Karlsruher Institut für Technologie

Corten: Refinement Types for Imperative Languages with Ownership

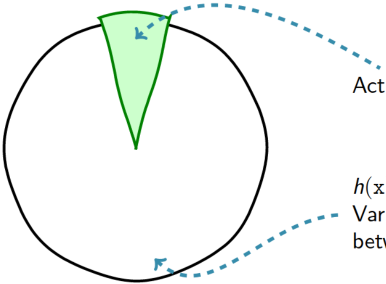
Abschlusspräsentation Masterarbeit

Carsten Csiky | 26th Oktober 2022

Inhaltsverzeichnis

Motivation

```
public IntList square(IntList list) {
  return list.map(x -> x*x);
}
```



Motivation

```rust
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) : $v \geq a \land v \geq b$

Motivation

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

- Return Value (v) : $v \geq a \land v \geq b$
- Rondon et al. [RKJ08]: Refinement Types for 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 $\tau = \{v : \texttt{i32} \mid v \geq a \wedge v \geq b\}$

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

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 $\tau = \{v : \texttt{i32} \mid v \geq a \land v \geq b\}$

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

Motivation

Karlsruher Institut für Technologie

```
//@ 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 $\tau = \{v : \texttt{i32} \mid v \geq a \land v \geq b\}$

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

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?

- In most imperative programming languages:
  - 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?

- In most imperative programming languages:
  - Could be: old `x` or `5`
  - But also `6` (if x aliases with y)!

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?

- In most imperative programming languages:
  - Could be: old `x` or `5`
  - But also `6` (if `x` aliases with `y`)!
- In Rust:
  - Just old `x` or `5`
  - And nothing else!

Motivation


```
fn  clamp(a: &mut i32, b: i32) {
  // borrows a
  // owns b
  if *a > b { *a = b }
  // "returns" the borrow of a
}
fn  client(...) { // owns x, y
  ...
  clamp(&mut x, 5); // lend x mutably
  clamp(&mut y, 6); // lend y mutably
  print!(x);
  ...
}
```

Ownership in Rust: Mutability XOR Aliasing

Each lexical scope tracks permissions for visible memory objects. Possible Permission Levels:

- Owner (e.g. `b`)
  - can: read, write
  - transfer ownership (if no outstanding borrows)
- Mutable Reference (e.g. `&mut x`)
  - can: read, write
  - guarantee: no aliasing
- Immutable Reference (e.g. `&v`)
  - can: read, alias
  - guarantee: no mutation

Motivation

Consequences:

- unique data owner
- no global, mutable state
- no cycles in memory structure

Ownership in Rust: Mutability XOR Aliasing

Each lexical scope tracks permissions for visible memory objects. Possible Permission Levels:

- Owner (e.g. `b`)
  - can: read, write
  - transfer ownership (if no outstanding borrows)
- Mutable Reference (e.g. `&mut x`)
  - can: read, write
  - guarantee: no aliasing
- Immutable Reference (e.g. `&v`)
  - can: read, alias
  - guarantee: no mutation

Motivation

Consequences:

- unique data owner
- no global, mutable state
- no cycles in memory structure

Used for:

- safe non-gc memory management
- safe concurrency
- safe low-level hardware access
- ...

Ownership in Rust: Mutability XOR Aliasing

Each lexical scope tracks permissions for visible memory objects. Possible Permission Levels:

- Owner (e.g. `b`)
  - can: read, write
  - transfer ownership (if no outstanding borrows)
- Mutable Reference (e.g. `&mut x`)
  - can: read, write
  - guarantee: no aliasing
- Immutable Reference (e.g. `&v`)
  - can: read, alias
  - guarantee: no mutation

Motivation

Karlsruher Institut für Technologie

Consequences:

- unique data owner
- no global, mutable state
- no cycles in memory structure

Used for:

- safe non-gc memory management
- safe concurrency
- safe low-level hardware access
- ...
- $\Rightarrow$ show: program verification as well

Ownership in Rust: Mutability XOR Aliasing

Each lexical scope tracks permissions for visible memory objects. Possible Permission Levels:

- Owner (e.g. `b`)
  - can: read, write
  - transfer ownership (if no outstanding borrows)
- Mutable Reference (e.g. `&mut x`)
  - can: read, write
  - guarantee: no aliasing
- Immutable Reference (e.g. `&v`)
  - can: read, alias
  - guarantee: no mutation

Refinement Types for Rust – Syntax

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

Addition of two macros

- `ty!`$\{l : b \mid \varphi\}$ in place of a type
- `relax_ctx!{ ... }` in place of a statement

Refinement Types for Rust – Syntax

Karlsruher Institut für Technologie

```
fn max(
  a: ty!{ av: i32 | true },
  b: ty!{ bv : i32 | true }
) -> ty!{ v : i32 | v >= av && v >= bv } {
  if a > b { a } else { b }
}
```

Addition of two macros

- `ty!`$\{l : b \mid \varphi\}$ in place of a type
- `relax_ctx!{ ... }` in place of a statement

Refinement Types for Rust – Syntax

```
fn max(
  a: ty!{ av: i32 },
  b: ty!{ bv : i32 }
) -> ty!{ v : i32 | v >= av && v >= bv } {
  if a > b { a } else { b }
}
```

Addition of two macros

- `ty!`$\{l : b \mid \varphi\}$ in place of a type
- `relax_ctx!{ ... }` in place of a statement

Refinement Types for Rust – Type Checking

```rust
fn max(a: ty!{ av: i32 }, b: ty!{ bv : i32 }) -> ty!{ v : i32 | v >= av && v >= bv } {
  if a > b { a as ty!{ r : i32 | r >= av && r >= bv } } else { b }
}
```

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

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

Refinement Types for Rust – Syntax

```
fn inc(a: &mut ty!{ a1: i32 | true => a2 | a2 == a1 + 1 }) {
  *a = *a + 1;
}
fn client(mut x: ty!{ xv: i32 | xv > 2 }) -> ty!{ v: i32 | v > 7 } {
  let mut y = 2;
  inc(&mut x); inc(&mut x);
  inc(&mut y)
  x + y
}
```

Refinement Types for Rust – Syntax

```
fn clamp(a: &mut ty!{ a1 : i32 | true => a2 | a2 <= b1 }, b: ty!{ b1: i32 }) {
  if *a > b { *a = b }
}
fn client(...) {
  ...
  clamp(&mut x, 5);
  clamp(&mut y, 6);
  print!(x);
  ...
}
```

Refinement Types for Rust – Syntax

```
fn clamp(a: &mut ty!{ a1 : i32 | true => a2 | a2 <= b1 }, b: ty!{ b1: i32 }) {
  // Γ1 = ({a ↦ &arg0, arg0 ↦ a1, b ↦ b1}, true ∧ true)
  if *a > b { *a = b }
  // Γ2 = ({arg0 ↦ a2, b ↦ b1}, a2 ≤ b1 ∧ true)
}
fn client(...) {
  ...
  // Γ1 = ({x ↦ v1, y ↦ v2}, ...)
  clamp(&mut x, 5);
  // Γ2 = ({x ↦ v3, y ↦ v2}, ... ∧ v3 ≤ 5)
  clamp(&mut y, 6);
  // Γ3 = ({x ↦ v3, y ↦ v4}, ... ∧ v3 ≤ 5 ∧ v4 ≤ 6)
  print!(x);
  ...
}
```

Soundness

Progress

If $\Gamma \vdash s_1, \sigma : \Gamma \Rightarrow \Gamma_2$ and $s_1 \neq \texttt{unit}$, then there is a s_2 and σ_2 with $\langle s_1 \mid \sigma_1 \rangle \rightsquigarrow \langle s_2 \mid \sigma_2 \rangle$.

Corten strictly refines the base language, therefore progress depends on base type system.

Preservation

If $\Gamma \vdash s \Rightarrow \Gamma_2, \sigma : \Gamma$ and $\langle s \mid \sigma \rangle \rightsquigarrow \langle s_1 \mid \sigma_1 \rangle$, then there is a Γ_1 with $\Gamma_1 \vdash s_1 \Rightarrow \Gamma_2$ and $\sigma_2 : \Gamma_2$

Stronger property than base language preservation: Show that refined types are preserved

State Conformance

State Conformance $\sigma : \Gamma$

A state σ is conformant with respect to a typing context $\Gamma = (\mu, \Phi)$ (written as $\sigma : \Gamma$), iff:

$$\Phi[\mu(x) \triangleright [\![\sigma(x)]\!] \mid x \in \mathrm{dom}(\mu)] \text{ is satisfiable}$$

I.e. a conformant type context does not contradict the execution state.

Examples:

- If $\sigma : (\emptyset, \Phi)$ then Φ is satisfiable
- If $\sigma : (\mu, \Phi_1 \wedge \Phi_2)$ then $\sigma : (\mu, \Phi_1)$ and $\sigma : (\mu, \Phi_1)$.
- If $\sigma : (\mu, \Phi)$ and $\mathrm{FV}(\Phi) \subseteq \mathrm{dom}(\mu)$, then $\vDash \Phi[\mu(x) \triangleright [\![\sigma(x)]\!] \mid x \in \mathrm{dom}(\mu)]$

Intermediate Steps

Karlsruher Institut für Technologie

Conformance of Symbolic Execution

If $\sigma : \Gamma, \Gamma \vdash \alpha$ fresh then $\sigma[x \mapsto [\![e]\!]\sigma] : \Gamma[x \mapsto \alpha], (\alpha \simeq [\![e]\!]\Gamma)$

where $(\alpha \simeq [\![e]\!]\Gamma)$ is the symbolic execution of e equated with α in context Γ

Reference Predicates are Conservative

If $\sigma : \Gamma$ and $\Gamma \vdash *x \in \{y_1, \ldots, y_n\}$ then $[\![\sigma(x)]\!] = \&y_i$ for some $i \in 1, \ldots, n$

Rare case where conservative typing requires

Sub-Context Relation is Conservative

If $\Gamma \preceq \Gamma'$ and $\sigma : \Gamma$ then $\sigma : \Gamma'$

Literatur

Karlsruher Institut für Technologie

Backup-Teil

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

[1] Patrick M. Rondon, Ming Kawaguci und Ranjit Jhala. „Liquid types“. In: *Proceedings of the 2008 ACM SIGPLAN conference on Programming language design and implementation - PLDI ’08*. the 2008 ACM SIGPLAN conference. Tucson, AZ, USA: ACM Press, 2008, S. 159. ISBN: 978-1-59593-860-2. DOI: `10.1145/1375581.1375602`. URL: `http://portal.acm.org/citation.cfm?doid=1375581.1375602` (besucht am 30. 06. 2022).

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