Zastosowanie metod formalnych do weryfikacji struktur wskaźnikowych w systemie PVS

Karol Kozlowski,

Wydzial elektryczny, Politechnika Warszawska

31 marca 2025

Metody formalne w inżynierii oprogramowania

Dlaczego metody formalne?

- Krytyczne systemy: medyczne, kosmiczne, transportowe
- Koszt błedów: katastrofy vs koszt wdrożenia
- Przykład: NASA i system PVS

Kluczowe zalety

- Pełna weryfikacja własności
- Wykrywanie wycieków pamieci
- Gwarancja niezmienników strukturalnych

System PVS w pigułce

- Logika wyższego rzedu
- Mechanizm dowodzenia twierdzeń
- Automatyczne generowanie TCC (Type Correctness Conditions)
- Parametryzacja teorii

```
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

- Dynamiczna alokacja pamieci
- Aliasing wskaźników
- Zachowanie niezmienników po operacjach
- Cykliczne struktury danych

Przykładowa specyfikacja listy

- $\forall l_1 \neq l_2 \Rightarrow \neg\exists n \in (l_1 \cap l_2)$
- $\forall p \in \text{pointer} \Rightarrow \exists! l : p \in l$

Proces weryfikacji w PVS

1. Modelowanie środowiska wskaźnikowego
2. Definicja niezmienników strukturalnych
3. Generowanie i dowodzenie TCC
4. Specyfikacja operacji (predykaty)
5. Dowód zachowania niezmienników

```
list_member?(l: pointer, vl: list): bool =
  IF nil?(vl) THEN false
  ELSE l = vl OR list_member?(l, next(vl))
  ENDIF
```

Studium przypadku: Lista jednokierunkowa

Kluczowe niezmienniki

- Spójność typów (TCC)
- Rozłaczność list
- Pełna pokrycie pamieci
- Brak cykli

Przykładowe twierdzenie

```
member_last: LEMMA
FORALL (vl: list):
  NOT nil?(vl) => list_member?(last(vl), vl)
```

Wyzwania i wnioski

Główne trudności

- Czasochłonność dowodów (do 1 tygodnia na predykat)
- Ograniczenia PVS w pracy z wieloma teoriami
- Trudności w automatyzacji dla grafów

Podsumowanie

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

Bibliografia


S. Owre et al. *PVS System Guide*. SRI International, 1999.


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