TODO

Sadržaj

1. Uvod

2. Coq

2.1. Što je Coq?

Alat za dokazivanje Coq[1], punog naziva *The Coq Proof Assistant*, programski je sustav pomoću kojeg korisnici mogu dokazivati matematičke tvrdnje. **Misao:** *ne sluzi samo tome, moze biti i opceniti funkcijski programski jezik, moze sluziti za programiranje sa zavisnim tipovima* Alat se temelji na λ-računu i teoriji tipova, a prva je inačica implementirana godine 1984. [1] Ovaj rad koristi inačicu 8.18 iz rujna godine 2023.

Program Coq može se pokrenuti u interaktivnom ili u skupnom načinu rada. Interaktivni način rada pokreće se naredbom `coqtop`, a korisniku omogućuje rad u ljusci sličnoj `bash` i `python` ljuskama. Interaktivna ljuska (također poznata pod imenom *toplevel*) služi unosu definicija i iskazivanju lema. Skupni način rada pokreće se naredbom `coqc`, a korisniku omogućuje semantičku provjeru i prevođenje izvornih datoteka u jednostavnije formate. Kod formaliziranja i dokazivanja, korisnik će najčešće koristiti interaktivni način rada, po mogućnosti kroz neku od dostupnih razvojnih okolina. [2]

Misao: *tu negdje treba spomenuti proof mode, koji je zaseban od toplevela*

Kao programski jezik, Coq se sastoji od više podjezika različitih namjena, kao što su *Vernacular*, *Gallina* i *Ltac*. **Vernacular** je jezik naredbi kojom korisnik komunicira sa sustavom (i u interaktivnom i u skupnom načinu rada); svaka Coq skripta (datoteka s nastavkom `.v`) je niz naredbi. Neke od najčešće korištenih naredbi su `Check`, `Definition`, `Inductive`, `Fixpoint` i `Lemma`. Pomoću naredbi za tvrdnje, kao što je `Lemma`, Coq prelazi iz *toplevela***Misao:** *treba bolji prevod* u način dokazivanja (engl.*proof mode*).

[1] `https://coq.inria.fr/`

[2] Autor rada koristio je paket *Proof General* za uređivač teksta *Emacs*. Druge često korištene okoline su *VsCoq* i *CoqIDE*.

Gallina je Coqov strogo statički tipiziran specifikacijski jezik. Glavnina programiranja u Coqu svodi se upravo na programiranje u Gallini. **Ltac** je Coqov netipiziran jezik za definiciju taktika. Taktike su pomoćne naredbe kojima se u načinu dokazivanja konstruira dokaz. Primjeri taktika su `intros`, `destruct`, `apply` i `rewrite`.

Misao: *spomenuti da je jezgra Coqa, a.k.a. typechecker, jako mala i zato joj mozemo vjerovati, de Bruijnovo nacelo za dokazivace*

Programski sustav type checker, kompajler

Skup jezika Vernacular, Gallina, Ltac, Ltac2 ...

Teorija tipova CoC, CIC, PCUIC, pravila "izvoda" i redukcije

usporedba s ostalim zavisnim jezicima

2.2. Programiranje u Coqu

Funkcijsko programiranje neki jednostavni primjer

Definiranje funkcija `Definition`, `Fixpoint`, `CoFixpoint`

Definiranje tipova `Inductive`, `CoInductive`

Ekstrakcija OCaml, Haskell, spomenuti da se radi na verificiranoj ekstrakciji

2.3. Kumulativna hijerarhija tipova

Ukratko objasniti. Lijepa skica koja prikazuje gdje su `nat`, `nat -> nat`, `nat -> Set`, `Prop -> Prop`, i njima srodni. Razlika između `Set` i `Prop`.

2.4. Propozicije i tipovi, dokazi i programi

Ukratko objasniti što je to Curry–Howard, možda najlakše pomoću BHK interpretacije.

Primjeri dokaznih terma, recimo ručno napisan dokazni term za komutiranje univerzalnih kvantifikacija, pa neki jednostavni induktivni dokaz.

Principi indukcije kao rekurzivne funkcije.

2.5. Ograničenja u programiranju i dokazivanju

Tu prvenstveno mislim na uvjete pozitivnosti i produktivnosti za induktivne i koinduktivne tipove, te na eliminaciju propozicija kod definiranja nečega u `Type`.

3. Logika prvog reda s induktivnim definicijama

3.1. Sintaksa

Signatura. Term. Formula.

3.2. Semantika

Struktura. Okolina. Evaluacija. Relacija ispunjivosti. Substitution sanity leme.

3.3. Standardni modeli

Produkcije. Skup induktivnih definicija. Operator φ_Φ. Aproksimanti. Standardni model.

3.4. Sistem sekvenata s induktivnim definicijama

LKID. Dopustiva pravila. Primjeri dokaza.

3.5. Adekvatnost

Lokalne adekvatnosti za pravila izvoda. Glavni teorem.

4. Ciklički dokazi

Koinduktivni tip podatka i koinduktivna propozicija. Jedan primjer su `Streamovi` i predikat `Infinite`. Jednostavniji primjer bi možda bio koinduktivni `nat` i koinduktivni `le`.

Kako bi izgledali ciklički dokazi u LKID? Ono što je tamo "repeat funkcija" je u Coqu `cofix`.

5. Zaključak

Literatura

[1] The Coq Development Team, “The Coq Reference Manual, Release 8.18.0”, https://coq.inria.fr/doc/v8.18/refman/, 2023.

[2] A. Chlipala, *Certified programming with dependent types: a pragmatic introduction to the Coq proof assistant*. MIT Press, 2022.

[3] Y. Bertot i P. Castéran, *Interactive theorem proving and program development: Coq'Art: the calculus of inductive constructions*. Springer Science & Business Media, 2013.

[4] G. Smolka, “Modeling and proving in computational type theory using the Coq proof assistant”, https://www.ps.uni-saarland.de/~smolka/drafts/mpctt.pdf, 2021., [mrežno; stranica posjećena: lipanj 2024.].

[5] B. C. Pierce, A. A. de Amorim, C. Casinghino, M. Gaboardi, M. Greenberg, C. Hriţcu, V. Sjöberg, i B. Yorgey, *Logical Foundations*, ser. Software Foundations, B. C. Pierce, Ur. Electronic textbook, 2023., sv. 1, version 6.5, http://softwarefoundations.cis.upenn.edu.

[6] B. C. Pierce, A. A. de Amorim, C. Casinghino, M. Gaboardi, M. Greenberg, C. Hriţcu, V. Sjöberg, A. Tolmach, i B. Yorgey, *Programming Language Foundations*, ser. Software Foundations, B. C. Pierce, Ur. Electronic textbook, 2024., sv. 2, version 6.5, http://softwarefoundations.cis.upenn.edu.

[7] A. W. Appel, *Verified Functional Algorithms*, ser. Software Foundations, B. C. Pierce, Ur. Electronic textbook, 2023., sv. 3, version 1.5.4, http://softwarefoundations.cis.upenn.edu.

[8] T. Coquand i G. Huet, “The calculus of constructions”, INRIA, teh. izv. RR-0530, svibanj 1986. [Mrežno]. Adresa: https://inria.hal.science/inria-00076024

[9] Y. Forster, D. Kirst, i D. Wehr, “Completeness theorems for first-order logic analysed in constructive type theory: Extended version”, *Journal of Logic and Computation*, sv. 31, br. 1, str. 112–151, 2021.

Sažetak

Primjene Coq alata za dokazivanje u matematici i računarstvu

Miho Hren

Unesite sažetak na hrvatskom.

Ključne riječi: prva ključna riječ; druga ključna riječ; treća ključna riječ

Abstract

Applications of the Coq Proof Assistant in mathematics and computer science

Miho Hren

Enter the abstract in English.

Keywords: the first keyword; the second keyword; the third keyword