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9回

Alloyによるモデリング
――クラスやインスタンスの概念をモデル化して検証する

藤倉 俊幸

はじめに――真理表からAlloyへ

● 本連載のテーマ

この連載では，「ソフトウェアの品質を向上させるには形式的なアプローチが必要だ」というメイン・テーマを掲げている．

しかし，それはなかなか難しいので，プログラムを書く人なら普通は知っている命題論理を使って形式的に要求分析したり設計したりする手法を説明してきた．

話の流れは，命題論理式を立ててその真理表を作成し，どの組み合わせで真になるか偽になるか，すべての組み合わせで真になるか偽になるか，という情報を使ってテスト・ケースの生成などに利用する，あるいは，推論自体が正しいかという基本的な問題を検証するというものである．

今までPrologで作った真理表を生成するプログラムを使用してきた．このプログラムを使うと真偽の組み合わせを網羅的にすべてチェックしてくれる．論理学は真と偽しか出てこないので組み合わせを作るのは簡単だが，組み合わせの数が膨大になり実際の問題では使えなくなってしまうこともある．実際の問題を扱いやすいように小分けにすることは重要である．しかし，真理表生成プログラムの扱える範囲は非常に小さく，真理表を使えるように設計問題などを小分けにすると小さくなりすぎてしまい，かえって効率が悪い．真理表は論理学の感覚を養うにはよいが，仕事で使うためにはそろそろ別のツールにステップアップする必要がある．

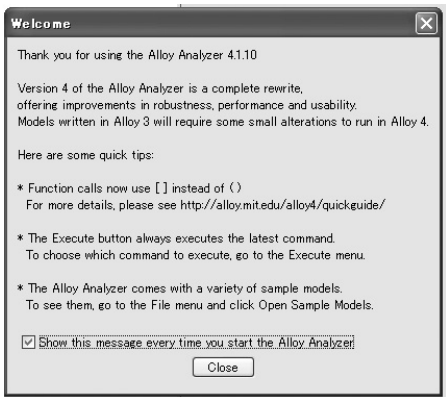

図1　AlloyのWelcomメッセージ

● 真理表では物足りなくなってきた

また，実際の問題は真と偽の組み合わせほど単純ではなく，もっと一般的な組み合わせとして考える必要がある．最終的には正しいか正しくないかに落とし込むにしても，その前の段階をいろいろとサポートしてもらわないと辛い．それで，組み合わせ問題とか写像などのモデリングの道具の説明もした．これは，ものごとを集合として扱ったり集合の要素として扱ったりするときに必要になる．オブジェクト指向と対応させた場合の集合はクラスで，集合の要素はクラスから生成されたインスタンスになる．

今回は，論理学については何となくわかった，写像の考え方も何となくわかった，その次のステップとして，集合をベースとして論理関係をモデリングして検証するツールであるAlloy[1]を紹介する．Alloyは与えられたモデルから論理式を生成し，SATソルバという検証エンジンで真偽の組み合わせを検索してくれる．たとえば，この連載の中でも紹介した(2009年5月号，pp.169-175)プロダクトライン開発で可変性を表現するFeature Modelを形式化して可能な製品機能の組み合わせを検査する手法は，Alloyを使って自動化することができる[2]．

1 モデル・ベース検証ツールAlloy

● Alloyの入手と注意点

Alloyは参考文献(3)のURLからダウンロードして入手

KEYWORD――命題論理，述語論理，真理表，Alloy