COQ

Daria Walukiewicz-Chrząszcz
Weryfikacja Wspomagana Komputerowo

4 czerwca 2012

Co to jest Coq

Coq to “System wspomagania dowodzenia” (Proof assistant)

Co to jest Coq

Coq to “System wspomagania dowodzenia” (Proof assistant)

`http://coq.inria.fr/`

Co to jest Coq

Coq to “System wspomagania dowodzenia” (Proof assistant)

`http://coq.inria.fr/`

- użytkownik musi sam wymyślić metodę dowodu,

Co to jest Coq

Coq to “System wspomagania dowodzenia” (Proof assistant)

`http://coq.inria.fr/`

- użytkownik musi sam wymyślić metodę dowodu,
- system weryfikuje, czy krok zaproponowany przez użytkownika jest dopuszczalny,

Co to jest Coq

Coq to “System wspomagania dowodzenia” (Proof assistant)

`http://coq.inria.fr/`

- użytkownik musi sam wymyślić metodę dowodu,
- system weryfikuje, czy krok zaproponowany przez użytkownika jest dopuszczalny,
- oraz rozwiązuje podproblemy, dla których zaimplementowano w nim algorytmy automatycznego dowodzenia,

Co to jest Coq

Coq to “System wspomagania dowodzenia” (Proof assistant)

`http://coq.inria.fr/`

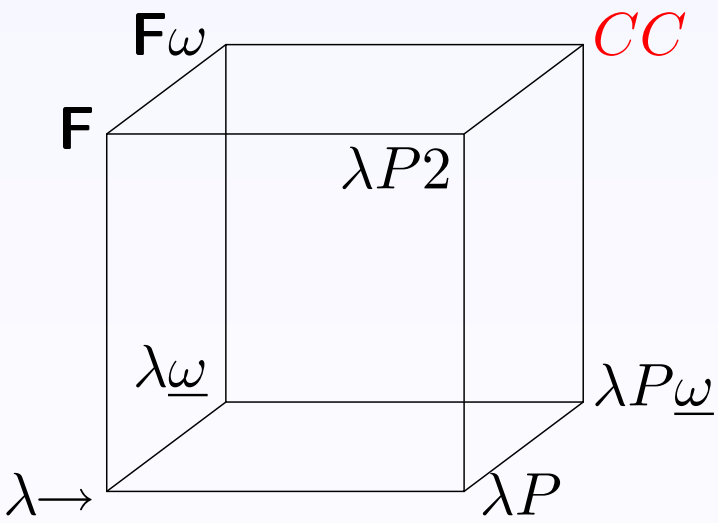
- użytkownik musi sam wymyślić metodę dowodu,
- system weryfikuje, czy krok zaproponowany przez użytkownika jest dopuszczalny,
- oraz rozwiązuje podproblemy, dla których zaimplementowano w nim algorytmy automatycznego dowodzenia,
- działanie systemu opiera się na stosowaniu reguł wnioskowania dla logiki, na której jest zbudowany.

Coq — formalizm

Coq — logika wyższego rzędu (rachunek konstrukcji (CC) + definicje indukcyjne)

Coq — formalizm

Coq — logika wyższego rzędu (rachunek konstrukcji (CC) + definicje indukcyjne)



↑ polimorfizm

↗ konstruktory typów

→ typy zależne

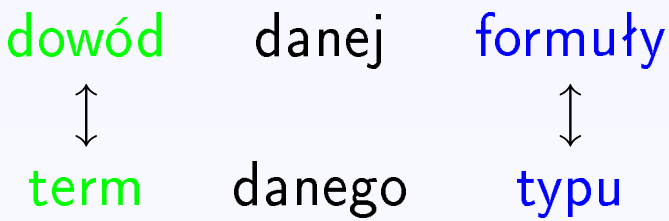
Dowodzenie w Coqu

Izomorfizm Curry'ego-Howarda

dowód danej formuły

Dowodzenie w Coqu

Izomorfizm Curry'ego-Howarda



Dowodzenie w Coqu

Izomorfizm Curry'ego-Howarda

dowód danej formuły

$\updownarrow$ $\updownarrow$

term danego typu

$$(A \to B \to C) \to (A \to B) \to (A \to C)$$

Izomorfizm Curry'ego-Howarda

dowód	danej	formuły
↕		↕
term	danego	typu

$$\lambda x^{A \to B \to C} \lambda y^{A \to B} \lambda z^{A}\ xz(yz) \ : \ (A \to B \to C) \to (A \to B) \to (A \to C)$$

Definicje indukcyjne w Coqu

- proste typy danych
  (np. liczby naturalne unarne)

Definicje indukcyjne w Coqu

- proste typy danych
  (np. liczby naturalne unarne)
- typy polimorficzne
  (np. listy)

Definicje indukcyjne w Coqu

- proste typy danych
  (np. liczby naturalne unarne)
- typy polimorficzne
  (np. listy)
- typy zależne
  (np. wektory danej długośc lub drzewa danego rozmiaru)

Definicje indukcyjne w Coqu

- proste typy danych
  (np. liczby naturalne unarne)
- typy polimorficzne
  (np. listy)
- typy zależne
  (np. wektory danej długośc lub drzewa danego rozmiaru)
- formuły
  (prawie cała logika Coqa)

Definicje indukcyjne w Coqu

- proste typy danych
  (np. liczby naturalne unarne)
- typy polimorficzne
  (np. listy)
- typy zależne
  (np. wektory danej długośc lub drzewa danego rozmiaru)
- formuły
  (prawie cała logika Coqa)
- predykaty
  (np. równość)

Coq – historia

1984 CoC - rachunek konstrukcji - G. Huet, T. Coquand

1989 pierwsze wydanie publiczne (wersja 4.10)

1991 Coq - rachunek konstrukcji indukcyjnych - C. Paulin (wersja 5.6)

⋮

2000 wersja 7.0 z nową (bezpieczną) architekturą

2003 wersja 7.4 z modułami

2004 wersja 8.0 z nową składnią

2009 wersja 8.2 z "type classes"

2012 wersja 8.4(beta) z eta-redukcją, strukturalną składnią dowodów

Znaczące formalizacje

- Zasadnicze Twierdzenie Algebry, Nijmegen 2000
- Formalizacja platformy JavaCard, Trusted Logic 2003
  September 2007: a big step in program certification in the real world: The Technology and Innovation group at Gemalto has successfully completed a Common Criteria (CC) evaluation on a Java Card based commercial product. This evaluation is the world's first CC certificate of a Java product involving EAL7 components (the official press release).
- Twierdzenie o 4 barwach, Cambridge 2004

Przykład 1: Sortowanie...

- Implementacja (Insertion Sort)
- Specyfikacja
- Dowód poprawności
- Ekstracja (Program w Ocamlu)

Podsumowanie

Coq - interaktywny system wspomagania dowodzenia

- Oparty o rachunek konstrukcji i izomorfizm Curry'ego-Howarda
- Definicje indukcyjne
- Język taktyk
- Sekcje, moduły
- Ekstrakcja do programów funkcyjnych