概要

1210016 小川　直哉

2014　2 月

本研究の目的はモデル検査ツール Spin を対象に、検証の誤りの原因を特定する手法を提案することである。

モデル検査はソフトウェアの信頼性を向上させる技術の 1 つである。モデル検査を行なうには検査対象のモデル ”M” と満たすべき性質を与える。M は仕様記述言語でモデル化された検査対象の振る舞いであり、P は検査対象が満たすべき性質を時相論理式などを用いてモデル化する。そして、モデル化した振る舞いが与えた性質を満たすか検査する。M の状態数は有限である。よって、全ての状態を網羅的に探索すれば、与えられた性質を満たすか検査できる。

ここで振る舞いや性質のモデル化自体に誤りがあると検査対象の不具合を発見することが出来ないという問題がある。本来のものと異なるモデルを探索し、そこで成り立つ性質を調べたとしてもその検証は無意味だからである。そこで本研究ではその原因が振る舞いのモデル化にあるのか性質の与え方に問題があるのか特定する手法を提案する。

本研究の特色は検査対象のモデル化が十分されていなくとも誤り原因の特定を見込めることである。

本研究では標本集合と呼ぶものを用意し反例と比較することで誤りを特定する手法を提案する。モデル検査では検査対象のモデル M が検査対象の性質 P を満たさないとき反例が出力される。Spin によるモデル検査の場合には、反例として誤りの状況になるような実行列を出力する。しかし、この M と P はモデル検査で扱うために、モデル作成者が作成したものである。反例が出力されたからといって検査対象に誤りがあるとは言えない。人による誤りが原因で反例が出力されることもある。

例えば、4 つの信号（信号 A, 信号 B, 信号 C, 信号 D）時差式信号機を検査対象として考えてみる。性質として信号の色の変化を検査する。信号機同士が同期を取りながら色を変化させる表現は時差式信号機の振る舞いを書く 1 つの方法である。信号機のモデルは信号機同士が同期を取りながら動くように作成したり、メッセージ通信を用いて各信号への命令を統括して行なうように作成したりする方法がある。他に、コントローラを使い各信号機にメッセージを送る方法がある。性質は時相論理式で表現する。時相論理式で次のように表現した：`"r → []⟨p U q⟩"`. `"r"`は信号が青であること、`"p"`は信号が青であること、`"q"`は信号が黄であることをそれぞれ意味する。よって、`"r → []⟨p U q⟩"`は信号が黄になるまでは青のままであることを意味する。この式を用いて、モデル検査を行なった結果、以下の実行列が出力されたとする。

`(blue, red, blue, red) → (yellow, red, blue, red) → (red, red, blue, red).`

実行列は青、黄、赤の値をとる変数の 4 つ組で表現される。一番左の変数は信号機 A の色, 次は信号機 B の色, 3 番目は信号機 C の色, 最後は信号機 D の色を表す。しかし一番左の変数は順番通りに変化している。この実行列は誤った反例である。本来、誤りではないものが出力されたと言う

ことは M に問題はないと言える。

よって P に誤りがあると特定できる。このように、誤りを特定するには反例が偽反例であるかどうか基準が必要となる。本研究では、正標本集合と負標本集合を用意する。正標本集合とは検査対象の性質を満たす振る舞いだと明らかに確信できるものである。負標本集合とは検査対象の振る舞いではないと明らかに確信できるものである。信号機の例を用いると、(blue, red, blue, red) → (yellow, red, blue, red) → (red, red, blue, red) は正標本集合の 1 つであり、(blue, red, blue, red) → (yellow, red, blue, red) → (blue, red, blue, red) は負標本集合の 1 つである。

誤りの原因は前もって用意した正標本集合、負標本集合と反例を比較することで特定する。まず、反例と比較する為に標本集合の書き方を決めることが必要となる。

実験の結果、負標本集合については有効な書き方を見つけることができ、振る舞いのモデル化の誤りを特定する手法を提案できた。しかし、正標本集合については有効な書き方及び、性質の与え方の誤りを特定する手法は提案できなかった。

負標本集合の書き方について、変数の組の遷移と変数に関する条件式を使うことにした。ある遷移列がこの遷移を含んでいるとき、この遷移列は負標本集合に含まれることで意味づけをした。

信号機の例を用いると、"$u_1 \equiv (A, B, C, D) \Rightarrow (A', B', C', D')\ \ when\ \ (A = blue \wedge A' = red) \vee (A = yellow \wedge A' = blue) \vee (A = red \wedge A' = yellow)$" は例の 1 つである。"$(A = blue \wedge A' = red)$" は信号機 A が青から赤に変わることを意味する。"$(A = yellow \wedge A' = blue)$" は信号機 A が黄から青に変わることを意味する。"$(A = red \wedge A' = yellow)$" は信号機 A が赤から黄に変わることを意味する。そのため、例の条件式は振る舞いとしてはおかしな式である。もし変数の遷移列がおかしな遷移を含んでいれば、遷移列は負標本集合の要素である。そして、反例が負標本集合に含まれる判定方法は疑似コードで示した。

標本集合の有効な書き方が見つからないと誤りの原因を特定する方法を提案することはできない。そのため、正標本集合の考察については正標本集合の書き方について述べた。