Zastosowanie metod formalnych

Karol Kozlowski
Wydzial 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. 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,