非同期系の代数的仕様とその実現

4J－6

侯 豫榕　杉山 裕二
岡山大学工学部

1　まえがき

並行プロセス系などの非同期系はその設計が難しく，動作の正当性を保証することが困難である．ここでは，正しく動作する非同期系を導くための形式的設計法の一環として，非同期系の代数的仕様とその実現の定式化を行い，実現関係が成り立つための十分条件を示す．

2　代数的仕様とその実現

非同期系は，複数のプロセスが，メッセージ交換などを介して所期の目的を達成するシステムと考えられる．この点は回路と類似性があり，非同期系の代数的仕様を回路と同様の形式[1,2]で記述することにする．すなわち，非同期系の代数的仕様は，各プロセスの記述とプロセス間の送受信関係の記述に分かれ，プロセスの記述では，状態遷移を表す遷移関数，並びに出力，メッセージおよび内部状態に関する情報（内部成分）を表す成分関数を導入して，これらの関数の関係を公理で定義する．また，状態 s が初期状態から到達可能であるか否かを表す関数（$valid$ で表す）を導入し，その意味を公理で定義することにより状態遷移の生起条件を記述する．送受信関係の記述では，各プロセスの状態からなる全体状態$< s_1,\cdots,s_N >$（s_iはプロセスの状態，Nはプロセスの個数）を導入し，この全体状態が全体状態の初期状態から到達可能か否かを表す関数$VALID$の定義の中でプロセス間の送受信関係を記述する．

一般の非同期系では，送受信関係が固定されず，メッセージ等が常時伝送されることもない．これらが回路と異る点であり，その差は$VALID$関数の公理の形の違いとして現れる．また，非同期系の詳細化では，上位レベルの一回のメッセージ交換が，下位レベルで複数のメッセージ交換により実現されるということが多いと思われる．そこでこの点に着目した実現関係を定式化する．まず，実現関係の定義に必要な諸概念を定義する．

［定義 2.1］ 状態 s における入力を $I(s)$ で表し，初期状態から s に至る入力の系列を入力履歴と呼び，$HI(s)$ で表す．また，状態 s における出力および内部成分をそれぞれ，$O(s)$ および $C(s)$ で表し，出力履歴 $HO(s)$ および内部成分履歴 $HC(s)$ を同様に定義する．以上の記号の定義域を（プロセス毎の値の並びとして）全体状態にも拡張する．

［定義 2.2］ A および Bを二つの非同期系の仕様とし，$X =< x_1,\cdots,x_l >$および$Y =< y_1,\cdots,y_m >$ を，それぞれ，A および Bの入力とする．各 x_iが Bの入力の系列 $eI_i(Y)$ で表されるとき，$EI(Y) =< eI_1(Y),\cdots,eI_l(Y) >$を入力の対応と呼ぶ．出力の対応 EOについても同様に定義する．また，A の内部成分 c_iが $eC_i(D)$（Dは Bの内部成分の並び）で表されるとき，$EC(D) =< eC_1(D),\cdots,eC_h(D) >$ を，内部成分の対応と呼ぶ．EI，EO，ECの定義域を，それぞれの履歴に拡張する．

［定義 2.3］ 二つの仕様 A と B，入力の対応 EI および出力の対応 EOに対して，下記条件 **(1)** および **(2)** が成り立つとき，かつそのときのみ，B は，$< EI, EO >$のもとで A の実現であるという．

(1) A のすべての$VALID$全体状態 S_Aに対し，B の$VALID$全体状態 S_Bが存在し，

$$HI(S_A) \equiv EI(HI(S_B))$$
$$HO(S_A) \equiv EO(HO(S_B))$$

(2) Bのすべての$VALID$全体状態 S_Bに対し，A の$VALID$全体状態 S_Aと，S_Bから到達可能な Bの$VALID$全体状態 S'_B が存在し，

$$HI(S_A) \equiv EI(HI(S'_B))$$
$$HO(S_A) \equiv EO(HO(S'_B))$$

上記条件の **(1)** は，仕様 A の動作を模倣する仕様 Bの動作が存在しなければならないことを表し，また条件 **(2)** では，仕様 Bの動作は仕様 A の動作を模倣するためのものに限られるということを表している．

Algebraic Specification of Asynchronous System and Its Implementation
Yurong Hou and Yuji Sugiyama
Faculty of Engineering, Okayama University, Okayama-shi, 700, Japan

3 実現のための十分条件

ここでは，上下のプロセス間に遷移の対応があり，その遷移の対応の下でプロセス毎の実現関係がある場合に，非同期系全体として実現関係が成立するための十分条件を示す．まず，(実現関係を全包する）遷移の対応について述べる．C_AおよびC_Bを，それぞれ，Aの状態s_aおよびBの状態s_bにおける全内部成分の並びとする．$C_A = EC(C_B)$が成り立つとき，$s_a \widetilde{EC} s_b$と書く．

［定義 3.1］ 二つの仕様 A と B，入力の対応 EI，出力の対応 EOおよび内部成分の対応 ECが与えられているものとする．a および b をそれぞれ，A および B のプロセスとする．a の任意の状態遷移 $t(x)$（x は入力）に対して，b の状態遷移列 $u_1(x_1)\cdots u_k(x_k)(\phi(t(x))$ で表す）が存在して以下が成り立つとき，$< EI, EO, EC >$のもとで a から b への遷移の対応があるという．

(1) $init_a$，$init_b$を，それぞれ，a および b の初期状態とすると，
$\phi(init_a) = init_b$ かつ $init_a \widetilde{EC} init_b$

(2) $x \equiv EI(x_1 \cdots x_k)$

(3) $O(t(x)) \equiv EO(O(u_1(x_1))\cdots O(u_k(x_k)))$

(4) $s_a \widetilde{EC} s_b$ ならば，
$valid(t(x)\cdot s_a) \equiv valid(u_1(x_1)\cdot s_b)$

(5) $u(y)\cdot s_b$の形（u は b の遷移）の任意の $valid$ 状態に対して，a の状態 s'_aと遷移 $t(x)$，並びに b の状態 $s'_b = \phi(s'_a)$ と遷移列 w'，w''が存在して，
$w''\cdot u(y)\cdot w'\cdot s'_b = \phi(t(x)\cdot s'_a)$，かつ
$valid(w''\cdot u(y)\cdot w'\cdot s'_b) \equiv 1$

次に，実現関係が成り立つための十分条件について述べる．

[定理]（十分条件）

次の (1) と (2) が成り立つとき，Bは$< EXP_I, EXP_O, EXP_C >$のもとで A の実現である．

(1) Aのプロセス集合から Bのプロセス集合への単射θ が存在し，A の各プロセス a から$\theta(a)$へは$< EXP_I, EXP_O, EXP_C >$のもとで遷移の対応がある．遷移の対応をϕで表す．

(2) Aにおいて，プロセス aの出力 oとプロセス a'の入力 xが接続されている（即ち，$x = o(s_a)$が $VALID$関数の定義に含まれる）とする．$\theta(a)$ の出力および$\theta(a')$ の入力の系列を，それぞれ，GおよびYとし，また，$eI_x(Y)$の中に現れる各入力系列（Yの要素）を，それと接続されている$\theta(a)$ の出力系列（G の要素）で置き換え得られるを$eI_x(G)$と書く．このとき，$eI_x(G)$は$eO_o(G)$と同じ表現式となる．

(3) $VALID(< t_1(x_1)\cdot s_{a1}, \cdots, t_n(x_n)\cdot s_{an} >) \equiv 1$ を満たす（A の各プロセスの）任意の遷移 $t_1(x_1), \cdots, t_n(x_n)$ および任意の全体状態$< s_{a1}, \cdots, s_{an} >$ に対して，$s_{ai} \widetilde{EC} s_{bi} (1 \le i \le n)$ ならば，
$VALID(< \phi(t_1(x_1))\cdot s_{b1}, \cdots, \phi(t_n(x_n))\cdot s_{bn} >) \equiv 1$

定理のもとで実現の (1) が成り立つことの証明は，A の $VALID$な全体状態 S_Aに到達するまでの遷移回数に関する帰納法を，(2) が成り立つことの証明は，Bの $VALID$な全体状態 S_Bに到達までの遷移回数に関する帰納法を用いて行なうことができる．

4 あとがき

以上，非同期系プロセス化された代数的仕様の実現関係と実現関係が成り立つするための一つの十分条件について述た．

参考文献

(1) 杉山，北道，谷口：“代数的手法を用いた順序回路の記述とその詳細化について”，信学技報，COMP 88-7 (1988-5).

(2) Y.R. Hou, A. Ohnishi, Y. Sugiyama and T. Okamoto: “An Algebraic Specification of a Dasiy Chain Arbiter”, the 1991 Pacific Rim Int. Symp. on Fault Tolerant Systems, pp.24-29 (1991).