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15回

総まとめ（最終回）

—— 推論，ステート・マシンと検証

藤倉 俊幸

はじめに

この連載を始めたのは2006年，第1回はガス・バーナー問題[(2)]を使ってインターバル・ロジックの話をした．その後，振る舞い系の話を進めてオーバラップ制御などのモデル検査に関連する話を2007年末まで続けた．その後，筆者の都合により中断して2008年末から「新・数理的アプローチ」と“新”を付けて論理系の話を中心に話を進めて現在に至っている．トータルの連載回数はチャンと数えてないが今回を含めて24回ぐらいになる．これだけの期間になると技術も進歩するし，世の中の状況も変わってくる．途中から連載を読み始めた人も増えてくるので既に書いたことを前提にすることができなくなってきた．また，何時までも“新”を付けておくのも気が引ける．なので，いったんこの連載は今回で終了することになった．

連載をやっている間の技術的進歩としては，例えば，ガス・バーナー問題などは当時は紙と鉛筆で解くしかなく，仕様のまとめ方の参考にするか考え方を理解する程度の情報提供でしかなかったが，今ではSAT/SMTソルバで証明することができる．さらにプログラム検証ツールと連携させればC言語でも証明できるようになった．また，連載の中では取り上げていないが，時相論理式から状態マシンを自動生成することもできる．いずれこれらの裏で何をやっているかという話を覆い隠して便利に使えるツールが開発されるだろう．

そうなると考え方を理解していることの重要さが増してくる．参考文献(1)に中国のことわざとともに面白い言葉が載っている．

> 「人にツールを与えれば修理屋になる．
> ツールの作り方を教えればエンジニアになる」

ちなみに中国のことわざは，

> 「人に魚を一尾与えれば一日食べさせてやれる．
> 魚の取り方を教えれば一生食べさせてやれる」

である．作業を自動化するのにツールは必須だが，ブラックボックスとして使うと極めて危険だ．ツールのバグか，入力データの間違いかの区別が付かない．そして，いつの間にかツールに使われてしまう．

ツールはクラウドの普及によって，ビジネスも利用形態も今までのような形ではなくなるといわれている．価格も安くなるだろう．メソドロジ（方法論）と自動化が一体化して肥大化したものや，メソドロジが独立した自動化中心のものなどが利用可能になるだろう．メソドロジ情報を提供する電子書籍と統合するのかもしれない．いずれにしても利用者自身がメソドロジの専門家でなくてはツールを使いこなせない．

今回は，まとめとして今まで扱った内容の重要な部分を振り返ってみる．

1 推論の正しさ

ソフトウェア開発では至るところで推論を行っている．推論というと堅苦しいが，要するに理由を考えたり，何かを説明したりするということである．この考え方の筋道を通して，モレやヌケがないことを確認するために，連載では最初に推論の正しさを確認する手法を説明した．命題論理を使った検証手法である．

推論の前提となることや結論を論理的に表現するだけでなく，推論の過程も論理的に表現することができる．そして論理的な表現から真理表を作る．もし，考え方にモレやヌケがあると真理表で偽になるところがあるので検出でき

KEYWORD——形式手法，推論，真理表，プログラム検証ツール，アブダクション，帰納，演繹