Univerzitet u Beogradu
Matematički fakultet
Katedra za računarstvo i informatiku

Šifra predmeta: R265
18.04.2023.

Uvod u interaktivno dokazivanje teorema

Vežbe 9

Zadatak 1 *Zasnivanje prirodnih brojeva.*

Definisati algebarski tip podataka *prirodni* koji predstavlja prirodni broj.

datatype *prirodni* = *undef*

Diskutovati o tipu *prirodni* i sledećim termovima.

typ *prirodni*

term *Nula*
term *Sled Nula*
term *Sled* (*Sled Nula*)

Definisati skraćenice za prirodne brojeve **1**, **2**, **3**.

abbreviation *jedan* :: *prirodni* (**1**) **where**
  1 ≡ *undefined*

abbreviation *dva* :: *prirodni* (**2**) **where**
  2 ≡ *undefined*

abbreviation *tri* :: *prirodni* (**3**) **where**
  3 ≡ *undefined*

Primitivnom rekurzijom definisati operaciju sabiranja. Uvesti levo asocijativni operator ⊕ za operaciju sabiranja.

fun *saberi* (**infixl** ⊕ *100*) **where**
  $a \oplus b = undefined$

Testirati funkciju sabiranjem nekih skraćenica za prirodne brojeve.

Pokazati da je sabiranje asocijativno.

lemma *saberi-asoc*:
  shows $a \oplus (b \oplus c) = a \oplus b \oplus c$

Pokazati da je sabiranje komutativno.
Savet: Potrebno je pokazati pomoćne lemu.

lemma *saberi-kom*:
  shows $a \oplus b = b \oplus a$

lemma *saberi-kom-isar*:
  shows $a \oplus b = b \oplus a$

Primitivnom rekurzijom definisati operaciju množenja. Uvesti levo asocijativni operator ⊗ za operaciju množenja.

fun *pomnozi* (**infixl** $\otimes$ *101*) **where**
$a \otimes b = \mathit{undefined}$

Pokazati komutativnost množenja.
Savet: Pokazati pomoćne lemme.

lemma *pomnozi-kom*:
shows $a \otimes b = b \otimes a$

Pokazati da je množenje asocijativno.

lemma *pomnozi-asoc*:
shows $a \otimes (b \otimes c) = a \otimes b \otimes c$

Primitivnom rekurzijom definisati operaciju stepenovanja. Uvesti desno asocijativni operator $\frown$ za operaciju stepenovanja.

fun *stepenuj* (**infixr** $\frown$ *102*) **where**
$a \frown b = \mathit{undefined}$

Pokazati da važi: $a^1 = a$.

lemma *stepenuj-jedan*:
shows $a \frown \mathbf{1} = a$

Pokazati da važi: $a^{(n+m)} = a^n b^m$.

lemma *stepenuj-na-zbir*[*simp*]:
shows $a \frown (n \oplus m) = a \frown n \otimes a \frown m$

Pokazati da važi: $a^{nm} = a^{n^m}$.

lemma *stepenuj-na-proizvod*:
shows $a \frown (n \otimes m) = (a \frown n) \frown m$

Zadatak 2 *Dodatni primeri.*

Pokazati sledeće teoreme u Isar-u. Kao dodatan izazov, dozvoljeno je korišćenje samo primenjivanje pravila *rule* i *subst* za dokazivanje među koraka, tj. bilo kakva automatizacija (*simp*, *auto*, *metis*, *blast*, *force*, *fastforce*, *sladgehammer*, ...) je zabranjena.

lemma $a \oplus \mathit{Nula} = a$

lemma $a \otimes (\mathit{Sled}\ b) = a \otimes b \oplus a$

lemma $a \otimes b \otimes c = a \otimes (b \otimes c)$

lemma $a \otimes b = b \otimes a$

lemma $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$