Rust i napredni tipski sustavi

8. Rust - Tipski sustav

Ivan Radiček

15. svibnja 2021.

Plan

- Prošli puta:
  - Rust: funkcije kao vrijednosti
  - Mali funkcijski jezik
- Danas:
  - Ponavljanje semantike funkcijskog jezika
  - Definiranje jednostavnog tipskog sustava za funkcijski jezik

Tipovi

- τ je tip
- Γ je lista tipova pridruženih varijablama (okolina/environment)
  - npr. $x : bool, y : (bool, List[int]), f : int \rightarrow bool$
  - na početku je okolina Γ prazna ($\emptyset$)
  - isto kao i kod semantike (samo tipovi umjesto vrijednosti)

Pod okolinom Γ, izraz e ima tip τ

$$\Gamma \vDash e : \tau$$

Tipovi

$$\tau := int \;\mid\; bool \;\mid\; List[\tau] \;\mid\; (\tau_1, \ldots, \tau_n) \;\mid\; (\tau_1, \ldots, \tau_n) \rightarrow t$$

let-izraz

$$\frac{x : \tau \in \Gamma}{\Gamma \vDash x : \tau} \qquad \frac{\Gamma \vDash e_1 : \tau_1 \qquad \Gamma, x : \tau' \vDash e_2 : \tau}{\Gamma \vDash \texttt{let } x : \tau' = e_1 \texttt{ in } e_2 : \tau}$$

Cijeli brojevi i primitivne operacije

$$\frac{}{\Gamma \vDash \overline{n} : int} \qquad \frac{\Gamma \vDash e_1 : int \qquad \Gamma \vDash e_2 : int \qquad \bullet \in \{+, -, *, /, \ldots\}}{\Gamma \vDash e_1 \bullet e_2 : int}$$

$$\frac{\Gamma \vDash e_1 : int \qquad \Gamma \vDash e_2 : int \qquad \bullet \in \{<, \leq, =, >, \geq \ldots\}}{\Gamma \vDash e_1 \bullet e_2 : bool}$$

$$\frac{\Gamma \vDash e_1 : bool \qquad \Gamma \vDash e_2 : bool \qquad \bullet \in \{\texttt{and}, \texttt{or}, \ldots\}}{\Gamma \vDash e_1 \bullet e_2 : bool}$$ [1]

[1] Slično i za `not`

Boolean tip i grananje

$$\frac{}{\Gamma \vDash \texttt{true} : \mathit{bool}} \qquad \frac{}{\Gamma \vDash \texttt{false} : \mathit{bool}}$$

$$\frac{}{\Gamma \vDash \texttt{if } e \texttt{ then } e_1 \texttt{ else } e_2 : \tau}$$

Boolean tip i grananje

$$\frac{}{\Gamma \vDash \texttt{true} : \mathit{bool}} \qquad \frac{}{\Gamma \vDash \texttt{false} : \mathit{bool}}$$

$$\frac{\Gamma \vDash e : \mathit{bool}}{\Gamma \vDash \texttt{if } e \texttt{ then } e_1 \texttt{ else } e_2 : \tau}$$

Boolean tip i grananje

$$\frac{}{\Gamma \vDash \texttt{true} : \mathit{bool}} \qquad \frac{}{\Gamma \vDash \texttt{false} : \mathit{bool}}$$

$$\frac{\Gamma \vDash e : \mathit{bool} \qquad \Gamma \vDash e_1 : \tau \qquad \Gamma \vDash e_2 : \tau}{\Gamma \vDash \texttt{if}\ e\ \texttt{then}\ e_1\ \texttt{else}\ e_2 : \tau}$$

n-torke

$$\frac{}{\Gamma \models (e_1, \dots, e_n) : (\tau_1, \dots, \tau_n)}$$

$$\frac{}{\Gamma \models e.i :}$$

n-torke

$$\frac{\Gamma \vDash e_1 : \tau_1 \qquad \dots \qquad \Gamma \vDash e_n : \tau_n}{\Gamma \vDash (e_1, \dots, e_n) : (\tau_1, \dots, \tau_n)}$$

$$\frac{}{\Gamma \vDash e.i :}$$

n-torke

$$\frac{\Gamma \vDash e_1 : \tau_1 \qquad \dots \qquad \Gamma \vDash e_n : \tau_n}{\Gamma \vDash (e_1, \dots, e_n) : (\tau_1, \dots, \tau_n)}$$

$$\frac{\Gamma \vDash e : (\tau_1, \dots, \tau_n)}{\Gamma \vDash e.i : \tau_i}$$

n-torke

$$\frac{\Gamma \vDash e_1 : \tau_1 \qquad \dots \qquad \Gamma \vDash e_n : \tau_n}{\Gamma \vDash (e_1, \dots, e_n) : (\tau_1, \dots, \tau_n)}$$

$$\frac{\Gamma \vDash e : (\tau_1, \dots, \tau_n) \qquad \text{tako da } 1 \leq i \leq n}{\Gamma \vDash e.i : \tau_i}$$

Liste

$$\frac{}{\Gamma \models \texttt{nil} : List[\tau]} \qquad \frac{\Gamma \models e_1 : \qquad \Gamma \models e_2 :}{\Gamma \models e_1 :: e_2 : List[\tau]}$$

Liste

$$\frac{}{\Gamma \vDash \texttt{nil} : List[\tau]} \qquad \frac{\Gamma \vDash e_1 : \tau \qquad \Gamma \vDash e_2 :}{\Gamma \vDash e_1 :: e_2 : List[\tau]}$$

Liste

$$\frac{}{\Gamma \vDash \texttt{nil} : \mathit{List}[\tau]} \qquad \frac{\Gamma \vDash e_1 : \tau \qquad \Gamma \vDash e_2 : \mathit{List}[\tau]}{\Gamma \vDash e_1 :: e_2 : \mathit{List}[\tau]}$$

Liste

$$\frac{}{\Gamma \vDash \texttt{nil} : List[\tau]} \qquad \frac{\Gamma \vDash e_1 : \tau \qquad \Gamma \vDash e_2 : List[\tau]}{\Gamma \vDash e_1 :: e_2 : List[\tau]}$$

$$\frac{\Gamma \vDash e :}{\Gamma \vDash \texttt{match}\ e\ \texttt{with}\ \ \texttt{nil} \Rightarrow e_1,\ \ h :: t \Rightarrow e_2 : \tau}$$

Liste

$$\frac{}{\Gamma \vDash \texttt{nil} : \mathit{List}[\tau]} \qquad \frac{\Gamma \vDash e_1 : \tau \qquad \Gamma \vDash e_2 : \mathit{List}[\tau]}{\Gamma \vDash e_1 :: e_2 : \mathit{List}[\tau]}$$

$$\frac{\Gamma \vDash e : \mathit{List}[\tau']}{\Gamma \vDash \texttt{match}\ e\ \texttt{with}\ \ \texttt{nil} \Rightarrow e_1,\ \ h :: t \Rightarrow e_2 : \tau}$$

Liste

$$\frac{}{\Gamma \vDash \texttt{nil} : \mathit{List}[\tau]} \qquad \frac{\Gamma \vDash e_1 : \tau \qquad \Gamma \vDash e_2 : \mathit{List}[\tau]}{\Gamma \vDash e_1 :: e_2 : \mathit{List}[\tau]}$$

$$\frac{\Gamma \vDash e : \mathit{List}[\tau'] \qquad \Gamma \vDash e_1 : \tau}{\Gamma \vDash \texttt{match}\ e\ \texttt{with}\ \ \texttt{nil} \Rightarrow e_1,\ h :: t \Rightarrow e_2 : \tau}$$

Liste

$$\frac{}{\Gamma \vDash \texttt{nil} : \mathit{List}[\tau]} \qquad \frac{\Gamma \vDash e_1 : \tau \qquad \Gamma \vDash e_2 : \mathit{List}[\tau]}{\Gamma \vDash e_1 :: e_2 : \mathit{List}[\tau]}$$

$$\frac{\Gamma \vDash e : \mathit{List}[\tau'] \qquad \Gamma \vDash e_1 : \tau \qquad \Gamma, \qquad\qquad\qquad \vDash e_2 : \tau}{\Gamma \vDash \texttt{match}\ e\ \texttt{with}\ \ \texttt{nil} \Rightarrow e_1,\ h :: t \Rightarrow e_2 : \tau}$$

Liste

$$\frac{}{\Gamma \vDash \texttt{nil} : \mathit{List}[\tau]} \qquad \frac{\Gamma \vDash e_1 : \tau \qquad \Gamma \vDash e_2 : \mathit{List}[\tau]}{\Gamma \vDash e_1 :: e_2 : \mathit{List}[\tau]}$$

$$\frac{\Gamma \vDash e : \mathit{List}[\tau'] \qquad \Gamma \vDash e_1 : \tau \qquad \Gamma, h : \tau', t : \mathit{List}[\tau'] \vDash e_2 : \tau}{\Gamma \vDash \texttt{match}\ e\ \texttt{with}\ \ \texttt{nil} \Rightarrow e_1,\ \ h :: t \Rightarrow e_2 : \tau}$$

Funkcije

$$\dfrac{\Gamma \qquad\qquad \vDash e_1 : \qquad \Gamma \qquad\qquad \vDash e_2 :}{\Gamma \vDash \texttt{let}\ f\ (x_1 : \tau_1, \ldots, x_n : \tau_n) \to \tau_r = e_1\ \texttt{in}\ e_2 : \tau}$$

Funkcije

$$\frac{\Gamma \qquad\qquad\qquad\qquad\qquad\qquad\qquad \vDash e_1 : \tau_r \qquad\qquad \Gamma \qquad\qquad\qquad\qquad \vDash e_2 :}{\Gamma \vDash \texttt{let}\ f\ (x_1 : \tau_1, \ldots, x_n : \tau_n) \to \tau_r = e_1\ \texttt{in}\ e_2 : \tau}$$

Funkcije

$$\frac{\begin{array}{l} \Gamma, x_1 : \tau_1, \cdots, x_n : \tau_n \vDash e_1 : \tau_r \\ \Gamma \vDash e_2 : \end{array}}{\Gamma \vDash \texttt{let}\ f\ (x_1 : \tau_1, \ldots, x_n : \tau_n) \rightarrow \tau_r = e_1\ \texttt{in}\ e_2 : \tau}$$

Funkcije

$$\frac{\begin{array}{c}\Gamma, x_1 : \tau_1, \cdots, x_n : \tau_n, f : (\tau_1, \ldots, \tau_n) \to \tau_r \vDash e_1 : \tau_r \\ \Gamma \qquad\qquad\qquad\qquad \vDash e_2 :\end{array}}{\Gamma \vDash \texttt{let}\ f\ (x_1 : \tau_1, \ldots, x_n : \tau_n) \to \tau_r = e_1\ \texttt{in}\ e_2 : \tau}$$

Funkcije

$$\frac{\begin{array}{c}\Gamma, x_1 : \tau_1, \cdots, x_n : \tau_n, f : (\tau_1, \ldots, \tau_n) \to \tau_r \models e_1 : \tau_r \\ \Gamma \qquad\qquad\qquad\qquad \models e_2 : \tau\end{array}}{\Gamma \models \texttt{let}\ f\ (x_1 : \tau_1, \ldots, x_n : \tau_n) \to \tau_r = e_1\ \texttt{in}\ e_2 : \tau}$$

Funkcije

$$\frac{\Gamma, x_1 : \tau_1, \cdots, x_n : \tau_n, f : (\tau_1, \ldots, \tau_n) \rightarrow \tau_r \vDash e_1 : \tau_r \qquad \Gamma, f : (\tau_1, \ldots, \tau_n) \rightarrow \tau_r \vDash e_2 : \tau}{\Gamma \vDash \texttt{let}\ f\ (x_1 : \tau_1, \ldots, x_n : \tau_n) \rightarrow \tau_r = e_1\ \texttt{in}\ e_2 : \tau}$$

Funkcije

$$\frac{\Gamma, x_1 : \tau_1, \cdots, x_n : \tau_n, f : (\tau_1, \ldots, \tau_n) \to \tau_r \vDash e_1 : \tau_r \quad \Gamma, f : (\tau_1, \ldots, \tau_n) \to \tau_r \vDash e_2 : \tau}{\Gamma \vDash \texttt{let}\ f\ (x_1 : \tau_1, \ldots, x_n : \tau_n) \to \tau_r = e_1\ \texttt{in}\ e_2 : \tau}$$

$$\frac{}{\Gamma \vDash f\ (e_1, \ldots, e_n) : \tau}$$

Funkcije

$$\frac{\Gamma, x_1 : \tau_1, \cdots, x_n : \tau_n, f : (\tau_1, \ldots, \tau_n) \to \tau_r \models e_1 : \tau_r \qquad \Gamma, f : (\tau_1, \ldots, \tau_n) \to \tau_r \models e_2 : \tau}{\Gamma \models \texttt{let}\ f\ (x_1 : \tau_1, \ldots, x_n : \tau_n) \to \tau_r = e_1\ \texttt{in}\ e_2 : \tau}$$

$$\frac{f : (\tau_1, \ldots, \tau_n) \to \tau \in \Gamma}{\Gamma \models f\ (e_1, \ldots, e_n) : \tau}$$

Funkcije

$$\frac{\begin{array}{c}\Gamma, x_1 : \tau_1, \cdots, x_n : \tau_n, f : (\tau_1, \ldots, \tau_n) \rightarrow \tau_r \vDash e_1 : \tau_r \\ \Gamma, f : (\tau_1, \ldots, \tau_n) \rightarrow \tau_r \vDash e_2 : \tau\end{array}}{\Gamma \vDash \texttt{let}\ f\ (x_1 : \tau_1, \ldots, x_n : \tau_n) \rightarrow \tau_r = e_1\ \texttt{in}\ e_2 : \tau}$$

$$\frac{f : (\tau_1, \ldots, \tau_n) \rightarrow \tau \in \Gamma \qquad \Gamma \vDash e_1 : \tau_1 \qquad \ldots \qquad \Gamma \vDash e_n : \tau_n}{\Gamma \vDash f\ (e_1, \ldots, e_n) : \tau}$$

Primjer tzv. strukturnog pravila

- Da li ovo pravilo ima smisla?
- Što znači?

$$\frac{\Gamma \vDash e : \tau}{\Gamma, x : \tau \vDash e : \tau}$$

Primjer tzv. strukturnog pravila

- Da li ovo pravilo ima smisla?
- Što znači?

$$\frac{\Gamma \vDash e : \tau}{\Gamma, x : \tau \vDash e : \tau}$$

- Pravilo jednostavno kaže da ne moramo koristiti sve varijable u okolini

Primjer pravila

$$\frac{}{\emptyset \vDash \begin{array}{l} \texttt{let}\ add\ (n : int) \rightarrow (int \rightarrow int) = \\ \quad \texttt{let}\ f\ (x : int) \rightarrow int = n + x\ \texttt{in}\ f \\ \texttt{let}\ add5 : int \rightarrow int = add\ (5)\ \texttt{in} \\ add5\ (10) \end{array} :}$$

Primjer pravila

$$\frac{}{\emptyset \vDash \begin{array}{l} \texttt{let}\ add\ (n : int) \rightarrow (int \rightarrow int) = \\ \quad \texttt{let}\ f\ (x : int) \rightarrow int = n + x\ \texttt{in}\ f \\ \texttt{let}\ add5 : int \rightarrow int = add\ (5)\ \texttt{in} \\ add5\ (10) \end{array} : int}$$

Primjer pravila

$$\frac{}{n : int \vDash \texttt{let}\ f\ (x : int) \to int = n + x\ \texttt{in}\ f : int \to int}$$

$$\frac{}{\emptyset \vDash \begin{array}{l} \texttt{let}\ add\ (n : int) \to (int \to int) = \\ \quad \texttt{let}\ f\ (x : int) \to int = n + x\ \texttt{in}\ f \\ \texttt{let}\ add5 : int \to int = add\ (5)\ \texttt{in} \\ add5\ (10) \end{array} : int}$$

Primjer pravila

$$\frac{n : int, x : int \vDash n + x : int}{n : int \vDash \texttt{let}\ f\ (x : int) \rightarrow int = n + x\ \texttt{in}\ f : int \rightarrow int}$$

$$\frac{}{\emptyset \vDash \begin{array}{l} \texttt{let}\ add\ (n : int) \rightarrow (int \rightarrow int) = \\ \quad \texttt{let}\ f\ (x : int) \rightarrow int = n + x\ \texttt{in}\ f \\ \texttt{let}\ add5 : int \rightarrow int = add\ (5)\ \texttt{in} \\ add5\ (10) \end{array} : int}$$

Primjer pravila

$$\frac{n : int, x : int \vDash n + x : int \qquad f : int \to int \vDash f : int \to int}{n : int \vDash \texttt{let } f\ (x : int) \to int = n + x \texttt{ in } f : int \to int}$$

$$\frac{}{\emptyset \vDash \begin{array}{l} \texttt{let } add\ (n : int) \to (int \to int) = \\ \quad \texttt{let } f\ (x : int) \to int = n + x \texttt{ in } f \\ \texttt{let } add5 : int \to int = add\ (5) \texttt{ in} \\ add5\ (10) \end{array} : int}$$

Primjer pravila

$$\frac{n : int, x : int \vDash n + x : int \qquad f : int \to int \vDash f : int \to int}{n : int \vDash \texttt{let}\ f\ (x : int) \to int = n + x\ \texttt{in}\ f : int \to int}$$

$$\frac{\overline{f : int \to int \vDash \texttt{let}\ add5 : int \to int = add\ (5)\ \texttt{in}\ add5\ (10) : int}}{\emptyset \vDash \begin{array}{l} \texttt{let}\ add\ (n : int) \to (int \to int) = \\ \quad \texttt{let}\ f\ (x : int) \to int = n + x\ \texttt{in}\ f \\ \texttt{let}\ add5 : int \to int = add\ (5)\ \texttt{in} \\ add5\ (10) \end{array} : int}$$

Primjer pravila

$$\dfrac{\dfrac{n : int, x : int \vDash n + x : int \qquad f : int \to int \vDash f : int \to int}{n : int \vDash \texttt{let}\ f\ (x : int) \to int = n + x\ \texttt{in}\ f : int \to int}}{add : int \to (int \to int) \vDash add\ (5) : int \to int}$$

$$\dfrac{\dfrac{}{f : int \to int \vDash \texttt{let}\ add5 : int \to int = add\ (5)\ \texttt{in}\ add5\ (10) : int}}{\emptyset \vDash \begin{array}{l} \texttt{let}\ add\ (n : int) \to (int \to int) = \\ \quad \texttt{let}\ f\ (x : int) \to int = n + x\ \texttt{in}\ f \\ \texttt{let}\ add5 : int \to int = add\ (5)\ \texttt{in} \\ add5\ (10) \end{array} : int}$$

Primjer pravila

$$
\dfrac{\dfrac{\dfrac{\dfrac{n : int, x : int \vDash n + x : int \qquad f : int \to int \vDash f : int \to int}{n : int \vDash \texttt{let } f\ (x : int) \to int = n + x \texttt{ in } f : int \to int}}{add : int \to (int \to int) \vDash add\ (5) : int \to int} \qquad \dfrac{}{add5 : int \to int \vDash add5\ (10) : int}}{f : int \to int \vDash \texttt{let } add5 : int \to int = add\ (5) \texttt{ in } add5\ (10) : int}}{\emptyset \vDash \begin{array}{l} \texttt{let } add\ (n : int) \to (int \to int) = \\ \quad \texttt{let } f\ (x : int) \to int = n + x \texttt{ in } f \\ \texttt{let } add5 : int \to int = add\ (5) \texttt{ in} \\ add5\ (10) \end{array} : int}
$$

Zadatak

- Kojeg je tipa sljedeći izraz?
- Derivacija/dokaz?

```
let insert (x : int, l : List[int]) -> List[int] =
  match l with
    nil => x::nil
    h::t => if x < h
            then x::h::t
            else h::(insert (x, t))
in
let isort (l : List[int]) -> List[int] =
  match l with
    nil => nil
    h::t => insert(h, isort(t))
```