Univerzitet u Beogradu
Matematički fakultet
Katedra za računarstvo i informatiku

Šifra predmeta: R265
04.03.2024.

Uvod u interaktivno dokazivanje teorema

Vežbe 03

Zadatak 1 *Intuicionistička pravila prirodne dedukcije u iskaznoj logici*

Diskutovati o pravilima uvođenja i pravilima eliminacije prirodne dedukcije iskazne logike. Pomoću ključne reči *thm* ispitati svako pravilo prirodne dedukcije. Primeniti odgovarajuće pravilo prirodne dedukcije na jednostavnim formulama i diskutovati o cilju koga treba dokazati pre i posle primene tog pravila.

Uvodjenje konjukcije: *conjI*

thm *conjI*

lemma $A \wedge B$
  apply (*rule conjI*)

Uvodjenje disjunkcije: *disjI1*/*disjI2*

thm *disjI1*
thm *disjI2*

lemma $A \vee B$
  apply (*rule disjI2*)

Uvodjenje implikacije: *impI*

thm *impI*

lemma $A \longrightarrow B$
  apply (*rule impI*)

Uvodjenje ekvivalencije: *iffI*

thm *iffI*

lemma $A \longleftrightarrow B$
  apply (*rule iffI*)

Uvodjenje negacije: *notI*

thm *notI*

lemma $\neg A$
  apply (*rule notI*)

Eliminacija konjukcije. *conjE*

thm *conjE*

lemma $A \wedge B \Longrightarrow C$
  apply (*erule conjE*)

Eliminacija disjunkcije. *disjE*

thm *disjE*

lemma $A \vee B \Longrightarrow C$
  apply (*erule disjE*)

Eliminacija implikacije. *impE*

thm *impE*

lemma $A \longrightarrow B \Longrightarrow C$
  apply (*erule impE*)

Eliminacija ekvivalencije. *iffE*

thm *iffE*

lemma $A \longleftrightarrow B \Longrightarrow C$
  apply (*erule iffE*)

Eliminacija negacije. *notE*

thm *notE*

lemma $\neg\ A \Longrightarrow B$
  apply (*erule notE*)

Zadatak 2 *Dokazi u prirodnoj dedukciji*

Pokazati da su sledeće formule tautologija u iskaznoj logici. Dozvoljeno je korišćenje samo intuicionističkih pravila prirodne dedukcije.

lemma $A \wedge B \longrightarrow B \wedge A$
  apply (*rule impI*)
  apply (*erule conjE*)
  apply (*rule conjI*)
   apply *assumption* +
  done

lemma $A \vee B \longrightarrow B \vee A$
  apply (*rule impI*)
  apply (*erule disjE*)
   apply (*rule disjI2*)
   apply *assumption*
  apply (*rule disjI1*)

```
  apply assumption
  done

lemma A ∧ B ⟶ A ∨ B
  apply (rule impI)
  apply (erule conjE)
  apply (rule disjI1)
  apply assumption
  done

lemma (A ∧ B ⟶ C) ⟶ (A ⟶ (B ⟶ C))
  apply (rule impI) +
  apply (erule impE)
   apply (rule conjI)
    apply assumption +
  done

lemma (A ⟶ (B ⟶ C)) ⟶ (A ∧ B ⟶ C)
  apply (rule impI) +
  apply (erule impE)
   apply (erule conjE)
   apply assumption
  apply (erule conjE)
  apply (erule impE)
   apply assumption +
  done

lemma ¬ (A ∨ B) ⟶ ¬ A ∧ ¬ B
  apply (rule impI)
  apply (rule conjI)
   apply (rule notI)
   apply (erule notE)
   apply (rule disjI1)
   apply assumption
  apply (rule notI)
  apply (erule notE)
  apply (rule disjI2)
  apply assumption
  done

lemma ¬ A ∧ ¬ B ⟶ ¬ (A ∨ B)
  apply (rule impI)
  apply (rule notI)
  apply (erule conjE)
  apply (erule disjE)
   apply (erule notE)
   apply assumption
  apply (erule notE) +
  apply assumption
  done
```

lemma $\neg (A \longleftrightarrow \neg A)$
  apply $(rule\ notI)$
  apply $(erule\ iffE)$
  apply $(erule\ impE)$ **back**
   apply $(rule\ notI)$
   apply $(erule\ impE)$
    apply *assumption*
   apply $(erule\ notE)$
   apply *assumption*
  apply $(erule\ impE)$
   apply *assumption*
  apply $(erule\ notE)$
  apply *assumption*
  done

Dodatni primeri

lemma $(Q \longrightarrow R) \wedge (R \longrightarrow P \wedge Q) \wedge (P \longrightarrow Q \vee R) \longrightarrow (P \longleftrightarrow Q)$
  apply $(rule\ impI)$
  apply $(rule\ iffI)$
   apply $(erule\ conjE)+$
   apply $(erule\ impE)$ **back back**
    apply *assumption*
   apply $(erule\ disjE)$
    apply *assumption*
   apply $(erule\ impE)$ **back**
    apply *assumption*
   apply $(erule\ conjE)$
   apply *assumption*
  apply $(erule\ conjE)+$
  apply $(erule\ impE)$
   apply *assumption*
  apply $(erule\ impE)$
   apply *assumption*
  apply $(erule\ conjE)$
  apply *assumption*
  done

lemma $(P \longrightarrow Q) \wedge (Q \longrightarrow R) \longrightarrow (P \longrightarrow Q \wedge R)$
  apply $(rule\ impI)+$
  apply $(erule\ conjE)$
  apply $(erule\ impE)$
   apply *assumption*
  apply $(rule\ conjI)$
   apply *assumption*
  apply $(erule\ impE)$
   apply *assumption* +
  done

lemma $(P \longrightarrow Q) \wedge \neg Q \longrightarrow \neg P$
  apply $(rule\ impI)$
  apply $(rule\ notI)$

apply (*erule conjE*)
apply (*erule impE*)
 apply *assumption*
apply (*erule notE*)
apply *assumption*
done

lemma $(P \longrightarrow (Q \longrightarrow R)) \longrightarrow (Q \longrightarrow (P \longrightarrow R))$
apply (*rule impI*) +
apply (*erule impE*)
 apply *assumption*
apply (*erule impE*)
 apply *assumption* +
done

lemma $\neg\ (P \wedge \neg P)$
apply (*rule notI*)
apply (*erule conjE*)
apply (*erule notE*)
apply *assumption*
done

lemma $A \wedge (B \vee C\ ) \longrightarrow (A \wedge B) \vee (A \wedge C)$
apply (*rule impI*)
apply (*erule conjE*)
apply (*erule disjE*)
 apply (*rule disjI1*)
 apply (*rule conjI*)
  apply *assumption* +
apply (*rule disjI2*)
apply (*rule conjI*)
apply *assumption* +
done

lemma $\neg\ (A \wedge B) \longrightarrow (A \longrightarrow \neg\ B)$
apply (*rule impI*) +
apply (*rule notI*)
apply (*erule notE*)
apply (*rule conjI*)
 apply *assumption* +
done

lemma $(A \longrightarrow C\ ) \wedge (B \longrightarrow \neg\ C\ ) \longrightarrow \neg\ (A \wedge B)$
apply (*rule impI*)
apply (*rule notI*)
apply (*erule conjE*) +
apply (*erule impE*)
 apply *assumption*
apply (*erule impE*)
 apply *assumption*

```
  apply (erule notE)
  apply assumption
  done

lemma (A ∧ B) ⟶ ((A ⟶ C ) ⟶ ¬ (B ⟶ ¬ C ))
  apply (rule impI) +
  apply (rule notI)
  apply (erule conjE)
  apply (erule impE)
   apply assumption
  apply (erule impE)
   apply assumption
  apply (erule notE)
  apply assumption
  done

lemma (A ⟷ B) ⟶ (¬ A ⟷ ¬ B)
  apply (rule impI)
  apply (erule iffE)
  apply (rule iffI)
   apply (rule notI)
   apply (erule impE) back
    apply assumption
   apply (erule notE)
   apply assumption
  apply (rule notI)
  apply (erule impE)
   apply assumption
  apply (erule notE)
  apply assumption
  done

lemma A ⟶ ¬ ¬ A
  apply (rule impI)
  apply (rule notI)
  apply (erule notE)
  apply assumption
  done

lemma ¬ (A ⟷ ¬ A)
  apply (rule notI)
  apply (erule iffE)
  apply (erule impE) back
   apply (rule notI)
   apply (erule impE)
    apply assumption
  apply (erule notE)
   apply assumption
  apply (erule impE)
   apply assumption
  apply (erule notE)
```

apply *assumption*
done

lemma $(A \longrightarrow B) \longrightarrow (\neg\ B \longrightarrow \neg\ A)$
apply (*rule impI*) +
apply (*rule notI*)
apply (*erule impE*)
 apply *assumption*
apply (*erule notE*)
apply *assumption*
done

lemma $\neg\ A \vee B \longrightarrow (A \longrightarrow B)$
apply (*rule impI*) +
apply (*erule disjE*)
 apply (*erule notE*)
 apply *assumption* +
done

Zadatak 3 *Intuicionistička pravila prirodne dedukcije u logici prvog reda*

Diskutovati o pravilima uvođenja i pravilima eliminacije prirodne dedukcije u logici prvog reda. Pomoću ključne reči *thm* ispitati svako pravilo prirodne dedukcije. Primeniti odgovarajuće pravilo prirodne dedukcije na jednostavnim formulama i diskutovati o cilju koga treba dokazati pre i posle primene tog pravila.

Za logiku prvog reda pored pravila prirodne dedukcije iskazne logike, važe i pravila uvođenja i elimenacije kvantifikatora.

Uvođenje univerzalnog kvantifikatora: *allI*

thm *allI*

lemma $\forall\ x.\ P\ x$
apply (*rule allI*)

Eliminacija univerzalnog kvantifikatora: *allE*

thm *allE*

lemma $\forall\ x.\ P\ x \Longrightarrow A$
apply (*erule-tac* $x = t$ **in** *allE*)

Uvođenje egzistencijalnog kvantifikatora: *exI*

thm *exI*

lemma $\exists\ x.\ P\ x$
apply (*rule-tac* $x = t$ **in** *exI*)

Eliminacija egzistencijalnog kvantifikatora: *exE*

thm *exE*

lemma $\exists\ x.\ P\ x \Longrightarrow A$
apply (*erule exE*)

Zadatak 4 *Dokazi u prirodnoj dedukciji*

Pokazati da su sledeće formule valjane u logici prvog reda. Dozvoljeno je korišćenje samo intuicionističkih pravila prirodne dedukcije.

lemma $(\forall\ x.\ Man\ x \longrightarrow Mortal\ x) \wedge Man\ Socrates \longrightarrow Mortal\ Socrates$
apply (*rule impI*)
apply (*erule conjE*)
apply (*erule-tac x = Socrates* **in** *allE*)
apply (*erule impE*)
apply *assumption* +
done

lemma *de-Morgan-1*: $(\exists\ x.\ \neg\ P\ x) \longrightarrow \neg\ (\forall\ x.\ P\ x)$
apply (*rule impI*)
apply (*rule notI*)
apply (*erule exE*)
apply (*erule-tac x = x* **in** *allE*)
apply (*erule notE*)
apply *assumption*
done

lemma *de-Morgan-2*: $(\forall\ x.\ \neg\ P\ x) \longrightarrow (\nexists\ x.\ P\ x)$
apply (*rule impI*)
apply (*rule notI*)
apply (*erule exE*)
apply (*erule-tac x = x* **in** *allE*)
apply (*erule notE*)
apply *assumption*
done

lemma *de-Morgan-3*: $(\nexists\ x.\ P\ x) \longrightarrow (\forall\ x.\ \neg\ P\ x)$
apply (*rule impI*)
apply (*rule allI*)
apply (*rule notI*)
apply (*erule notE*)
apply (*rule-tac x = x* **in** *exI*)
apply *assumption*
done

lemma $(\exists\ x.\ P\ x) \wedge (\forall\ x.\ P\ x \longrightarrow Q\ x) \longrightarrow (\exists\ x.\ Q\ x)$
apply (*rule impI*)
apply (*erule conjE*)
apply (*erule exE*)
apply (*erule-tac x = x* **in** *allE*)
apply (*rule-tac x = x* **in** *exI*)
apply (*erule impE*)

apply *assumption* +
done

Dodatni primeri:

lemma $(\forall\ m.\ Man\ m \longrightarrow Mortal\ m) \wedge$
$(\forall\ g.\ Greek\ g \longrightarrow Man\ g) \longrightarrow$
$(\forall\ a.\ Greek\ a \longrightarrow Mortal\ a)$
apply (*rule impI*)
apply (*erule conjE*)
apply (*rule allI*)
apply (*rule impI*)
apply (*erule-tac* $x = a$ **in** *allE*) +
apply (*erule impE*) +
apply *assumption* +
done

lemma $(\forall\ a.\ P\ a \longrightarrow Q\ a) \wedge (\forall\ b.\ P\ b) \longrightarrow (\forall\ x.\ Q\ x)$
apply (*rule impI*)
apply (*erule conjE*)
apply (*rule allI*)
apply (*erule-tac* $x = x$ **in** *allE*) +
apply (*erule impE*)
apply *assumption* +
done

lemma $(\exists\ x.\ A\ x \vee B\ x) \longrightarrow (\exists\ x.\ A\ x) \vee (\exists\ x.\ B\ x)$
apply (*rule impI*)
apply (*erule exE*)
apply (*erule disjE*)
apply (*rule disjI1*)
apply (*rule-tac* $x = x$ **in** *exI*)
apply *assumption*
apply (*rule disjI2*)
apply (*rule-tac* $x = x$ **in** *exI*)
apply *assumption*
done

lemma $(\forall\ x.\ A\ x \longrightarrow \neg\ B\ x) \longrightarrow (\nexists\ x.\ A\ x \wedge B\ x)$
apply (*rule impI*)
apply (*rule notI*)
apply (*erule exE*)
apply (*erule conjE*)
apply (*erule-tac* $x = x$ **in** *allE*)
apply (*erule impE*)
apply *assumption*
apply (*erule notE*)
apply *assumption*
done

Formulisati i dokazati naredna tvrđenja.

Ako za svaki broj koji nije paran važi da je neparan;

i ako za svaki neparan broj važi da nije paran;
pokazati da onda za svaki broj važi da nije istovremeno i paran i neparan

lemma
$(\forall\ x.\ \neg\ Paran\ x \longrightarrow Neparan\ x) \wedge$
$(\forall\ x.\ Neparan\ x \longrightarrow \neg\ Paran\ x) \longrightarrow$
$(\forall\ x.\ \neg\ (Paran\ x \wedge Neparan\ x))$
apply (*rule impI*)
apply (*erule conjE*)
apply (*rule allI*)
apply (*rule notI*)
apply (*erule conjE*)
apply (*erule-tac x = x* **in** *allE*) +
apply (*erule impE*) +
apply *assumption* +
apply (*erule impE*)
apply *assumption*
apply (*erule notE*)
apply *assumption*
done

Ako svaki konj ima potkovice;
i ako ne postoji čovek koji ima potkovice;
i ako znamo da postoji makar jedan čovek;
dokazati da postoji čovek koji nije konj.

lemma $(\forall\ x.\ Konj\ x \longrightarrow Potkovice\ x) \wedge$
$(\nexists\ x.\ Covek\ x \wedge Potkovice\ x) \wedge$
$(\exists\ x.\ Covek\ x) \longrightarrow$
$(\exists\ x.\ Covek\ x \wedge \neg\ Konj\ x)$
apply (*rule impI*)
apply (*erule conjE*) +
apply (*erule exE*)
apply (*erule-tac x = x* **in** *allE*)
apply (*rule-tac x = x* **in** *exI*)
apply (*rule conjI*)
apply *assumption*
apply (*rule notI*)
apply (*erule impE*)
apply *assumption*
apply (*erule notE*)
apply (*rule-tac x = x* **in** *exI*)
apply (*rule conjI*)
apply *assumption* +
done

Ako je svaki kvadrat romb;
i ako je svaki kvadrat pravougaonik;
i ako znamo da postoji makar jedan kvadrat;
onda postoji makar jedan romb koji je istovremeno i pravougaonik.

lemma $(\forall\ x.\ Kvadrat\ x \longrightarrow Romb\ x) \wedge$
$(\forall\ x.\ Kvadrat\ x \longrightarrow Pravougaonik\ x) \wedge$
$(\exists\ x.\ Kvadrat\ x) \longrightarrow$

    $(\exists\ x.\ Romb\ x \wedge Pravougaonik\ x)$
  apply (*rule impI*)
  apply (*erule conjE*) +
  apply (*erule exE*)
  apply (*erule-tac x = x* **in** *allE*) +
  apply (*rule-tac x = x* **in** *exI*)
  apply (*rule conjI*)
   apply (*erule impE*)
    apply *assumption* +
  apply (*erule impE*) +
    apply *assumption* +
  apply (*erule impE*)
   apply *assumption* +
  done

Ako je relacija R simetrična, tranzitivna
i ako za svako x postoji y koje je sa njim u relaciji,
onda je relacija R i refleksivna.

Savet: Pomoću ključne reči *definition* definisati osobinu refleksivnosti, tranzitivnosti i simetricnosti. Ta formulisati tvđenje i dokazati ga. Podsetiti se ključne reči *unfolding* za raspisivanje definicije.

definition *reflexive* $R \equiv \forall\ x.\ R\ x\ x$

definition *transitive* $R \equiv \forall\ x\ y\ z.\ R\ x\ y \wedge R\ y\ z \longrightarrow R\ x\ z$

definition *symmetric* $R \equiv \forall\ x\ y.\ R\ x\ y \longleftrightarrow R\ y\ x$

lemma *symmetric* $R \wedge$ *transitive* $R \wedge$
    $(\forall\ x.\ \exists\ y.\ R\ x\ y) \longrightarrow$
    reflexive R
  unfolding *reflexive-def transitive-def symmetric-def*
  apply (*rule impI*)
  apply (*erule conjE*) +
  apply (*rule allI*)
  apply (*erule-tac x = x* **in** *allE*) **back back**
  apply (*erule exE*)
  apply (*erule-tac x = x* **in** *allE*)
  apply (*erule-tac x = x* **in** *allE*)
  apply (*erule-tac x = y* **in** *allE*)
  apply (*erule-tac x = y* **in** *allE*)
  apply (*erule-tac x = x* **in** *allE*)
  apply (*erule iffE*)
  apply (*erule impE*)
   apply (*rule conjI*)
    apply *assumption*
   apply (*erule impE*)
    apply *assumption* +
  done

Zadatak 5 *Klasična pravilo prirodne dedukcije: ccontr.*

Diskutovati zašto sledeće tvrđenje može biti dokazano samo intuicionističkim pravilima prirodne dedukcije, dok to ne važi za tvrđenje nakon njega. Primetiti razliku između pravila *notI* i *ccontr*.

```
lemma ‹A ⟶ ¬ ¬ A›
  apply (rule impI)
  apply (rule notI)
  apply (erule notE)
  apply assumption
  done

thm notI
thm ccontr

lemma ¬ ¬ A ⟶ A
  apply (rule impI)
  apply (rule ccontr)
  apply (erule notE)
  apply assumption
  done
```

Dokazati sledeća tvrđenja:

```
lemma (¬ P ⟶ P) ⟶ P
  apply (rule impI)
  apply (rule ccontr)
  apply (erule impE)
   apply assumption
  apply (erule notE)
  apply assumption
  done

lemma ¬ (A ∧ B) ⟶ ¬ A ∨ ¬ B
  apply (rule impI)
  apply (rule ccontr)
  apply (erule notE)
  apply (rule conjI)
   apply (rule ccontr)
   apply (erule notE)
   apply (rule disjI1)
   apply assumption
  apply (rule ccontr)
  apply (erule notE)
  apply (rule disjI2)
  apply assumption
  done

lemma (¬ (∀ x. P x)) ⟶ (∃ x. ¬ P x)
  apply (rule impI)
  apply (rule ccontr)
  apply (erule notE)
  apply (rule allI)
```

apply (*rule ccontr*)
apply (*erule notE*)
apply (*rule-tac* $x = x$ **in** *exI*)
apply *assumption*
done

Dodatni primeri:

lemma $(\neg\ B \longrightarrow \neg\ A) \longrightarrow (A \longrightarrow B)$
apply (*rule impI*)
apply (*rule impI*)
apply (*rule ccontr*)
apply (*erule impE*)
apply *assumption*
apply (*erule notE*) **back**
apply *assumption*
done

lemma $(A \longrightarrow B) \longrightarrow (\neg\ A \vee B)$
apply (*rule impI*)
apply (*rule ccontr*)
apply (*erule impE*)
apply (*rule ccontr*)
apply (*erule notE*)
apply (*rule disjI1*)
apply *assumption*
apply (*erule notE*)
apply (*rule disjI2*)
apply *assumption*
done

lemma $(\neg\ P \longrightarrow Q) \longleftrightarrow (\neg\ Q \longrightarrow P)$
apply (*rule iffI*)
apply (*rule impI*)
apply (*rule ccontr*)
apply (*erule impE*)
apply *assumption*
apply (*erule notE*)
apply *assumption*
apply (*rule impI*)
apply (*rule ccontr*)
apply (*erule impE*)
apply *assumption*
apply (*erule notE*)
apply *assumption*
done

lemma $((P \longrightarrow Q) \longrightarrow P) \longrightarrow P$
apply (*rule impI*)
apply (*rule ccontr*)
apply (*erule impE*)
apply (*rule impI*)

```
  apply (rule ccontr)
  apply (erule notE)
  apply assumption
 apply (erule notE)
 apply assumption
 done
```

Zadatak 6 *Klasična pravilo prirodne dedukcije: classical.*

Pokazati naredna tvrđenja pomoću pravila *classical*. Zgodna alternativa ovog pravila je razdvajanje na slučajeve neke podformule.

```
thm classical

lemma P ∨ ¬ P
 apply (rule classical)
 apply (rule disjI1)
 apply (rule ccontr)
 apply (erule notE)
 apply (rule disjI2)
 apply assumption
 done

lemma (A ⟷ (A ⟷ B)) ⟶ B
 apply (rule impI)
 apply (cases A)
  apply (erule iffE)
  apply (erule impE)
   apply assumption
  apply (erule iffE)
  apply (erule impE) back
   apply assumption +
 apply (rule ccontr)
 apply (erule iffE)
 apply (erule impE) back
 apply (rule iffI)
   apply (erule notE)
   apply assumption
  apply (erule impE)
   apply (erule notE) back
   apply assumption
  apply (erule notE) back
  apply assumption
 apply (erule notE)
 apply assumption
 done
```

Paradoks pijanca:
Postoji osoba za koju važi, ako je on pijanac onda su i svi ostali pijanci.

```
lemma drinker's-paradox: ∃ x. drunk x ⟶ (∀ x. drunk x)
 apply (cases ∀ x. drunk x)
  apply (rule exI)
```

apply (*rule impI*)
apply *assumption*
apply (*rule ccontr*)
apply (*erule notE*)
apply (*rule allI*)
apply (*rule ccontr*)
apply (*erule notE*)
apply (*rule-tac* $x = x$ **in** *exI*)
apply (*rule impI*)
apply (*erule notE*)
apply *assumption*
done