

Corten: Refinement Types for Imperative Languages with Ownership

Abschlusspräsentation Masterarbeit

Carsten Csiky | 26th Oktober 2022

Inhaltsverzeichnis

1. Motivation

2. Type System

3. Soundness Justification

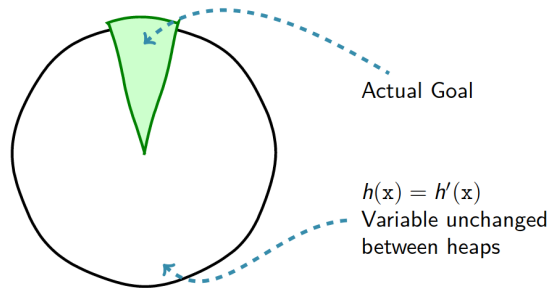
4. Related Work

5. Conclusion / Future Work

Motivation oooooooo	Type System oooooooooooo	Soundness Justification ooo	Related Work oo	Conclusion / Future Work oo	Literatur
------------------------	-----------------------------	--------------------------------	--------------------	--------------------------------	-----------

Motivation

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



Motivation

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

Motivation

```
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) : $v \geq a \wedge v \geq b$
- 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 ○○●○○○○○	Type System ○○○○○○○○○○	Soundness Justification ○○○	Related Work ○○	Conclusion / Future Work ○○	Literatur
------------------------	---------------------------	--------------------------------	--------------------	--------------------------------	-----------

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

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

Motivation	Type System	Soundness Justification	Related Work	Conclusion / Future Work	Literatur
ooo●oooo	oooooooooooo	ooo	oo	oo	

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

$$\frac{\Gamma, a > b \vdash a : \tau \quad \Gamma, \neg(a > b) \vdash b : \tau}{\Gamma \vdash \text{if } a > b \{a\} \text{ else } \{b\} : \tau}$$

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

$$\frac{
 \frac{
 \frac{
 \Gamma, a > b \vdash \{v : i32 \mid v \doteq a\} \preceq \tau
 }{
 \Gamma, a > b \vdash a : \tau
 }
 }{
 \Gamma \vdash \text{if } a > b \{a\} \text{ else } \{b\} : \tau
 }
 }{
 \Gamma, \neg(a > b) \vdash b : \tau
 }$$

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

$$\frac{\star \quad \frac{\Gamma, a > b \vdash a : \{v : i32 \mid v \doteq a\}}{\Gamma, a > b \vdash a : \tau} \quad \frac{\Gamma, a > b \vdash \{v : i32 \mid v \doteq a\} \preceq \tau}{\Gamma, a > b \vdash a : \tau}}{\Gamma \vdash \text{if } a > b \{a\} \text{ else } \{b\} : \tau} \quad \frac{}{\Gamma, \neg(a > b) \vdash b : \tau}$$

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

$$\frac{\star \quad \text{SMT-VALID} \left(\begin{array}{l} \text{true} \wedge \text{true} \wedge a > b \\ \wedge v \doteq a \\ \implies (v \geq a \wedge v \geq b) \end{array} \right)}{\frac{\Gamma, a > b \vdash a : \{v : i32 \mid v \doteq a\} \quad \Gamma, a > b \vdash \{v : i32 \mid v \doteq a\} \preceq \tau}{\Gamma, a > b \vdash a : \tau}} \quad \frac{}{\Gamma, \neg(a > b) \vdash b : \tau}$$

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

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

$$\frac{\star \quad \text{SMT-VALID} \left(\begin{array}{l} \text{true} \wedge \text{true} \wedge a > b \\ \wedge v \doteq a \\ \implies (v \geq a \wedge v \geq b) \end{array} \right)}{\frac{\Gamma, a > b \vdash a : \{v : i32 \mid v \doteq a\} \quad \Gamma, a > b \vdash \{v : i32 \mid v \doteq a\} \preceq \tau}{\Gamma, a > b \vdash a : \tau}} \quad \vdots \quad \frac{}{\Gamma, \neg(a > b) \vdash b : \tau}$$

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

Motivation

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

Motivation
○○○●○○○

Type System
○○○○○○○○○○

Soundness Justification
○○○

Related Work
○○

Conclusion / Future Work
○○

Literatur

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	Type System	Soundness Justification	Related Work	Conclusion / Future Work	Literatur
○○○●○○○	○○○○○○○○○○	○○○	○○	○○	

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	Type System	Soundness Justification	Related Work	Conclusion / Future Work	Literatur
○○○●○○○	○○○○○○○○○○	○○○	○○	○○	

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	Type System	Soundness Justification	Related Work	Conclusion / Future Work	Literatur
○○○○●○○	○○○○○○○○○○	○○○	○○	○○	

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

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

Contributions

- Empirical Use-Case Analysis
- Refinement Type System
 - Automatic & Decidable Type Checking
 - Path Sensitivity
 - Mutable Data & References
 - Modularity
 - Partial Mechanized Proof of Soundness
- Implementation
 - Accessible Interface
 - Type-Error Messages with Source Code Locations
 - Counter-Example Generation
- Evaluation
 - Automatic Verification of non-trivial Programs
 - Comparison to other tools

Motivation	Type System	Soundness Justification	Related Work	Conclusion / Future Work	Literatur
oooooooo●	oooooooooooo	oooo	oo	oo	

Contributions

- Empirical Use-Case Analysis
- Refinement Type System
 - Automatic & Decidable Type Checking
 - Path Sensitivity
 - Mutable Data & References
 - Modularity
 - Partial Mechanized Proof of Soundness
- Implementation
 - Accessible Interface
 - Type-Error Messages with Source Code Locations
 - Counter-Example Generation
- Evaluation
 - Automatic Verification of non-trivial Programs
 - Comparison to other tools

Restrictions

- No Inference
- Integers

Motivation	Type System	Soundness Justification	Related Work	Conclusion / Future Work	Literatur
oooooooo●	oooooooooooo	oooo	oo	oo	

Overview

- 1 Mutable Values
- 2 Mutable References
- 3 Function-Calls
- 4 Verification of `clamp` Example
- 5 Demo

Motivation
○○○○○○○

Type System
●○○○○○○○

Soundness Justification
○○○

Related Work
○○

Conclusion / Future Work
○○

Literatur

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
- $relax_ctx!\{ \dots \}$ in place of a statement

Refinement Types for Rust – Syntax

```
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 | φ }` 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 | φ }` in place of a type
- `relax_ctx!{ ... }` in place of a statement

Type Updates

```
fn decr() -> ty!{ w : i32 | w >= 0 } {
  let mut i = ... as ty!{ v: i32 | v > 0};
  i = i - 1;
  i
}
```

- Types need to change through execution
 - \Rightarrow type updates
 - Separation of program-variables and logic-variables
 - Γ association of program- to logic-variables and predicate
 - $\Gamma \vdash s \Rightarrow \Gamma'$ (Statement Type Checking)
 - $\Gamma \vdash e : \tau$ (Expression Typing)
 - on assignment: *replace* association, *append* predicate
 - observation: assignment can not invalidate existing predicates

Type Updates

```

fn decr() -> ty!{ w : i32 | w >= 0 } {
  //  $\Gamma_1 = (\{\}, \text{true})$ 
  let mut i = ... as ty!{ v: i32 | v > 0};
  //  $\Gamma_2 = (\{i \mapsto v\}, v > 0)$ 
  i = i - 1;
  //  $\Gamma_3 = (\{i \mapsto v_2\}, v > 0 \wedge v_2 \doteq v - 1)$ 
  i }

```

■ Types need to change through execution

- \Rightarrow type updates
- Separation of program-variables and logic-variables
- Γ association of program- to logic-variables and predicate
- $\Gamma \vdash s \Rightarrow \Gamma'$ (Statement Type Checking)
- $\Gamma \vdash e : \tau$ (Expression Typing)
- on assignment: *replace* association, *append* predicate
- observation: assignment can not invalidate existing predicates

Type Updates

```

fn decr() -> ty!{ w : i32 | w >= 0 } {
  //  $\Gamma_1 = (\{\}, \text{true})$ 
  let mut i = ... as ty!{ v: i32 | v > 0};
  //  $\Gamma_2 = (\{i \mapsto v\}, v > 0)$ 
  i = i - 1;
  //  $\Gamma_3 = (\{i \mapsto v_2\}, v > 0 \wedge v_2 \doteq v - 1)$ 
  i }

```

$$\begin{array}{c}
\text{INTRO-SUB} \quad \frac{\Gamma \vdash e : \tau \quad \Gamma \vdash \tau \preceq \tau'}{\Gamma \vdash e \text{ as } \tau' : \tau'} \\
\\
\text{DECL} \quad \frac{\Gamma \vdash e : \{\beta : b \mid \varphi\}}{\Gamma \vdash \text{let } x = e \Rightarrow \Gamma[x \mapsto \beta], \varphi}
\end{array}$$

Type Updates

```

fn decr() -> ty!{ w : i32 | w >= 0 } {
  //  $\Gamma_1 = (\{\}, \text{true})$ 
  let mut i = ... as ty!{ v : i32 | v > 0 };
  //  $\Gamma_2 = (\{i \mapsto v\}, v > 0)$ 
  i = i - 1;
  //  $\Gamma_3 = (\{i \mapsto v_2\}, v > 0 \wedge v_2 \doteq v - 1)$ 
  i }

```

$$\text{BINOP} \frac{\Gamma \vdash \alpha \text{ fresh}}{\Gamma \vdash x_1 \odot x_2 : \{\alpha : b \mid \alpha \simeq \llbracket x_1 \odot x_2 \rrbracket \Gamma\}}$$

$$\text{ASSIGN} \frac{\Gamma \vdash e : \{\beta : b \mid \varphi\}}{\Gamma \vdash x = e \Rightarrow \Gamma[x \mapsto \beta], \varphi}$$

Type Updates

```
fn decr() -> ty!{ w : i32 | w >= 0 } {
  //  $\Gamma_1 = (\{\}, \text{true})$ 
  let mut i = ... as ty!{ v: i32 | v > 0 };
  //  $\Gamma_2 = (\{i \mapsto v\}, v > 0)$ 
  i = i - 1;
  //  $\Gamma_3 = (\{i \mapsto v_2\}, v > 0 \wedge v_2 \doteq v - 1)$ 
  i }
```

$$\text{SEQ} \frac{\Gamma \vdash s_1 \Rightarrow \Gamma' \quad \Gamma' \vdash s_2 \Rightarrow \Gamma''}{\Gamma \vdash s_1; s_2 \Rightarrow \Gamma''}$$

References – Strong Updates

```

fn client() -> ty!{ v: i32 | v == 4 } {
  let a = 2;          // a : { v1 : i32 | v1 == 2 }
  let b = &mut a;     // b : { v2 : &i32 | v2 == &a }
  *b = 0; // changes a's value and type
  let c = &mut b;     // c : { v3 : &i32 | v3 == &b }
  **c = 4; // changes a's value and type
  a
}

```

Motivation
○○○○○○○

Type System
○○●○○○○○

Soundness Justification
○○○

Related Work
○○

Conclusion / Future Work
○○

Literatur

References – Strong Updates

```

fn client() -> ty!{ v: i32 | v == 4 } {
  let a = 2;           // a : { v1 : i32 | v1 == 2 }
  let b = &mut a;      // b : { v2 : &i32 | v2 == &a }
  *b = 0; // changes a's value and type
  let c = &mut b;      // c : { v3 : &i32 | v3 == &b }
  **c = 4; // changes a's value and type
  a
}

```

$$\text{LIT} \frac{\Gamma \vdash \alpha \text{ fresh}}{\Gamma \vdash v : \{\alpha : b \mid \alpha \simeq \llbracket v \rrbracket \Gamma\}}$$

References – Strong Updates

```

fn client() -> ty!{ v: i32 | v == 4 } {
  let a = 2;           // a : { v1 : i32 | v1 == 2 }
  let b = &mut a;      // b : { v2 : &i32 | v2 == &a }
  *b = 0; // changes a's value and type
  let c = &mut b;      // c : { v3 : &i32 | v3 == &b }
  **c = 4; // changes a's value and type
  a
}

```

$$\text{REF} \frac{\Gamma \vdash \alpha \text{ fresh}}{\Gamma \vdash \&x : \{\alpha : \&b \mid \alpha \simeq \llbracket \&x \rrbracket \Gamma\}}$$

References – Strong Updates

```
fn client() -> ty!{ v: i32 | v == 4 } {
  let a = 2;           // a : { v1 : i32 | v1 == 2 }
  let b = &mut a;      // b : { v2 : &i32 | v2 == &a }
  *b = 0; // changes a's value and type
  let c = &mut b;      // c : { v3 : &i32 | v3 == &b }
  **c = 4; // changes a's value and type
  a
}
```

$$\text{ASSIGN-STRONG} \frac{\Gamma(z) = \beta \quad \Gamma \vdash x \in \{\&y\} \quad \Gamma \vdash \gamma \text{ fresh}}{\Gamma \vdash *x = z \Rightarrow \Gamma[y \mapsto \gamma], \gamma \doteq \beta}$$

(Also ASSIGN-WEAK)

References – Strong Updates

```

fn client() -> ty!{ v: i32 | v == 4 } {
  let a = 2;           // a : { v1 : i32 | v1 == 2 }
  let b = &mut a;      // b : { v2 : &i32 | v2 == &a }
  *b = 0; // changes a's value and type
  let c = &mut b;      // c : { v3 : &i32 | v3 == &b }
  **c = 4; // changes a's value and type
  a
}
  
```

$$\text{VAR} \frac{\Gamma \vdash \alpha \text{ fresh}}{\Gamma \vdash x : \{\alpha : b \mid \alpha \simeq \llbracket x \rrbracket \Gamma\}}$$

Mutable Arguments

```

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);
    ...
}

```

Mutable Arguments

```

fn clamp(
  a: &mut ty!{ a1 : i32 | true => a2 | a2 <= b1 },
  b: ty!{ b1: i32 }
) {
  //  $\Gamma_1 = (\{a \mapsto v_1, arg_0 \mapsto a_1, b \mapsto b_1\},$ 
  //            $v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
  if *a > b { *a = b }
  //  $\Gamma_2 = (\{a \mapsto v_1, arg_0 \mapsto v_2, b \mapsto b_1\},$ 
  //            $v_2 \leq b_1 \wedge v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
}

```

Motivation	Type System	Soundness Justification	Related Work	Conclusion / Future Work	Literatur
oooooooo	ooooo●oooo	ooo	oo	oo	

Mutable Arguments

```
fn clamp(
  a: &mut ty!{ a1 : i32 | true => a2 | a2 <= b1 },
  b: ty!{ b1: i32 }
) {
  //  $\Gamma_1 = (\{a \mapsto v_1, arg_0 \mapsto a_1, b \mapsto b_1\},$ 
  //            $v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
  if *a > b { *a = b }
  //  $\Gamma_2 = (\{a \mapsto v_1, arg_0 \mapsto v_2, b \mapsto b_1\},$ 
  //            $v_2 \leq b_1 \wedge v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
}
```

- $ty! \{ \alpha : b \mid \varphi \Rightarrow \beta \mid \psi \}$
- Callee requires φ for reference destination α
- Callee ensures ψ for reference destination β
- Of course, multiple arguments possible

Mutable Arguments

```
fn clamp(
  a: &mut ty!{ a1 : i32 | true => a2 | a2 <= b1 },
  b: ty!{ b1: i32 }
) {
  //  $\Gamma_1 = (\{a \mapsto v_1, arg_0 \mapsto a_1, b \mapsto b_1\},$ 
  //            $v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
  if *a > b { *a = b }
  //  $\Gamma_2 = (\{a \mapsto v_1, arg_0 \mapsto v_2, b \mapsto b_1\},$ 
  //            $v_2 \leq b_1 \wedge v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
}
```

Mutable Arguments

```

fn clamp(
  a: &mut ty!{ a1 : i32 | true => a2 | a2 <= b1 },
  b: ty!{ b1: i32 }
) {
  //  $\Gamma_1 = (\{a \mapsto v_1, arg_0 \mapsto a_1, b \mapsto b_1\},$ 
  //            $v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
  if *a > b { *a = b }
  //  $\Gamma_2 = (\{a \mapsto v_1, arg_0 \mapsto v_2, b \mapsto b_1\},$ 
  //            $v_2 \leq b_1 \wedge v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
}

```

Motivation
○○○○○○○

Type System
○○○○●○○○

Soundness Justification
○○○

Related Work
○○

Conclusion / Future Work
○○

Literatur

Sub-Context

```

fn clamp(
  a: &mut ty!{ a1 : i32 | true => a2 | a2 <= b1 },
  b: ty!{ b1: i32 }
) {
  //  $\Gamma_1 = (\{a \mapsto v_1, arg_0 \mapsto a_1, b \mapsto b_1\},$ 
  //            $v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
  if *a > b { *a = b }
  //  $\Gamma_2 = (\{a \mapsto v_1, arg_0 \mapsto v_2, b \mapsto b_1\},$ 
  //            $v_2 \leq b_1 \wedge v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
}

```

- still left: proof obligation from signature
 $a_2 \leq b_1$
- i.e. is Γ_2 a valid end-state?

Sub-Context

```

fn clamp(
  a: &mut ty!{ a1 : i32 | true => a2 | a2 <= b1 },
  b: ty!{ b1: i32 }
) {
  //  $\Gamma_1 = (\{a \mapsto v_1, arg_0 \mapsto a_1, b \mapsto b_1\},$ 
  //            $v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
  if *a > b { *a = b }
  //  $\Gamma_2 = (\{a \mapsto v_1, arg_0 \mapsto v_2, b \mapsto b_1\},$ 
  //            $v_2 \leq b_1 \wedge v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
}

```

- still left: proof obligation from signature $a_2 \leq b_1$
- i.e. is Γ_2 a valid end-state?
- generalize notion of sub-types to context: sub-context

Sub-Context

```

fn clamp(
  a: &mut ty!{ a1 : i32 | true => a2 | a2 <= b1 },
  b: ty!{ b1: i32 }
) {
  //  $\Gamma_1 = (\{a \mapsto v_1, arg_0 \mapsto a_1, b \mapsto b_1\},$ 
  //            $v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
  if *a > b { *a = b }
  //  $\Gamma_2 = (\{a \mapsto v_1, arg_0 \mapsto v_2, b \mapsto b_1\},$ 
  //            $v_2 \leq b_1 \wedge v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
}

```

- still left: proof obligation from signature
 $a_2 \leq b_1$
- i.e. is Γ_2 a valid end-state?
- generalize notion of sub-types to context:
sub-context
- expected state:
 $\Gamma_e = (\{arg_0 \mapsto a_2, b \mapsto b_1\}, a_2 \leq b_1)$

Sub-Context

```

fn clamp(
  a: &mut ty!{ a1 : i32 | true => a2 | a2 <= b1 },
  b: ty!{ b1: i32 }
) {
  //  $\Gamma_1 = (\{a \mapsto v_1, arg_0 \mapsto a_1, b \mapsto b_1\},$ 
  //            $v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
  if *a > b { *a = b }
  //  $\Gamma_2 = (\{a \mapsto v_1, arg_0 \mapsto v_2, b \mapsto b_1\},$ 
  //            $v_2 \leq b_1 \wedge v_1 \doteq \&arg_0 \wedge true \wedge true)$ 
}

```

- still left: proof obligation from signature
 $a_2 \leq b_1$
- i.e. is Γ_2 a valid end-state?
- generalize notion of sub-types to context:
sub-context
- expected state:
 $\Gamma_e = (\{arg_0 \mapsto a_2, b \mapsto b_1\}, a_2 \leq b_1)$
- show: $\Gamma_2 \preceq \Gamma_e$

Sub-Context

$$\begin{array}{c} \models \Phi'[\mu'(x) \triangleright \mu(x) \mid x \in \text{dom}(\mu')] \rightarrow \Phi \\ \text{dom}(\mu') \subseteq \text{dom}(\mu) \\ \hline \preceq\text{-CTX} \quad (\mu, \Phi) \preceq (\mu', \Phi') \end{array}$$

- still left: proof obligation from signature
 $a_2 \leq b_1$
- i.e. is Γ_2 a valid end-state?
- generalize notion of sub-types to context: sub-context
- expected state:
 $\Gamma_e = (\{arg_0 \mapsto a_2, b \mapsto b_1\}, a_2 \leq b_1)$
- show: $\Gamma_2 \preceq \Gamma_e$

Mutable Calls

```
fn client(...) {
  ...
  //  $\Gamma_1 = (\{x \mapsto v_1, y \mapsto v_2\}, \dots)$ 
  clamp(&mut x, 5);
  //  $\Gamma_2 = (\{x \mapsto v_3, y \mapsto v_2\}, \dots \wedge v_3 \leq 5)$ 
  clamp(&mut y, 6);
  //  $\Gamma_3 = (\{x \mapsto v_3, y \mapsto v_4\}, \dots \wedge v_3 \leq 5 \wedge v_4 \leq 6)$ 
  print!(x);
  ...
}
```

- append predicates from callee to context
- update association of logic variables

SMT Request

...

Motivation
oooooooo

Type System
oooooooo●oo

Soundness Justification
ooo

Related Work
oo

Conclusion / Future Work
oo

Literatur

Example Error Message

...

Motivation
oooooooo

Type System
oooooooo●o

Soundness Justification
ooo

Related Work
oo

Conclusion / Future Work
oo

Literatur

Ecosystem Integration

...

Motivation
○○○○○○○

Type System
○○○○○○○○●

Soundness Justification
○○○

Related Work
○○

Conclusion / Future Work
○○

Literatur

Progress

If $\Gamma \vdash s_1, \sigma : \Gamma \Rightarrow \Gamma_2$ and $s_1 \neq \text{unit}$, 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

Partially Mechanized Proof in Lean 4

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:

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

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 $\sigma : (\mu, \Phi_2)$.
- If $\sigma : (\mu, \Phi)$ and $\text{FV}(\Phi) \subseteq \text{dom}(\mu)$, then $\models \Phi[\mu(x) \triangleright \llbracket \sigma(x) \rrbracket \mid x \in \text{dom}(\mu)]$

Intermediate Steps

Conformance of Symbolic Execution

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

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

Reference Predicates are Conservative

If $\sigma : \Gamma$ and $\Gamma \vdash *x \in \{y_1, \dots, y_n\}$ then $\llbracket \sigma(x) \rrbracket = \&y_i$ for some $i \in 1, \dots, n$

Rare case where conservative typing requires

Sub-Context Relation is Conservative

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

Related Work

Refinement Types and Mutability

- Rondon et al. [RKJ10], Bakst and Jhala [BJ16]: Refinement Types for C subset. Lack of guarantees requires ad-hoc mechanisms to control aliasing
- Lanzinger [Lan21]: Property Types in Java (only immutable). Bachmeier [Bac22]: Extension using Ownership System
- Toman et al. [Tom+20] (ConSORT): Fractional Ownership, strong and weak updates

Rust verification

- Ullrich [Ull16]: Translation to Lean; linear mutation chain. Denis et al [DJM21] similar, but to Why3
- Astrauskas et al. [Ast+19] (Prusti): heavy-weight verification, translation to separation logic (Viper)
- Matsushita et al. [MTK20] (RustHorn): constrained Horn clauses

Motivation ○○○○○○○	Type System ○○○○○○○○○	Soundness Justification ○○○	Related Work ●○	Conclusion / Future Work ○○	Literatur
-----------------------	--------------------------	--------------------------------	--------------------	--------------------------------	-----------

Related Work: Flux – Refinement Types for Rust

- MIR vs. HIR
- specification in comments vs. embedding in types
- context inclusions vs. sub context
- distinction strong and weak references vs. dynamic choice by typ checking rules
- explicit introduction of logic variables vs. ad-hoc
- formalization based on RustBelt vs. formalization based on own language
- missing in Corten: records & inference
- otherwise: similar capabilities

```
// Flux
//@ ensures *self: i32<n+1>;
fn increment(&strg v : i32<n>) -> ()
//@ requires n > 0
//@ ensures *self: i32<n-1>;
fn decrement(&strg v : i32<n>) -> ()

// Corten
fn increment(n: &mut ty!{
    n1: Nat => n1 | n1 == n1+1 }
) -> ();
fn decrement(n: &mut ty!{
    v1: Nat | v1 > 0 => v2 | v2 == v1-1 }
) -> ();
```

Motivation
○○○○○○○

Type System
○○○○○○○○○

Soundness Justification
○○○

Related Work
●○○

Conclusion / Future Work
○○

Literatur

Future Work

- Records & ADTs
 - More Syntax, Nested Structures
 - Variant Distinction
- Predicate Generics (Abstract Predicates)
 - Uninterpreted Functions in Types
- Concurrency using Predicate Generics?
 - Use Uninterpreted Functions
 - Interesting, because unusual guarantees in Rust

Conclusion

- Working Refinement Type System for Rust with Mutability
- Minimal Interface
- Soundness Justification
- Evaluation

Motivation
○○○○○○○

Type System
○○○○○○○○○

Soundness Justification
○○○

Related Work
○○

Conclusion / Future Work
○●

Literatur

Literatur I

- [1] Vytautas Astrauskas u. a. „Leveraging rust types for modular specification and verification“. In: *Proceedings of the ACM on Programming Languages* 3 (OOPSLA 10. Okt. 2019), S. 1–30. ISSN: 2475-1421. DOI: 10.1145/3360573. URL: <https://dl.acm.org/doi/10.1145/3360573> (besucht am 23.02.2022).
- [2] Joshua Bachmeier. *Property Types for Mutable Data Structures in Java*. 2022. DOI: 10.5445/IR/1000150318. URL: <https://publikationen.bibliothek.kit.edu/1000150318> (besucht am 03.10.2022).
- [3] Alexander Bakst und Ranjit Jhala. „Predicate Abstraction for Linked Data Structures“. In: *Verification, Model Checking, and Abstract Interpretation*. Hrsg. von Barbara Jobstmann und K. Rustan M. Leino. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2016, S. 65–84. ISBN: 978-3-662-49122-5. DOI: 10.1007/978-3-662-49122-5_3.

Motivation oooooooo	Type System oooooooooooo	Soundness Justification oooo	Related Work oo	Conclusion / Future Work oo	Literatur
------------------------	-----------------------------	---------------------------------	--------------------	--------------------------------	-----------

Literatur II

- [4] Xavier Denis, Jacques-Henri Jourdan und Claude Marché. „The Creusot Environment for the Deductive Verification of Rust Programs“. Diss. Inria Saclay-Île de France, 2021.
- [5] Florian Lanzinger. „Property Types in Java: Combining Type Systems and Deductive Verification“. Master Thesis. Karlsruher Institut für Technologie, Feb. 2021.
- [6] Yusuke Matsushita, Takeshi Tsukada und Naoki Kobayashi. „RustHorn: CHC-based verification for Rust programs“. In: *European Symposium on Programming*. Springer, Cham, 2020, S. 484–514.
- [7] Patrick M. Rondon, Ming Kawaguchi 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).

Motivation
○○○○○○○

Type System
○○○○○○○○○

Soundness Justification
○○○

Related Work
○○

Conclusion / Future Work
○○

Literatur

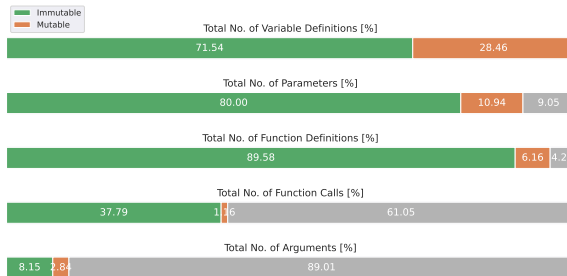
Literatur III

- [8] Patrick Maxim Rondon, Ming Kawaguchi und Ranjit Jhala. „Low-level liquid types“. In: *Proceedings of the 37th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages*. POPL '10. New York, NY, USA: Association for Computing Machinery, 17. Jan. 2010, S. 131–144. ISBN: 978-1-60558-479-9. DOI: 10.1145/1706299.1706316. URL: <https://doi.org/10.1145/1706299.1706316> (besucht am 16. 09. 2022).
- [9] John Toman u. a. „ConSORT: Context- and Flow-Sensitive Ownership Refinement Types for Imperative Programs“. In: *Programming Languages and Systems*. Hrsg. von Peter Müller. Cham: Springer International Publishing, 2020, S. 684–714. ISBN: 978-3-030-44914-8. DOI: 10.1007/978-3-030-44914-8_25.
- [10] Sebastian Ullrich. „Simple Verification of Rust Programs via Functional Purification“. In: (6. Dez. 2016), S. 65.

Motivation ○○○○○○○	Type System ○○○○○○○○○	Soundness Justification ○○○	Related Work ○○	Conclusion / Future Work ○○	Literatur
-----------------------	--------------------------	--------------------------------	--------------------	--------------------------------	-----------

Empirical Use-Case Analysis

- public open-source code (crates.io)
- about 64 million lines of Rust code
- syntactical analysis



decr Typing Tree

let $\Gamma_2 = \Gamma[i \mapsto v_1], v > 0$ and $\tau = \{v : i32 \mid v > 0\}$

$$\begin{array}{c}
 \text{INTRO-SUB} \frac{\Gamma_1 \vdash \dots : \tau' \quad \Gamma_1 \vdash \tau' \preceq \tau}{\Gamma_1 \vdash \dots \text{ as } \tau : \tau} \\
 \text{DECL} \frac{\Gamma_1 \vdash \dots \text{ as } \tau : \tau}{\Gamma_1 \vdash \text{let } i = \dots \text{ as } \tau \Rightarrow \Gamma_2} \\
 \text{SEQ} \frac{\Gamma_1 \vdash \text{let } i = \dots \text{ as } \tau \Rightarrow \Gamma_2 \quad \text{ASS} \frac{\text{BINOP} \frac{\Gamma_1 \vdash v_2 \text{ fresh}}{\Gamma_1 \vdash i - 1 : \{v_2 : i32 \mid v_2 \dot{=} v - 1\}}}{\Gamma_2 \vdash i = i - 1 \Rightarrow \Gamma[i \mapsto v_2], v > 0, v_2 \dot{=} v - 1}}{\Gamma_1 \vdash \text{let } i = \dots \text{ as } \tau; i = i - 1 \Rightarrow \Gamma[i \mapsto v_2], v > 0, v_2 \dot{=} v - 1}
 \end{array}$$

Expression Typing $\Gamma \vdash e : \tau$

$$\begin{array}{c}
 \text{LIT} \frac{\Gamma \vdash \alpha \text{ fresh}}{\Gamma \vdash v : \{\alpha : b \mid \alpha \simeq \llbracket v \rrbracket \Gamma\}} \quad \text{BINOP} \frac{\Gamma \vdash \alpha \text{ fresh}}{\Gamma \vdash x_1 \odot x_2 : \{\alpha : b \mid \alpha \simeq \llbracket x_1 \odot x_2 \rrbracket \Gamma\}} \\
 \text{VAR} \frac{\Gamma \vdash \alpha \text{ fresh}}{\Gamma \vdash x : \{\alpha : b \mid \alpha \simeq \llbracket x \rrbracket \Gamma\}} \quad \text{INTRO-SUB} \frac{\Gamma \vdash e : \tau \quad \Gamma \vdash \tau \preceq \tau'}{\Gamma \vdash e \text{ as } \tau' : \tau'}
 \end{array}$$

Statement Type Checking $\Gamma \vdash s \Rightarrow \Gamma'$

$$\begin{array}{c}
 \text{IF} \frac{\Gamma, \Gamma(x) \doteq \text{true} \vdash s_t \Rightarrow \Gamma' \quad \Gamma, \Gamma(x) \doteq \text{false} \vdash s_e \Rightarrow \Gamma'}{\Gamma \vdash \text{if } x \text{ then } s_t \text{ else } s_e \Rightarrow \Gamma'} \\
 \text{SEQ} \frac{\Gamma \vdash s_1 \Rightarrow \Gamma' \quad \Gamma' \vdash s_2 \Rightarrow \Gamma''}{\Gamma \vdash s_1; s_2 \Rightarrow \Gamma''} \\
 \text{DECL} \frac{\Gamma \vdash e : \{\beta : b \mid \varphi\}}{\Gamma \vdash \text{let } x = e \Rightarrow \Gamma[x \mapsto \beta], \varphi} \quad \text{ASSIGN} \frac{\Gamma \vdash e : \{\beta : b \mid \varphi\}}{\Gamma \vdash x = e \Rightarrow \Gamma[x \mapsto \beta], \varphi}
 \end{array}$$

Expression Typing $\Gamma \vdash e : \tau$

$$\text{REF} \frac{\Gamma \vdash \alpha \text{ fresh}}{\Gamma \vdash \&x : \{\alpha : \&b \mid \alpha \simeq \llbracket \&x \rrbracket \Gamma\}}$$

$$\text{VAR-DEREF} \frac{\Gamma \vdash x \in \{\&y\} \quad \Gamma \vdash y : \tau}{\Gamma \vdash *x : \tau}$$

Statement Type Checking $\Gamma \vdash s \Rightarrow \Gamma'$

$$\text{ASSIGN-STRONG} \frac{\Gamma(z) = \beta \quad \Gamma \vdash x \in \{\&y\} \quad \Gamma \vdash \gamma \text{ fresh}}{\Gamma \vdash *x = z \Rightarrow \Gamma[y \mapsto \gamma], \gamma \doteq \beta}$$

Expression Typing $\Gamma \vdash e : \tau$

$$\text{REF} \frac{\Gamma \vdash \alpha \text{ fresh}}{\Gamma \vdash \&x : \{\alpha : \&b \mid \alpha \simeq \llbracket \&x \rrbracket \Gamma\}}$$

$$\text{VAR-DEREF} \frac{\Gamma \vdash x \in \{\&y\} \quad \Gamma \vdash y : \tau}{\Gamma \vdash *x : \tau}$$

Statement Type Checking $\Gamma \vdash s \Rightarrow \Gamma'$

$$\text{ASSIGN-STRONG} \frac{\Gamma(z) = \beta \quad \Gamma \vdash x \in \{\&y\} \quad \Gamma \vdash \gamma \text{ fresh}}{\Gamma \vdash *x = z \Rightarrow \Gamma[y \mapsto \gamma], \gamma \doteq \beta}$$

$$\text{ASSIGN-WEAK} \frac{\Gamma \vdash e : \tau \quad \Gamma \vdash x \in \{\&y_1, \dots, \&y_n\}}{\Gamma \vdash y_i : \{\beta_i : b_i \mid \varphi_i\} \quad \Gamma \vdash \tau \preceq \{\beta_i : b_i \mid \varphi_i\}} \Gamma \vdash *x = e \Rightarrow \Gamma$$

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

Empirical Analysis
○○○○○

Zweiter Abschnitt
○○○●

Farben
○

Farbpalette

