名前全体の集合として、 $\perp, * \notin \mathcal{N}, X \subset \mathcal{N}, X^* = X \cup \{\perp, *\}$  である。

仮名関数の入力と返り値の関係は、以下のような意味を持つ。

$f(x) = \perp$	$x$ が正規の名前のとき
$f(x) = *$	$x$ が環境から隠されている名前であるとき
$f(x) = y \notin \{\perp, *\}$	アクター $y$ の仮の名前が $x$ であるとき

### 3.2.2 仮名関数の構築

仮名関数は以下に示す  $ch$  関数、仮名関数の合成、仮名関数の制限のいずれかで作ることができる。

**定義 3.2** ( $ch$ ).  $ch$  は名前の組をとり、仮名関数を返す関数である。組の長さは任意である。組を  $\langle x_1, x_2, \dots, x_n \rangle$  としたとき、 $ch(\langle x_1, x_2, \dots, x_n \rangle)$  は以下のような仮名関数となる。

$$ch(\langle x_1, x_2, \dots, x_n \rangle)(x_i) = \begin{cases} x_{i+1} & 1 \leq i < n \text{ のとき} \\ \perp & i = n \text{ のとき} \end{cases}$$

**定義 3.3** (仮名関数の合成).  $f_1 : \rho_1 \rightarrow \rho_1^*, f_2 : \rho_2 \rightarrow \rho_2^*$  とする。仮名関数の合成を表す二項演算子  $f_1 \oplus f_2 : \rho_1 \cup \rho_2 \rightarrow (\rho_1 \cup \rho_2)^*$  を以下のように定義する。

$$(f_1 \oplus f_2)(x) = \begin{cases} f_1(x) & x \in \rho_1 \text{ かつ } f_1(x) \neq \perp, \text{ また} \\ & \text{は } x \in \rho_1 \text{ かつ } x \notin \rho_2 \text{ のとき} \\ f_2(x) & \text{その他} \end{cases}$$

**定義 3.4** (仮名関数の定義域の制限).  $f : \rho_1 \rightarrow \rho_1^*, \rho \subset \rho_1$  である  $f, \rho$  に対して定義域の制限を表す二項演算子  $f|_\rho : \rho \rightarrow \rho^*$  を以下のように定義する。

$$(f|_\rho)(x) = \begin{cases} f(x) & f(x) \in \rho \text{ のとき} \\ * & \text{その他} \end{cases}$$

### 3.2.3 仮名関数が満たすべき性質

仮名関数  $f$  はその定義から、以下を満たすべきである。

- $f(x) \neq x$
- $f(x) = f(y) \notin \{\perp, *\} \Rightarrow x = y$
- $f^*(f(x)) = \perp$

$f(x) \neq x$  は、仮の名前から正規の名前を得たとき、それは仮の名前と同名ではないという性質である。 $f(x) = f(y) \notin \{\perp, *\} \Rightarrow x = y$  は、正規のアクターは 2 個以上の仮の名前をとれないという性質である。 $f^*(f(x)) = \perp$  は、仮の名前のアクターはさらに仮の名前を持つことはできないという性質である。

また、互換性という性質を定義する。

**定義 3.5** (互換性 (compatible)). 二つの仮名関数  $f_1, f_2$  が以下の性質を満たすとき、 $f_1, f_2$  は互換性を持つという。また、この性質を満たすという述語を  $compatible(f_1, f_2)$  と書く。

- $f_1 \oplus f_2 = f_2 \oplus f_1$
- $f_1 \oplus f_2$  が仮名関数の性質を満たす

### 3.3 型付け規則

$\Lambda\pi$  計算が先に述べた性質を満たすようにするための型付け規則は 図 3 のようになっている。配置  $P$ 、 $P$  の窓口集合  $\rho$ 、 $P$  中の仮の名前から正規の名前への写像  $f : \rho \rightarrow \rho^*$  で、 $\rho; f \vdash P$  が成り立つとき、 $P$  は正しく型付けされている。

$$\begin{array}{c}
\frac{}{\emptyset; \{\} \vdash 0} \quad (\text{NIL}) \\
\\
\frac{}{\emptyset; \{\} \vdash \bar{x}y} \quad (\text{MSG}) \\
\\
\frac{\rho; f \vdash P \quad \rho - \{x\} = \hat{z} \quad y \notin \rho \quad f = \begin{cases} ch(\langle x \rangle \dot{+} \langle \hat{z} \rangle) & x \in \rho \text{ のとき} \\ ch(\langle \hat{z} \rangle) & \text{その他} \end{cases}}{\{x\} \cup \hat{z}; ch(\langle x \rangle \dot{+} \langle \hat{z} \rangle) \vdash x(y).P} \quad (\text{ACT}) \\
\\
\frac{\forall 1 \leq i, j \leq n, i \neq j, \rho_i; f_i \vdash P_i \quad \text{compatible}(f_i, f_j)}{(\cup_i \rho_i); (f_i \oplus f_2 \oplus \dots \oplus f_n) \vdash \text{case } x \text{ of } (y_1 : P_1, \dots, y_n : P_n)} \quad (\text{CASE}) \\
\\
\frac{\rho_1; f_1 \vdash P_1 \quad \rho_2; f_2 \vdash P_2 \quad \rho_1 \cap \rho_2 = \phi}{\rho_1 \cup \rho_2; f_1 \oplus f_2 \vdash P_1 | P_2} \quad (\text{COMP}) \\
\\
\frac{\rho; f \vdash P}{\rho - \{x\}; f | (\rho - \{x\}) \vdash (\nu x)P} \quad (\text{RES}) \\
\\
\frac{\{\tilde{u}\}; ch(\tilde{u}) \vdash u_1(z).P \quad \text{len}(\tilde{x}) = 2 \Rightarrow x_1 \neq x_2}{\{\tilde{x}\}; ch(\tilde{x}) \vdash ((\tilde{u}, \tilde{v})u_1(z).P)(\tilde{x}, \tilde{y})} \quad (\text{INST})
\end{array}$$

図 3: 型付け規則

### 3.4 型システムの健全性

$A\pi$  計算の型システムにおける健全性は、この型システムを満たした  $A\pi$  計算の配置はアクターモデルとしての振る舞いを示すということを表した性質である。単純型付き 計算における型システムの健全性のような、正しく型付けされるならば stuck 状態にならないという性質とは少し異なることに注意されたい。

$A\pi$  計算の型システムの健全性は以下のように定義されている。

**定理 3.1** ( $A\pi$  計算の健全性). 配置  $P$  について、 $\rho; f \vdash P$  で型付けできたとき、以下の 3 つの性質を満たす。

- $\rho$  は  $P$  中に現れる自由名の部分集合である (窓口集合の健全性)
- 以下の 3 つを満たす (仮名の取り方の健全性)
  1.  $f(x) \neq x$
  2.  $f^*(f(x)) = \perp$

$$3. f(x) = f(y) \neq \{\perp, *\} \Rightarrow x = y$$

- $\rho'; f' \vdash P$  ならば、 $\rho = \rho'$  かつ  $f = f'$  (型付けの一意性)

それぞれは以下の意味を持っている。

**窓口集合の健全性**

窓口集合に属するアクターはメッセージとして送られてきた名前で作られたものではなく、かつ環境から隠されたものでもない。

**仮名の取り方の健全性**

アクターが仮の名前をとったとき、それは同名のものではなく、さらに仮の名前を持つこともない。また、アクターが複数の仮の名前を持つことはない。

**型付けの一意性**

配置に型が付いたとき、その型付けは一意である。

## 4 Coq による形式化

本節では、3 節で述べた  $A\pi$  計算についてどのように Coq で記述していくかについて説明する。まず仮名関数およびその性質についての Coq での表現を述べる。次に型付け規則を Coq で使いやすくなるための規則の具体化を説明し、最後に型システムの健全性の Coq での証明方針を述べる。

### 4.1 仮名関数

仮につけた名前から正規の名前を得る 仮名関数の Coq での定義について述べる。

仮名関数  $f$  の型は  $X \rightarrow X^*$  であり、定義域と値域の集合は  $\perp$  と  $*$  を除くと等しくなっている。Coq では簡単にするためにその情報を捨て、任意の name 型の値から任意の option star 型への関数とした。定義域の範囲に入っていない入力には None を返すことを想定している。

この変更により、以下の述語が必要となる。 $f : X \rightarrow X^*$  ということを示す  $in\_range\_in\_domain(f)$  を満たすことで表している。

**定義 4.1 ( $in\_domain$ ).** 名前  $x$  , 仮名関数  $f$  について、 $x \in domain(f)$  を  $in\_domain(f, x)$  で表す。ただし  $domain(f)$  は  $f$  の定義域である。

**定義 4.2 ( $in\_range$ ).** 名前  $x$  , 仮名関数  $f$  について、 $x \in range(f)$  を  $in\_range(f, x)$  で表す。ただし  $range(f)$  は  $f$  の値域である。

**定義 4.3 ( $in\_range\_in\_domain$ ).** ある 仮名関数  $f$  が、任意の名前  $x$  について  $in\_range(f, x) \Rightarrow in\_domain(f, x)$  を満たすということを  $in\_range\_in\_domain(f)$  で表す。

また、2 つの 仮名関数の定義域が重なっていないことを表す述語  $fun\_exclusive$  を定義する。

**定義 4.4 ( $fun\_exclusive$ ).** 2 つの 仮名関数  $f : X \rightarrow X^*, g : Y \rightarrow Y^*$  について、 $X \cap Y = \emptyset$  であるという述語を  $fun\_exclusive$  と定義する。

#### 4.1.1 仮名関数の構築

仮名関数は  $ch$  関数、仮名関数の合成、仮名関数の定義域の制限、のいずれかで作ることができる。ここで、 $ch$  関数が使われている型付け規則は ACT の

みであるが、この中で使われている  $ch$  関数は入力の要素数が 0 個、1 個、2 個のものしかない。よって、 $ch$  関数はこの 3 パターンに限定でき、それぞれ  $ch_0, ch_1, ch_2$  と書くこととする。また、仮名関数の定義域の制限を行う二項演算子 ( $|$ ) の右手は要素が 1 個の場合しかなく、要素を 1 個に限定して定義すると、証明が簡単になる。よって、仮名関数の定義域の制限は、以下の定義を用いる。

**定義 4.5 (仮名関数の定義域の制限).**  $f : \rho \rightarrow \rho^*, x \in \rho$  である  $f, x$  に対して定義域の制限を表す二項演算子  $f|x : \rho - x \rightarrow (\rho - x)^*$  を以下のように定義する。

$$(f|x)(y) = \begin{cases} * & f(y) = x \text{ のとき} \\ f(y) & \text{その他} \end{cases}$$

また、 $ch_0, ch_1, ch_2, \oplus, |$  について仮名関数の性質を満たすことを証明した。その際、 $ch_2$  は引数である 2 つの名前が異なることを、 $\oplus$  は  $in\_domain\_in\_range, fun\_exclusive$  が成り立つという前提を加えている。

### 4.2 型付け規則

$A\pi$  計算の型付け規則には、Coq 上で定義しにくい、またはそのままでは証明を進めにくいものがある。実際に Coq で型付け規則を定義する前に、型付け規則を再定義する。

#### 4.2.1 Act 規則の分割

型付け規則 ACT はアクターが作られる際に考えられるパターンを複数まとめたものであり、このままの定義を用いると証明を進めることが難しくなってしまう。そこで、具体化のため、図 4 のように  $\rho$  の要素数によって場合分けを行い 4 つに分割する。

ここで、 $ch$  関数の入力としてとりうる組は要素数が 0, 1, 2 のものしかないことに注意されたい。

#### 4.2.2 Case 規則の分割

型付け規則 CASE は、前提の数がパターンの数に依存して変動するので、Coq で定義しにくい。よって図 5 のように CASE をパターンが 0 個の場合と  $i + 1$  に分割し、帰納的に定義する。これで、CASE 規則の前提の数はパターンの数によらず一定となる。

$$\begin{array}{c}
\frac{\emptyset; ch_0 \vdash P}{\{x\}; ch_1(x) \vdash x(y).P} \quad (\text{ACT-EMPTY}) \\
\\
\frac{\{x\}; ch_1(x) \vdash P \quad x \neq y}{\{x\}; ch_1(x) \vdash x(y).P} \quad (\text{ACT-X}) \\
\\
\frac{\{z\}; ch_1(z) \vdash P \quad x \neq z \quad y \neq z}{\{x, z\}; ch_2(x, z) \vdash x(y).P} \quad (\text{ACT-Z}) \\
\\
\frac{\{x, z\}; ch_2(x, z) \vdash P \quad x \neq z \quad x \neq y \quad y \neq z}{\{x, z\}; ch_2(x, z) \vdash x(y).P} \quad (\text{ACT-XZ})
\end{array}$$

図 4: 型付け規則 ACT の分割

$$\begin{array}{c}
\frac{}{\emptyset; \{\} \vdash \text{case } x \text{ of } ()} \quad (\text{CASE-NIL}) \\
\\
\frac{\rho; f \vdash \text{case } x \text{ of } (y_1 : P_1, \dots, y_i : P_i) \quad \rho'; f' \vdash P \quad \text{compatible}(f, f')}{\rho \cup \rho'; f \oplus f' \vdash \text{case } x \text{ of } (y : P, y_1 : P_1, \dots, y_i : P_i)} \quad (\text{CASE-CONS})
\end{array}$$

図 5: 型付け規則 CASE の分割

また、この定義によって作られる型付け  
 $(\dots((\rho_1 \cup \rho_2) \cup \rho_3) \dots \cup \rho_n) \cup \rho; (\dots((f_1 \oplus f_2) \oplus f_3) \dots \oplus f_n) \oplus f \vdash \text{case } x \text{ of } (y : P, y_1 : P_1, \dots, y_n : P_n)$

において、元の定義では  $f, f_1, f_2, \dots, f_n$  が相互に互換性を持つことを条件としているが、 $f, f_1, \dots, f_n$  が相互に互換性を持つことは自明ではない。よって以下の補題が必要となる。

**補題 4.1.** 仮名関数  $f, f_1, f_2$  について、 $f$  と  $f_1 \oplus f_2$  が互換性を持ち、 $f_1$  と  $f_2$  もまた互換性を持つとき、 $f, f_1, f_2$  は相互に互換性を持つ。

この補題によって、 $f, f_1, \dots, f_n$  が相互に互換性を持つことが帰納的に保証される。

#### 4.2.3 Res 規則

仮名関数の定義域の制限を行う二項演算子の定義を変更したことに合わせて、型付け規則 RES は図 6 のようになる。

#### 4.2.4 Inst 規則の分割

Coq による定義では振る舞いの雛形からアクターを作る配置を二つに分割している。よって型付け規則

も二つに分割する必要がある。図 7 のようになる。

#### 4.3 健全性の証明

健全性の証明は関数の同値性についての議論が必要となるので、関数の外延的同値という公理を用いる。これは以下のような公理であり、Coq の標準ライブラリで提供されているものを使用した。

**公理 4.1** (関数の外延的同値)。関数  $f, g$  が任意の入力に対して等しい結果を返すならば  $f, g$  は等しい。

また、以下の 3 つの補題を証明しておく、健全性の証明を行いやすい。

**補題 4.2** (定義域と値域の一致)。  $\rho; f \vdash P$  ならば、 $\text{in\_range\_in\_domain}(f)$  が成り立つ。

**補題 4.3** (仮名関数の定義域と窓口集合の一致)。  $\rho; f \vdash P$  ならば、任意の名前  $x$  について  $\text{in\_domain}(f, x)$  であるとき、かつそのときに限り、 $x \in \rho$  が成り立つ。

**補題 4.4** ( $\text{fun\_exclusive}$  における集合の一致)。  $\rho_1; f_1 \vdash P_1$  かつ  $\rho_2; f_2 \vdash P_2$  であり  $\rho_1 \cap \rho_2 \neq \emptyset$  ならば、 $\text{fun\_exclusive}(f_1, f_2)$  を満たす。

$$\frac{\rho; f \vdash P}{\rho - \{x\}; f|x \vdash (\nu x)P} \quad (\text{RES})$$

図 6: 型付け規則 RES

$$\frac{\{u\}; ch_1(u) \vdash u(z).P}{\{x\}; ch_1(x) \vdash ((\langle u \rangle, \tilde{v})u(z).P)(\langle x \rangle, \tilde{y})} \quad (\text{INST-1})$$

$$\frac{\{u_1, u_2\}; ch_2(u_1, u_2) \vdash u_1(z).P \quad x_1 \neq x_2}{\{x_1, x_2\}; ch_2(x_1, x_2) \vdash ((\langle u_1, u_2 \rangle, \tilde{y})u_1(z).P)(\langle x_1, x_2 \rangle, \tilde{y})} \quad (\text{INST-2})$$

図 7: 型付け規則 INST の分割

健全性は，以上の公理と補題を利用して，型付け規則の構造に関する帰納法で証明できる．Coq による定義と証明の全文は GitHub リポジトリ [4] に公開している．

## 5 まとめ

$A\pi$  計算における型システムの定義を Coq で証明を行いやすいように再定義し， $A\pi$  計算の型付けの健全性を形式的に証明した．これによって  $A\pi$  計算の型システムが確かにアクターとしての振る舞いを強制することを示した．

今後の課題としては， $A\pi$  計算における型保存性の証明が上げられる． $A\pi$  計算の操作的意味論は  $\pi$  計算と同様にラベル付き遷移 (labeled transition system) を用いており， $A\pi$  計算における型保存性は  $A\pi$  計算の正しく型がついた配置は遷移を行っても正しく型がつく，というものである．この操作的意味論の Coq での形式化および型保存性の証明が課題として残っている．

謝辞 本研究の一部は JSPS 科研費 24500033 の助成を受けている．

## 参考文献

- [1] Agha, G.: *Actors: A Model of Concurrent Computation in Distributed Systems*, MIT Press, 1986.
- [2] Agha, G., Mason, I. A., Smith, S. F., and Talcott, C.: A foundation for actor computation, *Journal of Functional Programming*, Vol. 7, No. 1(1997),

- pp. 1–72.
- [3] Agha, G. and Thati, P.: An Algebraic Theory of Actors and Its Application to a Simple Object-Based Language, *From Object-Oriented to Formal Methods*, Lecture Notes in Computer Science, Vol. 2635, Springer-Verlag, 2004, pp. 26–57.
- [4] A formalization of  $A\pi$ -calculus, <https://github.com/amutake/a-pi>.
- [5] Clinger, W. D.: Foundations of Actor Semantics, Technical Report AITR-633, AI Lab., MIT, 1981.
- [6] The Coq Proof Assistant, <http://coq.inria.fr/>.
- [7] Garnock-Jones, T., Tobin-Hochstadt, S., and Felleisen, M.: The Network as a Language Construct, *Programming Languages and Systems (ESOP 2014)*, Lecture Notes in Computer Science, Vol. 8410, Springer-Verlag, 2014, pp. 473–492.
- [8] Gonthier, G.: A computer-checked proof of the Four-Colour Theorem, 2004.
- [9] Milner, R.: *Communicating and Mobile Systems: The  $\pi$ -calculus*, Cambridge University Press, New York, NY, USA, 1999.
- [10] Musser, D. R. and Varela, C. A.: Structured Reasoning About Actor Systems, *Workshop on Programming based on Actors, Agents, and Decentralized Control (AGERE!@SPLASH 2013)*, ACM, oct 2013, pp. 37–48.
- [11] Sirjani, M. and Jaghoori, M. M.: Ten Years of Analyzing Actors: Rebeca Experience, *Formal Modeling: Actors, Open Systems, Biological Systems*, Agha, G., Danvy, O., and Meseguer, J.(eds.), Lecture Notes in Computer Science, Vol. 7000, Springer-Verlag, 2011, pp. 20–56.
- [12] Yonezawa, A., Briot, J.-P., and Shibayama, E.: Object-Oriented Concurrent Programming in ABCL/1, *OOPSLA '86 Conference Proceedings on Object-Oriented Programming Systems, Languages and Applications*, 1986, pp. 258–268.