新 組み込みソフトへの数理的アプローチ

～形式仕様記述をどのように使うか～

第1回

仕様の形式化のはじめの一歩
――真理表を使いこなす

藤倉 俊幸

はじめに

● モデル検査は市民権を得たが，形式仕様記述はまだ

月日がたつのは早いもので，うっかりしていたら連載が長いこと中断してしまった．その間に，モデルを使った「モデル検査」という言葉が市民権を得たような感がある．モデル検査を使うと「何ができて，何ができないのか」ということもだいぶ明確になってきたように思う．

しかし，本連載で扱う形式仕様記述[注1]については，まだこれからではないかと思う．そこで，形式仕様記述をどのように使うのかという点にフォーカスして連載を仕切り直したいと思う．

● 中学で習った命題論理から始めよう

形式仕様記述というとVDM++[注2]が思い浮かぶが，いきなり使おうとしてもちょっと難しい．何が難しいかというと，仕様を形式化するために述語論理という馴染みのないものを使うところである．

そこで，まず一般的な命題論理から始めて，命題論理が使いづらいと感じるようになったところで述語論理に移るのがよいのではないかと思う．命題論理は，中学や高校の数学でも出てくるし，C言語ならandやorやnotで表現できる．最初は，命題論理式に馴染むことだ．また，命題論理もいろいろと便利な使い方があり，それを知っておいて損はない．

第1回目の今回は，命題論理を中心にして仕様を形式化するということを考える．

一般に，仕様書の中には，「構造に関する記述」，「動作に関する記述」，「条件に関する記述」が含まれている（**図1**）．組み込みソフトウェアの仕様書では，動作や操作に関する記述が重要だ．そこで，動作に関する記述については論理式ではなく，LTSA[注3]などを利用して動作モデルによって形式化した方がよい．そのため，モデル検査が先行して使われるが，モデル検査を行うためには検査式が必要になる．検査式というのは時相論理式のことであり，最終的には論理式の扱いに慣れておく必要がある．論理式には命題論理と述語論理，時相論理の3種類があり，この順に難しくなる．つまり，命題論理をやっておくとモデル検査でも役に立つのである（**図2**）．

● 仕様書を論理式で書き直す

当面の目的は，仕様書に書いてあることを命題論理式に書き直すことだ．仕様書の何パーセントが命題論理式に変換できるのかというと，おそらく10%から20%ではないか

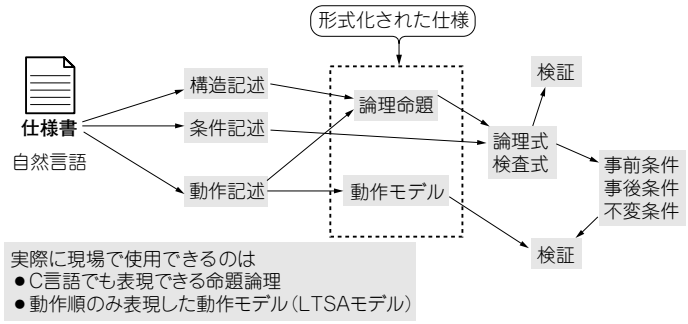

図1 仕様の形式化

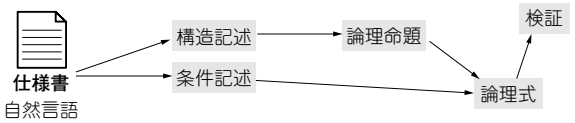

図2 当面の目的

注1：数学的な手法を用いて仕様を記述すること．専用の形式使用言語などを用いる．
注2：形式検証ツール．国内ではhttp://www.vdmtools.jp/が詳しい．
注3：形式検証ツール．http://www.doc.ic.ac.uk/ltsa/

と思う．これは，「かつ」，「または」，「ならば」，「〜でない」だけで表現できる部分に対応する．少ないと思うかもしれないが，これでも御利益はある．

1 形式化すると何が嬉しいのか

● $x^2=1$ の解を例に考えてみよう

仕様書を命題論理式で形式化すると，何が嬉しいのかということが重要である．まずは，そのことを実感してみよう．

例として，方程式 $x^2=1$ の解について考える．$x=1$ は解の一つであるが，それで十分だろうか？ 実は十分ではなく，$x=-1$ も解であるといわなくてはならない．しかし，$x=-1$ はしばしば見落としてしまう．形式化すれば，このようなモレを検出することができる．

問題を以下のような形に整理する．

「$x^2=1$ のとき，x はいくつか？」
に対する以下の推論は正しいか
「$x=1$ ならば $x^2=1$，よって $x=1$ である」

まず，この記述の中から命題を選び出す．ここでは，次の二つとする．

A：$x^2=1$
B：$x=1$

そして，推論をこれらの命題を使った論理式で表現する．

① $x^2=1$ のとき	A のとき
② $x=1$ ならば $x^2=1$	B → A である
よって $x=1$ である	よって B である

さらに，この推論の構造そのものも論理式で表現する．具体的にいうと，前提①②をすべて AND で結んで，「ならば→」の後ろに結論③を持つような論理式を作ればよい．つまり，「①かつ②ならば③」という論理式である．具体的には以下のようになる．

表1　式(1)の真理表

A	B	(A ∧ (B → A)) → B
T	T	T
T	F	F
F	T	T
F	F	T

← 成立しないところがある

A：x^2 である
B：$x=1$ である

$$(A \wedge (B \rightarrow A)) \rightarrow B \quad \cdots\cdots (1)$$

この論理式が常に成立すれば，モレのない推論ということになる．成立しない場合があれば，それが推論の穴になる．しかし，ある論理式が常に成立することを証明するのは，結構難しい話である．そこで，証明の部分はツールを使用する．証明する方法には定理証明と網羅的検査の二つがあるが，網羅的検査に対応する手法として真理表の作成がある．

実際に真理表を作成してみると，**表1**のようになる．**表1**から，式(1)が成立しない場合があることが分かる．それは，A が真で，B が偽になる場合である．つまり

「$x=1$ ならば $x^2=1$，よって $x=1$ である」

という推論にはモレがあることを示している．実際，$x=-1$ の場合がそのモレに該当する．つまり何が嬉しいのかというと，完璧な推論かどうかを判定することができて，もしモレがある場合にはそれを指摘してどのような場合かに関するヒントをもらえるということである．

ただし，どうすれば正しい答えを得られるかについては，自分で考えなくてはならない．すなわち，$x=-1$ を見つけ出すのは自分でやらなければならない．これは，扱う問題領域の専門知識が必要になる．

しかし，$x=-1$ を見つけ出せたとして，以下のように説明したのでは駄目である．命題として，

C：$x=-1$

を追加して，

$x^2=1$ のとき	A のとき
$x=1$ ならば $x^2=1$	B → A である
$x=-1$ ならば $x^2=1$	C → A である
よって $x=1$ または $x=-1$ である	よって B または C である

表2　式(2)の真理表

A	B	C	式(2)
T	T	T	T
T	T	F	T
T	F	T	T
T	F	F	F
F	T	T	T
F	T	F	T
F	F	T	T
F	F	F	T

← 成立しないところがある