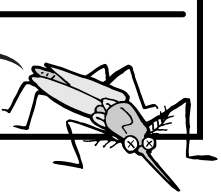
虫のつかない

連 載（最終回）

フォーマルな開発手法

第６回　組み込み応用のための実時間系と混合系

山崎利治



今回は，家庭などで用いられている加湿温風器の仕様を例に，実時間系と混合系について解説する．前回述べたオートマトンを基礎にして，UML（Unified Modeling Language）などでも用いられているステートチャートに時間変数を加えて，実際に仕様を書いてみる．（編集部）

今回は，実時間系（real-time system）と混合系（hybrid system）を取り上げます．これまでは，札付き推移系を応答系の抽象したものと考えてきました．今回も推移系を基礎として，その上で議論を進めます．

今まで，事象は瞬時に生起するものとし，経過時間が必要であるとは考えませんでした．事象に時間がかかったり，状態にある時間とどまったりする状況を無視できない系があります．このような応答系を実時間系といいます．

また，状態推移が離散的に生起したり，連続的に生起したりする系もあります．このような系を混合系といいます．実時間系や混合系としての仕様記述と検証は組み込み系（embedded system）では特に重要になります．

●加湿温風器を例に考える

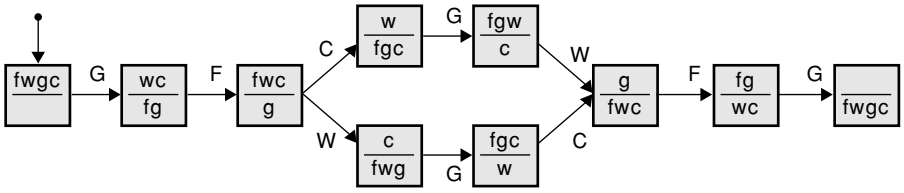
具体例として，身近にある家電器具を考えてみましょう．水を含んだフィルタに温風を通すことによって加湿暖房できる加湿温風器です．この器具の仕様を書くときには，時間を明示的に扱ったほうがいいようです．

例えば，水を含んだフィルタは汚れるので，２週間ごとに掃除することにします．そのために，なんらかの時計を用意して，掃除する時期を知らせて作動を停止します（ここでは，汚れを見つける感知器は付いていないものとする）．掃除して再作動させるときには，作動再開ボタンを３秒押し続ける必要があります．また，「お休みタイマ」という１時間後，２時間後に作動を停止させるボタンもあります．

この器具の具体的な仕様を書こうというわけですが，それは後にして，まず推移系に時間要素を導入することを考えましょう．これを時間推移系（timed transition system）といいます．

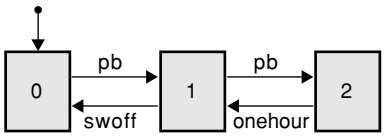
●時間推移系とは

時間推移系は時間を無視しない推移系です．そこで，時間を表す時間変数を導入します．推移系の状態は，時々刻々と連続的に変化しています．一方，本来，興味のあった事象は離散的に生起します．事象の生起に伴う状態の変化を時間変数の変化と区別し，それをオートマトンで示し



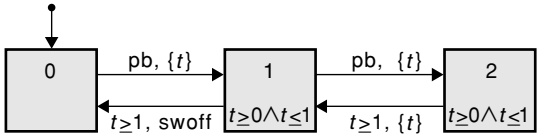
〔図1〕川渡りオートマトン

おおかみw，やぎgを連れて，キャベツcを持った農夫fが川を渡ろうとしている．小舟には農夫のほかにはおおかみ，やぎ，キャベツのいずれか一つしか乗せられない．農夫がいなくてもおおかみもやぎも逃げないが，おおかみはやぎを，やぎはキャベツを食べてしまう．どのようにして農夫は川を渡るべきか？ このオートマトンはその解を示す．Fは農夫だけが，W，G，Cはおおかみ，やぎ，キャベツと農夫が川を渡る事象を，wc/fgなどは川岸の一方におおかみとキャベツ，片方に農夫とやぎがいる状態を示す．



〔図2〕時間スイッチのオートマトン

始状態0にいて，事象pb（切ボタンを押す）が生起すれば状態1に移り，そのまま経過すればやがて事象swoff（電源を切る）が起こる．また，状態1にいるときに再度pbが起これば，状態2に移る．状態2にいると，やがて事象onehourが起こり，状態1に推移し，ついで事象swoffが生起することになる．



〔図3〕時間変数を導入した時間スイッチのオートマトン

図2に時間変数を導入した図．{t}はt:=0の意味である．

ます．そこで時間推移系を次のような順序で説明します．はじめにオートマトンを定義します．次にオートマトンに時間変数を導入して時間オートマトンに拡張します．

ここでは，この時間オートマトンの解釈として，オートマトンから派生する時間推移系を考えます．

まず，オートマトンの説明から始めます．**図1**に例を示します．これは川渡り問題の解をオートマトンとして表したものです．

グラフの点は状態を，辺は状態の推移を表しています．辺に付けた札は事象です．最初は始点（初期状態）にいて，事象の生起とともに状態が推移していきます．ここでは，細かく見れば推移や状態が連続的に変化しているという時間的側面を完全に無視しています．

このようなオートマトンを形式的に次のような4組A＝(N，N_0，Σ，E)と定義します．

- N：点の有限集合
- N_0（⊆L）：始点の集合
- Σ：事象の有限集合
- E(⊆N×Σ×N)：辺の有限集合

辺e＝(n_1，σ，n_2)は，点n_1から点n_2へ向かう札σを持つ辺であることを意味します（普通，オートマトンは最終状態を考えるが，ここでは省略する）．

さて，時間オートマトンは次のようにオートマトンを拡張したものです．例を示すとすぐにわかるでしょう．家電器具についている電源を切る時間スイッチで，「切ボタン」を1度押すと1時間後に，2度押すと2時間後に切れるという機能を考えます．これを時間オートマトンとして記述したものが**図2**です．

ここで時間を無視して事象だけに注目すると，**図2**のようにオートマトンがかけます．始状態0にいて，事象pb（切ボタンを押す）が生起すれば状態1に移り，時間がそのまま経過すればやがて事象swoff（電源を切る）が起こるでしょう．また，状態1にいるときに再度pbが起これば，状態2に移ります．状態2にいると，やがて事象onehourが起こり，状態1に推移し，ついで事象swoffが生起することになります．しかし，これでは課題を記述したことにはなりません．そこで，時計である時間変数を導入するのです（**図3**）．

図3は状態0が始点で，はじめに系はここにとどまっています．そこで，事象pbが起こると，時間変数tを0に設定して状態1に推移します．それ以降tは変化し続けます．

状態1では，時間変数tに関する不変式$t \geq 0 \wedge t \leq 1$が成立することを要請しています．つまり，

- 時間変数tは区間[0，1]内になければならない
- 時計の単位を時間とすれば，この状態に1時間以内はとどまっていいが，それ以上はとどまれない

ことを意味します．これを時間制約といいます．また，$t \geq 1$が成立すると状態1から状態0への推移を引き起こす事象swoffが生起します．また，生起しなければなりません．すなわち，時間オートマトンにおいては，推移の生起に時間制約があり，また，状態に停留している時間にも制約があるわけです．**時間オートマトン**を次のような6組A＝(N，N_0，Σ，T，ι，E)と定義します．

- N：点の有限集合
- N_0（⊆L）：初期点の集合
- Σ：事象の有限集合
- T：時間変数の有限集合
- ι：N→C(T)点に時間制約を対応させる関数
- E(⊆N×Σ×ℙ(T)×C(T)×N)辺の有限集合

この定義において，時間変数tに関する時間制約とは次のような式をいいます．

$$\phi, \psi ::= \mathrm{true} \mid t \leq c \mid t \geq c \mid t < c \mid t > c \mid \phi \wedge \psi$$

ここで，cは非負有理数を表し，時間変数全体の上の時間制約の全体をC(T)と書いたのです．辺e＝(n_1，σ，τ，φ，n_2)は，点n_1から点n_2へ向かう辺であり，それは事象σによって生起する推移を意味し，時間変数集合τ（⊆