6A-04

拡張プレース/トランジションネットに基づく VDM 仕様の構築手法の提案

高木 智彦　　赤木 章紀

香川大学工学部

1. はじめに

PN（place/transition net）は，並行処理を含むソフトウェアの振舞いを形式的に記述することに適した表記法のひとつである．我々は，仕様書に基づいて，テスト対象ソフトウェアの期待される振舞いを PN によって記述し，体系的にテストする手法を提案した[1]．この手法の有効性は，テスト対象ソフトウェアの期待される振舞いを，PN によって如何に精密に表現できるかによって左右される．そこで本研究では，テスト対象ソフトウェアの複雑な振舞いを精密に表現できるように拡張された PN を示す．そしてこの拡張 PN に基づいて，実行可能な形式的仕様記述言語 VDM++ [2]によって記述された VDM（Vienna Development Method）仕様を構築する手法を提案する．VDM 仕様は，従来の PN よりも精密な動作シミュレーションが可能になるため，テストの有効性向上に役立つと考えられる．

本稿では，まず 2 節で拡張 PN を定義し，これと VDM 仕様との対応関係を明らかにする．そして 3 節で，ソフトウェアの仕様の動的検証やテストケースの設計，評価などにこの VDM 仕様を応用する方法を考察する．

2. 提案手法

2.1 拡張 PN

PN は主に，プレース，トークン，トランジションから構成される形式的モデルである．PN によってテスト対象ソフトウェアの期待される振舞いをモデリングする場合，プレースはテスト対象ソフトウェアを構成するコンポーネントの状態を，トークンは各コンポーネントの現在状態を表すと解釈できる．PN におけるトークンの配置は一般的にマーキングと呼ばれ，テスト対象ソフトウェアの状態に対応する．そして，トランジションの発火によって生じるトークンの配置の変化が，テスト対象ソフトウェアの状態遷移を表す．したがって，PN における連続するマーキングとトランジションの列をテストケースとして利用することができる．

PN におけるトランジションの発火条件は入力アークによって定義されるが，これだけでは実際のテスト対象ソフトウェアの複雑な振舞いを精密に表現することが困難な場合がある．特に，トランジションの発火に際して外部から入力される値（引数）や，変数の更新を伴う処理（アクション），変数の値に基づくトランジションの発火条件（ガード）は，テスト対象ソフトウェアの本質的な振舞いを表現する上で重要である．そこで本研究では，拡張 PN，すなわち，引数，アクション，およびガードを VDM++の文法に基づいて追記した PN を提案する．

図 1 は，単純化された ATM の入出金処理を表す拡張 PN である．「…」は紙面の都合で省略していることを意味する．「出金」トランジションに着目すると，まず，これの発火に際しては，自然数（nat 型）の引数「金額」をとること，そして，変数「残高」から「金額」を減算するというアクションを行うこと，さらに，このトランジションが発火するには「残高」が「金額」以上でなければならないというガードが存在することが定義されている．これらは，一般的な PN においては表現することが困難である．

2.2 VDM 仕様の構築

先述の拡張 PN に基づいて，VDM++で記述された VDM 仕様を構築する手法を提案する．

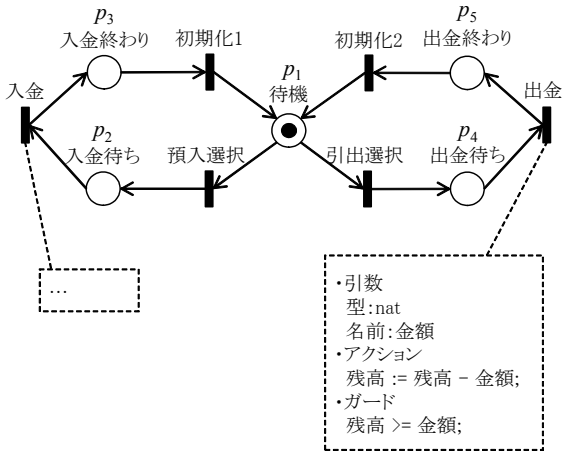

図 1. ATM の入出金処理を表す拡張 PN（一部）

Construction Technique of VDM Specifications based on Extended Place/Transition Nets
Tomohiko Takagi, Akinori Akagi
Faculty of Engineering, Kagawa University, Takamatsu, Kagawa 761-0396, Japan

図 2 は，図 1 に基づいて構築した VDM 仕様の例である．(a)(b)に示すように，拡張 PN のマーキング（プレースの定義を含む）をインスタンス変数として定義し，初期マーキングのトークン数で初期化する．そして(c)に示すように，アクションやガードで使用する変数があれば，同様にインスタンス変数として定義する．トランジションは(d)に示すように操作定義として記述する．たとえば，破線で囲んだ部分は，図 1 の「出金」トランジションに対応している．(e)の操作の引数の型と名前は，拡張 PN に与えられた定義に基づいている．また，操作の内容を，(f)の当該トランジション発火に伴うトークンの移動処理と，(g)のアクションから構成する．そして操作の事前条件として，従来の入力アークによるトランジション発火条件に加えて，(h)のガードを記述している．

拡張 PN と VDM 仕様の間のこのような明確な対応関係に基づいて，拡張 PN から VDM 仕様を生成することが可能であり，本研究ではツールを開発中である．

3. 考察

ソフトウェアの仕様の動的検証やテストケースの設計，評価などに，前節で述べた VDM 仕様を活用する方法を考察する．

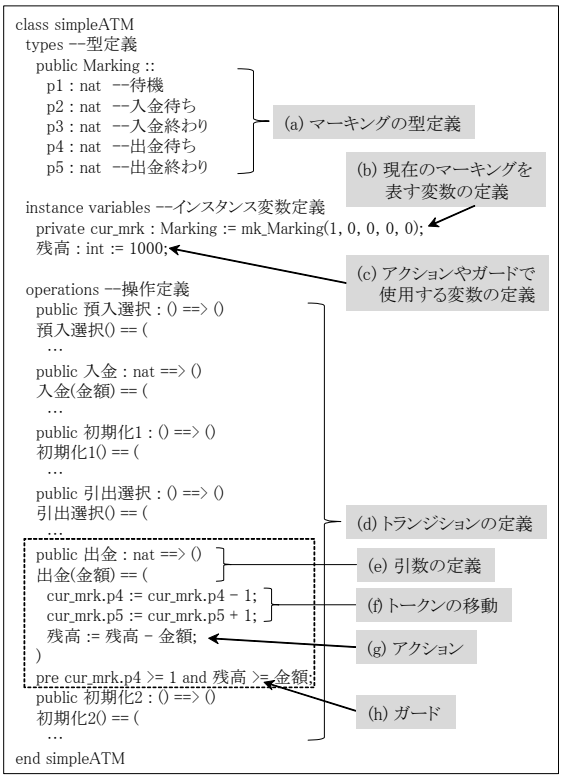

図 2. ATM の入出金処理の VDM 仕様（一部）

VDM++の導入によって拡張 PN は高い表現力を得ている．そこから生成される VDM 仕様には，従来の PN では表現が困難なテスト対象ソフトウェアの重要な振舞いを含めることができる．VDM 仕様はツール上で実行可能であり，仕様の検証をより効果的に行うことができると考えられる．仕様の動的検証において使用したテストケースは，その仕様に基づいて実装したソフトウェアをテストする際にも利用することができる．

本研究の VDM 仕様からテストケースを生成する際には，従来の PN 用のテスト網羅基準が利用できる．ただし，トランジションのガードを満たすテストデータを探索的に導出するなどの工夫が必要である．あるいは，網羅性を指向するのではなく，VDM 仕様に対して fault-proneness 情報を付与し，効果的なテストケースを最適化手法によって導出する方法も考えられる．

既存テストケースの品質を評価，改善したり，想定される誤りに効果的なテストケースを生成したりするために，本研究の VDM 仕様に基づいてミューテーションテストを行うことができる．これは Model-Based Mutation Testing の一種であり，VDM 仕様に対するミューテーション操作として，従来のコードベースのものや PN ベースのものを利用する．効果的なミュータントを生成するには，ミューテーション操作を探索的に適用し，メトリクスに基づく評価が高いものを選択する．

4. おわりに

テスト対象ソフトウェアの複雑な振舞いを精密に表現できるように拡張された PN に基づき，VDM++によって記述された VDM 仕様を構築する手法を提案した．今後の研究では，開発中のツールを拡張し，テストケースの最適化や評価，改善などの機能を実装することを検討する．

謝辞

本研究は JSPS 科研費 26730038 の助成を受けた．

参考文献

[1] T. Takagi, T. Arao, "Overview of a Place/Transition Net-Based Mutation Testing Framework to Obtain Test Cases Effective for Concurrent Software", *Proc. of 16th Int. Conf. on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, 3 pages, June 2015.

[2] J. Fitzgerald, P.G. Larsen, P. Mukherjee, N. Plat, M. Verhoef, *Validated Designs for Object-Oriented Systems*, Springer-Verlag London, 2005.