Varnost MiniML

Če ima program p tip, potem se ob evaluaciji "ne zatakne".

Program p (izraz brez prostih spremenljivk)

Evaluacija $p \mapsto p_1 \mapsto p_2 \mapsto p_3 \mapsto \cdots$

- (if $3 < 5$ then 6 else 7) $\mapsto$ (if true then 6 else 7) $\longmapsto$ 6 vrednost
- (if $(3 < 5) + 1$ then 6 else 7) $\mapsto$ (if true $+ 1$ then 6 else 7) blokira

Blokiran program je tak p, ki ni vrednost in nima naslednjega koraka. Možnosti: 1) p divergira $p \mapsto p_1 \mapsto p_2 \mapsto p_3 \mapsto \cdots$

2) p se evaluira v vrednost

$p \mapsto p_1 \mapsto \cdots \mapsto p_n$ vrednost

BAD $\longrightarrow$ 3) p blokira $p_1 \mapsto \cdots \mapsto p_n$ ni vrednost

Izrek o varnosti

Če ima program p tip, potem se evaluira v vrednost ali divergira.
(ne blokira)

Opomba: program

$(\text{if true then true else } 5) \mapsto \text{true}$

se evaluira v vrednost, a nima tipa.

$$\underbrace{\boxed{(\mathrm{Foo})\,0}}_{\text{float\_of-int } 7} : \mathrm{Foo}$$

Izrek o ohranitvi: Če ima program p tip τ in $p \mapsto p'$, potem ima p' tip τ.

Izrek o napredku: Če ima p tip, potem je vrednost ali pa obstaja p' da $p \mapsto p'$,

Dokaz izreka o varnosti

$\overset{\tau}{p}$ (napredek) ⇒ (1) p je vrednost ✓

(2) $p \mapsto p'$ (ohranitev) ⇒ $\overset{\tau}{p'}$

⇙ napredek

(1) p' vrednost ✓

(2) $p' \mapsto p''$

⇙ ohranitev

$\overset{\tau}{p''}$

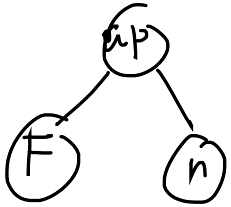
$$\begin{tikzcd}
\overset{\tau}{p} \arrow[r] \arrow[dr, mapsto] & \text{vrednost} & & & \\
& \overset{\tau}{p'} \arrow[r] \arrow[dr, mapsto] & \text{vrednost} & & \\
& & \overset{\tau}{p''} \arrow[r] \arrow[dr, mapsto] & \text{vrednost} & \\
& & & \overset{\tau}{p'''} \arrow[r] \arrow[dr, mapsto] & \dots \\
& & & & \dots
\end{tikzcd}$$

$$(\underbrace{\texttt{fun } f(x : \texttt{int}) : \texttt{int is } f(x+1)}_{F})\ 0 \mapsto$$

$F(1+0) \mapsto F(1) \mapsto$

$F(1+1) \mapsto F(2) \mapsto$

$F(2+1) \mapsto F(3) \mapsto \dots$



Izrek o napredku, kako do dokaza?

Če ima p tip τ, je p vrednost ali obstaja p', da $p \mapsto p'$.

Primer: $p = p_1 + p_2$ in ima tip τ:

Inverzija: $$\frac{?\quad ?\quad ?}{\cdot \mid p_1 + p_2 : \tau}$$

$$\frac{\cdot \mid p_1 : \mathrm{int} \qquad \cdot \mid p_2 : \mathrm{int}}{\cdot \mid p_1 + p_2 : \mathrm{int}}$$

$\Rightarrow \tau = \mathrm{int}$

$\Rightarrow p_1 : \mathrm{int}$

$\Rightarrow p_2 : \mathrm{int}$

Dokaz: indukcija po strukturi p.

Primer 1: $p = n$ celoštevilska konstanta $\Rightarrow$ p je vrednost

Primer 2: $p = \mathrm{true}$ $\Rightarrow$ p je vrednost

Primer 3: $p = \mathrm{false}$ $\Rightarrow$ p je vrednost

Primer 4: $p = (\mathrm{fun} \ldots\ldots)$ $\Rightarrow$ p je vrednost

Izrek o napredku

Primer 5: $p = p_1 + p_2$ in $p : \tau$. Inverzija $\tau = int$

$p_1 : int$

$p_2 : int$

Po I.H. p_1 je vrednost ali $p_1 \mapsto p_1'$.

1) p_1 je vrednost, $p_1 : int \Rightarrow p_1 = n_1$ za neko celo število n_1

1.1) p_2 je vrednost, $p_2 : int \Rightarrow p_2 = n_2$

$\Rightarrow p = n_1 + n_2$

$$\frac{n \text{ vsota } n_1 \text{ in } n_2}{\underbrace{n_1 + n_2}_{p} \mapsto \underbrace{n}_{p'}}$$

$p' =$ vsota n_1 in n_2

1.2) $p_2 \mapsto p_2'$

$$\frac{p_2 \mapsto p_2'}{\underbrace{n_1 + p_2}_{p} \mapsto \underbrace{n_1 + p_2'}_{p'}}$$

Izrek o napredku

2) $p_1 \mapsto p_1'$

$$\frac{p_1 \mapsto p_1'}{\underbrace{p_1 + p_2}_{p} \mapsto \underbrace{p_1' + p_2}_{p'}}$$

Primer 6 & 7 : $p_1 - p_2$, $p_1 * p_2$

Primer 8 : $p = \text{if } p_1 \text{ then } p_2 \text{ else } p_3 \; : \tau \overset{\text{inverzija}}{\Longrightarrow}$ $p_1 : \text{bool}$

$p_2 : \tau$

$p_3 : \tau$

Po I.H. je p_1 vrednost ali $p_1 \mapsto p_1'$

1) p_1 vrednost , $p_1 : \text{bool} \Rightarrow p_1 = \text{true}$ ali $p_1 = \text{false}$

1.1) $p_1 = \text{true}$

$$\underbrace{\text{if true then } p_2 \text{ else } p_3}_{p} \mapsto \underbrace{p_2}_{p'}$$

1.2) $p_1 = \text{false}$ ....

2) $p_1 \longmapsto p_1$

$$\frac{p_1 \mapsto p_1'}{\underbrace{\text{if } p_1 \text{ then } p_2 \text{ else } p_3}_{p} \longmapsto \text{if } \underbrace{p_1' \text{ then } p_2 \text{ eke } p_3}_{p'}}$$

Ostali primeri:

$$\left.\begin{array}{l} p = (p_1 = p_2) \\ p = (p < p_2) \end{array}\right\} \text{vaja}$$

$$p = p_1 \, p_2$$

∎

Izrek o ohranitvi

Če ima p tip τ in obstaja p', da $p \mapsto p'$, potem $p' : \tau$.

Dokaz: Indukcija po strukturi p. (p ni vrednost)

Primer: $p = p_1 + p_2$ inverzija $\Rightarrow$ $\tau = \mathrm{int}$, $p_1 : \mathrm{int}$, $p_2 : \mathrm{int}$

$$p \mapsto p'$$

1) $$\frac{p_1 \mapsto p_1'}{p_1 + p_2 \mapsto p_1' + p_2}$$

I.H. za $p_1 \Rightarrow p_1' : \mathrm{int}$

$$\frac{p_1' : \mathrm{int} \qquad p_2 : \mathrm{int}}{\underbrace{p_1' + p_2}_{p'} : \mathrm{int}}$$

2) $$\frac{p_2 \mapsto p_2'}{\underbrace{n_1 + p_2}_{p} \mapsto \underbrace{n_1 + p_2'}_{p'}}$$

I.H. za $p_2 \Rightarrow p_2' : \mathrm{int}$

$$\frac{\frac{}{n_1 : \mathrm{int}} \qquad p_2' : \mathrm{int}}{\underbrace{n_1 + p_2'}_{p'} : \mathrm{int}}$$

3) $$\frac{n \text{ je vsota } n_1 \text{ in } n_2}{\underbrace{n_1 + n_2}_{p} \mapsto \underbrace{n}_{p'}}$$

$n : \mathrm{int}$ ✓

Izrek o ohranitvi, aplikacija

Primer: $p = p_1\, p_2$ $\quad$ inverzija $\overset{p:\tau}{}$ $\Rightarrow$ $p_1 : \sigma \to \tau$

$p_2 : \sigma$

inverzija $p \mapsto p'$:

1) $$\frac{p_1 \mapsto p_1'}{p_1\, p_2 \mapsto p_1'\, p_2} \quad ✓$$

2) $$\frac{p_2 \mapsto p_2'}{(\text{fun} \cdots\cdots)\; p_2 \mapsto (\text{fun} \cdots\cdots)\; p_2'} \quad ✓$$

3) $$(\text{fun } f(x:\sigma):\tau \text{ is } e)\; v_2 \;\mapsto\; \underbrace{e[\, x \mapsto v_2,\, f \mapsto (\text{fun } f(x:\sigma):\tau \text{ is } e\,]}_{\text{zakaj ima tole tip } \tau\ ?}$$

Ali substitucija ohranja tip?

$$\frac{f:\sigma\to\tau,\; x:\sigma \mid e:\tau}{\mid (\text{fun } f(x:\sigma):\tau \text{ is } e\,) : \sigma \to \tau} \quad ⇗$$

⇑ ⇑ $v_2 : \sigma$

$(\text{fun } f(x:\sigma):\tau \text{ is } e\,) : \sigma \to \tau$

MiniML + error

Kako reagiramo ob napaki? 1/0, open("ne_obstaja.txt"),
a[-17]

1) Znajdemo se:

   1/0 := 42

2) Nedefinirano

3) Javimo napako:

   open("dat.txt") → ~~objekt~~ ~~Datoteka~~

   → ~~null~~

```
type α result =
    | Ok of α
    | Error of error
```

Sintaksa

Izrazi $e ::= \underbrace{n \mid \text{true} \mid \text{false} \mid x \mid e_1 + e_2 \mid \dots\dots}_{\text{MiniML}} \mid \underbrace{e_1 / e_2 \mid \text{error}}_{\text{novo}}$

Tipi: $\dfrac{\Gamma \mid e_1 : \text{int} \quad \Gamma \mid e_2 : \text{int}}{\Gamma \mid e_1 / e_2 : \text{int}}$ $\qquad \dfrac{}{\Gamma \mid \text{error} : \tau}$ error ima vse tipe!

Evaluacija:

$\dfrac{p_1 \mapsto p_1'}{p_1 / p_2 \mapsto p_1' / p_2}$ $\qquad \dfrac{n_2 \neq 0 \quad n \text{ je celoštevilski kvocient } n_1 \text{ in } n_2}{n_1 / n_2 \mapsto n}$

$\dfrac{p_2 \mapsto p_2'}{n_1 / p_2 \mapsto n_1 / p_2'}$ $\qquad \dfrac{}{n_1 / 0 \mapsto \text{error}}$

Vrednost $v ::= n \mid \text{true} \mid \text{false} \mid (\text{fun} \dots\dots) \mid \text{error}$

Error

$\text{error} + p_2 \mapsto \text{error}$ $\quad$ $n_1 + \text{error} \mapsto \text{error}$ $\quad$ podobno $-, \times, =, <$

$\text{error} / p_2 \mapsto \text{error}$ $\quad$ $n_1 / \text{error} \mapsto \text{error}$

$\text{if error then } p_1 \text{ else } p_2 \mapsto \text{error}$

$\text{error } p_2 \mapsto \text{error}$ $\quad$ $(\text{fun} \overset{\sigma\to\tau}{\text{-----}}) \overset{\sigma}{\text{error}} \mapsto \text{error}$

Ali velja izrek o ohranitvi?

Ce $p : \tau$ in $p \mapsto p'$, potem $p' : \tau$.

Izrek o napredku?

Če $p : \tau$, je p vrednost ali $p \mapsto p'$.