Obliczenia i wnioskowanie w systemie Coq

Małgorzata Biernacka

Instytut Informatyki UWr

Wykład 1
21.02.2019

Cel przedmiotu

Coq jako narzędzie wspierające interaktywne dowodzenie twierdzeń

- podstawy teoretyczne
- architektura systemu
- modelowanie problemów weryfikacyjnych
- konstrukcja dowodów jako obiektów formalnych

Organizacja zajęć

- zaliczenie pracowni: listy zadań, mały projekt/prezentacja
- egzamin końcowy
- zadania można oddawać tylko w czasie pracowni
- bieżące ogłoszenia, materiały i listy zadań w SKOSie

Motywacja

- problemy weryfikacji systemów/zagadnień informatycznych
- używamy narzędzi matematycznych do modelowania i wnioskowania o tych zagadnieniach
- używajmy narzędzi informatycznych, żeby wspierać wnioskowanie matematyczne

Korzyści

- zwiększenie pewności poprawności dowodu, algorytmu, itp.
- formalna weryfikacja ujawnia luki w rozumowaniu i pomaga wykrywać błędy
- możliwość automatyzacji wspiera tworzenie skomplikowanych dowodów
- dowodzenie jest jak programowanie

Zagadnienia

- konstrukcja i weryfikacja dowodów formalnych
- używamy analogii dowodzenie = programowanie
- wybór systemu formalnego – wyrażalność, łatwość użycia, intuicyjność
- modelowanie problemów – odpowiada doborowi struktur danych
- jak wygląda implementacja takiego systemu?

Teoria typów

- formalizm logiczny, którego obiektami są termy rachunku lambda
- konstruktory typów i system typów
- systemy oparte na izomorfizmie Curry'ego-Howarda (dowód - term, formuła - typ, dowód formuły jest termem typu tej formuły)
- nie musimy rozróżniać między termami i dowodami
- formalna reprezentacja dowodu pozwala na manipulację nim

Historia

- Automath - de Bruijn, 1967
- Mizar - A. Trybulec, 1973
- LCF - R. Milner, 1972
- HOL - M. Gordon, 1988
- Agda - Th. Coquand, 1990
- Coq - G. Huet, Th. Coquand, 1984

Przykładowe projekty akademickie

Coq, Isabelle/HOL

- CompCert (X. Leroy, INRIA) – certyfikowany kompilator języka C
- formalizacja semantyki (fragmentu) języka C++ (X. Leroy)
- weryfikacja Java Card
- formalizacja algebry relacji i DBMS (projekt Ynot)
- certyfikowane serwisy www (projekt Ynot)
- certyfikowany kompilator synchronicznego języka Lustre (M. Pouzet, INRIA)
- projekt DeepSpec
- formalizacja matematyki (twierdzenie o 4 kolorach, hipoteza Keplera, algebra)
- weryfikacja mikrojądra SO (seL4)
- back-end dla innych narzędzi

W przemyśle

- Adacore
- Gemalto
- ClearSy
- Internet of Trust
- SafeRiver

Wyzwania

Obecnie:

- stabilna podstawa teoretyczna
- rozwój technologii dowodzenia od 30 lat (inżynieria dowodzenia)
- potrzeby i możliwości formalnej weryfikacji oprogramowania

Rozwój:

- języki używane w asystentach dowodzenia (wyrażalność, styl, wygoda)
- środowiska dowodzenia (taktyki, biblioteki, efektywność)
- automatyzacja dowodzenia

Czym jest Coq

ang. *proof assistant/proof management system*

System interaktywnego dowodzenia twierdzeń

- system ogólnego przeznaczenia
- *język specyfikacji* – matematyczne definicje, twierdzenia, dowody, wykonywalne programy funkcyjne
- *język taktyk* – interaktywne środowisko dowodzenia
- *automatyzacja* dowodzenia
- programowalna automatyzacja dowodzenia
- ekstrakcja programów z dowodów

Potrzebne narzędzia

- rachunek lambda z typami prostymi
- wnioskowanie w systemach dedukcji naturalnej w logikach intuicjonistycznej i klasycznej
- definicje indukcyjne obiektów i własności
- dowód przez indukcję strukturalną; dowód przez indukcję względem drzewa wyprowadzenia