Zastosowanie metod formalnych

Karol Kozlowski
Wydzial elektryczny
Politechnika Warszawska

Katarzyna Mielęcka
Wydział elektryczny
Politechnika Warszawska

I. Wprowadzenie do metod formalnych

Metody formalne to matematyczne techniki wspomagające projektowanie i analizę systemów informatycznych. Ich istotę stanowią trzy kluczowe elementy:

- **Specyfikacja** - precyzyjny opis systemów za pomocą języków matematycznych (np. logika temporalna, rachunek procesów), eliminujący niejednoznaczności typowe dla dokumentacji tekstowej.
- **Weryfikacja** - formalne dowodzenie poprawności systemów poprzez:
  - model checking (np. narzędzie SPIN do weryfikacji protokołów).
  - dowody twierdzeń (np. w systemach Coq, Isabelle).
- **Automatyzacja analizy** - wykrywanie sprzeczności i luk na etapie modelowania (np. weryfikacja struktur wskaźnikowych w PVS).

Główną zaletą metod formalnych są **matematyczne gwarancje poprawności**, szczególnie istotne w systemach krytycznych (medycznych, transportowych). Pozwalają one identyfikować złożone błędy, takie jak zakleszczenia czy warunki wyścigu, które często wymykają się tradycyjnym metodom testowania.

II. System PVS

System PVS (Prototype Verification System) to zaawansowane narzędzie do opracowywania i weryfikacji formalnych specyfikacji, które pozwala na modelowanie i dowodzenie poprawności złożonych systemów. PVS wyróżnia się rozbudowaną składnią i możliwością operowania w logice wyższego rzędu, co umożliwia definiowanie własnych typów, podtypów oraz tworzenie teorii parametryzowanych. Dzięki temu system jest szczególnie przydatny do weryfikacji struktur dynamicznych, takich jak układy wskaźnikowe, gdzie często dochodzi do wycieków pamięci, nieprawidłowych dereferencji czy zakleszczeń w systemach współbieżnych. PVS umożliwia formalne określenie niezmienników i warunków spójności, a następnie ich automatyczną lub półautomatyczną weryfikację.

III. Formalna weryfikacja z użyciem TLA+

TLA+ (Temporal Logic of Actions) to język specyfikacji formalnej zaprojektowany przez Lesliego Lamporta do opisu i analizy systemów współbieżnych i rozproszonych. Umożliwia modelowanie systemu jako zbioru zmiennych oraz akcji – przejść między stanami – z wykorzystaniem logiki temporalnej i matematyki zbiorów. Język ten pozwala na tworzenie deklaratywnych specyfikacji, które opisują zamierzone zachowanie systemu niezależnie od jego implementacji. Weryfikacja poprawności odbywa się za pomocą narzędzia TLC, które stosuje technikę model checking, przeszukując przestrzeń stanów w celu sprawdzenia, czy system spełnia zadane własności.

TLA+ wykorzystuje trzy główne podejścia formalne. Pierwszym z nich jest matematyczne modelowanie systemu – precyzyjne określenie przestrzeni stanów i możliwych akcji, z użyciem obiektów takich jak zbiory, funkcje czy sekwencje. Drugim jest weryfikacja inwariantów, czyli logicznych warunków, które muszą być spełnione w każdym stanie systemu, co pozwala wykrywać istotne błędy, np. naruszenia spójności lub niedozwolone operacje. Trzecim podejściem jest analiza własności temporalnych w logice – umożliwiająca weryfikację zachowań systemu w czasie, takich jak osiągalność pewnych stanów, brak zakleszczeń czy deterministyczne następstwo zdarzeń. TLA+ znajduje zastosowanie w projektowaniu i weryfikacji złożonych systemów rozproszonych w środowiskach przemysłowych, m.in. w Amazonie, Microsoftcie i Google, gdzie wykorzystywany jest do analizy protokołów, systemów bazodanowych i usług chmurowych.

IV. Bibliografia

Literatura

[1] Leslie Lamport, *Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers*, Addison-Wesley, 2002.
[2] Chris Newcombe et al., *How Amazon Web Services Uses Formal Methods*, Communications of the ACM, 2015.
[3] Igor Konnov, Jure Kukovec, Thanh-Hai Tran, *TLA+ Model Checking Made Symbolic*, CAV 2019.
[4] Hillel Wayne, *Practical TLA+: Planning Driven Development*, Lospinato Books, 2018.
[5] S. Poreda, *Wykorzystanie metod formalnych do specyfikacji struktur wskaźnikowych*, Uniwersytet Warszawski, 2023.
[6] Sławomir Lasota, *Weryfikacja protokołu Needhama-Schroedera przy użyciu narzędzi SPIN i UPPAAL*, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski,
[7] Igor Wojnicki, *Weryfikacja własności systemów współbieżnych z użyciem metod formalnych*, Praca doktorska, Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, 2019,
[8] Leslie Lamport, *Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers*, Addison-Wesley, 2002.
[9] Chris Newcombe et al., *How Amazon Web Services Uses Formal Methods*, Communications of the ACM, 2015.
[10] Igor Konnov, Jure Kukovec, Thanh-Hai Tran, *TLA+ Model Checking Made Symbolic*, CAV 2019.
[11] Hillel Wayne, *Practical TLA+: Planning Driven Development*, Lospinato Books, 2018.
[12] S. Poreda, *Wykorzystanie metod formalnych do specyfikacji struktur wskaźnikowych*, Uniwersytet Warszawski, 2023.

[13] Chris Newcombe, Tim Rath, Fan Zhang, Bogdan Munteanu, Marc Brooker, Michael Deardeuff, *How Amazon Web Services Uses Formal Methods*, Communications of the ACM, Vol. 58, No. 4, pp. 66–73, 2015.