Karlsruher Institut für Technologie

Bitte Logo über
\grouplogo{}
festlegen.

Corten: Refinement Types for Imperative Languages with Ownership

Abschlusspräsentation Masterarbeit

Carsten Csiky | 26th Oktober 2022

KIT – Die Forschungsuniversität in der Helmholtz-Gemeinschaft

www.kit.edu

Inhaltsverzeichnis

1. Motivation
2. Empirical Analysis
3. Solution
4. Soundness Justification
5. Related Work
6. Conclusion / Future Work

Motivation

```
fn max(a: i32, b: i32) {
        if a > b { a } else { b }
}
```

Motivation

```rust
fn max(a: i32, b: i32) {
        if a > b { a } else { b }
}
```

Return Value $(v) : v \geq a \wedge v \geq b$

Motivation

```
fn max(a: i32, b: i32) {
        if a > b { a } else { b }
}
```

Return Value $(v) : v \geq a \wedge v \geq b$

Refinement Types**rondon_liquid_2008** in Functional Programming Languages

Motivation

```
//@ max(a: i32, b: i32) -> {v:i32 | v >= a && v >= b }
fn  max(a: i32, b: i32) -> i32 {
        if a > b { a } else { b }
}
```

Motivation

```
//@ max(a: i32, b: i32) -> {v:i32 | v >= a && v >= b }
fn  max(a: i32, b: i32) -> i32 {
        if a > b { a } else { b }
}
```

let $\Gamma = (a : \{v : \texttt{i32} \mid \text{true}\}, b : \{v : \texttt{i32} \mid \text{true}\})$ and $\tau = \{v : \texttt{i32} \mid v \geq a \land v \geq b\}$

$$\frac{}{\Gamma \vdash \texttt{if}\ a > b\ \{a\}\ \texttt{else}\ \{b\} : \tau}$$

Motivation

```
//@ max(a: i32, b: i32) -> {v:i32 | v >= a && v >= b }
fn  max(a: i32, b: i32) -> i32 {
        if a > b { a } else { b }
}
```

let $\Gamma = (a : \{v : \texttt{i32} \mid \text{true}\}, b : \{v : \texttt{i32} \mid \text{true}\})$ and $\tau = \{v : \texttt{i32} \mid v \geq a \wedge v \geq b\}$

$$\dfrac{\dfrac{}{\Gamma, a > b \vdash a : \tau} \qquad \dfrac{}{\Gamma, \neg(a > b) \vdash b : \tau}}{\Gamma \vdash \texttt{if } a > b \; \{a\} \; \texttt{else} \; \{b\} : \tau}$$

Motivation

```
//@ max(a: i32, b: i32) -> {v:i32 | v >= a && v >= b }
fn  max(a: i32, b: i32) -> i32 {
        if a > b { a } else { b }
}
```

let $\Gamma = (a : \{v : \texttt{i32} \mid \text{true}\}, b : \{v : \texttt{i32} \mid \text{true}\})$ and $\tau = \{v : \texttt{i32} \mid v \geq a \land v \geq b\}$

$$\dfrac{\dfrac{\overline{\Gamma, a > b \vdash \{v : \texttt{i32} \mid v \doteq a\} \preceq \tau}}{\Gamma, a > b \vdash a : \tau} \qquad \overline{\Gamma, \neg(a > b) \vdash b : \tau}}{\Gamma \vdash \texttt{if}\ a > b\ \{a\}\ \texttt{else}\ \{b\} : \tau}$$

Motivation

```
//@ max(a: i32, b: i32) -> {v:i32 | v >= a && v >= b }
fn  max(a: i32, b: i32) -> i32 {
    if a > b { a } else { b }
}
```

let $\Gamma = (a : \{v : \texttt{i32} \mid \text{true}\}, b : \{v : \texttt{i32} \mid \text{true}\})$ and $\tau = \{v : \texttt{i32} \mid v \geq a \wedge v \geq b\}$

$$\dfrac{\dfrac{\dfrac{\star}{\Gamma, a > b \vdash a : \{v : \texttt{i32} \mid v \doteq a\}} \qquad \dfrac{}{\Gamma, a > b \vdash \{v : \texttt{i32} \mid v \doteq a\} \preceq \tau}}{\Gamma, a > b \vdash a : \tau} \qquad \dfrac{}{\Gamma, \neg(a > b) \vdash b : \tau}}{\Gamma \vdash \texttt{if}\ a > b\ \{a\}\ \texttt{else}\ \{b\} : \tau}$$

Motivation

```
//@ max(a: i32, b: i32) -> {v:i32 | v >= a && v >= b }
fn  max(a: i32, b: i32) -> i32 {
        if a > b { a } else { b }
}
```

let $\Gamma = (a : \{v : \texttt{i32} \mid \text{true}\}, b : \{v : \texttt{i32} \mid \text{true}\})$ and $\tau = \{v : \texttt{i32} \mid v \geq a \wedge v \geq b\}$

$$\dfrac{\dfrac{\dfrac{\star}{\Gamma, a > b \vdash a : \{v : \texttt{i32} \mid v \doteq a\}} \qquad \dfrac{\text{SMT-VALID}\left(\begin{array}{l}\text{true} \wedge \text{true} \wedge a > b \\ \wedge\, v \doteq a \\ \qquad \Longrightarrow \ (v \geq a \wedge v \geq b)\end{array}\right)}{\Gamma, a > b \vdash \{v : \texttt{i32} \mid v \doteq a\} \preceq \tau}}{\Gamma, a > b \vdash a : \tau} \qquad \dfrac{}{\Gamma, \neg(a > b) \vdash b : \tau}}{\Gamma \vdash \texttt{if}\ \ a > b\ \{a\}\ \ \texttt{else}\ \ \{b\} : \tau}$$

Motivation

```
//@ max(a: i32, b: i32) -> {v:i32 | v >= a && v >= b }
fn  max(a: i32, b: i32) -> i32 {
        if a > b { a } else { b }
}
```

let $\Gamma = (a : \{v : \mathtt{i32} \mid \text{true}\}, b : \{v : \mathtt{i32} \mid \text{true}\})$ and $\tau = \{v : \mathtt{i32} \mid v \geq a \land v \geq b\}$

$$\dfrac{\dfrac{\dfrac{\star}{\Gamma, a > b \vdash a : \{v : \mathtt{i32} \mid v \doteq a\}} \qquad \dfrac{\text{SMT-VALID}\begin{pmatrix} \text{true} \land \text{true} \land a > b \\ \land\, v \doteq a \\ \implies (v \geq a \land v \geq b) \end{pmatrix}}{\Gamma, a > b \vdash \{v : \mathtt{i32} \mid v \doteq a\} \preceq \tau}}{\Gamma, a > b \vdash a : \tau} \qquad \dfrac{\vdots}{\Gamma, \neg(a > b) \vdash b : \tau}}{\Gamma \vdash \mathtt{if}\ a > b\ \{a\}\ \mathtt{else}\ \{b\} : \tau}$$

Motivation

```
fn  clamp(a: &mut i32, b: i32) {
        if *a > b { *a = b }
}
```

Motivation

```
fn  clamp(a: &mut i32, b: i32) {
        if *a > b { *a = b }
}
fn  client(...) {
        ...
        clamp(&mut x, 5);
        clamp(&mut y, 6);
        print(x);
        ...
}
```

Motivation

```
fn clamp(a: &mut i32, b: i32) {
    if *a > b { *a = b }
}
fn client(...) {
    ...
    clamp(&mut x, 5);
    clamp(&mut y, 6);
    print(x);
    ...
}
```

What does this it `print(x)` output?

- Could be: old `x` or `5`

Motivation

```
fn  clamp(a: &mut i32, b: i32) {
        if *a > b { *a = b }
}
fn  client(...) {
        ...
        clamp(&mut x, 5);
        clamp(&mut y, 6);
        print(x);
        ...
}
```

What does this it `print(x)` output?

- Could be: old x or 5
- But also 6 (if x aliases with y)!

Literatur

Backup-Teil

Folien, die nach `\beginbackup` eingefügt werden, zählen nicht in die Gesamtzahl der Folien.

Blöcke

in den KIT-Farben

Greenblock

Standard (`block`)

Blueblock

= `exampleblock`

Redblock

= `alertblock`

Brownblock

Purpleblock

Cyanblock

Yellowblock

Lightgreenblock

Orangeblock

Grayblock

Contentblock

(farblos)

Auflistungen

Text

- Auflistung
  Umbruch
- Auflistung
  - Auflistung
  - Auflistung

Bei Frames ohne Titel wird die Kopfzeile nicht angezeigt, und der freie Platz kann für Inhalte genutzt werden.

Bei Frames mit Option `[plain]` werden weder Kopf- noch Fußzeile angezeigt.

Beispielinhalt

Bei Frames mit Option `[t]` werden die Inhalte nicht vertikal zentriert, sondern an der Oberkante begonnen.

Beispielinhalt: Literatur

Farbpalette

kit-green100 kit-green90 kit-green80 kit-green70 kit-green60 kit-green50 kit-green40 kit-green30 kit-green25 kit-green20 kit-green15 kit-green10 kit-green5

kit-blue100 kit-blue90 kit-blue80 kit-blue70 kit-blue60 kit-blue50 kit-blue40 kit-blue30 kit-blue25 kit-blue20 kit-blue15 kit-blue10 kit-blue5

kit-red100 kit-red90 kit-red80 kit-red70 kit-red60 kit-red50 kit-red40 kit-red30 kit-red25 kit-red20 kit-red15 kit-red10 kit-red5

kit-gray100 kit-gray90 kit-gray80 kit-gray70 kit-gray60 kit-gray50 kit-gray40 kit-gray30 kit-gray25 kit-gray20 kit-gray15 kit-gray10 kit-gray5

kit-orange100 kit-orange90 kit-orange80 kit-orange70 kit-orange60 kit-orange50 kit-orange40 kit-orange30 kit-orange25 kit-orange20 kit-orange15 kit-orange10 kit-orange5

kit-lightgreen100 kit-lightgreen90 kit-lightgreen80 kit-lightgreen70 kit-lightgreen60 kit-lightgreen50 kit-lightgreen40 kit-lightgreen30 kit-lightgreen25 kit-lightgreen20 kit-lightgreen15 kit-lightgreen10 kit-lightgreen5

kit-brown100 kit-brown90 kit-brown80 kit-brown70 kit-brown60 kit-brown50 kit-brown40 kit-brown30 kit-brown25 kit-brown20 kit-brown15 kit-brown10 kit-brown5

kit-purple100 kit-purple90 kit-purple80 kit-purple70 kit-purple60 kit-purple50 kit-purple40 kit-purple30 kit-purple25 kit-purple20 kit-purple15 kit-purple10 kit-purple5

kit-cyan100 kit-cyan90 kit-cyan80 kit-cyan70 kit-cyan60 kit-cyan50 kit-cyan40 kit-cyan30 kit-cyan25 kit-cyan20 kit-cyan15 kit-cyan10 kit-cyan5