5H-09

状態遷移図と抽象的仕様記述のマッチングによる仕様の誤り検出

岡野 純平†
電気通信大学大学院情報工学研究家情報学専攻

織田 健‡
電気通信大学情報理工学研究科情報学専攻

1 はじめに

ソフトウェアにおける誤りとは要求の段階で混入することが多く、信頼性の高いソフトウェアの開発には質の高い要求の記述が不可欠である。しかし、誤りのない仕様を記述することは困難であり、一つの仕様記述方法では何かしらの誤りが存在する可能性がある。そこで我々は異なる手法で記述された要求を比較することで、一つの手法では検出出来ない誤りを検出出来ると考えた。

本研究では要求の無矛盾性が保証出来る形式手法 B-Method とソフトウェアの振る舞いを視覚的に記述する状態遷移図の二つの異なる仕様記述を比較し、手法に整合性がない時、その誤りを提示する手法を提案する。

2 背景と目的

2.1 B-Method

形式手法の一つである B-Method は、要求仕様を集合論と述語論理を用い記述し、それを段階的に詳細化することで実装を導出する [1]。以降 B-Method の仕様をモデルとする。モデルは大きく分けて不変条件と操作の二つで構成され、モデルの操作の実行後に不変条件を満たすかどうかを検証することで、仕様の無矛盾性を証明できる。

2.2 本研究の目的

B-Method は数学的に仕様の無矛盾性を検証出来るが、出力されたソフトウェアの振る舞いが利用者の期待している振る舞いと一致するとは限らない。その原因の一つとして、制約条件の欠落が挙げられる。制約条件が欠落したモデルでは、正しいモデルでは通らない証明が条件の欠落のために通ってしまうため、誤りを検出出来ない。そこで我々は形式手法 Z と状態遷移図のマッチングの研究に着目し [2]、それを B のモデルに適用することで、その課題を解決できると考えた。

本研究の目的は B のモデルと状態遷移図の二つの手法で要求を記述し、それらの整合性を確認することで仕様記述の誤りを検出することである。

3 B のモデルと状態遷移図のマッチング

3.1 状態遷移図

利用者は各エンティティ毎に状態遷移図を記述する。エンティティとは仕様内の実体を示すものであり、モデルの集合の型情報に対応する。各エンティティはモデルの型を、エンティティ内の状態はその型の部分集合を、そして遷移は操作と対応させることで状態遷移図とモデルのマッチングを行う。

---

formal

†Jumpei Okano, The University of Electro-Communications department school of Informatics

‡Takeshi Oda, The University of Electro-Communications graduate school of Informatics

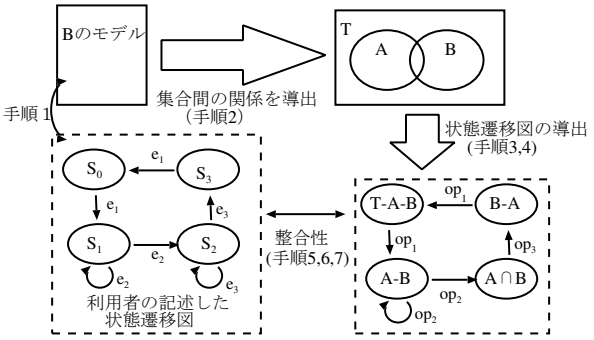

図 1: 仕様の誤り検出手順

3.2 マッチング手順

B のモデルと状態遷移図のマッチングは、モデルから状態遷移図を導出し、二つの状態遷移図を比較することで行う。その手順は以下である。

手順 1 型とエンティティの対応付け (人の手)
手順 2 モデルの型に内包された集合の包含関係の計算
手順 3 手順 2 から互いに素な集合をモデルの状態として導出
手順 4 モデルの操作による状態遷移の導出
手順 5 状態遷移図内の状態とモデルの状態数の確認
手順 6 状態のマッチング
手順 7 状態遷移のマッチング

手順 1 でモデルで定義された型と状態対遷移図のエンティティを対応させる。手順 2, 3, 4 でモデルから状態遷移図を導出し、手順 5, 6, 7 で導出した状態遷移図と利用者が記述した状態遷移図を比較し、整合性が取れているかを検証する (図 1)。

3.3 各手順における課題とその解決

マッチングでは各手順において以下の課題を持つ。

1 状態遷移図の状態に対応する集合の導出
2 事前状態と事後状態の導出方法
3 モデルと状態遷移図のマッチング手法

以下ではこれらの課題と解決方法について述べる。

3.3.1 状態に対応する集合の導出

モデルから出力される状態遷移図の状態は、互いに素な集合に対応させる必要がある。よって、各集合の包含関係を求める必要がある。

B-Method における集合とは利用者が定義した関数以外の変数及び、関数の定義域と値域に当たる。集合の包含関係は関数の定義域、値域を導出するルール、及び集合に関する不変条件を用いることで求められる。その後、重なり合った集合間の差や積集合を計算することで、状態に当たる互いに素である集合を導出出来る。

3.3.2 操作による遷移の導出

モデルから導出する遷移は操作と集合間の関係によって決定する。操作が集合 A の要素を集合 B に移すとき、

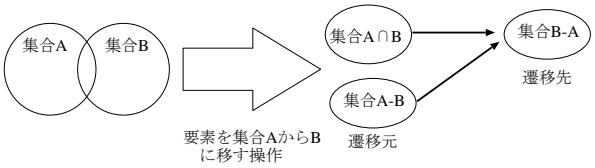

図 2: 状態遷移図の導出例

他に制約が無い場合、集合 A に内包されている集合全てに対して遷移を引き起こす (図 2)。操作が起こす遷移は各操作の事前状態と事後状態から求められる。事前状態に関しては、その操作の事前条件、及び IF 文などの条件式の積を取ることで計算する。事後状態はモデルで記述出来る各関数と操作で利用されている演算子、そして集合間の包含関係を利用することで計算する。

3.4 B-Method と状態遷移図のマッチング

欠落判定には、モデルから求めた状態遷移図と、利用者が記述した状態遷移図の対応関係を定める必要がある。今回は最適な対応関係を導出するための適切なアルゴリズムがまだ提案出来ていないためこちらは手作業で行い、アルゴリズムの方針については考察で述べる。

4 欠落判定方法

B のモデルから導出した状態遷移図が利用者の記述した状態遷移図と異なる場合、モデルの不変条件、操作の事前条件、操作の代入文、もしくは記述した状態遷移図に誤りがある等が考えられる。ここではモデルに誤りがある場合について述べる。

4.1 状態数の不一致

B のモデルから導出した状態遷移図の状態数は集合間の関係で決定する。このことから状態の数が一致しない場合、不変条件の欠落が考えられる。

状態数の不一致にはどちらの状態数の方が多いかで欠落している不変条件の種類が異なる。モデルからの状態の方が多い場合、集合間の関係に部分的な重なり合いが生じていると考えられるため、これを抑制する条件が欠落しているといえる。例えば B のモデルから導出した状態数が 3、利用者が記述した状態数が 2 の場合、$A \cap B = \phi$ もしくは $A \subseteq B$ のような条件が足りないと考えられる。

逆に利用者が記述した状態数のほうが多い場合、同じ状態を異なる状態と定義している可能性が存在する。よって 2 つの集合 A、B とすると $A = B$ のような条件が欠落している、もしくは関数の定義を全射で記述すべきところをそうでない関数を利用していると考えられる。

4.2 遷移の不一致

遷移の不一致はそれが自己遷移によるものかどうかで原因が異なる。

不一致の遷移が自己遷移ではない場合、操作の事前条件の欠落、もしくは操作内の代入文に誤りがあると考えられる。事前条件が欠落した場合、出力される遷移の数が変わる。例えば本来 $A \cap B$ から $B - A$ への状態遷移を正しい仕様とした場合、事前条件に $ee \in A \wedge ee \in B$ を記述しなければならない。しかし 2 つの事前条件の内 $ee \in B$ が抜けると、本来の遷移である $A \cap B \rightarrow B - A$ に加えて、$A - B \rightarrow B - A$ という遷移が起ることになる。

不一致の遷移が自己遷移による場合、関数の型定義に誤りがあると考えらる。自己遷移の存在の有無に関わると考えられる。モデルの型定義が単射でない場合、その値域を減算すると自己遷移が発生するが、単射の場合自己遷移が発生しない。そのため自己遷移の不一致の場合は、本来単射で記述すべき関数をそうでない関数を利用していると考えられる。

5 考察

モデルの振る舞いを検証するアニメーションとの比較及び今後の課題について記述する。

5.1 アニメーションとの比較

アニメーションとは B のモデル検証法の一つであり、記述したモデルを実際に動かして振る舞いを検証する手法である。アニメーションによる誤りを発見は、実際にそのパターンで動かす必要がある。そのため誤りを見落とす可能性が存在する。今回提案した手法は、システムの誤りを静的に発見できるため、誤りの見落としが起きづらいという点で有用である。

5.2 マッチング手法の具体的な提案

今回の研究では B の集合と利用者の状態遷移図の状態の対応について具体的な提案を行うことが出来なかった。

方針としては B のモデルから導出した状態遷移図と利用者の記述した状態遷移図を行列に落し込み、各要素の差の絶対値の合計が一番小さいものを状態遷移図の状態とモデルの集合に対応関係として扱うようにする。しかしこのやり方だとモデルの操作と状態遷移図の状態遷移の名前の対応について上手く対応関係が取れない場合が存在する。よって行列に落し込む際、名前に紐付けした手法を考える必要がある。

5.3 状態遷移数が異なる時の欠落条件

マッチングにおいて際状態遷移の数が異なった場合、どのような原因があるかについて述べたが、具体的にどのような条件が欠落しているかについてまでは言及出来なかった。今後の研究で欠落した具体的な条件について提案するアルゴリズムを考える必要がある。

6 終わりに

本研究では B-Method のモデルと状態遷移図、異なる二つの手法で要求を記述しそれらの整合性を確認することで仕様の正しさを検証するという考えを基に B-Method と状態遷移図を重ね合わせる手順と整合性がない時、どのような誤りが存在するのかを示した。しかし、いくつか考慮不足の点が存在するため今後の研究ではそれらの課題を解決する必要がある。

参考文献

[1] J-R Abrial, *The B-Book*CAMBRIDGE UNIVERSITY PRESS

[2] 楊 洋, エンティティの振る舞いに着目した Z による仕様記述と状態遷移規則の比較に基づく誤り検出法, 第 6 回情報科学技術フォーラム論文集, vol1.1 pp 119-120.(2007.09).