Univerzitet u Beogradu
Matematički fakultet
Katedra za računarstvo i informatiku

Šifra predmeta: R265
11.03.2024.

Uvod u interaktivno dokazivanje teorema

Vežbe 04

Zadatak 1 *Algebra skupova*

Diskutovati o sledećim termovima:

term $\{1, 2, 3\}$
term $\{1::nat, 2, 3\}$
term $(\in)$
term $(\cap)$
term $(\cup)$
term $(\cup)\ A$
term $A \cup B$
term $(A::'a\ set) - B$

Zadatak 2 *Isar dokazi*

Pokazati sledeća tvrđenja o skupovima pomoću jezika Isar.

Napomena: Dozvoljeno je korišćenje samo *simp* metode za dokazivanje pojedinačnih koraka.

```
lemma - (A ∪ B) = - A ∩ - B
proof
  show - (A ∪ B) ⊆ - A ∩ - B
  proof
    fix x
    assume x ∈ - (A ∪ B)
    then have x ∉ A ∪ B by simp
    then have x ∉ A ∧ x ∉ B by simp
    then have x ∈ - A ∧ x ∈ - B by simp
    then show x ∈ - A ∩ - B by simp
  qed
next
  show - A ∩ - B ⊆ - (A ∪ B)
  proof
    fix x
    assume x ∈ - A ∩ - B
    then have x ∈ - A ∧ x ∈ - B by simp
    then have x ∉ A ∧ x ∉ B by simp
    then have x ∉ A ∪ B by simp
    then show x ∈ - (A ∪ B) by simp
  qed
qed
```

Savet: Iskoristiti *find-theorems* - ∨ - ⟷ - ∨ - za pronalaženje odgovarajuće teoreme.

```
lemma A ∪ B = B ∪ A
proof
```

```
  show A ∪ B ⊆ B ∪ A
  proof
    fix x
    assume x ∈ A ∪ B
    then have x ∈ A ∨ x ∈ B by simp
    then have x ∈ B ∨ x ∈ A using disj-commute[of x ∈ A x ∈ B] by simp
    then show x ∈ B ∪ A by simp
  qed
next
  show B ∪ A ⊆ A ∪ B
  proof
    fix x
    assume x ∈ B ∪ A
    then have x ∈ B ∨ x ∈ A by simp
    then have x ∈ A ∨ x ∈ B using disj-commute[of x ∈ A x ∈ B] by simp
    then show x ∈ A ∪ B by simp
  qed
qed
```

Savet: Iskoristiti aksiomu isključenja trećeg $A \vee \neg A$ u kontekstu operacije pripadanja $(\in) :: {'a} \Rightarrow {'a}\ set \Rightarrow bool$.

```
lemma A ∪ (B ∩ C) = (A ∪ B) ∩ (A ∪ C) (is ?left = ?right)
proof
  show ?left ⊆ ?right
  proof
    fix x
    assume x ∈ ?left
    then have x ∈ A ∨ x ∈ B ∩ C by simp
    then show x ∈ ?right
    proof
      assume x ∈ A
      then have x ∈ A ∪ B ∧ x ∈ A ∪ C by simp
      then show x ∈ ?right by simp
    next
      assume x ∈ B ∩ C
      then have x ∈ B ∧ x ∈ C by simp
      then have x ∈ A ∪ B ∧ x ∈ A ∪ C by simp
      then show x ∈ ?right by simp
    qed
  qed
next
  show ?right ⊆ ?left
  proof
    fix x
    assume x ∈ ?right
    then have *: x ∈ A ∪ B ∧ x ∈ A ∪ C by simp
    have x ∈ A ∨ x ∉ A by simp
    then show x ∈ ?left
    proof
      assume x ∈ A
      then show x ∈ ?left by simp
```

```
    next
      assume x ∉ A
      from this and ∗ have x ∈ B ∧ x ∈ C by simp
      then have x ∈ B ∩ C by simp
      then show x ∈ ?left by simp
    qed
  qed
qed

lemma A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C) (is ?left = ?right)
proof
  show ?left ⊆ ?right
  proof
    fix x
    assume x ∈ ?left
    then have ∗: x ∈ A ∧ x ∈ B ∪ C by simp
    then have x ∈ A by simp
    from ∗ have x ∈ B ∪ C by simp
    then have x ∈ B ∨ x ∈ C by simp
    from this and ‹x ∈ A› have x ∈ A ∩ B ∨ x ∈ A ∩ C by simp
    then show x ∈ ?right by simp
  qed
next
  show ?right ⊆ ?left
  proof
    fix x
    assume x ∈ ?right
    then have x ∈ A ∩ B ∨ x ∈ A ∩ C by simp
    then show x ∈ ?left
    proof
      assume x ∈ A ∩ B
      then have x ∈ A ∧ x ∈ B by simp
      then have x ∈ A ∧ x ∈ B ∪ C by simp
      then show x ∈ ?left by simp
    next
      assume x ∈ A ∩ C
      then have x ∈ A ∧ x ∈ C by simp
      then have x ∈ A ∧ x ∈ B ∪ C by simp
      then show x ∈ ?left by simp
    qed
  qed
qed

lemma A − (B ∩ C) = (A − B) ∪ (A − C) (is ?left = ?right)
proof
  show ?left ⊆ ?right
  proof
    fix x
    assume x ∈ ?left
    then have ∗: x ∈ A ∧ x ∉ B ∩ C by simp
    then have x ∈ A by simp
```

```
    from ∗ have x ∉ B ∩ C by simp
    then have x ∉ B ∨ x ∉ C by simp
    then show x ∈ ?right
    proof
      assume x ∉ B
      with ‹x ∈ A› have x ∈ A − B by simp
      then show x ∈ ?right by simp
    next
      assume x ∉ C
      with ‹x ∈ A› have x ∈ A − C by simp
      then show x ∈ ?right by simp
    qed
  qed
next
  show ?right ⊆ ?left
  proof
    fix x
    assume x ∈ ?right
    then have x ∈ A − B ∨ x ∈ A − C by simp
    then show x ∈ ?left
    proof
      assume x ∈ A − B
      then have x ∈ A ∧ x ∉ B by simp
      then have x ∈ A ∧ x ∉ B ∩ C by simp
      then show x ∈ ?left by simp
    next
      assume x ∈ A − C
      then have x ∈ A ∧ x ∉ C by simp
      then have x ∈ A ∧ x ∉ B ∩ C by simp
      then show x ∈ ?left by simp
    qed
  qed
qed
```