

ユースケース記述の規則への整合性検査に向けて

中村 遼太郎¹ 林 晋平¹ 佐伯 元司¹

概要: ユースケースが示唆する機能要求が、法律をはじめとする規則を遵守するかについて、モデル検査によって検査する手法を述べる。ユースケースのドメインと規則の知識表現をもとに、ユースケースから、ユースケースに関わる規則の検査式と状態遷移モデルを生成する。生成された状態遷移モデルと検査式に、モデル検査を適用した結果から、機能要求が規則を遵守しているかを判定する。

1. はじめに

法令をはじめとする規則と機能要求間の整合性は、開発初期に確保されることが望ましい。規則に反する機能要求の獲得は、開発の後戻りやコンプライアンス違反を引き起こす。

機能要求と規則間の整合性を、開発初期に検査するための材料として、我々はユースケースの利用を考えた。ユースケースには、獲得された機能要求が記述される [1]。よって、ユースケースのアクタとシステム間のやり取りを、規則と照合することで、そのやり取りで実現される機能要求の規則への整合性を、要求分析段階で検査できると考えられる。

これまでに、ユースケースの検査手法がいくつか提案されているものの、社会一般の規則との整合性を検査できるものは限られる。検査可能な手法であっても、支援範囲の狭さや自然言語解析の向上などの課題が残る。

本稿では、ユースケースが示す機能要求の規則への整合性をモデル検査技術を応用し機械的に検査する手法について議論する。モデル検査を用いた2つの既存手法とその課題をとりあげ、両者の組み合わせによる支援範囲の拡大と課題の解決の方針を紹介する。

2. 格文法による自然言語解析

佐伯らのユースケースモデルの法令への遵守性検査手法 [2] は、検査式で表された法令とユースケースモデルに対するモデル検査の適用結果から、法令違反や法令自体の欠陥を検査する。検査式は、格フレームという動詞がとりえる格構造のパターンを項とする CTL 式で記述される。この手法では、検査式の格フレーム部分を、ユースケース文の格構造で置換することで、ユースケースモデルの検査

式を生成する。

例えば、個人情報保護法のもとに、 x が個人情報を y から取得した場合、 x が個人情報の利用目的を y に通知しなければならないという義務が、(動詞: 取得, 主格: x , 対象格: 個人情報, 源泉格: y) $\rightarrow$ AF (動詞: 通知, 主格: x , 対象格: 利用目的, 目標格: y) という形で定義されているとする。このとき、「電子ショップが個人情報を利用者から取得する」というユースケース文から、(動詞: 取得, 主格: 電子ショップ, 対象格: 個人情報, 源泉格: 利用者) という格構造を得た場合、この格構造は規則の「取得」の格フレームに対応するので、変数 x, y に「電子ショップ」と「利用者」を埋めることで、ユースケースの文脈に則した規則の検査式が得られる。

この格構造と格フレームの照合手法では、格フレームの深層格の意味を考慮しないので、規則とは無関係な検査式が生成されるおそれがある。例えば、個人情報の利用目的の通知義務は個人情報取扱事業者のみが負う義務とされている。しかし、格フレームの深層格に意味的制約が定義されていないので、ユースケース文の主格が個人情報取扱事業者にあたらくとも、検査すべき規則として検査式が生成される。

高久らや鈴木はユースケースのモデル検査による検査のために、ユースケースから状態遷移モデルを生成する手法を提案した [3], [4]。これらの手法は、ユースケース文そのものではなく、その格構造に着目することで、構文や活用が異なる文の間の同義関係を見つける。例えば、「利用者は広告メール配信を承諾する」と「広告メール配信を利用者は承認している」はともに、(動詞: 承諾, 主格: 利用者, 対象格: 広告メール配信) という格構造なので、等しい意味の文として扱われる。しかし、たとえ「利用者」と「ユーザ」のような同義関係にある単語でも、深層格の単語が全て一致しなければ、意味が異なる文として扱われてしまう。

¹ 東京工業大学大学院情報理工学研究科計算工学専攻

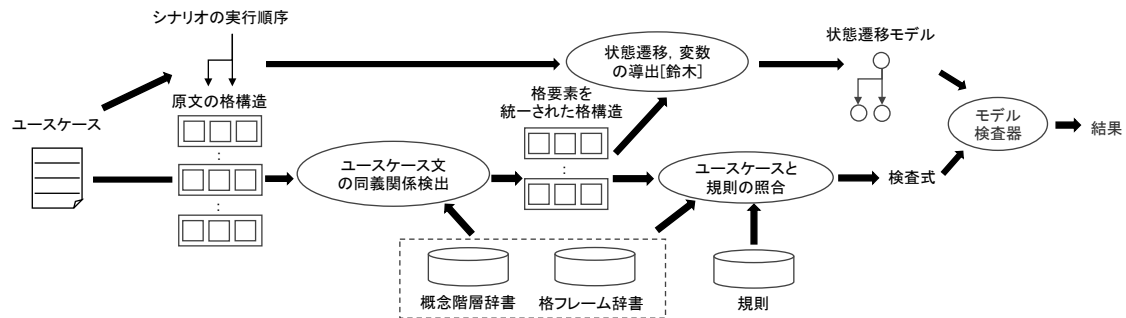


図 1 提案手法の概要

3. 状態遷移モデルと検査式の生成

本手法の概要を図 1 に示す。本手法は、我々のこれまでの取り組み [5] に基づき、格フレームの深層格に意味的制約を与え、これを格構造との比較に用いることで、2 章で述べた規則と無関係な検査式が生成される問題と深層格の単語が異なる同義文を検出できない問題を解決する。問題を解決しつつ、両手法を組み合わせることで、アクタとシステムの振舞いをモデル化した状態遷移モデルと守るべき規則を示す検査式を生成する。これらへのモデル検査の適用により、反例が出力されれば、反例が示唆する振舞いと検査式が示す規則間に不整合があることが読み取れる。また、検査式が満たされれば、両者の整合性がとれていることが分かる。本手法は、モデル検査器により、アクタとシステムの振舞いを検査することで、機能要求の規則への整合性の機械的な検査を支援する。

本手法は、概念階層辞書、格フレーム辞書、規則をドメイン知識として、ユースケースから状態遷移モデルと検査式を生成する。概念階層辞書は、単語の概念間の is-a 関係や同義語関係にある単語のペアを定義する。例えば、「利用者」と「人」は is-a 関係で結ばれる。格フレーム辞書は、深層格に意味的な制約を付与した格フレームを定義する。制約の一例としては、動詞「送る」の主格は、「人」または「組織」の子概念でなければならない。説明のために、以降では、 a が b の子概念でなければならないという制約を $a \preceq b$ と記述する。規則は、深層格に意味的制約を付与した格フレームを項とする CTL 式として定義される。例えば、1 章であげた個人情報保護法の規則は、(動詞: 取得, 主格: $x \preceq$ 個人情報取扱事業者, 対象格: $w \preceq$ 個人情報, 源泉格: $y \preceq$ 人) $\rightarrow$ AF (動詞: 通知, 主格: $x \preceq$ 個人情報取扱事業者, 対象格: $u \preceq$ 利用目的, 源泉格: $y \preceq$ 人) のように定義できる。

ユースケース文の同義関係検出は、同義関係をふまえた状態遷移モデルと検査式の生成のために行う。ユースケースから抽出された原文の格構造間に同義関係があるものがあれば、格要素を揃えることで、一方の格構造に統一する。例えば、概念階層辞書で「利用者」と「ユーザ」が同義語関

係にあるとされていれば、(動詞: 送る, 主格: 利用者, 対象格: 個人情報, 目標格: システム) と、(動詞: 送る, 主格: ユーザ, 対象格: 個人情報, 目標格: システム) は、同義関係にあると判定され、一方の格構造にそろえられる。また、同義関係にある格構造を統一後、これらとユースケースのシナリオの実行順序から、鈴木の手法 [3] に従い、状態遷移と変数を導出することで、状態遷移モデルを生成する。

ユースケースと規則の照合では、2 章で述べたようにユースケース文の格構造の深層格を格フレームに代入することで検査式を生成する。ただし、格フレームの動詞と深層格に意味的制約が付与されている場合は、ユースケース文の格構造の深層格の単語や動詞が制約を満たさない限り、規則は生成されない。例えば、格フレームの一部が (動詞: 取得, 主格: $x \preceq$ 個人情報取扱事業者, 対象格: $w \preceq$ 個人情報, 源泉格: $y \preceq$ 人) とあれば、対応する格構造の主格は、個人情報取扱事業者と is-a 関係になければならない。

検査式にモデル検査を適用するために、生成された検査式を、状態遷移モデルの状態変数を用いたものに交換する。生成される状態遷移モデルは、格構造から作られた状態変数の値を真にすることで、対応するユースケース文が実行中であることを表す。

4. 課題

手法の実装を行い、例題に実装された手法を適用することで、評価と手法の改良を行う。

参考文献

- [1] Schneider, G. and Winters, J. P.: *Applying use cases: a practical guide*, Pearson Education (2001).
- [2] Saeki, M., Kaiya, H. and Hattori, S.: Detecting Regulatory Vulnerability in Functional Requirements Specifications, *Proc. ICSOFT*, pp. 105–114 (2009).
- [3] 鈴木啓史: ユースケース記述の検査を目的とした状態遷移モデル生成の研究 (2012). 東京工業大学 学士論文.
- [4] 高久陽平, 林晋平, 佐伯元司: ユースケース記述からの状態遷移モデル生成, 情報処理学会研究報告. Vol. 2010, No.17, pp. 1–8 (2010).
- [5] 中村遼太郎, 林晋平, 佐伯元司: ユースケース記述の検査のための自然言語要求文の解析, 電子情報通信学会技術研究報告, Vol. 113, No.489, pp.25–30 (2014).