Primjene Coq alata za dokazivanje u matematici i računarstvu

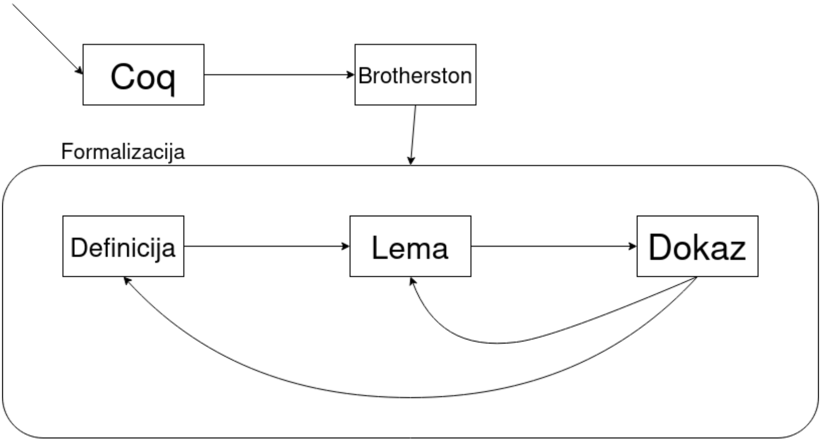
Logika prvog reda s induktivnim definicijama

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;
  }.
```

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

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

```
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

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

Semantika: produkcije