Zastosowanie metod formalnych

Karol Kozlowski,

Wydzial elektryczny, Politechnika Warszawska

5 kwietnia 2025

Czym sa metody formalne?

Definicja

Metody formalne to techniki matematyczne służące do:

- Specyfikacji - precyzyjnego opisu systemów za pomocą języków matematycznych (np. logika temporalna, rachunek procesów)
- Weryfikacji - dowodzenia poprawności systemów poprzez np. model checking (np. narzędzie SPIN) lub dowody twierdzeń (np. Coq, Isabelle)
- Automatyzacji analizy wykrywania sprzeczności lub luk w projektach na etapie modelowania (np. weryfikacja protokołów kryptograficznych)

Wiecej na ten temat mozna znalezc w [1].

Kluczowe zalety

- Formalne gwarancje poprawności - zapewnienie matematycznie udowodnionej poprawności systemów, szczególnie w przypadku wymagań bezpieczeństwa.
- Precyzyjna specyfikacja wymagań - eliminacja niejednoznaczności dzięki matematycznym modelom i notacjom.
- Wykrywanie złożonych błędów - identyfikacja problemów takich jak zakleszczenia (deadlocks) czy warunki wyścigu (race conditions), które trudno wykryć tradycyjnymi metodami testowania.

Wiecej na ten temat mozna znalezc w [3].

System PVS w pigułce

System PVS służy do opracowania i weryfikacji specyfikacji opisujących różne zagadnienia. PVS posiada rozbudowaną składnię i umożliwia operowanie w logice wyższego rzędu, definiowanie własnych typów i podtypów danych oraz tworzenie teorii parametryzowanych [2].

```
pointer_env [P: TYPE, T: TYPE]: THEORY
BEGIN
  pointer: TYPE = P + {nil}
  env: TYPE = [pointer -> (T + {undefined})]
END pointer_env
```

Problem: Weryfikacja struktur dynamicznych

Główne wyzwania

- **Złożoność struktur wskaźnikowych**:
  - Wycieki pamięci
  - Nieprawidłowe dereferencje
  - Zakleszczenia w systemach współbieżnych
- **Niejednoznaczność specyfikacji**:
  - Niewystarczalność logiki pierwszego rzędu
  - Potrzeba logiki wyższego rzędu (PVS)
- **Krytyczne zastosowania**:
  - Systemy sterowania (metro, koleje)
  - Aplikacje medyczne
  - Systemy awioniki i kosmiczne

Wiecej na ten temat mozna znalezc w [2].

Rozwiazanie PVS

- Formalna specyfikacja niezmienników
- Automatyczna weryfikacja warunków spójności
- Półautomatyczne dowodzenie poprawności

Przyklad

Przyklad

```
accessed_disjoint?(accessed? : pred[pointer[P]]) :
boolean =
FORALL(v11,v12 : (valid_finseq_list?)) :
   (accessed?(v11) AND accessed?(v12) AND v11
   /= v12 =>
    FORALL(1 : pointer[P]) : value?(1) =>
    NOT list_member?(1,v11) OR NOT
    list_member?(1,v12))
```

Przyklad

TCC1 dla niepustosci listy, TCC2 dla zachowania typu w rekurencji, TCC3 dla warunku stopu rekurencji

```
last_TCC1: OBLIGATION
FORALL (vl: (valid_finseq_list?)): NOT empty?(vl)


last_TCC2: OBLIGATION
FORALL (vl: (valid_finseq_list?)):
  length(vl) > 1 IMPLIES valid_finseq_list?(tail(vl))


last_TCC3: OBLIGATION
FORALL (vl: (valid_finseq_list?)):
  length(vl) > 1 IMPLIES length(tail(vl)) < length(vl)
```

Podsumowanie

- Metoda skuteczna dla list i drzew.
- Wymaga dużego nakładu pracy.
- Obiecujące wyniki dla systemów krytycznych.

Bibliografia

Sławomir Lasota.
Weryfikacja protokołu needhama-schroedera przy użyciu narzędzi SPIN i UPPAAL.

S. Poreda.
Wykorzystanie metod formalnych do specyfikacji struktur wskaźnikowych.
Uniwersytet Warszawski, 2023.

Igor Wojnicki.
Weryfikacja własności systemów współbieżnych z użyciem metod formalnych.
PhD thesis, Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, 2019.
Praca doktorska.