Usable Language-Based Verification

Niki Vazou
University of Maryland

Formal Verification

Prove Properties of Software

Formal Verification

Prove Properties of Real Software

Formal Verification

Prove Properties of Real Software

“A plane will not crush”

Formal Verification

Prove Properties of Real Software

"Medical Equipments will properly work"

Formal Verification

Prove Properties of Real Software

"You passwords are SAFE"

Formal Verification, in Practise

Prove Properties of ~~Real Software~~

in Verification Specific Tools

Formal Verification, in Practice

Prove Properties ~~of Real Software~~

in Verification Specific Tools

Verification Specific Tools

```
Lemma plus_Snm_nSm : forall n m, S n + m = n + S m.
intros.
simpl in |- *.
rewrite (plus_comm n m).
rewrite (plus_comm n (S m)).
trivial with arith.
Qed.
```

"Plus is indeed associative!"

Verification Specific Tools

Difficult to use for Real Programs

Difficult to install

Special Syntax

No Compiler Optimizations

No Parallelism

Very Few Users!

Verification Specific Tools

Verification

Manual
Translation

Real Programs

My goal:

Verification of Real Programs

Verification of Real Programs

My approach:

Turn a Language into a Verifier

Reuse language's syntax, runtime, and users!

Verification of Real Programs

My approach:

Turn a Language into a Verifier

Target Language: Haskell

Turn a Haskell into a Verifier

Reuse language's syntax, runtime, and **users**!

I: Target Real Haskell Code

II: Application in **Industry**
Use Verification to speedup code

III: Application in **Education**
Teach verification in Haskell courses!

Haskell

+

Refinement Types

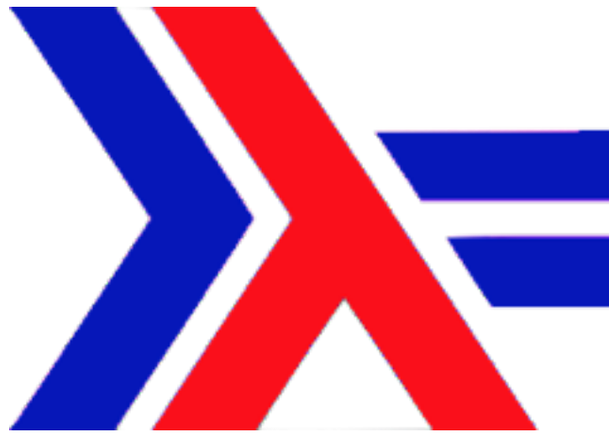
=

Haskell

Functional Programing Language

Based on

Strong Typing + λ-calculus

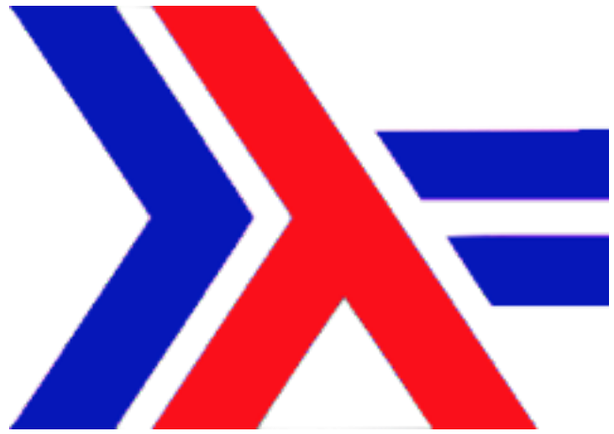


Well Typed Programs cannot go wrong!

Functional Programing Language

Based on

g Typing + λ-calculus



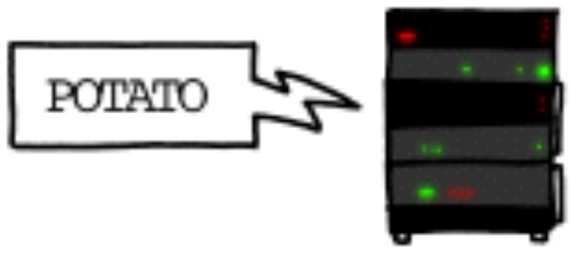
Fact Check.

Can we encode Heartbleed?

The Heartbleed Bug.
Buffer overflow in OpenSSL. 2015

HOW THE HEARTBLEED BUG WORKS:

SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).



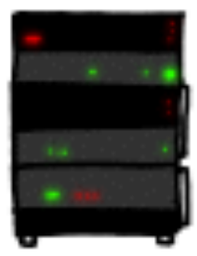
SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).

User Olivia from London wants pages about "man bees in car why". Note: Files for IP 375.381. 283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2cab9ff89bd3bff8

HMM...

User Olivia from London wants pages about "man bees in car why". Note: Files for IP 375.381. 283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2cab9ff89bd3bff8

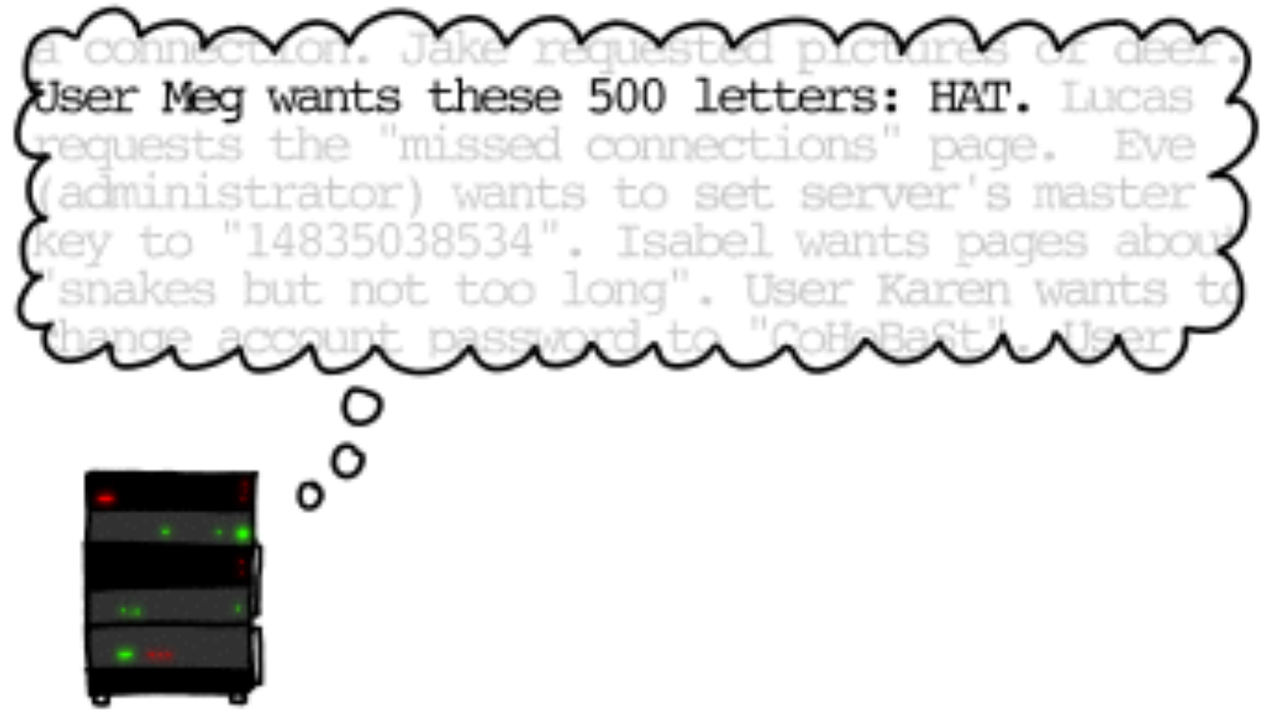
BIRD

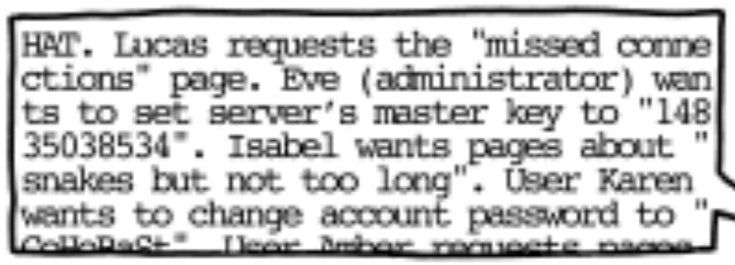


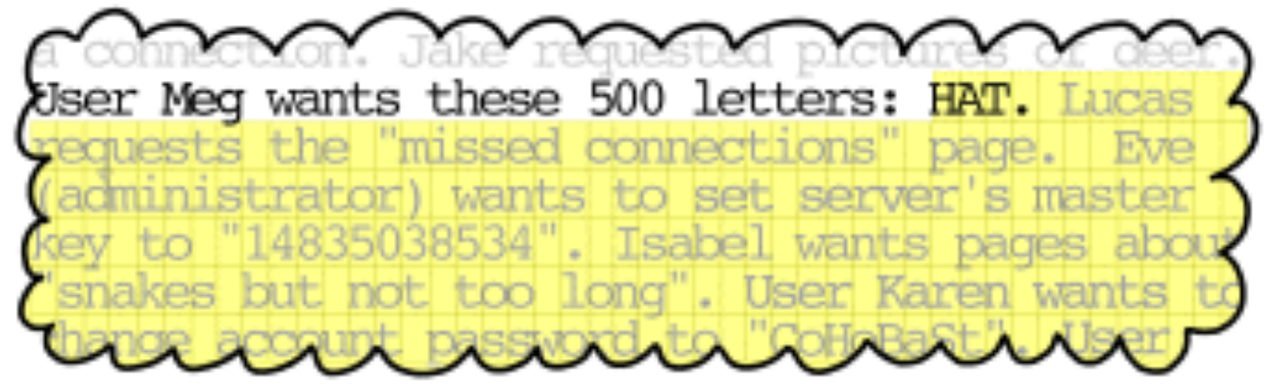
SERVER, ARE YOU STILL THERE?

User Meg wants these 500 letters: HAT. Lucas

SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).







VS.

VS.

```
λ>  :m +Data.Text Data.Text.Unsafe
λ> let pack = "hat"

λ> :t takeWord16
   takeWord16 :: Text -> Int -> Text
```

VS.

```
λ>  :m +Data.Text Data.Text.Unsafe
λ> let pack = "hat"

λ> takeWord16 pack True
    Type Error: Cannot match Bool vs Int
```

VS.

```
λ>  :m +Data.Text Data.Text.Unsafe
λ> let pack = "hat"

λ> takeWord16 pack 500
   “hat\58456\2594\SOH\NUL…
```


VS.

Valid Values for `takeWord16`?

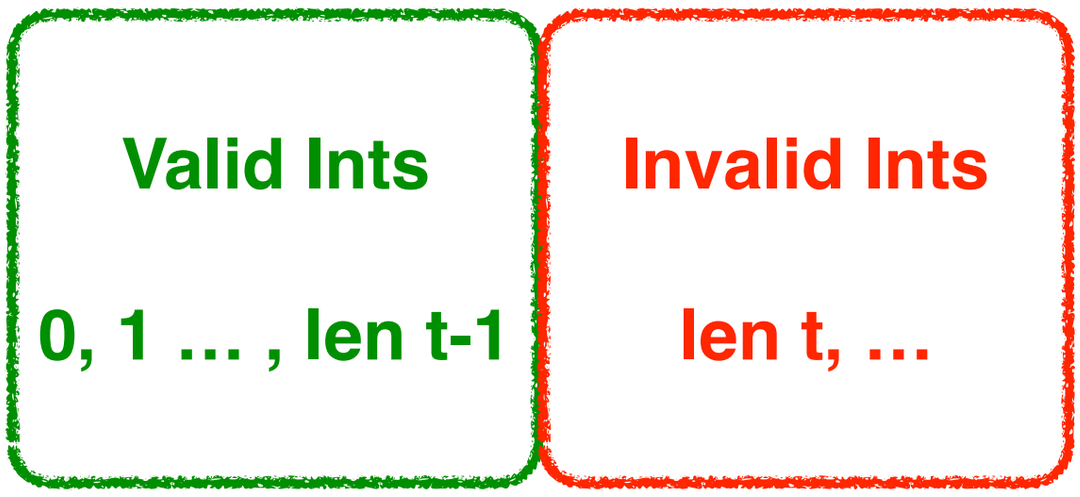
```
takeWord16 :: t:Text -> i:Int -> Text
```

All Ints

…, -2, -1, 0, 1, 2, 3, …

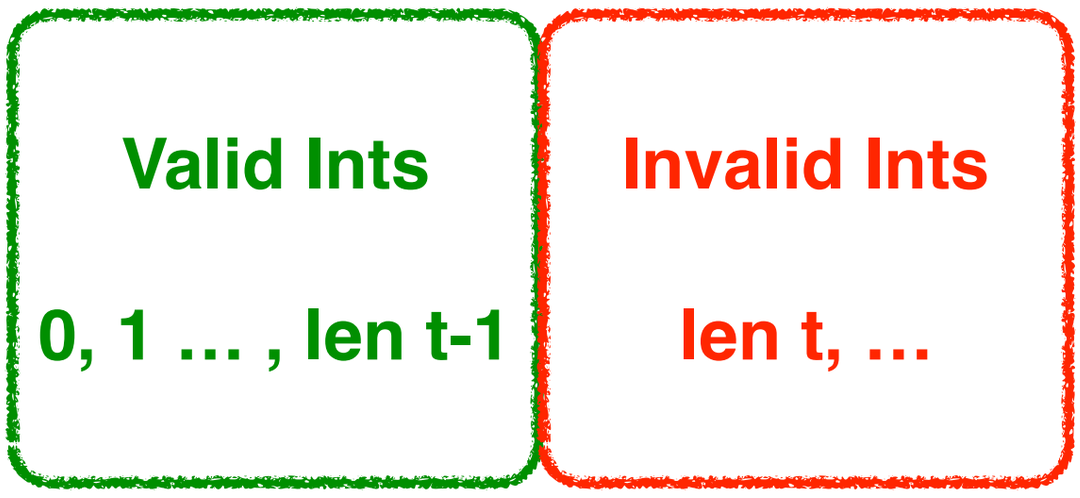
Valid Values for `takeWord16`?

```
takeWord16 :: t:Text -> i:Int -> Text
```



Refinement Types

```
take :: t:Text -> {v:Int | v < len t} -> Text
```



Refinement Types

```
take :: t:Text -> {v:Int | v < len t} -> Text
```

```
λ> :m +Data.Text Data.Text.Unsafe
λ> let pack = "hat"

λ> take pack 500
   Refinement Type Error
```

i.e. catch bugs before they occur!

Refinement Types

Checks valid arguments, under facts.

Checks valid arguments, under facts.

```
take :: t:Text->{v|v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in take x 500
```

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text
heartbleed = let x = "hat"
             in  take x 500
```

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

SMT-query

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v|v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

SMT-invalid

`len x = 3 => v = 500 => v < len x`

Checks valid arguments, under facts.

```
take :: t:Text->{v|v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

Checker reports **Error**

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in  take x 500
```

Checker reports **Error**

```
len x = 3 => v = 500 => v < len x
```

Checks valid arguments, under facts.

```
take :: t:Text->{v | v < len t}->Text

heartbleed = let x = "hat"
             in  take x 2
```

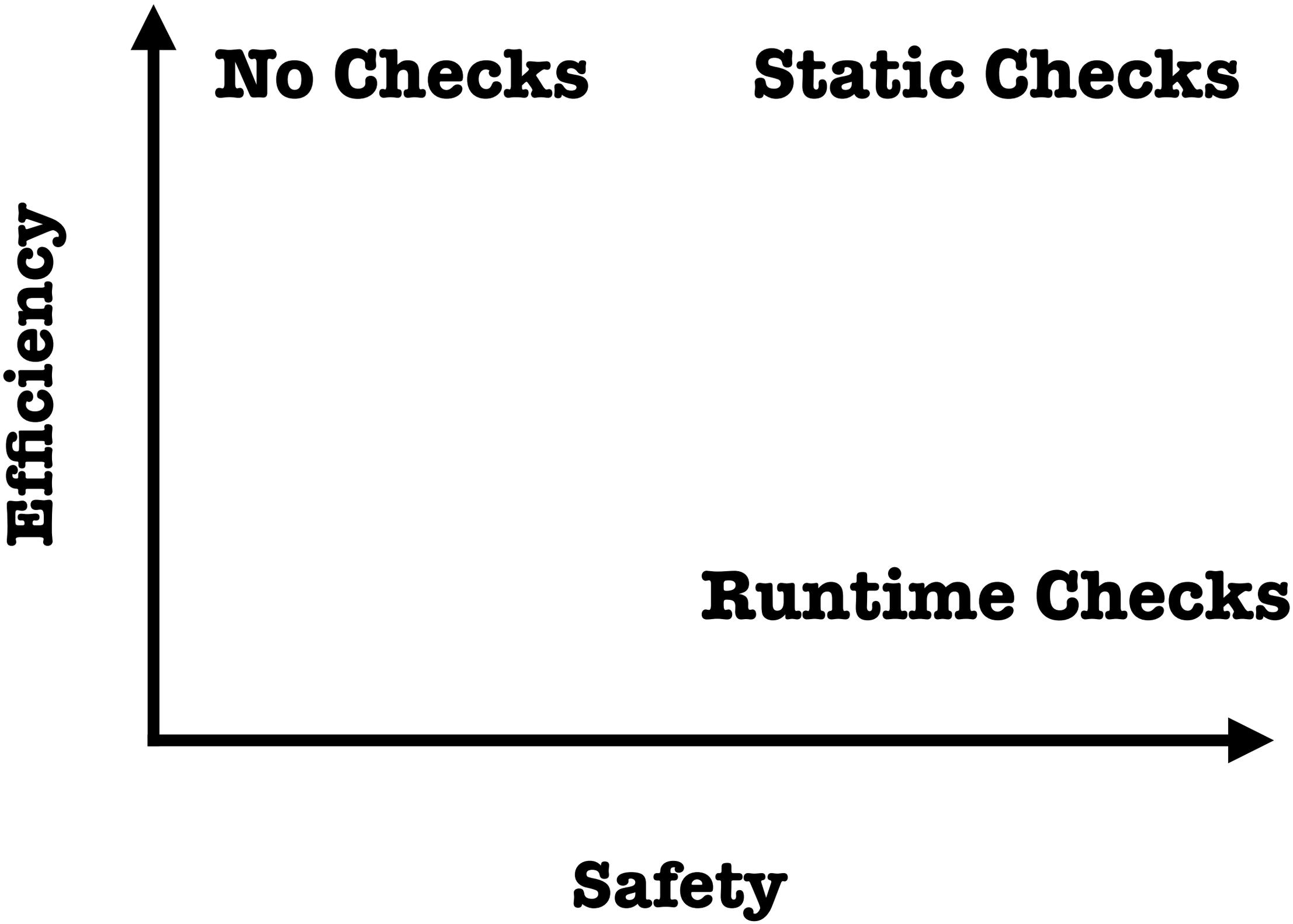
Checker reports **OK**

SMT-valid

```
len x = 3 => v = 2 => v < len x
```

Checks valid arguments, under facts.

Static Checks


No Checks
Static Checks
Efficiency
Runtime Checks
Safety

No Checks

```
take :: t:Text -> i:Int -> Text
take i t
  = Unsafe.takeWord16 i t
```

No Checks

```
take :: t:Text -> i:Int -> Text
take i t
 = Unsafe.takeWord16 i t
```

```
heartbleed = take "hat" 500
```

OK

No Checks

```
take :: t:Text->i:Int->Text
take i t
 = Unsafe.takeWord16 i t
```

```
heartbleed = take "hat" 500
```

OK

```
λ> heartbleed
λ> “hat\58456\2594\SOH\NUL…
```

UNSAFE

Runtime Checks

```
take :: t:Text -> i:Int -> Text
take i t | i < len t
  = Unsafe.takeWord16 i t
take i t
  = error “Out Of Bounds!”
```

Runtime Checks

```
take :: t:Text -> i:Int -> Text
take i t | i < len t
  = Unsafe.takeWord16 i t
take i t
  = error “Out Of Bounds!”
```

Runtime Checks

```
take :: t:Text -> i:Int -> Text
take i t | i < len t
  = Unsafe.takeWord16 i t
take i t
  = error “Out Of Bounds!”
```

```
heartbleed = take "hat" 500
```

OK

Runtime Checks

```
take :: t:Text->i:Int->Text
take i t | i < len t
 = Unsafe.takeWord16 i t
take i t
 = error “Out Of Bounds!”
```

OK

```
heartbleed = take "hat" 500
```

SAFE

```
λ> heartbleed
λ> *** Exception: Out Of Bounds!
```

Runtime Checks are expensive

```
take :: t:Text -> i:Int -> Text
take i t | i < len t
  = Unsafe.takeWord16 i t
take i t
  = error “Out Of Bounds!”
```

Static Checks

```
take :: t:Text->i:{i < len t}->Text
take i t | i < len t
  = Unsafe.takeWord16 i t
take i t
  = error “Out Of Bounds!”
```

Static Checks

```
take :: t:Text -> i:{i < len t} -> Text
take i t | i < len t
  = Unsafe.takeWord16 i t
  = take i t
  = error “Out Of Bounds!”
```

Static Checks

```
take :: t:Text->i:{i < len t}->Text
take i t
  = Unsafe.takeWord16 i t
```

Static Checks

```
take :: t:Text->i:{i < len t}->Text
take i t
 = Unsafe.takeWord16 i t
```

```
heartbleed = take "hat" 500
```

UNSAFE

Static Checks

Safe & Fast Code!

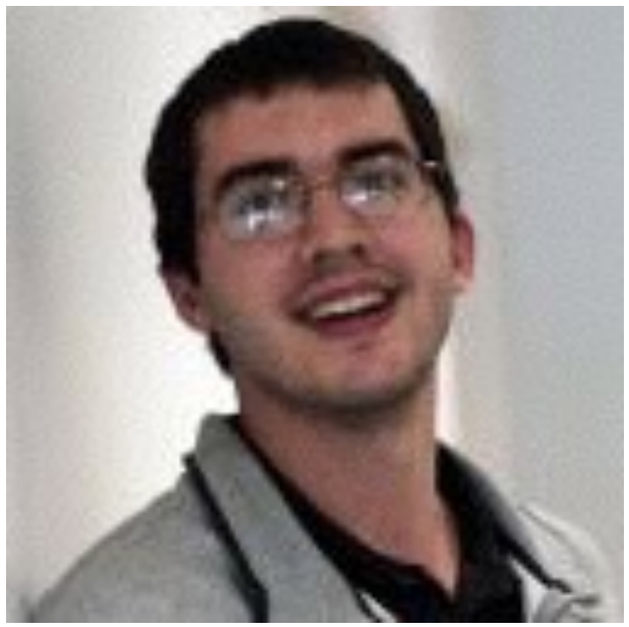
Static Checks

Safe & Fast Code!

Application: Speedup Parsing

Application: Speedup Parsing

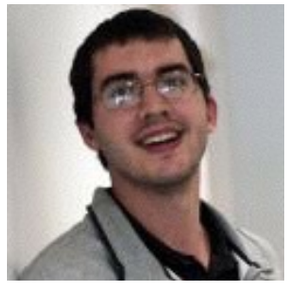
UDP:User Datagram Protocol



Gabriel Gonzalez

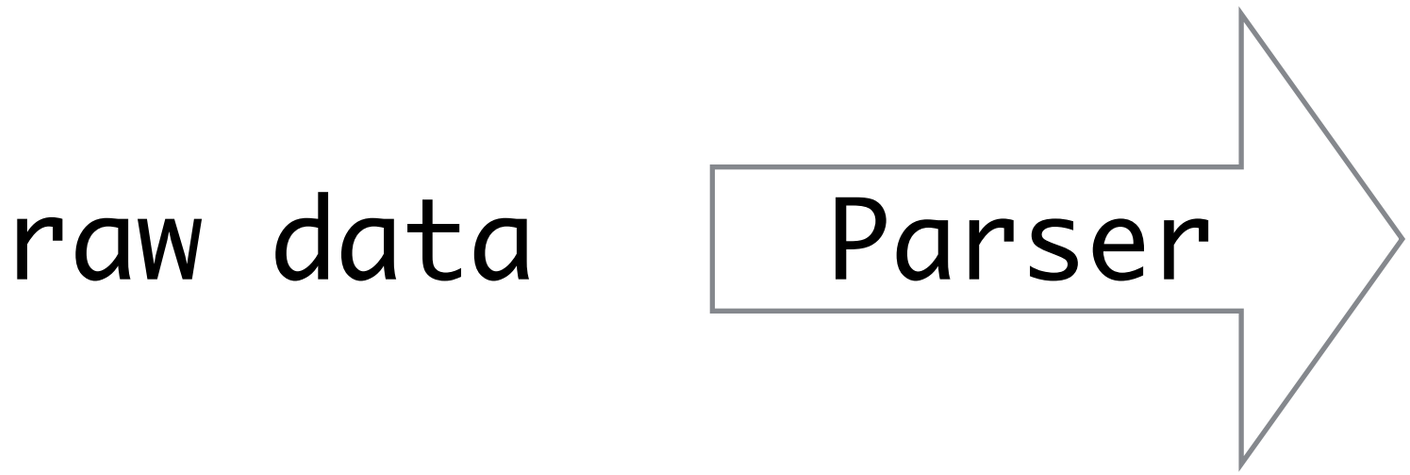
AWAKE

Application: Speedup Parsing

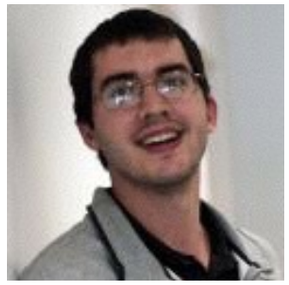


Gabriel Gonzalez
AWAKE

UDP:User Datagram Protocol



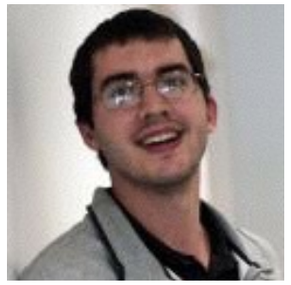
Application: Speedup Parsing



Gabriel Gonzalez
AWAKE

```
data UDP = UDP
    { udpSrcePort :: Text  -- 2 chars
    , udpDestPort :: Text  -- 2 chars
    , udpLength   :: Text  -- 2 chars
    , udpChecksum :: Text  -- 2 chars
    }
```

Application: Speedup Parsing



Gabriel Gonzalez
AWAKE

```
udpP :: Text -> UDP
udpP bs =
  let (udp1, bs1) = splitAt 2 bs
  let (udp2, bs2) = splitAt 2 bs1
  let (udp3, bs3) = splitAt 2 bs2
  let (udp4, bs4) = splitAt 2 bs3
  in UDP (udp1 upd2 udp3 upd4)
```

Safe but Slow (4 runtime checks)

Solution: Merge checks

Application: Speedup Parsing

Gabriel Gonzalez
AWAKE

```
udpP :: Text -> Maybe UDP
udpP bs =
  if length bs < 8 then
    let (udp1, bs1) = US.splitAt 2 bs
    let (udp2, bs2) = US.splitAt 2 bs1
    let (udp3, bs3) = US.splitAt 2 bs2
    let (udp4, bs4) = US.splitAt 2 bs3
    in Just (UDP udp1 upd2 udp3 upd4)
  else Nothing
```

Safe and Fast (1 runtime check!)

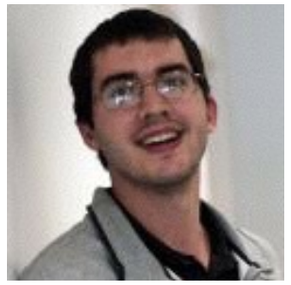
Application: Speedup Parsing

Gabriel Gonzalez
AWAKE

```
udpP :: Text -> Maybe UDP
udpP bs =
  if length bs < 8 then
    let (udp1, bs1) = US.splitAt 2 bs
    let (udp2, bs2) = US.splitAt 2 bs1
    let (udp3, bs3) = US.splitAt 4 bs2
    let (udp4, bs4) = US.splitAt 2 bs3
    in Just (UDP udp1 upd2 udp3 upd4)
  else Nothing
```

Safe and Fast, bur error prone

Application: Speedup Parsing



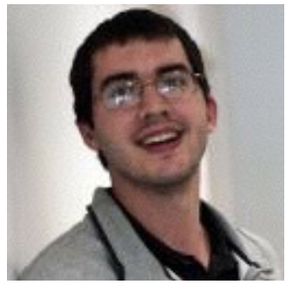
Gabriel Gonzalez
AWAKE

```
udpP :: Text -> Maybe UDP
udpP bs =
  if length bs < 8 then
    let (udp1, bs1) = US.splitAt 2 bs
        (udp2, bs2) = US.splitAt 2 bs1
        (udp3, udp4) = US.splitAt 2 bs2
    in Just (UDP udp1 udp2 udp3 udp4)
  else Nothing
```

```
splitAt :: i:Int -> t:{i < len t} ->
 (tl:{i = len tl}, tr:{len tr = len t - i})
```

Enforce Static Checks!

Application: Speedup Parsing



Gabriel Gonzalez

UNSAFE

```
udpP :: Text -> Maybe UDP
udpP bs =
  if length bs < 8 then
    let (udp1, bs1) = US.splitAt 2 bs0
    let (udp2, bs2) = US.splitAt 2 bs1
    let (udp3, bs3) = US.splitAt 4 bs2
    let (udp4, bs4) = US.splitAt 2 bs3
    in Just (UDP udp1 upd2 udp3 upd4)
  else Nothing
```

Enforce Static Checks!

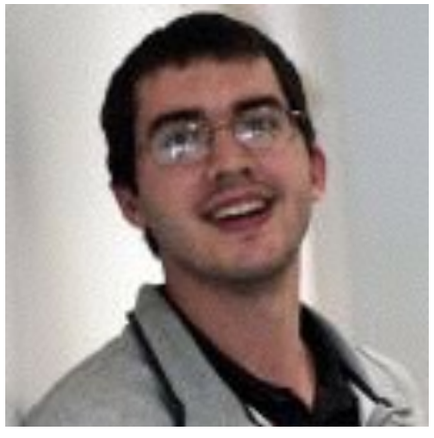
Application: Speedup Parsing

Gabriel Gonzalez
AWAKE

SAFE

```
udpP :: Text -> Maybe UDP
udpP bs =
  if length bs < 8 then
    let (udp1, bs1) = US.splitAt 2 bs
    let (udp2, bs2) = US.splitAt 2 bs1
    let (udp3, bs3) = US.splitAt 2 bs2
    let (udp4, bs4) = US.splitAt 2 bs3
    in Just (UDP udp1 upd2 udp3 upd4)
  else Nothing
```

Provably Correct & Faster (x6) Code!



Gabriel Gonzalez

AWAKE

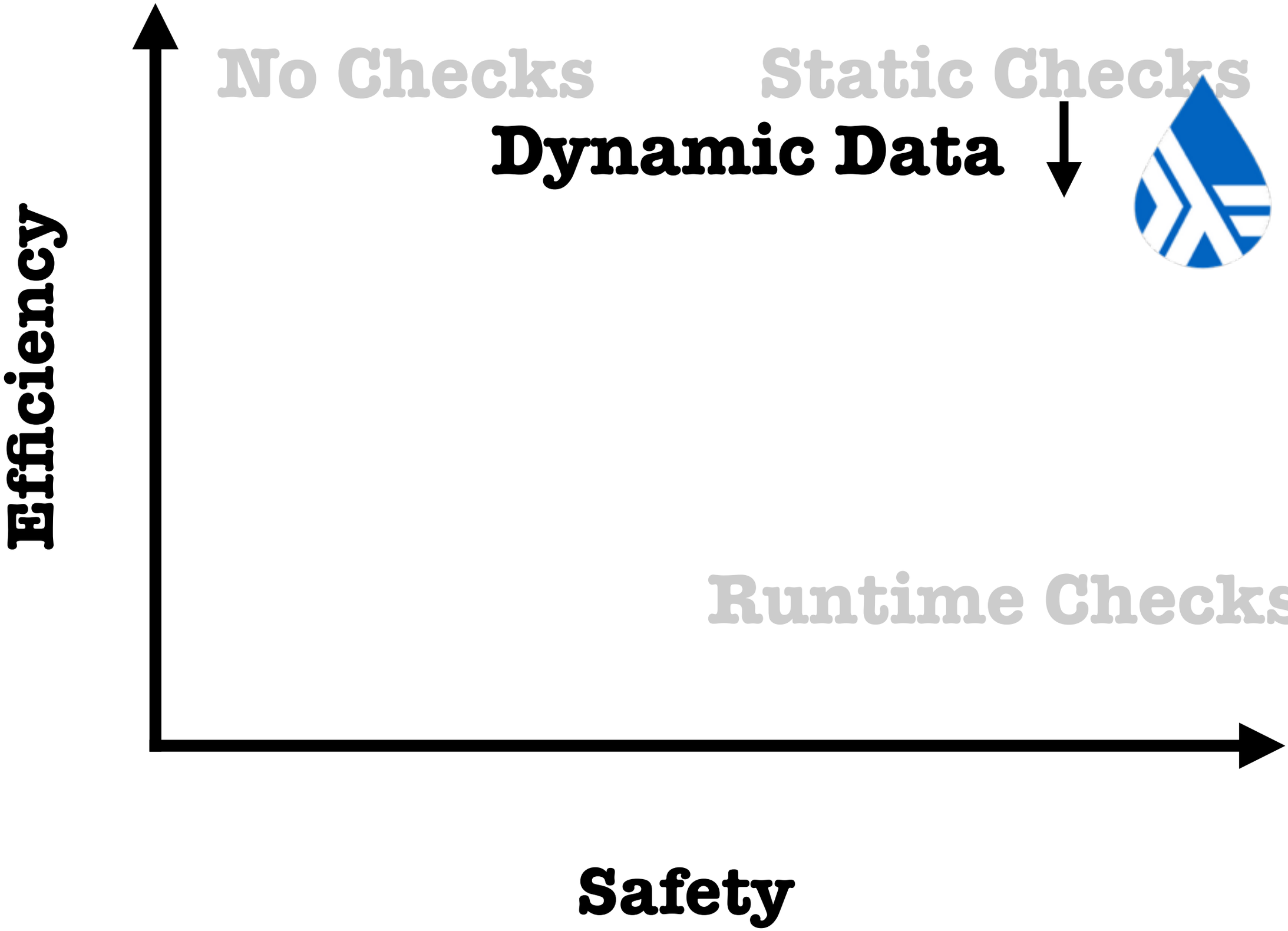
Application: Speedup Parsing

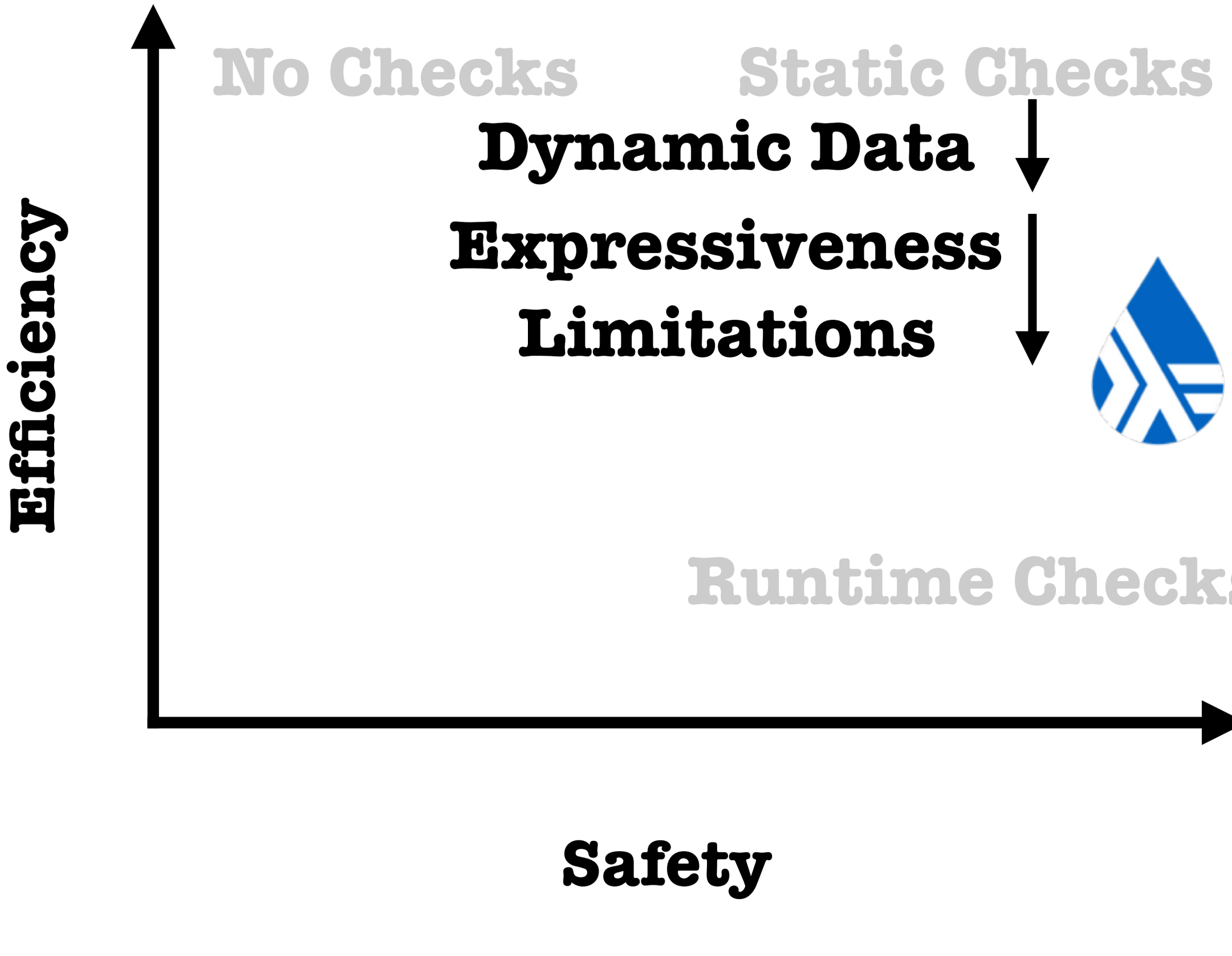
Provably Correct & Faster (x6) Code!

Safe & Efficient Code!

Safe & Efficient Code!


No Checks
Static Chec
Runtime Checks
Efficiency
Safety


No Checks
Static Checks
Dynamic Data
Runtime Checks
Efficiency
Safety


No Checks
Static Checks
Dynamic Data
Expressiveness
Limitations
Runtime Checks
Efficiency
Safety

Expressiveness

What properties can be expressed in types?

Expressiveness vs. Automation

Expressiveness vs. Automation

If p is safe indexing ...

```
{t:Text | i < len t }
```

... then SMT-automatic verification.

Expressiveness vs. Automation

If p from decidable theories ...

{t:a | p}

... then SMT-automatic verification.

Expressiveness vs. Automation

If p from decidable theories ...

$$\{t : a \mid p\}$$

Boolean Logic

(QF) Linear Arithmetic

Uninterpreted Functions ...

... then SMT-automatic verification.

What about expressiveness?

Automation

Refinement Types

Refinement Reflection

(Vazou *et al.* '18)

F*, Dafny

Tactics

Dependent Types
(Coq, Agda, ...)

Expressiveness

Classic Refinement Types

```
fib :: i:{Int|0≤i} -> {v:Int|0<v∧i≤v}
fib i
  | i≤1          = 1
  | otherwise = fib (i-1) + fib (i-2)
```

SAFE

Can we increase expressiveness?

Can we increase expressiveness?

```
fib :: i:{Int|0≤i} -> {v:Int|0<v∧i≤v}
fib i
  | i≤1          = 1
  | otherwise = fib (i-1) + fib (i-2)
```

How to express **theorems** about functions?

```
\forall i. 0 ≤ i => fib i ≤ fib (i+1)
```

How to express **theorems** about functions?

Step 1: Definition

In SMT `fib` is "Uninterpreted Function"

```
\forall i j. i = j => fib i = fib j
```

How to connect logic fib with target fib?

How to connect logic `fib` with target `fib`?

```
fib :: i:{Int|0≤i} → {v:Int|0<v∧i≤v}
fib i
  | i≤1       = 1
  | otherwise = fib (i-1) + fib (i-2)
```

SMT Axiom

```
\forall i.
    if i≤1 then fib i = 1
    else fib i = fib (i-1) + fib (i-2)
```

Not Decidable

How to connect logic fib with target fib?

```
fib :: i:{Int|0≤i} -> {v:Int|0<v∧i≤v}
fib i
  | i≤1          = 1
  | otherwise = fib (i-1) + fib (i-2)
```

Refinement Reflection

```
fib :: i:{Int|0≤i} -> {v:Int| v=fib i ∧
    if i≤1 then fib i = 1
    else fib i = fib (i-1) + fib (i-2)
}
```

Refinement Reflection

Step 1: Definition

Step 2: Reflection

```
fib :: i:{Int|0≤i} -> {v:Int| v=fib i ∧
    if i≤1 then fib i = 1
    else fib i = fib (i-1) + fib (i-2)
}
```

Refinement Reflection

Step 1: Definition

Step 2: Reflection

```
fib :: i:{Int|0≤i} -> {v:Int| v=fib i ∧
    if i≤1 then fib i = 1
    else fib i = fib (i-1) + fib (i-2)
}
```

Step 3: Application

```
fib 0 :: {v:Int| v=fib 0 ∧ fib 0 = 1}
```

Application is Type Level Computation

```
fib 0
```

```
fib 0 = 1
```

Application

Type Level Computation

```
fib 0
```

```
fib 0 = 1
```

```
fib 1
```

```
fib 1 = 1
```

```
fib 2
```

```
fib 2 = fib 1 + fib 0
```

```
fib i
```

?

?

```
if i≤1 then fib i = 1
else fib i = fib (i-1) + fib (i-2)
```

Application　Type Level Computation

```
fib 0
```

```
fib 0 = 1
```

```
fib 1
```

```
fib 1 = 1
```

```
fib 2
```

```
fib 2 = fib 1 + fib 0
```

```
if 1<i then
```

```
fib i
```

```
fib i = fib (i-1) + fib (i-2)
```

```
if i≤1 then fib i = 1
else fib i = fib (i-1) + fib (i-2)
```

Application

```
fib 0
```

```
fib 1
```

```
fib 2
```

```
if 1<i then
```

```
fib i
```

```
fib (i+1)
```

Type Level Computation

```
fib 0 = 1
```

```
fib 1 = 1
```

```
fib 2 = fib 1 + fib 0
```

```
fib i = fib (i-1) + fib (i-2)
```

```
fib (i+1) = fib i + fib (i-1)
```

Theorem Proving

```
fibUp :: i:Nat -> {fib i ≤ fib (i+1)}
fibUp i
 | i == 0
 =    fib 0 <. fib 1
 *** QED
 | i == 1
 =    fib 1 <=. fib 1 + fib 0 <=. fib 2
 *** QED
 | otherwise
 =    fib i
 <=. fib i + fib (i-1)
 <=. fib (i+1)
 *** QED
```

Reflection for Theorem Proving

Theorems are refinement types.

Proofs are functions.

Check that functions prove theorems.

Proofs are functions.

```
fibUp :: i:Nat -> {fib i ≤ fib (i+1)}
```

Proofs are functions.

```
fibUp :: i:Nat -> {fib i ≤ fib (i+1)}
```

Let's call them!

```
fibUp 4 :: {fib 4 ≤ fib 5}
fibUp i :: {fib i ≤ fib (i+1)}
fibUp (j-1) :: {fib (j-1) ≤ fib j}
```

Proofs are functions. Let's call them!

```
fibMono :: i:Nat -> j:{Nat| i < j}
        -> {fib i ≤ fib j}

fibMono i j
 | i + 1 == j
 =    fib i
 <=. fib (i+1) ? fibUp i
 ==. fib j
 *** QED
 | otherwise
 =    fib i
 <=. fib (j-1) ? fibMono i (j-1)
 <=. fib j     ? fibUp (j-1)
 *** QED
```

Proofs are functions. Let's call them!

```
fibMono :: i:Nat -> j:{Nat| i < j}
        -> {fib i ≤ fib j}

fibMono i j
 | i + 1 == j
 =    fib i
 <=. fib (i+1) ? fibUp i
 ==. fib j
 *** QED
 | otherwise
 =    fib i
 <=. fib (j-1) ? fibMono i (j-1)
 <=. fib j     ? fibUp (j-1)
 *** QED
```

Proofs are functions. Let's abstract them!

```
fibMono :: i:Nat -> j:{Nat| i < j}
        -> fib:(Nat -> Int)
        -> (k:Nat -> {fib k ≤ fib (k+1)})
        -> {fib i ≤ fib j}

fibMono i j fib fibUp
  | i + 1 == j
  =    fib i
  <=. fib (i+1) ? fibUp i
  ==. fib j
  *** QED
  | otherwise
  =    fib i
  <=. fib (j-1) ? fibMono i (j-1)
  <=. fib j     ? fibUp (j-1)
  *** QED
```

Refinement Reflection for **Expressiveness**

Refinement Reflection for **Expressiveness**

Idea:

Encode HO specs in FO SMT decidable logic

Metatheory:

THEOREM 4.1. *[Soundness of λ^R]*

- ***Denotations*** *If* $\Gamma; R \vdash p : \tau$ *then* $\forall \theta \in [\![\Gamma]\!].\theta \cdot p \in [\![\theta \cdot \tau]\!]$.
- ***Preservation*** *If* $\emptyset; \emptyset \vdash p : \tau$ *and* $p \hookrightarrow^\star w$, *then* $\emptyset; \emptyset \vdash w : \tau$.

Metatheory:

THEOREM 4.1. *[Soundness of λ^R]*

- ***Denotations*** *If* $\Gamma; R \vdash p : \tau$ *then* $\forall \theta \in [\![\Gamma]\!].\theta \cdot p \in [\![\theta \cdot \tau]\!]$.
- ***Preservation*** *If* $\emptyset; \emptyset \vdash p : \tau$ *and* $p \hookrightarrow^\star w$, *then* $\emptyset; \emptyset \vdash w : \tau$.

E PROOF OF SOUNDNESS

We prove Theorem 4.1 of § D by reduction to Soundness of λ^U [Vazou et al. 2014a].

THEOREM E.1. *[Denotations] If* $\Gamma \vdash p : \tau$ *then* $\forall \theta \in [\![\Gamma]\!].\theta \cdot p \in [\![\theta \cdot \tau]\!]$.

PROOF. We use the proof from [Vazou et al. 2014b] and specifically Lemma 4 that is identical to the statement we need to prove. Since the proof proceeds by induction in the type derivation, we need to ensure that all the modified rules satisfy the statement.

- T-EXACT Assume $\Gamma \vdash e : \{v : B \mid \{\!|r|\!\} \wedge v = e\}$. By inversion $\Gamma \vdash e : \{v : B \mid \{\!|r|\!\}\}(1)$. By (1) and IH we get $\forall \theta \in [\![\Gamma]\!].\theta \cdot e \in [\![\theta \cdot \{v : B \mid \{\!|r|\!\}\}]\!]$. We fix a $\theta \in [\![\Gamma]\!]$ We get that if $\theta \cdot e \hookrightarrow^\star w$, then $\theta \cdot \{\!|r|\!\}[v/w] \hookrightarrow^\star \mathsf{True}$. By the Definition of = we get that $w = w \hookrightarrow^\star \mathsf{True}$. Since $\theta \cdot (v = e)[v/w] \hookrightarrow^\star w = w$, then $\theta \cdot (\{\!|r|\!\} \wedge v = e)[v/w] \hookrightarrow^\star \mathsf{True}$. Thus $\theta \cdot e \in [\![\theta \cdot \{v : B \mid \{\!|r|\!\} \wedge v = e\}]\!]$ and since this holds for any fixed θ, $\forall \theta \in [\![\Gamma]\!].\theta \cdot e \in [\![\theta \cdot \{v : B \mid \{\!|r|\!\} \wedge v = e\}]\!]$.

Refinement Reflection, POPL'18

by **Vazou**, Tondwalkar, Choudhury, Scott, Newton, Wadler, and Jhala

E PROOF OF SOUNDNESS

We prove Th

Theorem

Proof. W
the statemer
need to ensu

- T-Exa
(1) an
$\theta \cdot e$
True.
$e \in [[$
$\{v : B$
- T-Let
τ (2), a
(2'). By
(3) $\forall \theta$
- T-Refi
e in p
are cl
- T-Fix
and Pa

Theorem

Proof. In
Lemma 7. T
Lemma.

Lemma E.

Proof. Si
need to ensu

- T-Exa
$\emptyset \vdash p'$
is clos
T-Sub

By 25, the ab

Example: Fi
the term `fib`

Thus, by The

- T-Let A
(2), and
et al. 2
$p' \equiv p$ [
- T-Refl A
$x : \tau'_x \vdash$
(1'), (2)
τ [fix x
- T-Fix T

F ALGORI

Next, we desc
rule is replace
the same sour

F.1 The SM

Syntax: Term
of quantifier-f
2010; Nelson
(encoded as c
uninterpreted
integers and b
function sort
represented as
other values.

Semantics: S
$\sigma \doteq \{x_1 \mapsto p$
$\sigma\, p$ "is true" [
for all assignm

Predicates $p ::= p \bowtie p \mid \oplus_1 p$
$\mid n \mid b \mid x \mid D \mid x\,\overline{p}$

Transformation $\boxed{\Gamma \vdash e \rightsquigarrow p}$

rule $- \models F \hookrightarrow^* \text{UN}$. The term $\lambda x.e$ of type $\tau_x \to \tau$ is transformed to $\text{lam}_s^{s_x}\ x\ p$ of sort Fun s_x s, where s_x and s are respectively $(\!|\tau_x|\!)$ and $(\!|\tau|\!)$, $\text{lam}_s^{s_x}$ is a special uninterpreted function of sort

Fun $(\!|\tau|\!)$ $(\!|\tau_{i,j}|\!)$
using the chec
example, follo

```
[]       +
(x:xs)   +
```

is reflected int

We favor selec
et al. 2016] to

F.2 Trans

The judgme
term p. The

Embedding

Embedding
ments includ
$(- \models B \hookrightarrow^*$
in λ^S, all fun
constants an
like (+ 1) to

Embedding
ing the unin

F.3 Correct

Informally, the
expression the

Definition F.
the axioms of

Semantics Pr
ment as $(\!|e|\!)$ $\doteq$
the substitutio
We connect th

Theorem F
$p = (\!|v|\!)$.

Corollary
every $\sigma \in \theta^\perp$,

F.4 Decida

Figure 17 sum
types are exte

Termination
ness of refine
that refineme
et al. 2014a].
refinements t

Verification
described by
conjoining (t
2014a]:

where we em

Subtyping v
denotational
SMT solver to
subtyping.

Lemma F.4.

Soundness o

Theorem F

G SOUND

In this sectio
referring to th

Where x_i^s are

We modify
minimum gl
helper functi

Lemma G.2

Proof. We
- $- \models B$
- $- \models I$
- $- \models U$
$\Delta_0, (\!|\Gamma|\!)$
- $- \models B$
Since Γ
$\Delta_0, (\!|\Gamma|\!)$
- If $\bowtie$
- If $\bowtie$
- If $\bowtie$
- If $\bowtie$
- $- \models V$

$\Gamma \vdash e : x$
- $- \models I \hookrightarrow$
Since Γ
$\Gamma \vdash e_2 : \tau$
Thus, Δ_0
- $- \models C \hookrightarrow$
and $\Gamma \vdash$
$e_i[\overline{y_i}/\overline{se}]$
we get Δ

Theorem G
$\theta^\perp \cdot e \hookrightarrow^* v$ th

Proof. We
2014b]. Since θ

with $\theta_1^\perp \equiv \theta^\perp$
translation $\Gamma \vdash$
value the extra

For Boolean

Corollary
model $\sigma \in [\![\theta^\perp$

Proof. We
- $\Rightarrow$ By di
- $\Leftarrow$ Since
then by

Lemma G.5
and every mod

$\vdash e \rightsquigarrow p$

rsion
y IH
τ)
$= \text{if is}_{D_i}\ p' \text{ then } p_1 \text{ else } \ldots \text{ else } p_n(\!|\tau|\!)$.
- Assume $\langle \theta^\perp; D\,\overline{e_i}\ e\ \overline{e_j} \rangle \hookrightarrow \langle \theta_2^\perp; D\,\overline{e_i}\ e'\ \overline{e_j} \rangle$. By inversion $\langle \theta^\perp; e \rangle \hookrightarrow \langle \theta_2^\perp; e' \rangle$. Assume $\Gamma \vdash e \rightsquigarrow p$, $\Gamma \vdash e_i \rightsquigarrow p_i, \Gamma \vdash e' \rightsquigarrow p'$. By IH $\sigma^\beta \cup (\sigma_2^\beta \setminus \sigma^\beta) \models p = p'$, thus $\sigma^\beta \cup (\sigma_2^\beta \setminus \sigma^\beta) \models \text{app}\ D\,\overline{p_i}\ p\ \overline{p_j} = \text{app}\ D\,\overline{p_i}\ p'\ \overline{p_j}$.
- Assume $\langle \theta^\perp; c\ w \rangle \hookrightarrow \langle \theta^\perp; \delta(c, w) \rangle$. By the definition of the syntax, $c\ w$ is a fully applied logical operator, thus $\sigma^\beta \cup (\sigma_2^\beta \setminus \sigma^\beta) \models c\ w = [\![\delta(c, w)]\!]$
- Assume $\langle \theta^\perp; (\lambda x.e) e_x \rangle \hookrightarrow \langle \theta^\perp; e[x/e_x] \rangle$. Assume $\Gamma \vdash e \rightsquigarrow p, \Gamma \vdash e_x \rightsquigarrow p_x$. Since σ^β is defined to satisfy the β-reduction axiom, $\sigma^\beta \cup (\sigma_2^\beta \setminus \sigma^\beta) \models \text{app}\ (\text{lam}\ x\ e)\ p_x = p[x/p_x]$.
- Assume $\langle \theta^\perp; \text{case}\ x = D_j\ \overline{e}\ \text{of}\ \{D_i\ \overline{y_i} \to e_i\} \rangle \hookrightarrow \langle \theta^\perp; e_j[x/D_j\ \overline{e}][y_i/\overline{e}] \rangle$. Also, let $\Gamma \vdash e \rightsquigarrow p$, $\Gamma \vdash e_i[x/D_j\ \overline{e}][y_i/\overline{e_i}] \rightsquigarrow p_i$. By the axiomatic behavior of the measure selector $\text{is}_{D_j}\ \overline{p}$, we get $\sigma^\beta \models \text{is}_{D_j}\ \overline{p}$. Thus, σ^β if $\text{is}_{D_i}\ p$ then p_1 else $\ldots$ else $p_n = p_j$.
- Assume $\langle (x, e_x)\theta^\perp; x \rangle \hookrightarrow \langle (x, e'_x)\theta_2^\perp; x \rangle$. By inversion $\langle \theta^\perp; e_x \rangle \hookrightarrow \langle \theta_2^\perp; e'_x \rangle$. By identity of equality, $(x, p_x)\sigma^\beta \cup (\sigma_2^\beta \setminus \sigma^\beta) \models x = x$.
- Assume $\langle (y, e_y)\theta^\perp; x \rangle \hookrightarrow \langle (y, e_y)\theta_2^\perp; e_x \rangle$. By inversion $\langle \theta^\perp; x \rangle \hookrightarrow \langle \theta_2^\perp; e_x \rangle$. Assume $\Gamma \vdash e_x \rightsquigarrow p_x$. By IH $\sigma^\beta \cup (\sigma_2^\beta \setminus \sigma^\beta) \models x = p_x$. Thus $(y, p_y)\sigma^\beta \cup (\sigma_2^\beta \setminus \sigma^\beta) \models x = p_x$.
- Assume $\langle (x, w)\theta^\perp; x \rangle \hookrightarrow \langle (x, w)\theta^\perp; w \rangle$. Thus $(x, [\![w]\!])\sigma^\beta \models x = [\![w]\!]$.
- Assume $\langle (x, D\,\overline{y})\theta^\perp; x \rangle \hookrightarrow \langle (x, D\,\overline{y})\theta^\perp; D\,\overline{y} \rangle$. Thus $(x, \text{app}\ D\,\overline{y})\sigma^\beta \models x = \text{app}\ D\,\overline{y}$.
- Assume $\langle (x, D\,\overline{e})\theta^\perp; x \rangle \hookrightarrow \langle (x, D\,\overline{y}), \overline{(y_i, e_i)}\theta^\perp; D\,\overline{y} \rangle$. Assume $\Gamma \vdash e_i \rightsquigarrow p_i$. Thus $(x, \text{app}\ D\,\overline{y})$, $\overline{(y_i, x = \text{app}\ D\,\overline{y}}$.

□

G.2 Soundness of Approximation

Theorem G.6 (Soundness of Algorithmic). *If* $\Gamma \vdash_S e : \tau$ *then* $\Gamma \vdash e : \tau$.

Proof. To prove soundness it suffices to prove that subtyping is appropriately approximated, as stated by the following lemma. □

Lemma G.7. *If* $\Gamma \vdash_S \{v : B \mid e_1\} \leq \{v : B \mid e_2\}$ *then* $\Gamma \vdash \{v : B \mid e_1\} \leq \{v : B \mid e_2\}$.

Proof. By rule $\leq$-Base-λ^S, we need to show that $\forall \theta \in [\![\Gamma]\!].[\![\theta \cdot \{v : B \mid e_1\}]\!] \subseteq [\![\theta \cdot \{v : B \mid e_2\}]\!]$. We fix a $\theta \in [\![\Gamma]\!]$. and get that forall bindings $(x_i : \{v : B^\downarrow \mid e_i\}) \in \Gamma$, $\theta \cdot e_i[v/x_i] \hookrightarrow^*$ True.
Then need to show that for each e, if $e \in [\![\theta \cdot \{v : B \mid e_1\}]\!]$, then $e \in [\![\theta \cdot \{v : B \mid e_2\}]\!]$.

Liquid Haskell on papers

Expressiveness

Refinement Reflection, POPL'18

by **Vazou**, Tondwalkar, Choudhury, Scott, Newton, Wadler, and Jhala

Refinement Types for Haskell, ICFP'14

by **Vazou**, Seidel, Jhala, Vytiniotis, and Peyton-Jones

Liquid Haskell on papers

Expressiveness

Refinement Reflection, POPL'18

by **Vazou**, Tondwalkar, Choudhury, Scott, Newton, Wadler, and Jhala

Refinement Types for Haskell, ICFP'14

by **Vazou**, Seidel, Jhala, Vytiniotis, and Peyton-Jones

Liquid Haskell on papers

Expressiveness

Refinement Reflection, POPL'18

by **Vazou**, Tondwalkar, Choudhury, Scott, Newton, Wadler, and Jhala

Refinement Types for Haskell, ICFP'14

by **Vazou**, Seidel, Jhala, Vytiniotis, and Peyton-Jones

Liquid Haskell on papers

Expressiveness

Refinement Reflection, POPL'18
by **Vazou**, Tondwalkar, Choudhury, Scott, Newton, Wadler, and Jhala

Bounded Refinement Types, ICFP'15
by **Vazou**, Bakst, and Jhala

Abstract Refinement Types, ESOP'13
by **Vazou**, Rondon, and Jhala

Refinement Types for Haskell, ICFP'14
by **Vazou**, Seidel, Jhala, Vytiniotis, and Peyton-Jones

Liquid Haskell on github

ucsd-progsys / liquidhaskell

Unwatch 22 | Star 473 | Fork 75

Code | Issues 201 | Pull requests 5 | Projects 0 | Wiki | Insights | Settings

Liquid Types For Haskell

Edit

Add topics

8,382 commits | 94 branches | 19 releases | 38 contributors

Branch: develop | New pull request | Create new file | Upload files | Find file | Clone or download

nikivazou Merge pull request #1223 from ucsd-progsys/HaskellFunInRefs ... Latest commit 82f5baa 5 days ago

benchmarks	move tests into pos	a month ago
devel	Fix travis error	6 days ago

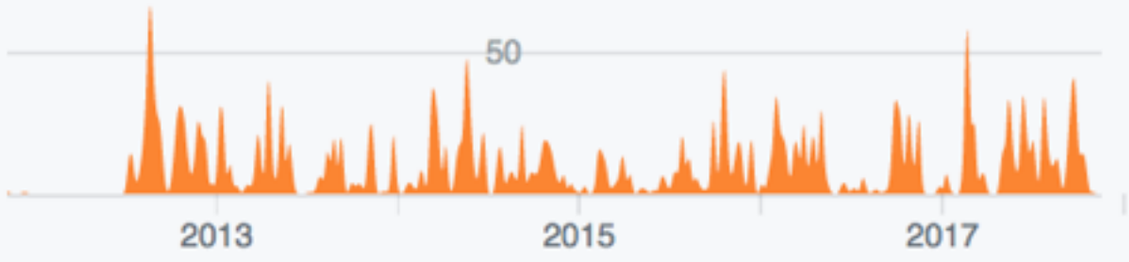
Liquid Haskell on github

Jan 15, 2012 – Jan 25, 2018

Contributions: **Commits**

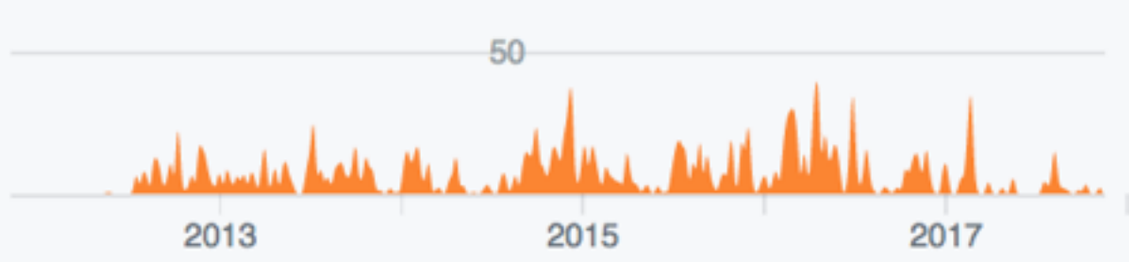
ranjitjhala — #1

3,093 commits 474,271 ++ 304,536 --



nikivazou — #2

2,113 commits 358,364 ++ 294,962 --



gridaphobe — #3

814 commits 114,731 ++ 79,008 --

spinda — #4

155 commits 7,430 ++ 5,350 --

Liquid Haskell dev team

Niki Vazou & Ranjt Jhala,
Liquid Haskell dev team

Liquid Haskell in the real world

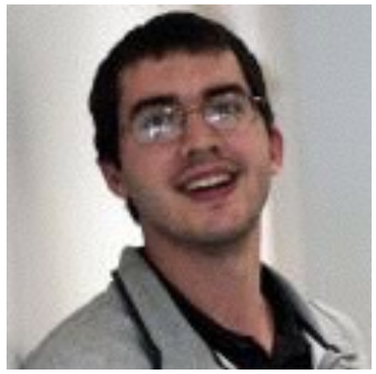
Education

Will Kunkel,
undergrad @UMD

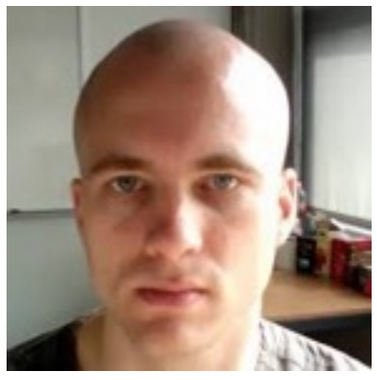
Rachel Xu & Xinyue Zhang,
undergrads @Bryn Mawr College

Niki Vazou & Ranjt Jhala,
Liquid Haskell dev team

Industry



Gabriel Gonzalez
Awake Security



Edsko de Vries
Well-Typed

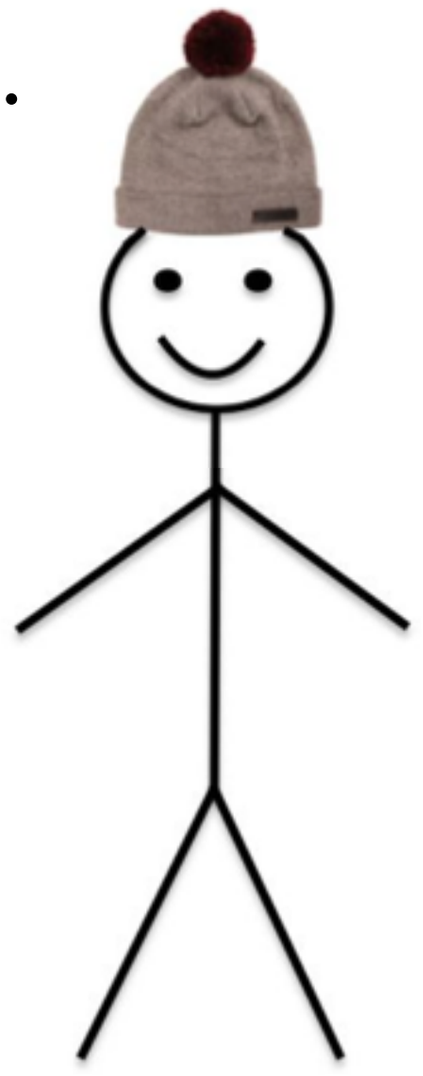
Liquid Haskell in Education

This is Will Kunkel.

Will took my undergrad course on Haskell.

Will learnt Liquid Haskell in 2 weeks.

Will was **3rd** in POPL'18 **Student Research Competition** with his project "Comparing Liquid Haskell and Coq"



Will is smart.

Be like Will.

Liquid Haskell in Education

Two winners in POPL'18 Student Research Competition

"Comparing Liquid Haskell and Coq"

Will Kunkel,
undergrad @UMD

"Comparing Dependent Haskell, Liquid Haskell and F*"

Rachel Xu & Xinyue Zhang,
undergrads @Bryn Mawr College

Liquid Haskell in the real world

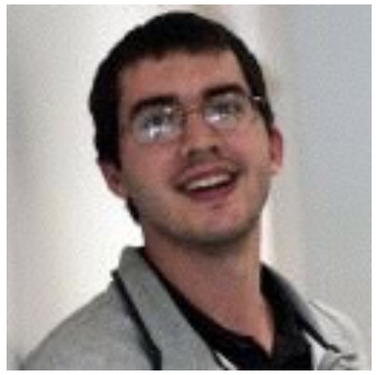
Education

Will Kunkel,
undergrad @UMD

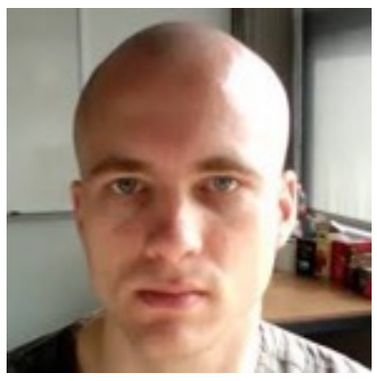
Niki Vazou & Ranjt Jhala,
Liquid Haskell dev team

Rachel Xu & Xinyue Zhang,
undergrads @Bryn Mawr College

Industry



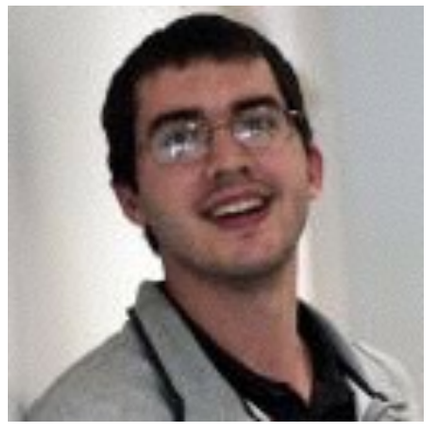
Gabriel Gonzalez
Awake Security



Edsko de Vries
Well-Typed

Liquid Haskell in Industry

Gabriel Gonzalez



AWAKE

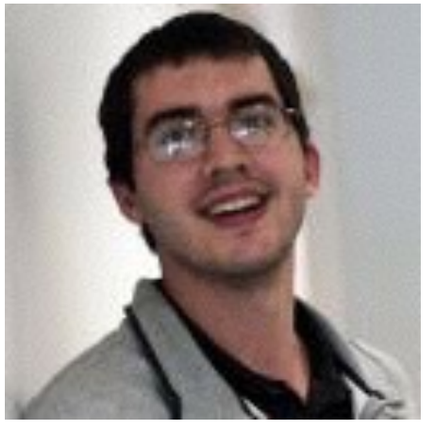
Static checks during parsing.

Provably Correct & Faster (x6) Code!

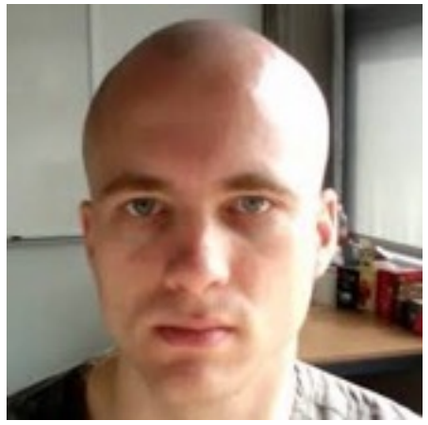
Huge speedup for internet traffic parsing.

Liquid Haskell in Industry

Gabriel Gonzalez

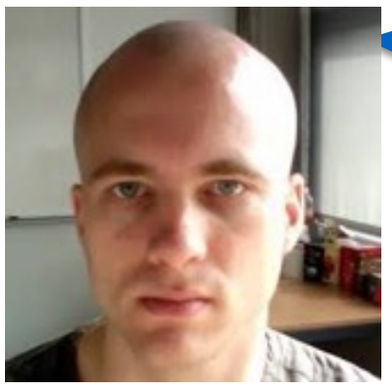


AWAKE

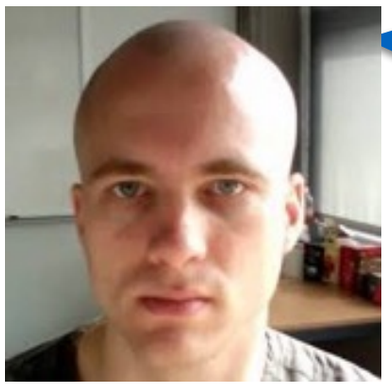


Well-Typed

Edsko de Vries

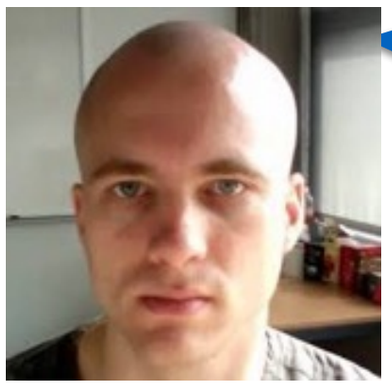


I am a Haskell consultant at a **cryptocurrency/blockchain** company.
We have a blockchain algorithm written **in paper** & a **Haskell implementation**.
We want Liquid Haskell to connect them.



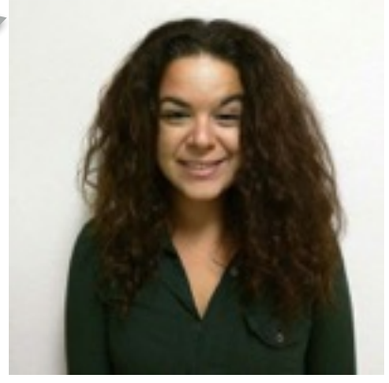
I am a Haskell consultant at a **cryptocurrency/blockchain** company. We have a blockchain algorithm written **in paper** & a **Haskell implementation**. We want Liquid Haskell to connect them.

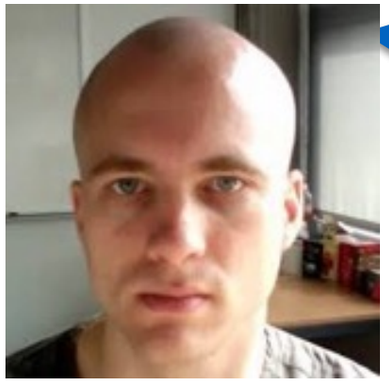
Awesome! Lmk if you need anything!



I am a Haskell consultant at a **cryptocurrency/blockchain** company. We have a blockchain algorithm written **in paper** & a **Haskell implementation**. We want Liquid Haskell to connect them.

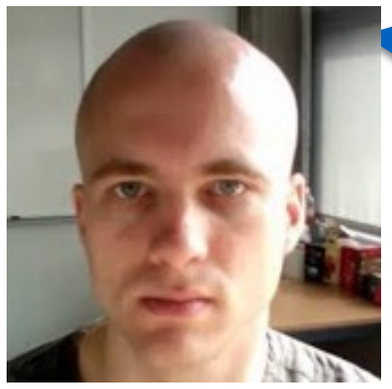
Awesome! Lmk if you need anything!





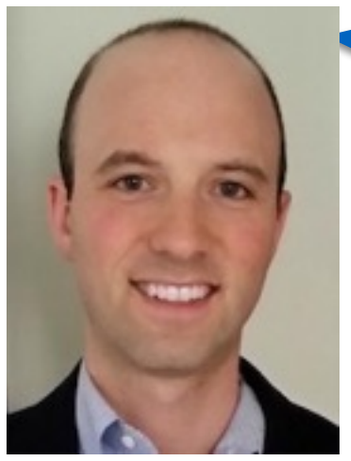
I want **interactive proof generation**!

Future work ideas are crowd sourced!



Edsko de Vries
industrial rep.

I want **interactive proof generation**!



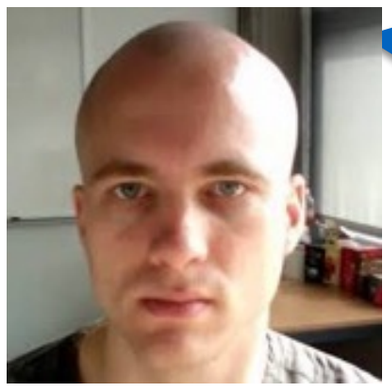
Richard Eisenberg
ghc devs rep.

Can we use Liquid Haskell proofs for **compiler optimizations**?

Leo Lambropoulos
Coq rep.

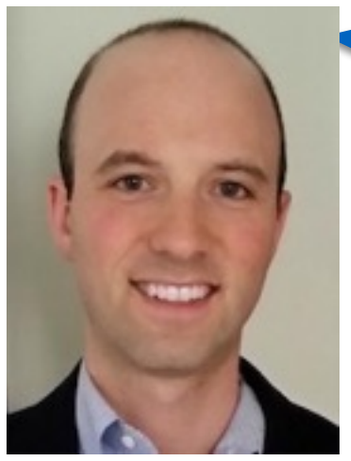
I do not trust it! Liquid Haskell should generate **proof certificates**!

Future work ideas are crowd sourced!



Edsko de Vries
industrial rep.

I want **interactive proof generation**!



Richard Eisenberg
ghc devs rep.

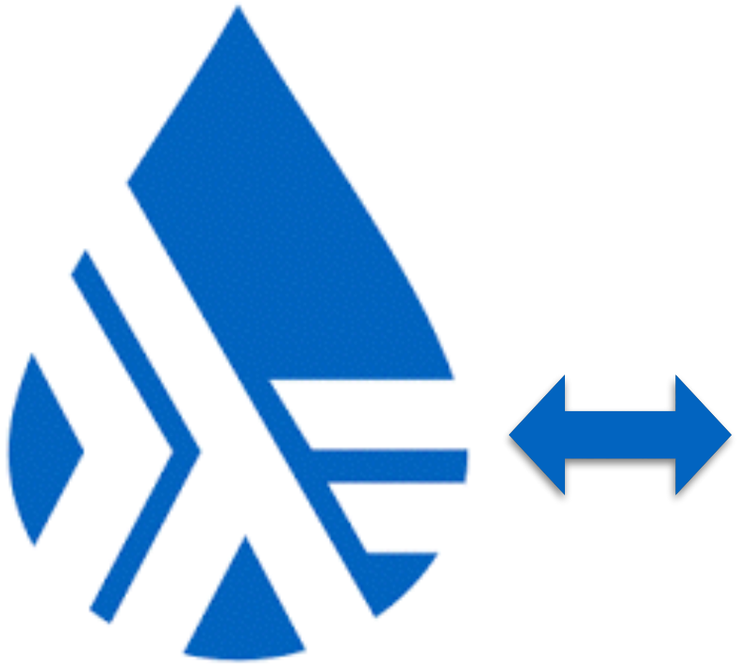
Can we use Liquid Haskell proofs for **compiler optimizations**?

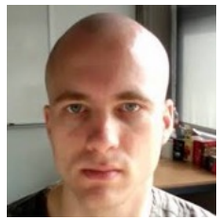
Leo Lambropoulos
Coq rep.

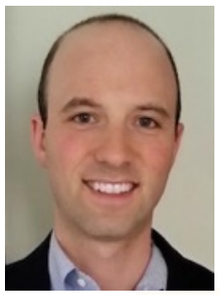
I do not trust it! Liquid Haskell should generate **proof certificates**!

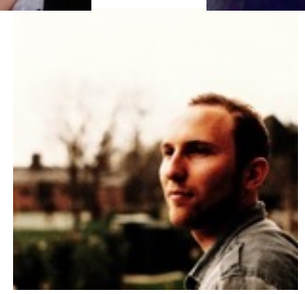
Liquid Haskell has many users

7,765 downloads

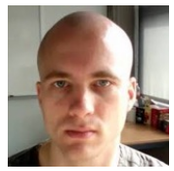




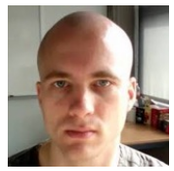


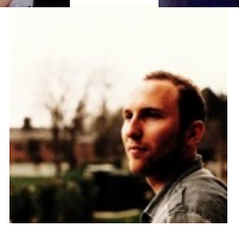


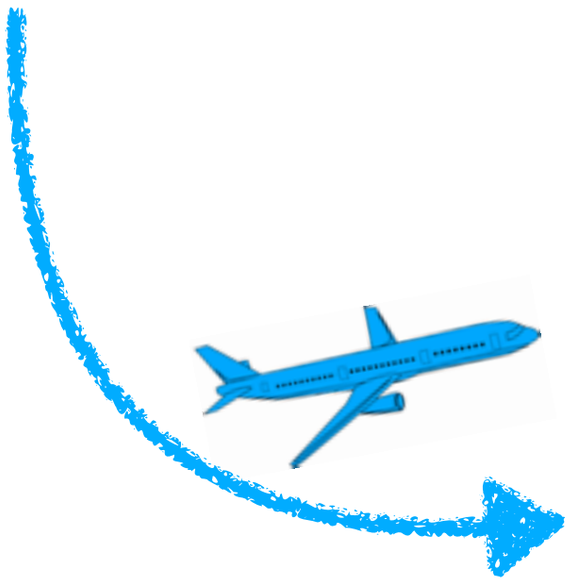
many users, but two main devs



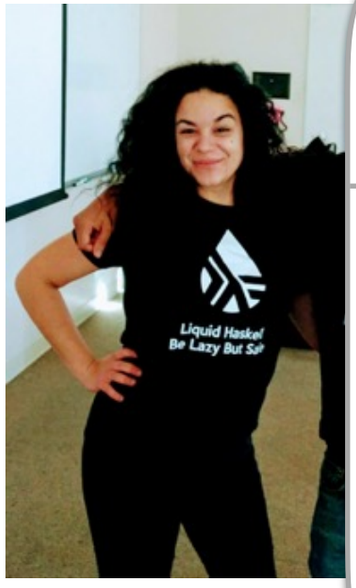
many users, but two main devs







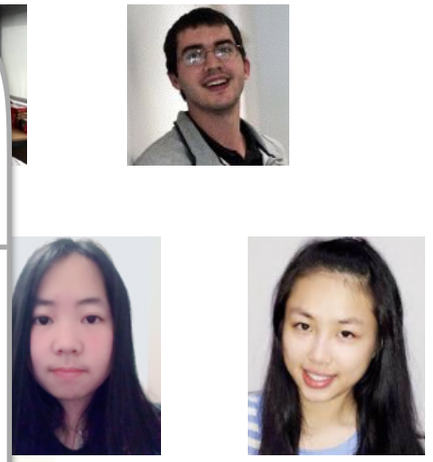
many users, but two main devs

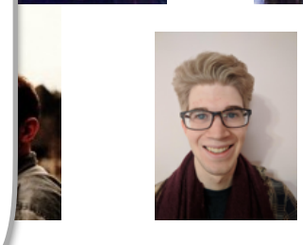


EMERGENCY ALERTS

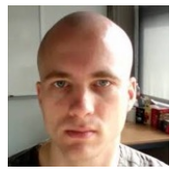
Emergency Alert

Liquid Haskell is not updated!
SEEK IMMEDIATE SHELTER.





many users, but two main devs



Goal: Expand the Liquid Haskell Dev Team

Goal: Expand the Liquid Haskell Dev Team

for

compiler optimizations,

interactive proof generation,

easy verification of real-world applications, ...

Vision:

Use verification to aid programming in Haskell

Vision:
Use verification to aid programming in Haskell

Specs are just comments **inside** the languages, ...
thus, learning effort is small.

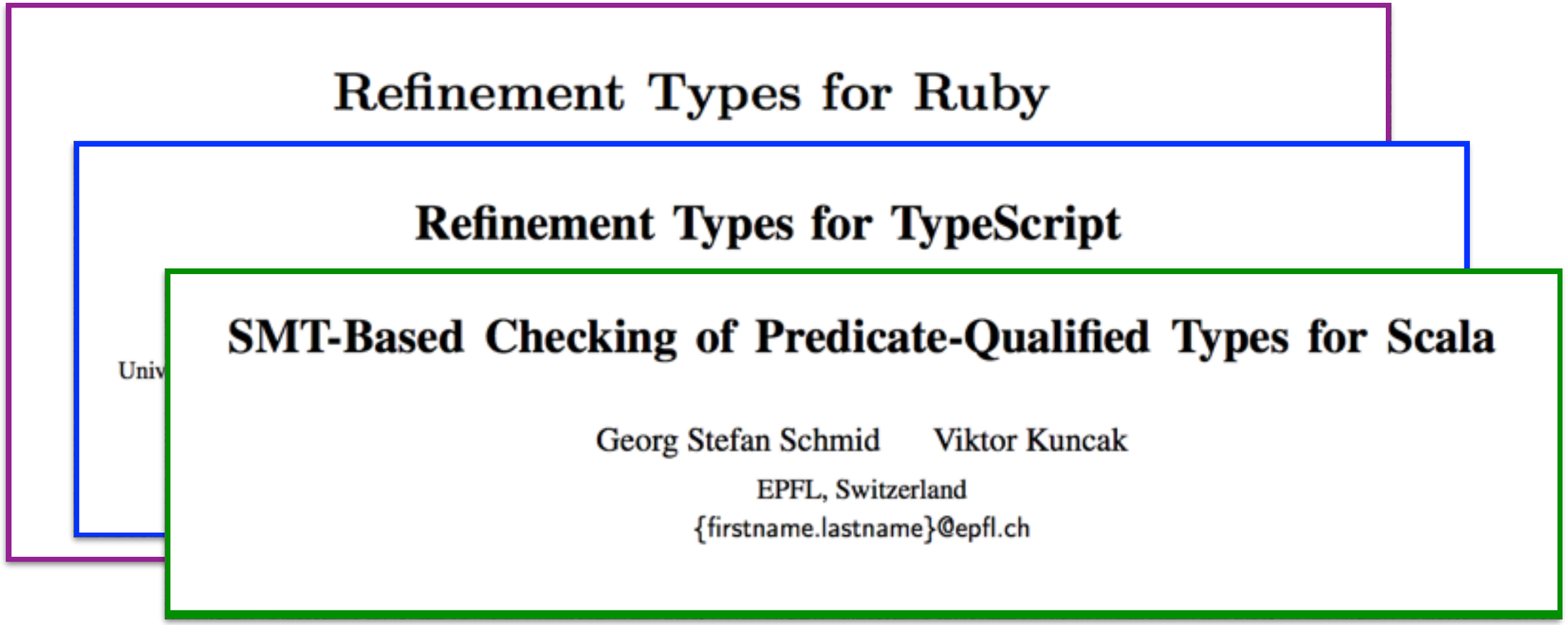
Semi-**automatically** machine checked, via SMTs.

For runtime **optimizations**, by the user or the compiler.

Vision:
Use verification to aid programming in ~~Haskell~~

X language

X = Ruby, JavaScript, Scala, ...



Use verification to aid programming in Haskell

Use verification to aid programming in Haskell

Fast & Safe Code
Static Checks

Theorem Proving
Refinement Reflection

Applications
Education & Industry

Thanks!