自然語要求仕様記述の形式検証に向けて
—話題沸騰ポットのモデル検査—

遠藤健, 小形真平, 岡野浩三†, 関澤俊弦††

アブストラクト
自然語記述された要求仕様記述からその記述の問題点を洗い出すことができれば手戻りの解決に繋がる. 本研究では自然語記述された要求仕様記述から半自動変換を経て形式手法を適用する方法を考案することを目標にその準備研究を行っている. 本報告ではその準備研究の一環として話題沸騰ポットの要求仕様記述を人手で状態遷移モデルに変換し, NuSMV でモデル検査を行った取り組みについて報告する.

Towards Formal Verification on Specification in a Natural Language
-Model Checking for “Electric pot, GOMA type 1015”-

Ken Endo, Shinpei Ogata, Kozo Okano†, Toshifusa Sekizawa††

Abstract
Formal verification on specification in a natural language would be great challenge in software engineering. It would help for software engineers to reduce rework in development stages. We now considering a semi-auto translation method from specification in a natural language into formal specification which can be an input to usual formal method tools. As a first step of the challenge, we perform model checking on a behavioral model obtained from specification of an electric pot written in a Japanese. This report describes the translation method and obtained results of the model checking.

1.はじめに

著者らの研究グループでは自然語記述された要求仕様記述から半自動変換を経て形式手法を適用する方法を考案することを目標にその準備研究を行っている. 本報告ではその準備研究の一環として話題沸騰ポットの要求仕様記述[1] を人手で状態遷移モデルに変換し, NuSMV[2]でモデル検査を行った結果について報告する. 以下, 2 章でモデル検査器 NuSMV と例題に用いた話題沸騰ポットの要求仕様記述について述べる. 3 章では現在考案中の変換プロセスについて, 4 章ではその変換プロセスに基づいて人手で変換した要求仕様記述の変換例について, それぞれ, 述べる. 5 章ではモデル検査の実際について触れる. 6 章でまとめる.

†信州大学 工学部 情報工学科
†Faculty of Engineering, Shinshu University
††日本大学工学部情報工学科
††College of Engineering, Nihon University

2.準備

NuSMV[2]はオープンソースのモデル検査ツールであり, 有限値を持つ有限個の変数の変化を状態遷移として記述し, 有限オートマトンモデルを表現する. また, これら複数の状態機械を同期モデル, 非同期モデルとして並列合成できる. また, NuSMV の特徴としてモデル検査の検査式に LTL に基づく式と CTL に基づく式の 2 つを指定することができる.

話題沸騰ポットの要求仕様記述は組込みソフトウェア管理者・技術者育成研究会（SESSAME）が組み込み

システムの教材として開発した記述であり，タイマなどの機能がついた電気ポットの要求仕様が日本語で記述されている．7 版までの改訂がされており，現在，そのうちの複数のバージョンが公開されている．

3.変換プロセス概要

もともとの要求仕様記述のうち，ポットの基本構成と基本機能が記述されている,「ハードウェア構成とハードウェア要求仕様」,「操作要求仕様」,「温度制御行為」の項目を今回は対象とした．
これら 86 個の記述をまず，制約を表す記述，振る舞いを表す記述，定義を表す記述，その他に分類した．分類の結果を表 1 に示す．

表 1:分類結果(文数)

制約	振る舞い	定義	その他
11	51	20	8

ただし，制約と振る舞いの両方に分類される記述が 4 個あった．
さらに状態変数となりうる単語を抜き出し，またこれらの単語を変数とみなしたときの，取りうる値の範囲を設定した変数の数は 28 であった．次に，振る舞いをあらわす文章を解析し，すべて単文形式とし，主語，条件，動作を特定した．動作は変数の更新，または外部への出力(イベント)とした．次に，条件を変数の制約式として変換を行った．以上の結果をもとに状態機械を構成し，NuSMV の状態機械を構成した．時間変数は離散値をとるものとし，タイマごと，状態機械を構成した．

4.変換例と考察

次の 2 つの文章は要求仕様書内のタイマに関する機能要求記述の例である．
「タイマが起動している/していないにかかわらず,タイマボタンを 100msec 以上押されるたびにタイムアップまでの残り時間の分に 1 分を加算し,秒の単位を 0sec にクリアした値にセットし,セットした値(タイムアップまでの時間)を分単位のみで操作パネルのタイマ残り時間を表示窓に表示する.」
「タイマ起動中に.タイマボタンを 3sec 以上続けて長押ししたら,ブザーを 100msec 鳴らした後.0min0sec にリセットされ,タイマが停止する.」
ブザーを 100msec 鳴らし，同時にタイマボタンを 100msec 押すと，タイムアップまでの時間に 1 分加算する(timer が setting 状態に遷移する)状態遷移とタイマの停止(timer が stop 状態に遷移する)という 2 つの状態遷移が発生してしまうのではと考えた．
タイマの状態遷移について変換すると,以下の通りになった．

```
next(timer) := case
  …
  press_button0.press_type = push
  press_button0.press_type = hold : setting;
  …
  timer = countdown & press_button0.press_type = hold : buzzer;
  timer = buzzer & msec0.lapse = passage : stop;
```

5.モデル検査の実際

上記の問題を検査するため，次式により「timer が buzzer 状態になった場合 timer は次の状態で必ず stop になるか」を検査した．

CTLSPEC AG(timer = buzzer -> AX (timer = stop))

結果は真となり期待と異なったが，検査式やモデルをそれぞれ 4 回，3 回にわたり修正追記した結果，timer が buzzer 状態に遷移しない場合を発見した．timer = countdown & press_button0.press_type = hold が成り立つ場合 timer が buzzer ではなく setting に遷移する可能性がある．これは「タイマボタンを 100msec 以上押されるたびに」という記述が「タイマボタンを 3sec 以上続けて長押ししたら」と被るためである．

6.まとめと今後の展望

自然語要求仕様記述レベルでのモデル検査の必要性がわかった．今後はモデル検査を行い，また変換プロセスを精緻化し，半自動生成を目指したい．

謝辞

本研究は JSPS 科研費 26330092 の助成を受けた．

参考文献

1. 組込みシステム教育教材　話題沸騰ポット GOMA-1015 型 要求仕様書 http://www.sessame.jp/workinggroup/WorkingGroup2/POT_Specification.htm <2015/12/22 accessed>
2. A. Cimatti, E. M. Clarke, E. Giunchiglia, F. Giunchiglia, M. Pistore, M. Roveri, R. Sebastiani, and A. Tacchella: “NuSMV 2: An OpenSource Tool for Symbolic Model Checking,” In Proceeding of International Conference on Computer-Aided Verification (CAV 2002).