Primjene Coq alata za dokazivanje u matematici i računarstvu

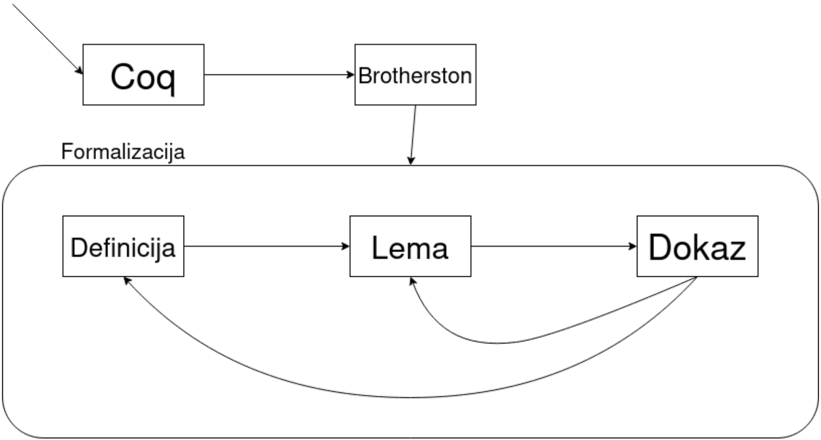
Logika prvog reda s induktivnim definicijama

Miho Hren

Mentori: Vedran Čačić, Marko Doko + Ante Đerek
Fakultet Elektrotehnike i Računarstva

2023./2024.

Proces



Sintaksa: signatura

```
Structure signature := {
    FuncS : Set;
    fun_ar : FuncS -> nat;
    PredS : Set;
    pred_ar : PredS -> nat;
    IndPredS : Set;
    indpred_ar : IndPredS -> nat;
  }.

Context {Σ : signature}.
```

Peanova signatura

$$\sigma_{PA} = \{\{o^0, s^1, +^2, \cdot^2\}, \{=^2\}, \{Nat^1, Even^1, Odd^1\}\}$$

Sintaksa: termi, formule

```
Inductive term  : Set :=
| var_term : var -> term
| TFunc : forall (f : FuncS Σ),
    vec term (fun_ar f) -> term.

Inductive formula : Set :=
| FPred (P : PredS Σ)
    : vec (term Σ) (pred_ar P) -> formula
| FIndPred (P : IndPredS Σ)
    : vec (term Σ) (indpred_ar P) -> formula
| FNeg : formula -> formula
| FImp : formula -> formula -> formula
| FAll : formula -> formula.
```

Sintaksa: produkcije

$$\frac{Q_1 \mathsf{u}_1 \ldots Q_n \mathsf{u}_n \quad P_1 \mathsf{v}_1 \ldots P_m \mathsf{v}_m}{P \mathsf{t}}$$

```
Record production :=
  mkProd {
      preds
        : list {P: PredS Σ & vec (term Σ) (pred_ar P)};
      indpreds
        : list {P: IndPredS Σ & vec (term Σ) (indpred_ar P)};
      indcons : IndPredS Σ;
      indargs : vec (term Σ) (indpred_ar indcons);
    }.
```

Biti prirodan broj.

$$\frac{}{Nat(o)} \qquad \frac{Nat(x)}{Nat(s(x))}$$

Biti paran, odnosno neparan broj.

$$\frac{}{Even(o)} \qquad \frac{Odd(x)}{Even(s(x))} \qquad \frac{Even(x)}{Odd(s(x))}$$

Semantika: struktura, okolina

```
Structure structure := {
    domain :> Set;
    interpF (f : FuncS Σ)
        : vec domain (fun_ar f) -> domain;
    interpP (P : PredS Σ)
        : vec domain (pred_ar P) -> Prop;
    interpIP (P : IndPredS Σ)
        : vec domain (indpred_ar P) -> Prop;
  }.
```

```
Definition env := var -> M.
```

Standardna Peanova struktura

$$M_{PA} = (\mathbb{N}, 0, S, +, \cdot, =, \mathbb{N}, \mathbb{E}, \mathbb{O})$$

Semantika: istinitost formule

```
Fixpoint Sat (ρ : env M) (F : formula Σ) : Prop :=
  match F with
  | FPred P args => interpP P (V.map (eval ρ) args)
  | FIndPred P args => interpIP P (V.map (eval ρ) args)
  | FNeg G => ~ Sat ρ G
  | FImp F G => Sat ρ F -> Sat ρ G
  | FAll G => forall d, Sat (d .: ρ) G
  end.
```

Primjer

$$(M_{PA}, \rho) \models \forall x, Nat(x) \rightarrow Even(x) \vee Odd(x)$$

Semantika: produkcije

```
Definition InterpInd :=
    forall P : IndPredS Σ, vec M (indpred_ar P) -> Prop.

Fixpoint φ_Φ_n (α : nat) : InterpInd :=
  match α with
  | 0 => fun _ _ => False
  | S α => φ_Φ (φ_Φ_n α)
  end.

Definition φ_Φ_ω : InterpInd :=
    fun P v => exists α, φ_Φ_n α P v.
```

Semantika: standardni modeli

```
Lemma φ_Φ_ω_least_prefixed : least prefixed φ_Φ_ω.

Definition standard_model
  (Φ: IndDefSet Σ)
  (M : structure Σ)
  : Prop :=
    forall (P : IndPredS Σ) ts,
      interpIP P ts <-> φ_Φ_ω Φ M P ts.
```

Sekvente

```
Inductive sequent : Set :=
| mkSeq (Γ Δ : list (formula Σ)).
```

$$\Gamma \vdash \Delta$$

```
Definition Sat_sequent (s : sequent) : Prop :=
  let '(Γ ⊢ Δ) := s in
  forall (M : structure Σ),
      standard_model Φ M -> forall (ρ : env M),
        (forall φ, In φ Γ -> ρ ⊨ φ) ->
        exists ψ, In ψ Δ /\ ρ ⊨ ψ.
```

$$\Gamma \models \Delta$$

Sistem sekvenata: „obična” pravila izvoda

$$\frac{\Gamma \cap \Delta \neq \varnothing}{\Gamma \vdash \Delta}\,(Ax) \qquad \frac{\Gamma' \vdash \Delta' \qquad \Gamma' \subseteq \Gamma \qquad \Delta' \subseteq \Delta}{\Gamma \subseteq \Delta}\,(Wk)$$

$$\frac{\Gamma \vdash \varphi, \Delta \qquad \varphi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta}\,(Cut) \qquad \frac{\Gamma \vdash \Delta}{\Gamma[\sigma] \vdash \Delta[\sigma]}\,(Subst)$$

$$\frac{\Gamma \vdash \varphi, \Delta}{\neg\varphi, \Gamma \vdash \Delta}\,(NegL) \qquad \frac{\varphi, \Gamma \vdash \Delta}{\Gamma \vdash \neg\varphi, \Delta}\,(NegR)$$

$$\frac{\Gamma \vdash \varphi, \Delta \qquad \psi, \Gamma \vdash \Delta}{\varphi \to \psi, \Gamma \vdash \Delta}\,(ImpL) \qquad \frac{\varphi, \Gamma \vdash \psi, \Delta}{\Gamma \vdash \varphi \to \psi, \Delta}\,(ImpR)$$

$$\frac{\varphi[t \cdot \sigma_{id}], \Gamma \vdash \Delta}{\forall\varphi, \Gamma \vdash \Delta}\,(AllL) \qquad \frac{\Gamma^{\uparrow} \vdash \varphi, \Delta^{\uparrow}}{\Gamma \vdash \forall\varphi, \Delta}\,(AllR)$$

Sistem sekvenata: produkcijska pravila

Produkcija

$$\frac{Q_1\mathrm{u}_1 \ldots Q_n\mathrm{u}_n \qquad P_1\mathrm{v}_1 \ldots P_m\mathrm{v}_m}{P\mathrm{t}}$$

Pravilo

$$\frac{\Gamma \vdash Q_1\mathrm{u}_1[\sigma], \Delta \quad \ldots \quad \Gamma \vdash Q_n\mathrm{u}_n[\sigma], \Delta \qquad \Gamma \vdash P_1\mathrm{v}_1[\sigma], \Delta \quad \ldots \quad \Gamma \vdash P_m\mathrm{v}_m[\sigma], \Delta}{\Gamma \vdash P\mathrm{t}[\sigma], \Delta}$$

Primjer

$$\frac{Odd(x)}{Even(s(x))} \qquad\qquad \frac{\Gamma \vdash Odd(x), \Delta}{\Gamma \vdash Even(s(x)), \Delta}$$

Primjer

$$\frac{\Gamma \vdash G(o), \Delta \qquad G(x), \Gamma \vdash G(s(x)), \Delta \qquad G(t), \Gamma \vdash \Delta}{Nat(t), \Gamma \vdash \Delta}\,(NatInd)$$

Primjer primjene pravila *NatInd*

$$\frac{\dfrac{\vdots}{\vdash Eo \lor Oo, Ex \lor Ox} \qquad \dfrac{\vdots}{Ey \lor Oy \vdash Esy \lor Osy, Ex \lor Ox} \qquad \dfrac{\vdots}{Ex \lor Ox \vdash Ex \lor Ox}}{Nx \vdash Ex \lor Ox}$$

Adekvatnost

Teorem

Ako je sekventa **dokaziva** u sustavu *LKID*,
onda je **istinita** na standardnim modelima.

Dokaz

Indukcijom po strukturi dokaza sekvente $\Gamma \vdash \Delta$.

Problemi kod formalizacije dokaza:

- što je pisac htio reći?
- implicitne pretpostavke
- implicitno domensko znanje

Zaključak

Formalizacija

- sintaksa i semantika logike prvog reda s induktivnim definicijama
- dokazni sustav *LKID*
- oko **140 lema i dokaza**

Tekst

- osnovno o Coqu
- **opis formalizacije**
- ilustracija cikličkih dokaza

Što dalje?

- potpunost
- dokazni sustav $CLKID^{\omega}$
- formalno verificirani dokazivač teorema