Loop Verification with Invariants and Contracts

Gidon Ernst, LMU Munich gidon.ernst@lmu.de

January 17, VMCAI 2022

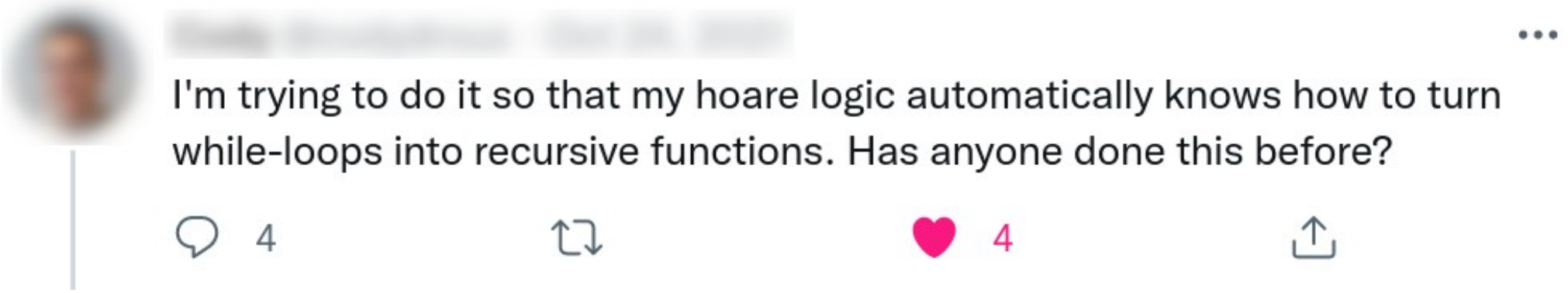
Preprint: https://arxiv.org/abs/2010.05812

https://www.sosy-lab.org

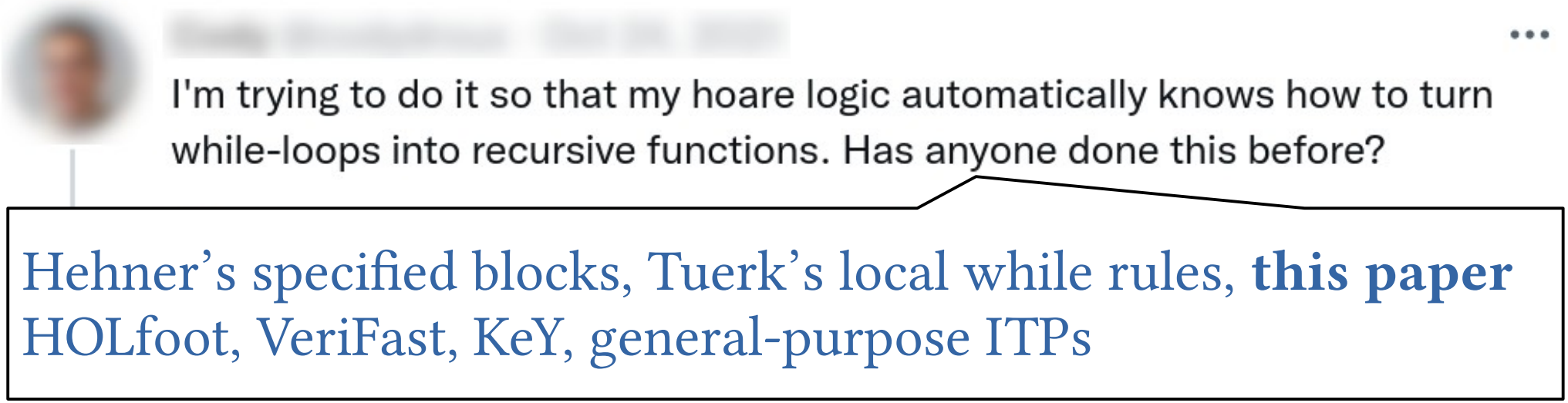
“ recursive algorithms
are easier to prove correct
than iterative ones ” --- folklore

Scope of this paper: deductive proofs of
strong functional specifications

“ recursive algorithms
are easier to prove correct
than iterative ones ” --- folklore



“ recursive algorithms
are easier to prove correct
than iterative ones ” --- folklore



1/17—Loop Contracts generalize Proofs with Invariants

$$\frac{\{\ t(x)\ \wedge\ I(x)\ \}\ \texttt{body}\ \{\ I(x)\ \}}{\{\ I(x)\ \}\ \texttt{while t do B}\ \{\ \neg t(x)\ \wedge\ I(x)\ \}}$$

invariant

“canonical” conclusion

1/17—Loop Contracts generalize Proofs with Invariants

$$\frac{\{\ t(x)\ \wedge\ I(x)\ \}\ \texttt{body}\ \{\ I(x)\ \}}{\{\ I(x)\ \}\ \texttt{while t do B}\ \{\ \neg t(x)\ \wedge\ I(x)\ \}}$$

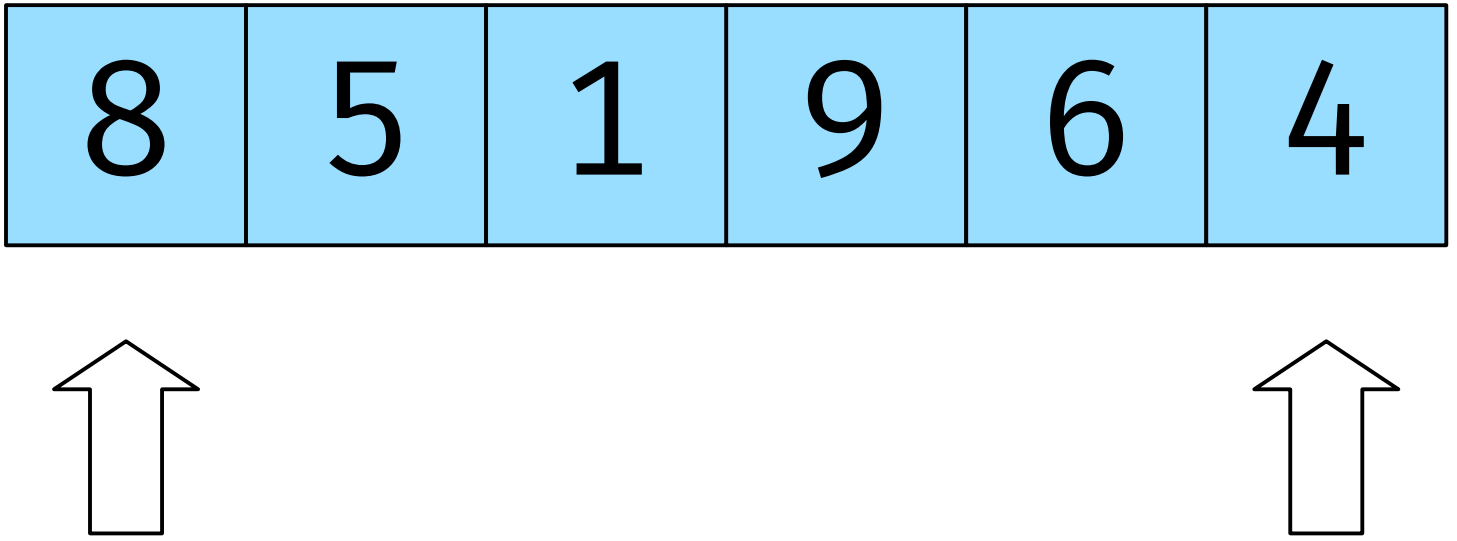
invariant

"canonical" conclusion

$$\frac{\texttt{(treat loop as tail-recursive procedure)}}{\{\ I(x)\ \wedge\ x = x_0\ \}\ \texttt{while t do B}\ \{\ R(x_0, x)\ \}}$$

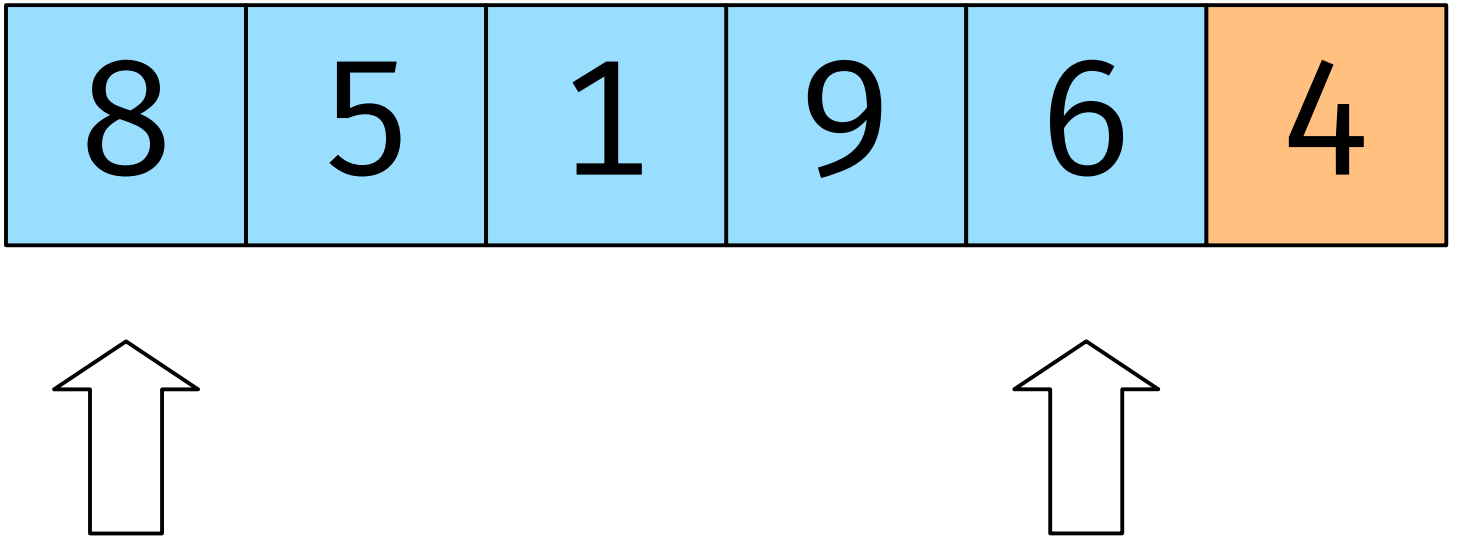
contract = invariant + **relational** summary

2/17—Find max by elimination (VerifyThis 2011)



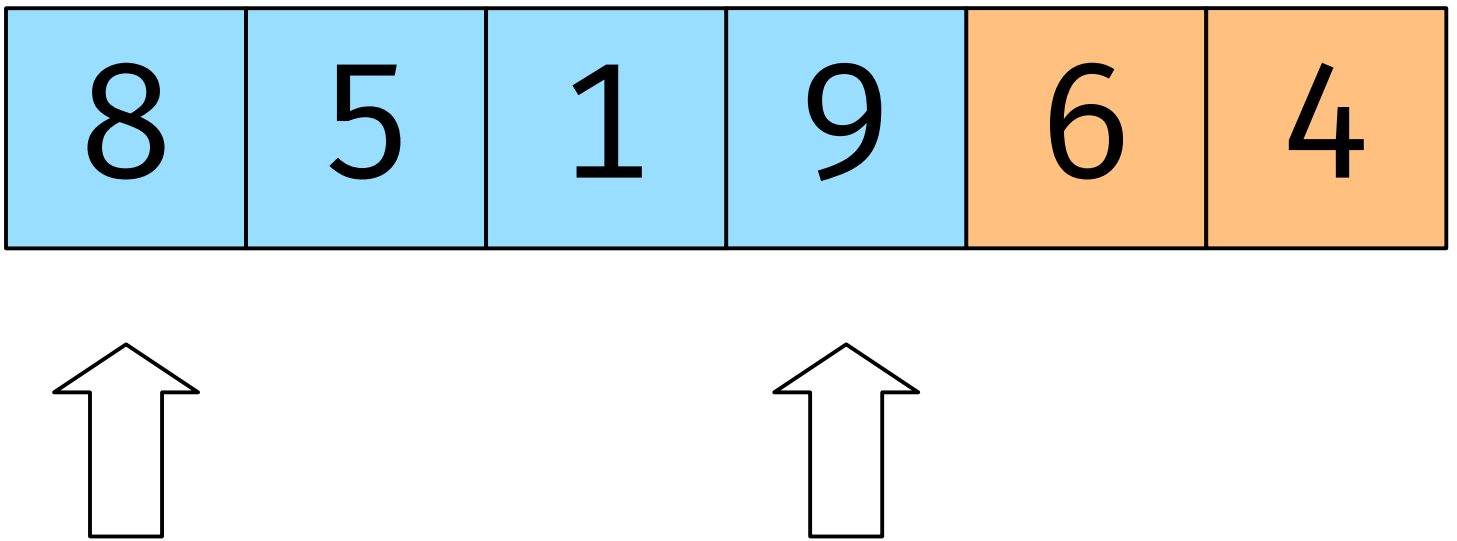
2/17—Find max by elimination (VerifyThis 2011)

eliminate 4 because $4 \leqslant 8$



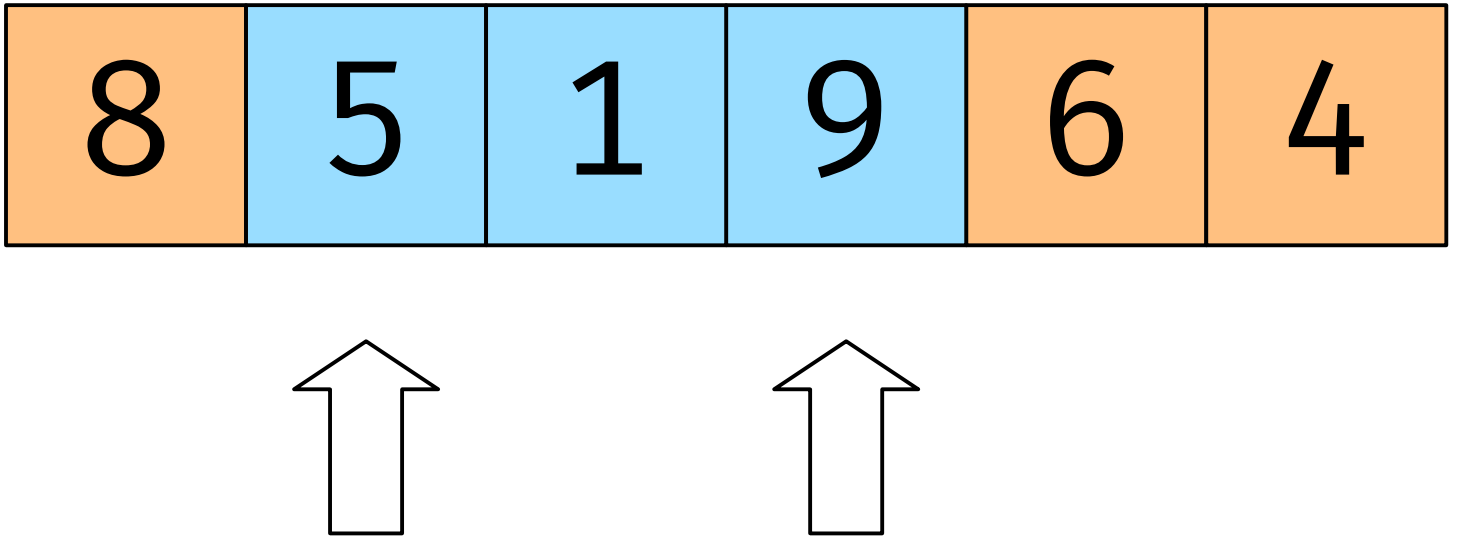
2/17—Find max by elimination (VerifyThis 2011)

eliminate 6 because $6 \leqslant 8$

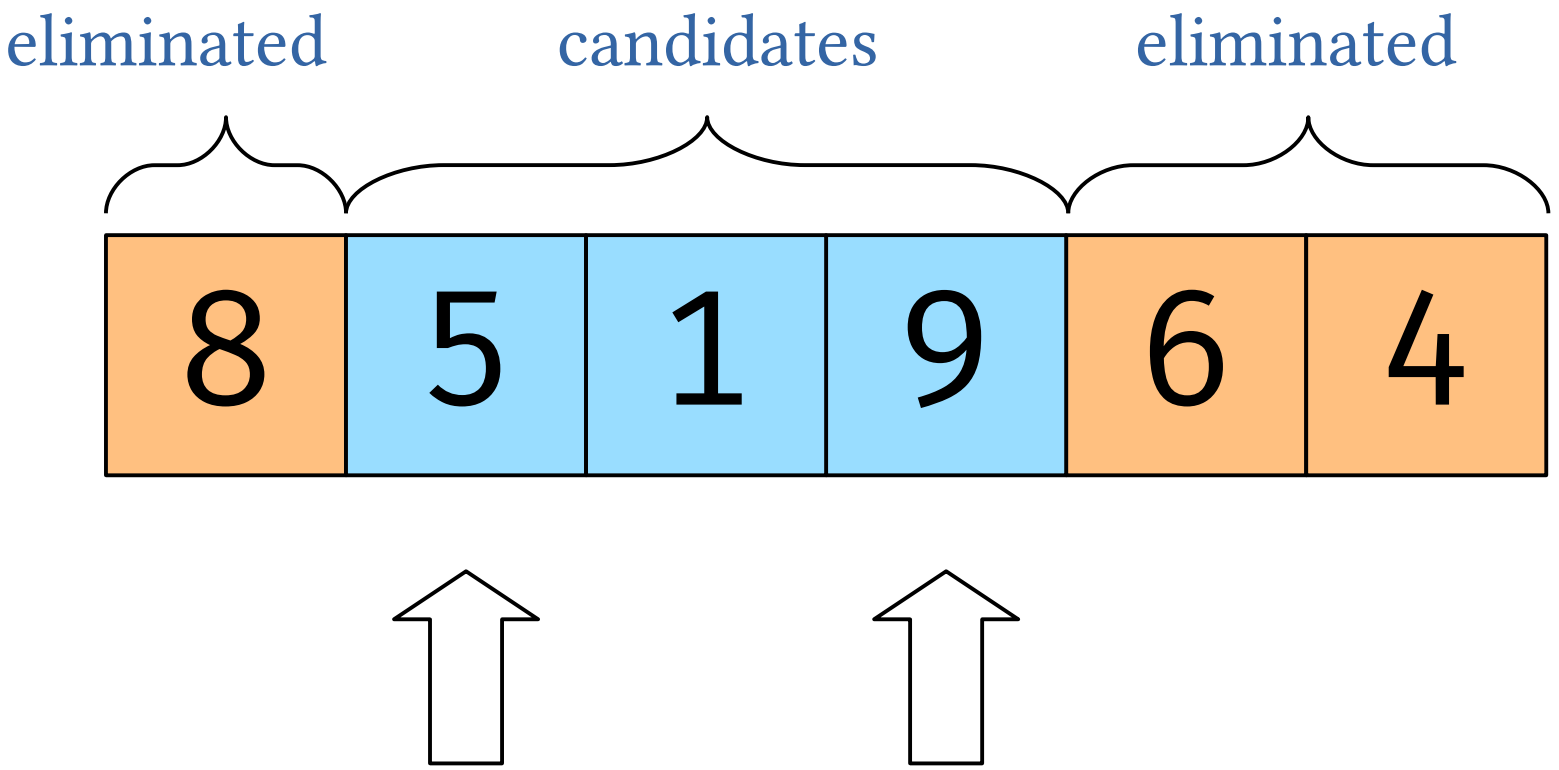


2/17—Find max by elimination (VerifyThis 2011)

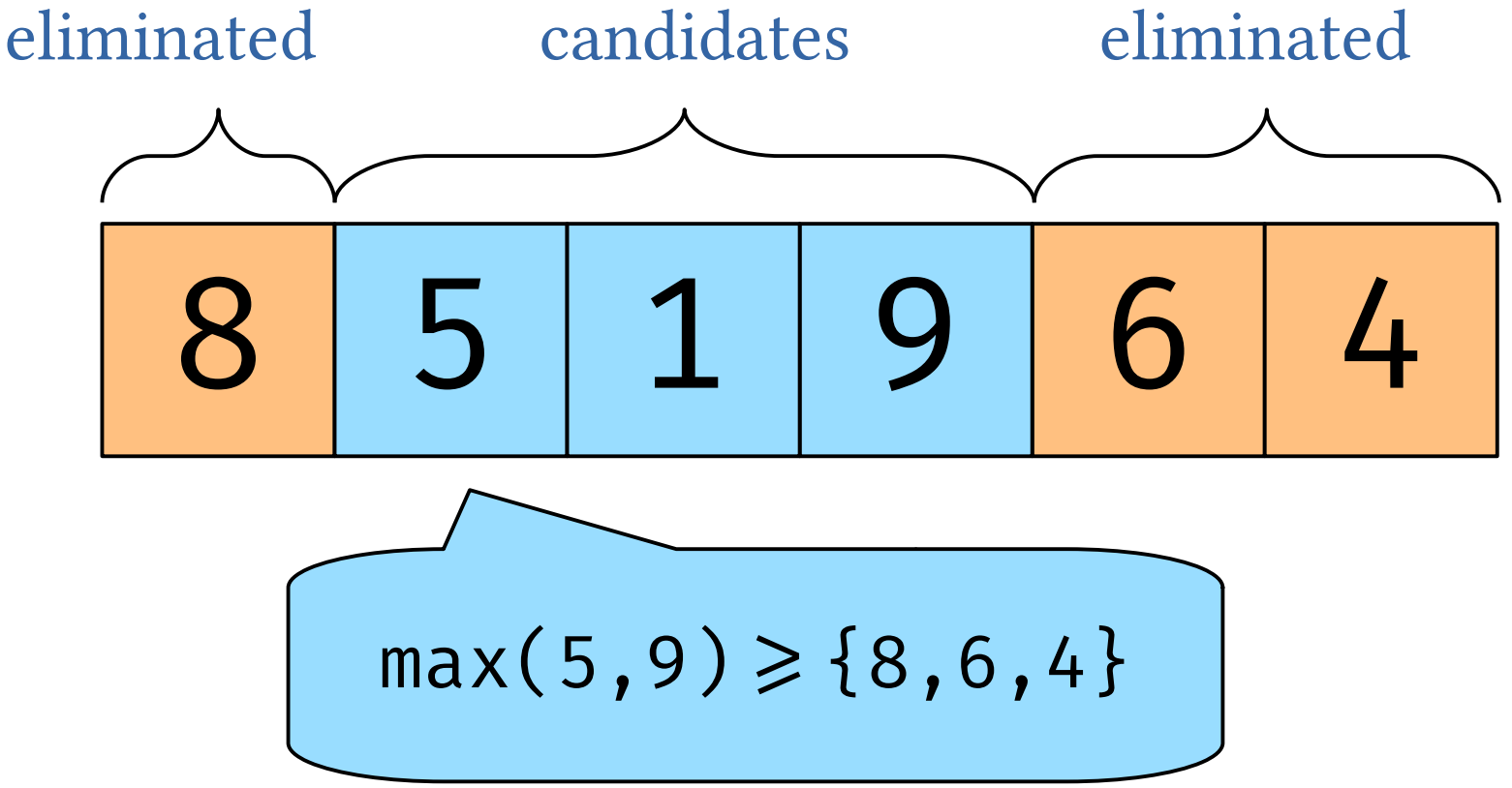
eliminate 8 because $8 \leqslant 9$



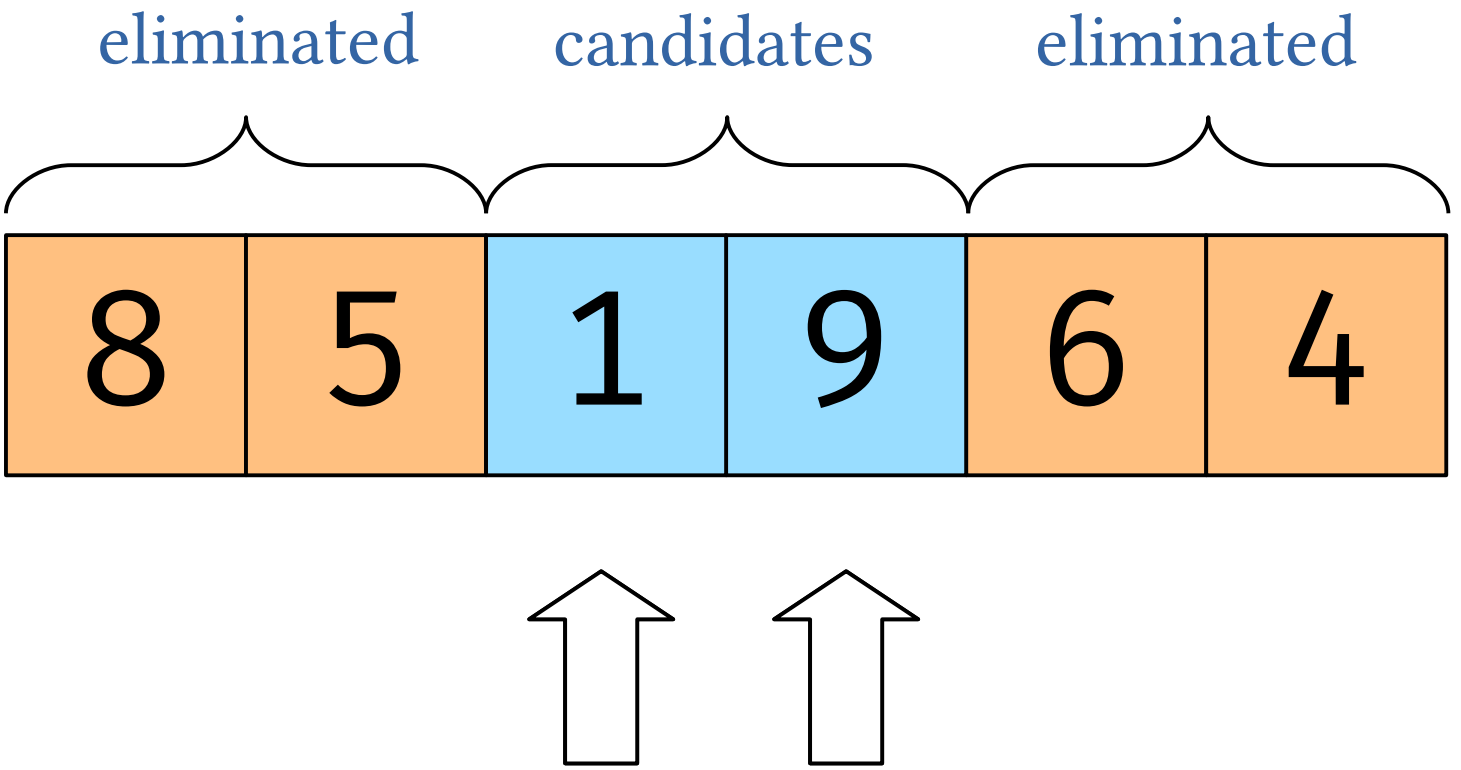
2/17—Find max by elimination (VerifyThis 2011)



2/17—Find max by elimination (VerifyThis 2011)

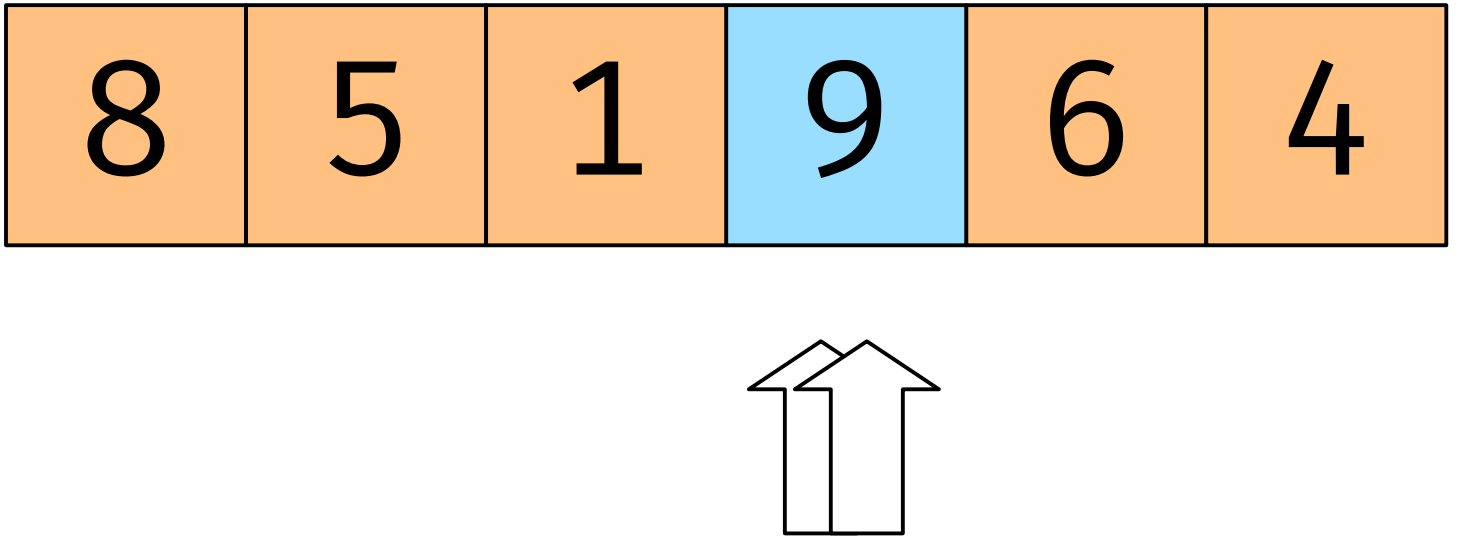


2/17—Find max by elimination (VerifyThis 2011)

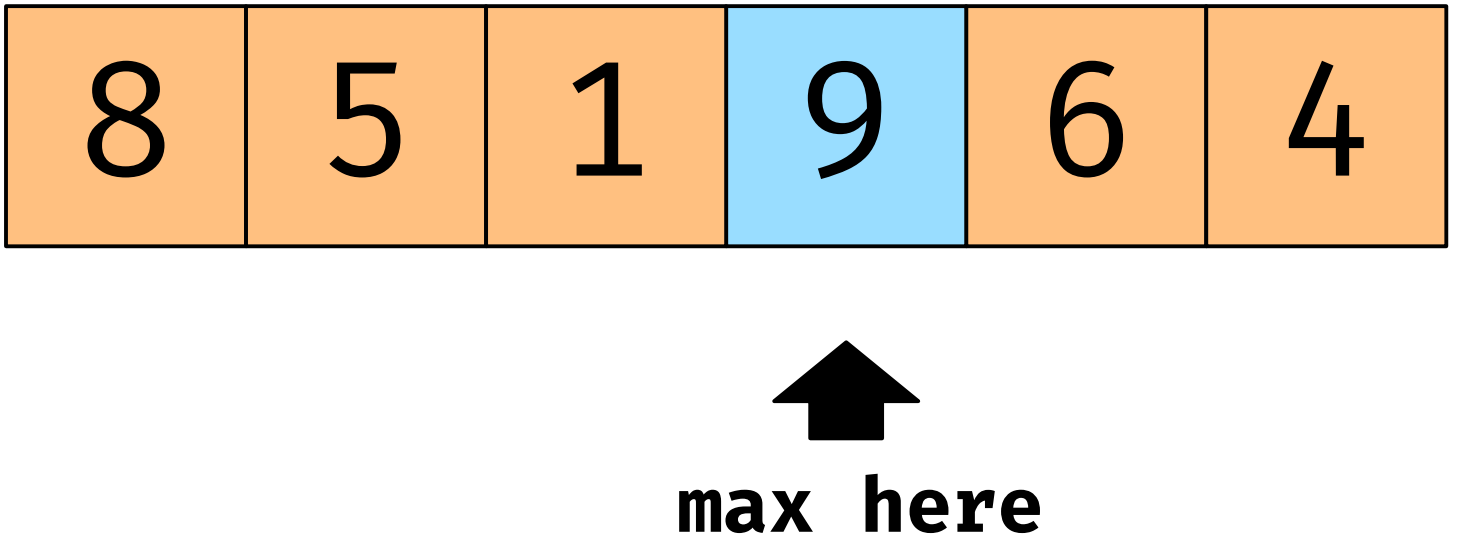


2/17—Find max by elimination (VerifyThis 2011)

eliminate 5 and 1 $\leqslant$ 9



2/17—Find max by elimination (VerifyThis 2011)



3/17—Recursive algorithm

```
int findMax(int a[], int l, int r)
  requires ???
  ensures  ???


  if l == r then return l
  else if a[l] ⩽ a[r] then return findMax(a, l+1, r)
  else if a[l] ⩾ a[r] then return findMax(a, l, r-1)
```

3/17—Recursive algorithm

```
int findMax(int a[], int l, int r)
  requires 0 ⩽ l ⩽ r < a.length
  ensures  a[\result] == max(a[l..r+1])


  if l == r then return l
  else if a[l] ⩽ a[r] then return findMax(a, l+1, r)
  else if a[l] ⩾ a[r] then return findMax(a, l, r-1)
```

relation between parameters and return value

3/17—Recursive algorithm

```
int findMax(int a[], int l, int r)
  requires 0 ⩽ l ⩽ r < a.length
  ensures a[\result] == max(a[l..r+1])
```

$$\forall\ i.\quad l \leqslant i < r+1 \implies a[i] \leqslant a[\result]$$

```
  if l == r then return l
  else if a[l] ⩽ a[r] then return findMax(a, l+1, r)
  else if a[l] ⩾ a[r] then return findMax(a, l, r-1)
```

3/17—Recursive algorithm

```
int findMax(int a[], int l, int r)
  requires 0 ≤ l ≤ r < a.length
  ensures  a[\result] == max(a[l..r+1])

  ∀ i.  l ≤ i < r+1  ⟹  a[i] ≤ a[\result]

  if l == r then return l
  else if a[l] ≤ a[r] then return findMax(a, l+1, r)
  else if a[l] ≥ a[r] then return findMax(a, l, r-1)
```

sufficient for
- automatic proof
- calling context

4/17—Iterative algorithm

```
l := 0,  r := a.length - 1
```

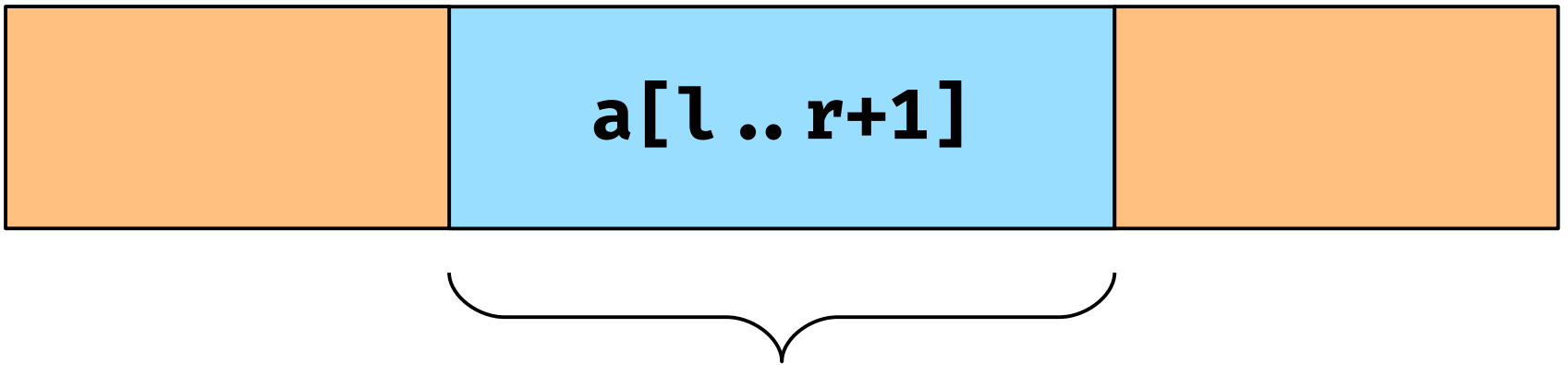
initial state
(omitted previously)

```
while true do
    invariant ???

  if l = r then return l
  else if a[l] ⩽ a[r] then l := l+1
  else if a[l] ⩾ a[r] then r := r-1
```

in-place update
(cf. tail-recursion
elimination)

5/17—Invariant for max by elimination



contains overall max

(see VerifyThis 2011 report for a variety of formalizations)

6/17—Iterative algorithm

```
l := 0,  r := a.length - 1


while true do
  invariant ∃ k.      0 ⩽ l ⩽ k ⩽ r < a.length
                    ∧ a[k] == max(a[0..a.length])
  if l == r then return l
  else if a[l] ⩽ a[r] then l := l+1
  else if a[l] ⩾ a[r] then r := r-1
```

sufficient for
- automatic proof
- postcondition (omitted)

7/17—“Invariant” proof of the recursive algorithm

```
int findMax(int a[], int l, int r)
  requires ∃ k.  0 ⩽ l ⩽ k ⩽ r < a.length
                   ∧ a[k] == max(a[0..a.length])
  ensures  ∃ k.  0 ⩽ \result ⩽ k ⩽ \result < a.length
                   ∧ a[k] == max(a[0..a.length])
```

7/17—"Invariant" proof of the recursive algorithm

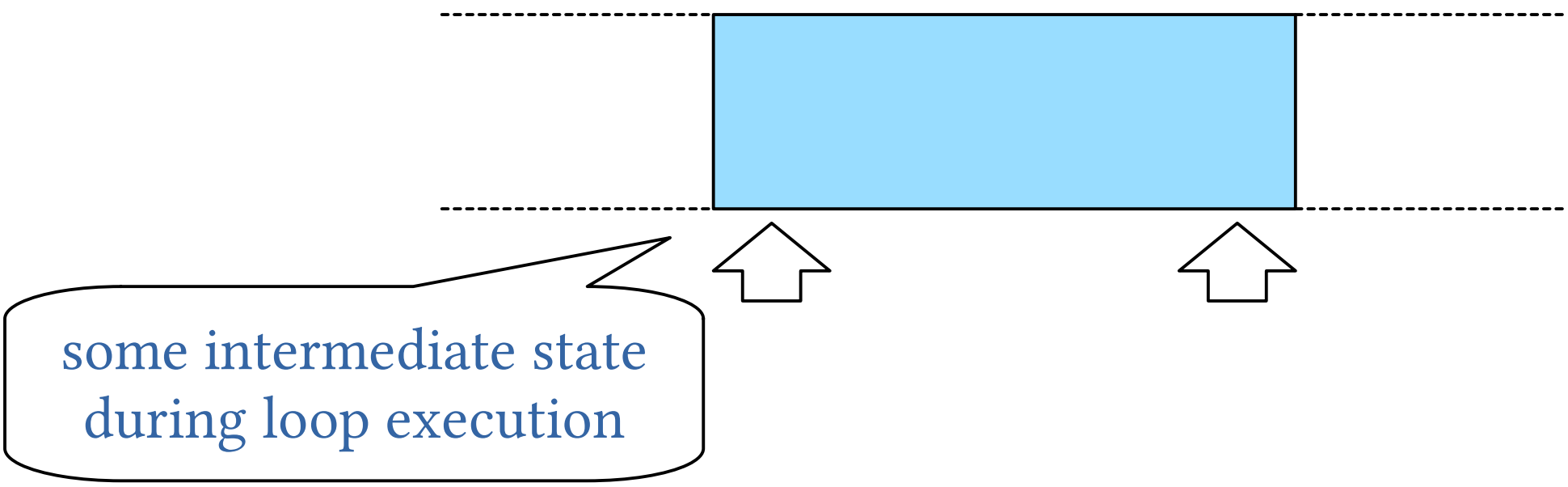
```
int findMax(int a[], int l, int r)
  requires ∃ k.  0 ⩽ l ⩽ k ⩽ r < a.length
                   ∧ a[k] == max(a[0..a.length])
  ensures  ∃ k.  0 ⩽ \result ⩽ k ⩽ \result < a.length
                   ∧ a[k] == max(a[0..a.length])
```

Self-imposed limitation:

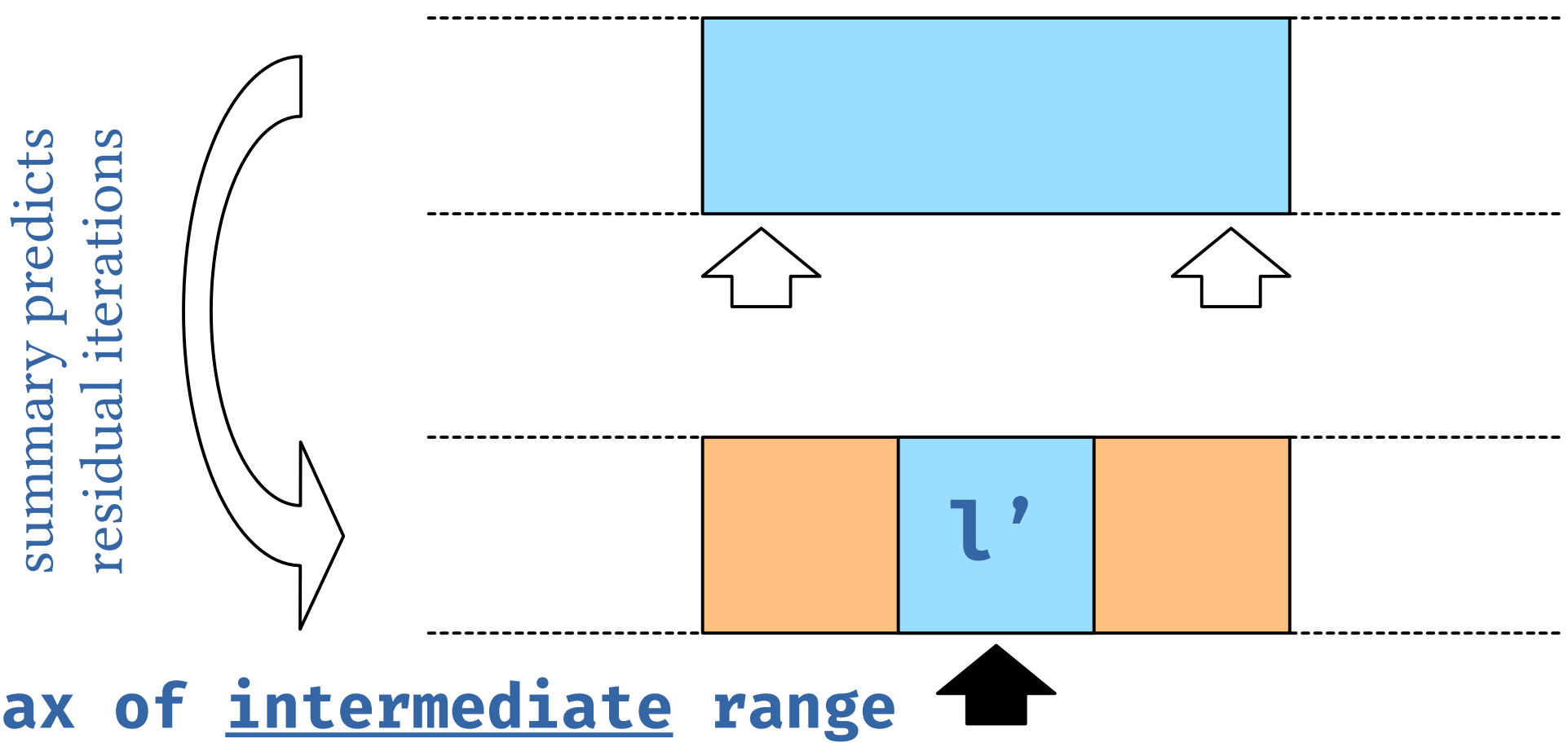
loops with invariants $\Longleftrightarrow$

tail recursion where pre-/postcondition are the same

8/17—Relational summary: `a[l'] == max(a[l..r+1])`



8/17—Relational summary: `a[l'] == max(a[l..r+1])`



9/17—Loop Contract for iterative version

```
l := 0,  r := a.length - 1


while true do
  requires 0 ⩽ l ⩽ r < a.length
  ensures  a[l'] == max(a[l..r+1])
assert  a[l] == max(a[0..a.length])
```

syntactic reference to final value of `l`

loop summary very similar to postcondition!

Loop Contracts **[Hehner, Tuerk, …]**

1. … generalize proofs with invariants
2. … sometimes capture proofs quite naturally

Invariant

- describes work done so far
- reasons about *partial* results

Summary

- describes residual work
- reasons about *complete* results but for intermediate states

Loop Contracts [Hehner, Tuerk, ...]

1. ... generalize proofs with invariants
2. ... sometimes capture proofs quite naturally

This paper: <u>explain</u> loop contracts

- *simple* formalization of verification conditions
- clarify correspondence between invariants and summaries
- tool construction guidelines
- examples with text-book verification challenges

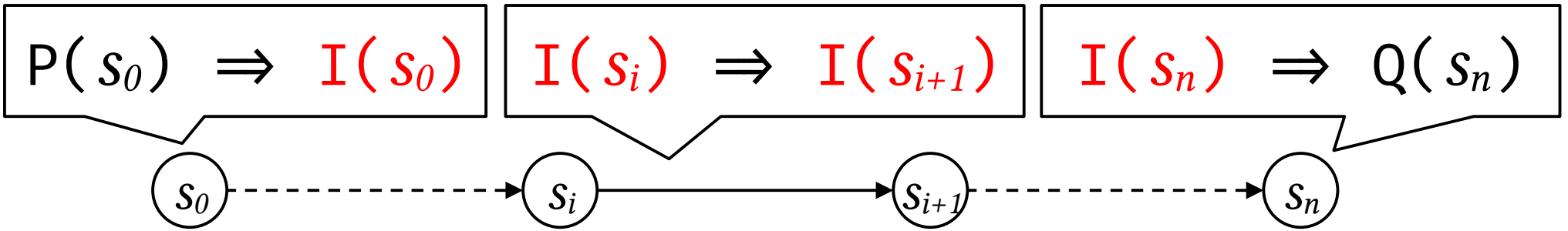
Loop Contracts [Hehner, Tuerk, ...]

1. ... generalize proofs with invariants
2. ... sometimes capture proofs quite naturally

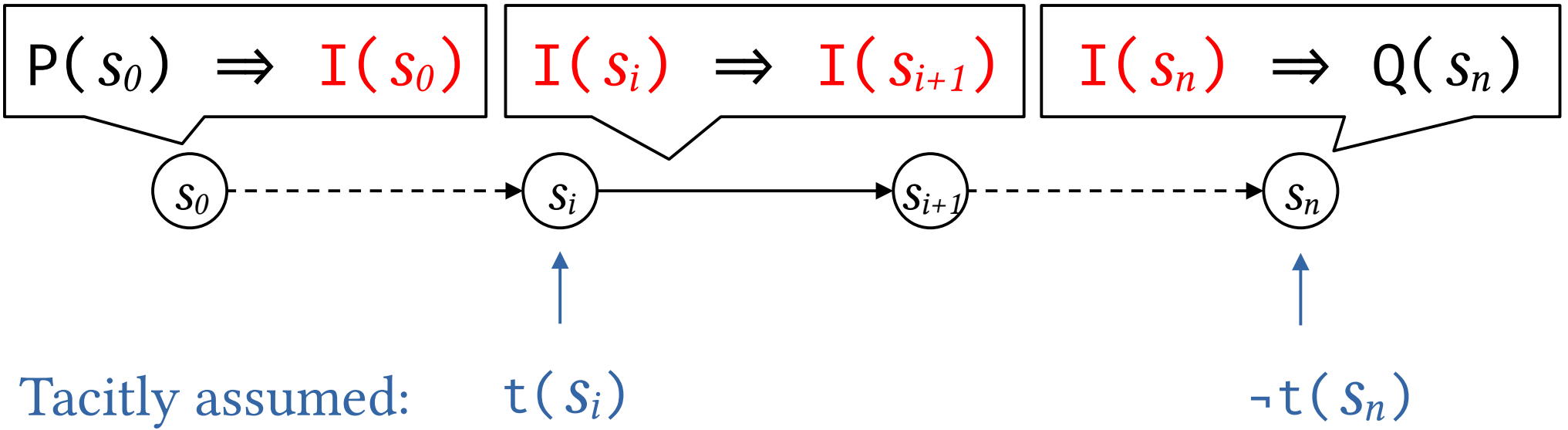
This paper: explain loop contracts

- *simple* formalization of verification conditions
- clarify correspondence between invariants and summaries
- tool construction guidelines
- examples with text-book verification challenges

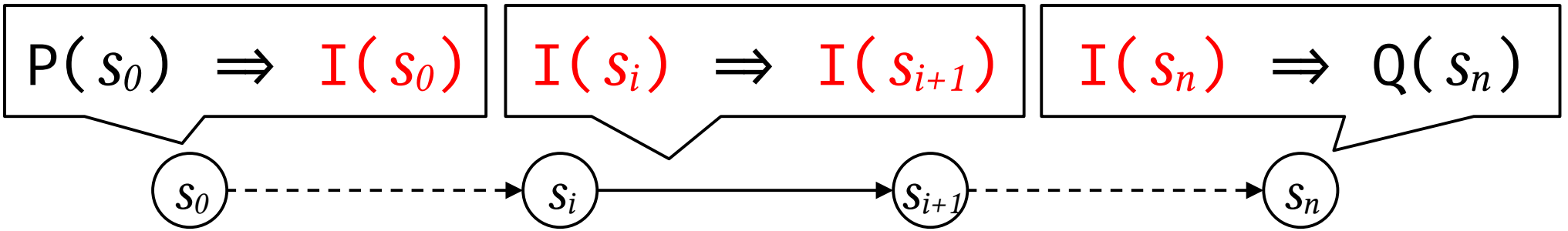
10/17—Verification of `{ P } while t do B { Q }`



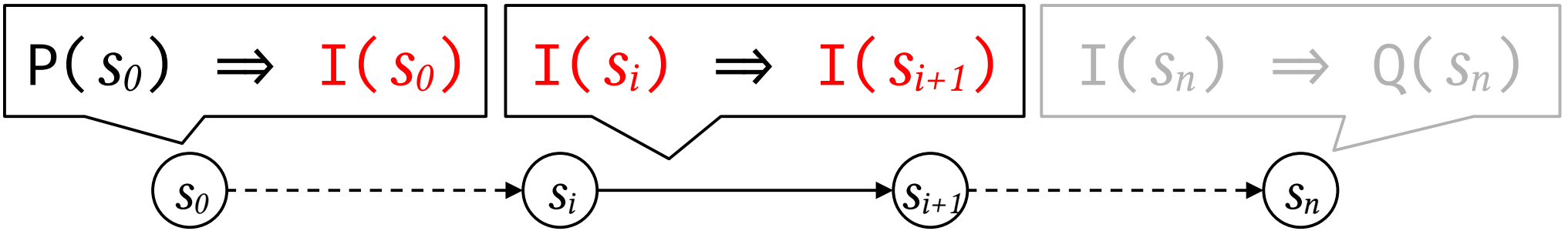
10/17—Verification of `{ P } while t do B { Q }`



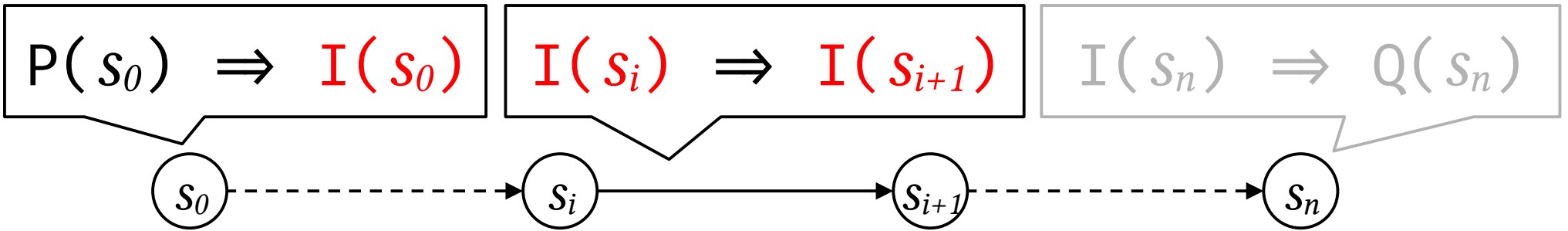
10/17—Verification of `{ P } while t do B { Q }`



10/17—Verification of `{ P } while t do B { Q }`

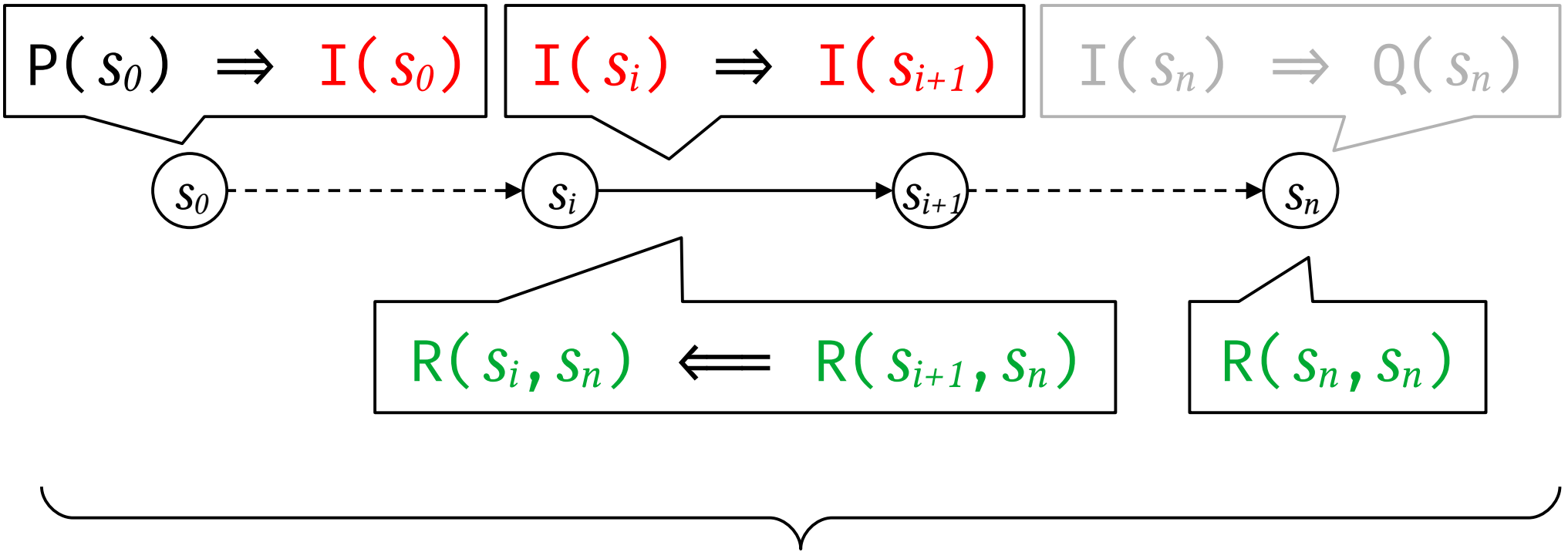


10/17—Verification of `{ P } while t do B { Q }`



$$P(s_0) \land R(s_0, s_n) \Longrightarrow Q(s_n)$$

10/17—Verification of `{ P } while t do B { Q }`



$$P(s_0) \land R(s_0, s_n) \implies Q(s_n)$$

Loop Contracts [Hehner, Tuerk, ...]

1. ... generalize proofs with invariants
2. ... sometimes capture proofs quite naturally

This paper: explain loop contracts

- *simple* formalization of verification conditions
- clarify correspondence between invariants and summaries
- syntactic proof rule for tool implementations
- examples with text-book verification challenges

11/17—Constructive Translations

1. “Canonical” summary recovers standard approach

$$R(s, s') := \neg t(s') \wedge I(s')$$

2. Encoding of summaries as part of invariants

$$I(s) := \exists\ s_0.\ P(s_0) \wedge (\forall\ s'.\ R(s, s') \implies R(s_0, s'))$$

11/17—Constructive Translations

1. "Canonical" summary recovers standard approach

$$R(s, s') := \neg t(s') \wedge I(s')$$

Result: characterization of completeness

summaries: functionality
invariants: no runtime errors / functionality
variants: termination

11/17—Constructive Translations

we can re-use existing tools with
“just” frontend engineering

(no excuse to not have loop contracts with summaries)

2. Encoding of summaries as part of invariants

$$I(s) := \exists\ s_0.\ P(s_0) \wedge (\forall\ s'.\ R(s, s') \implies R(s_0, s'))$$

11/17—Constructive Translations

Drawback: additional Quantifiers! But sometimes not needed:

∃ s_0 obsolete with `\old( ... )` in invariants

∀ s' can be eliminated for variables with `x' = f(s)`

2. Encoding of summaries as part of invariants

$$I(s) := \exists\ s_0.\ P(s_0) \wedge (\forall\ s'.\ R(s,s') \implies R(s_0,s'))$$

12/17—Loop Contract = Invariant + Summary

Invariant	Summary
• what has been done	• what is left to do

constructive translations:
can choose how to encode correctness properties

Key Insight:
can decouple *conceptual solution* from *technical approach*

Loop Contracts [Hehner, Tuerk, ...]

1. ... generalize proofs with invariants
2. ... sometimes capture proofs quite naturally

This paper: explain loop contracts

- *simple* formalization of verification conditions
- clarify correspondence between invariants and summaries
- syntactic proof rule for tool implementations
- examples with text-book verification challenges

13/17—Hoare Logic proof rule (same for `wp`/`sp`)

(treat loop as tail-recursive procedure)

$$\{\ \mathtt{I(x)} \wedge \mathtt{x} = x_0\ \}\ \mathtt{while\ t\ do\ B}\ \{\ \mathtt{R}(x_0, \mathtt{x})\ \}$$

13/17—Hoare Logic proof rule (same for `wp`/`sp`)

$$\frac{\{\ t(x) \wedge I(x) \wedge x = x_i\ \}\ B;\ x:\ [I,\ R]\ \{\ R(x_i,\ x)\ \} \qquad \{\ \neg\ t(x) \wedge I(x) \wedge x = x_n\ \}\ \texttt{skip}\ \{\ R(x_n,\ x)\ \}}{\{\ I(x) \wedge x = x_0\ \}\ \texttt{while t do B}\ \{\ R(x_0,\ x)\ \}}$$

13/17—Hoare Logic proof rule (same for `wp`/`sp`)

Key Idea:
specification statement [Morgan 88]
embeds application of inductive hypothesis into program

$$\frac{\{\ t(x) \wedge I(x) \wedge x = x_i\ \}\ B;\ \boxed{x:\ [I,\ R]}\ \{\ R(x_i,\ x)\ \} \qquad \{\ \neg\ t(x) \wedge I(x) \wedge x = x_n\ \}\ \texttt{skip}\ \{\ R(x_n,\ x)\ \}}{\{\ I(x) \wedge x = x_0\ \}\ \texttt{while t do B}\ \{\ R(x_0,\ x)\ \}}$$

13/17—Hoare Logic proof rule (same for `wp`/`sp`)

Key Idea:
specification statement [Morgan 88]
embeds application of inductive hypothesis into program

`assert I(x);` x_{i+1} `:= x; havoc x; assume R(`x_{i+1}`, x)`

$$\frac{\{\ t(x) \wedge I(x) \wedge x = x_i\ \}\ B;\ \boxed{x: [I, R]}\ \{\ R(x_i, x)\ \} \qquad \{\ \neg\, t(x) \wedge I(x) \wedge x = x_n\ \}\ \texttt{skip}\ \{\ R(x_n, x)\ \}}{\{\ I(x) \wedge x = x_0\ \}\ \texttt{while t do B}\ \{\ R(x_0, x)\ \}}$$

13/17—Hoare Logic proof rule (same for `wp`/`sp`)

Key Idea:
specification statement [Morgan 88]
embeds application of inductive hypothesis into program

Implementation is simple! No "meta" embedding like Tuerk

$$\frac{\{\ t(x) \wedge I(x) \wedge x = x_i\ \}\ B;\ \texttt{x: [I, R]}\ \{\ R(x_i, x)\ \} \qquad \{\ \neg\, t(x) \wedge I(x) \wedge x = x_n\ \}\ \texttt{skip}\ \{\ R(x_n, x)\ \}}{\{\ I(x) \wedge x = x_0\ \}\ \texttt{while t do B}\ \{\ R(x_0, x)\ \}}$$

Loop Contracts [Hehner, Tuerk, ...]

1. ... generalize proofs with invariants
2. ... sometimes capture proofs quite naturally

This paper: explain loop contracts

- *simple* formalization of verification conditions
- clarify correspondence between invariants and summaries
- syntactic proof rule for tool implementations
- examples with text-book verification challenges (more: paper)

14/17—Example: `bsearch(int x, int[] a)`

invariant `x ∉ a[0..l] ∧ x ∉ a[r+1..a.length]`

summary `\result ⟺ x ∈ a[l..r+1]`

14/17—Example: `bsearch(int x, int[] a)`

invariant `x ∉ a[0..l] ∧ x ∉ a[r+1..a.length]`

summary `\result ⟺ x ∈ a[l..r+1]`

Comparison: summary often captures *intention* really well

14/17—Example: `bsearch(int x, int[] a)`

invariant `x ∉ a[0..l] ∧ x ∉ a[r+1..a.length]`

summary `\result ⟺ x ∈ a[l..r+1]`

Comparison: summary often captures *intention* really well

summary encoded as invariant and simplified

`x ∈ a[l..r+1] ⟺ a[0..a.length]`

15/17—Example: `copy(int[] a, int[] b)`

invariant `b[..i] = a[..i]`

summary `b'[i..] = a[i..]` $\wedge$ ...

15/17—Example: `copy(int[] a, int[] b)`

invariant `b[..i] = a[..i]`

summary `b'[i..] = a[i..]` ∧

`b'[..i] = b[..i]`

Comparison: summary may require *additional framing*

completing the loop "forgets" leading `b[i] := a[i]`

16/17—Example: “right-fold” specifications

```
f :: State ⟶ List
```

$$f(s) = \begin{cases} [] & \text{if } \neg\, t(s) \\ x :: f(s') & \text{if } \quad t(s) \wedge B(s,s') \end{cases}$$

typical specification pattern:
abstraction with algebraic lists produces
first element in recursion (“right-fold”)

16/17—Example: "right-fold" specifications

```
f :: State ⟶ List
```

$$f(s) = \begin{cases} [] & \text{if } \neg\, t(s) \\ x :: f(s') & \text{if } \quad t(s) \wedge B(s,s') \end{cases}$$

Comparison:

Invariants: need lemma to translate `f` into *left-fold*

Summaries: matches *right-fold* `f` **directly**

(cf. phone number example in the paper)

17/17—Preliminary: Automatic Inference of Summaries?

- Generalize postconditions by initial values:

  `max(a[0..a.length])` $\rightsquigarrow$ `max(a[l..r+1])`

  $\rightarrow$ works for simple examples only

- Experiment: ask Horn solvers (see extended version)

  $\rightarrow$ typical benchmarks either too hard or too simple

Thanks for your attention!

Loop Contract

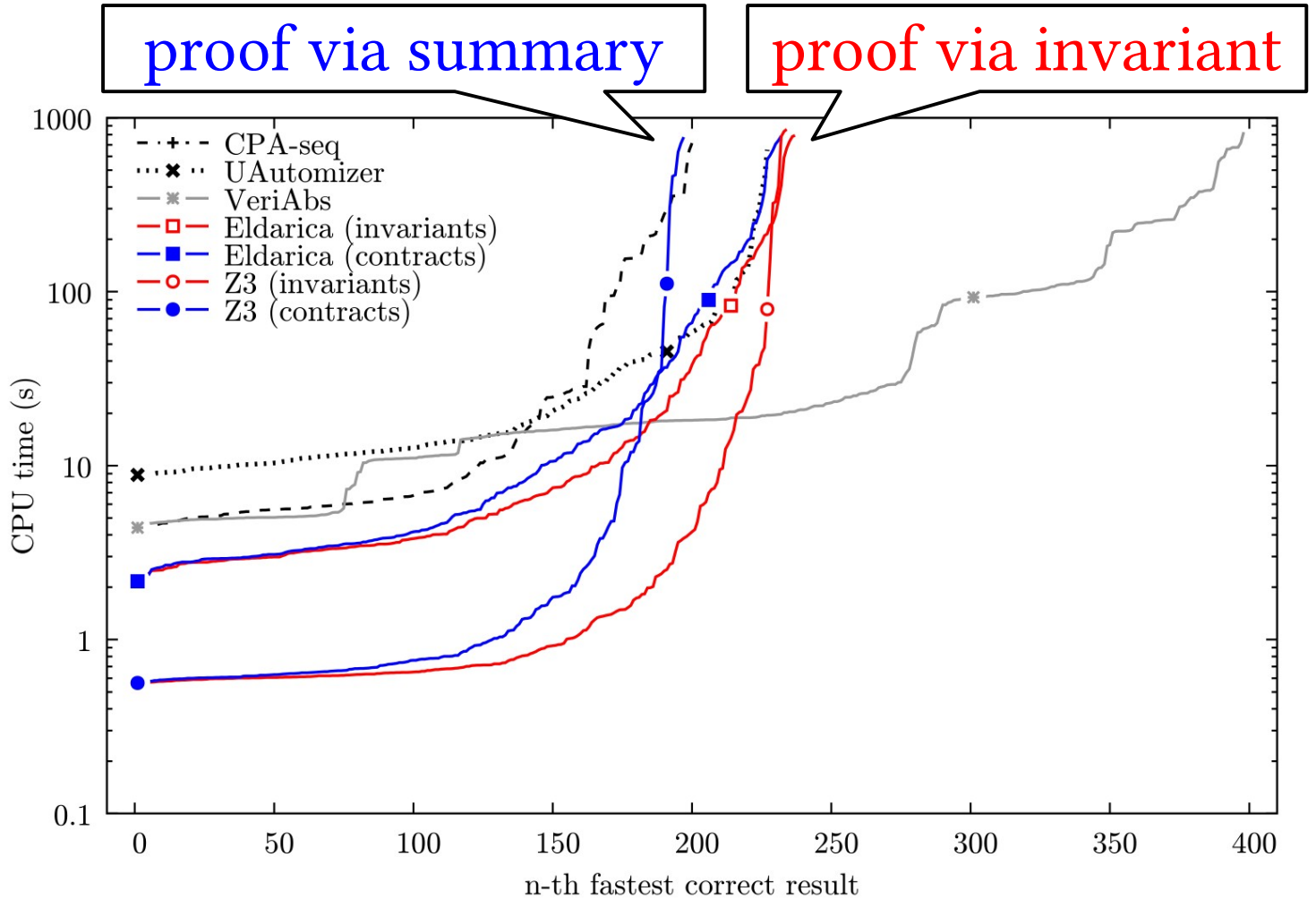
Invariant	Summary
well-known & researched	→ full potential to be explored
forwards / left-fold	backwards / right-fold
fewer frame conditions	similar to postcondition (= intention)

Conclusion: Want both! Theory & Tool support is easy.

Appendix

1. Evaluation of Proof Automation
2. Invariants for maxElim from VerifyThis 2011
3. Example of a backwards propagation proof
4. Bubble Sort and Insertion Sort

Proof Automation: off-the-shelf Horn Solvers



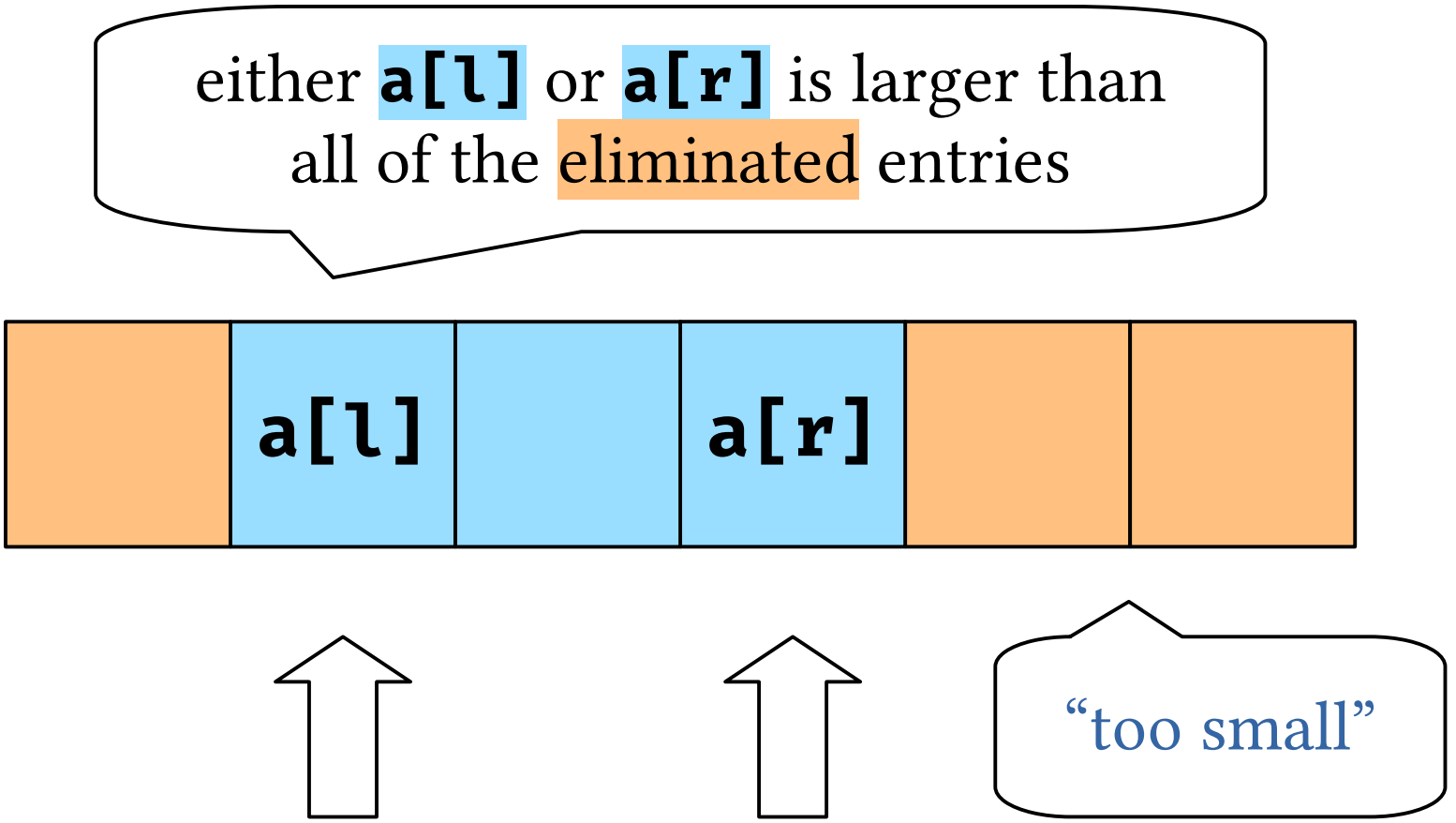
Evaluation like SV-Comp 2020

Categories: Loops, Recursive, Arrays, ControlFlow

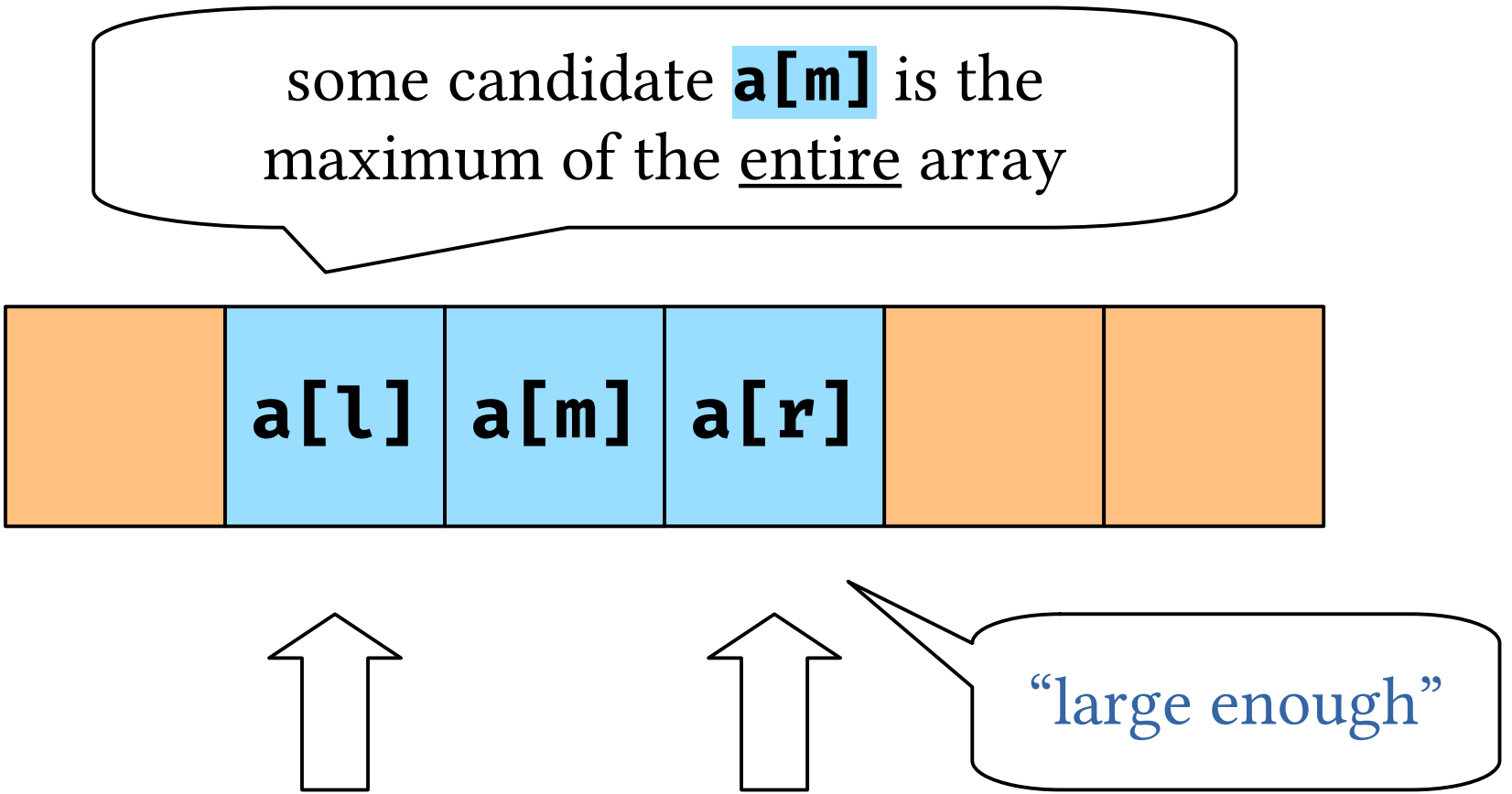
Inconclusive!

- LIA: too easy
- Arrays: too hard

1st Invariant (Filliâtre & Marché)



2nd Invariant (Ernst, Schellhorn, Tofan)



Some Invariants for maxElim, formally

Filliâtre & Marché:

- `0 ≤ l ≤ r < a.length`
- `∀ k. 0 ≤ k < l ∨ r < k < n`
  `⟹ a[k] ≤ a[l] ∨ a[k] ≤ a[r])`

Ernst, Schellhorn, Tofan:

- `∃ k. 0 ≤ l ≤ k ≤ r < a.length`
  `∧ a[k] = max(a[0..a.length])`

Summaries propagate backwards

$$R(s_i, s_n) \Longleftarrow R(s_{i+1}, s_n)$$

- case `if a[l] ⩽ a[r] then l := l+1`

Summaries propagate backwards

$$R(s_i, s_n) \Longleftarrow R(s_{i+1}, s_n)$$

- case `if a[l] ⩽ a[r] then l := l+1`
  - assume `isMax(l', a[l+1 .. r+1])`

Summaries propagate backwards

$$R(s_i, s_n) \Longleftarrow R(s_{i+1}, s_n)$$

- case `if a[l] ⩽ a[r] then l := l+1`
  - assume `isMax(l', a[l+1 .. r+1])`

    therefore `a[l'] ⩾ a[r]`

`a[r]` is part of `a[l+1 .. r+1]`

Summaries propagate backwards

$$R(s_i, s_n) \Longleftarrow R(s_{i+1}, s_n)$$

- case `if a[l] ⩽ a[r] then l := l+1`
  - assume `isMax(l', a[l+1 .. r+1])`

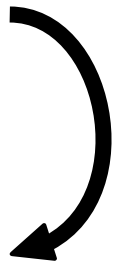
    therefore `a[l'] ⩾ a[r]`
  - prove `isMax(l', a[l .. r+1])`

Summaries propagate backwards

$$R(s_i, s_n) \Longleftarrow R(s_{i+1}, s_n)$$

- case `if a[l] ⩽ a[r] then l := l+1`
  - assume `isMax(l', a[l+1 .. r+1])`

    therefore `a[l'] ⩾ a[r]`
  - prove `isMax(l', a[l .. r+1])`



additional element in range: `a[l]`

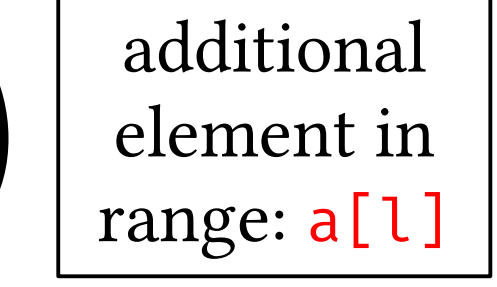
Summaries propagate backwards

$$R(s_i, s_n) \Longleftarrow R(s_{i+1}, s_n)$$

- case `if a[l] ⩽ a[r] then l := l+1`
  - assume `isMax(l', a[l+1 .. r+1])`

    therefore `a[l'] ⩾ a[r]`
  - prove `isMax(l', a[l .. r+1])`

    because `a[l'] ... ⩾ ... a[l]`



Summaries propagate backwards

$$R(s_i, s_n) \Longleftarrow R(s_{i+1}, s_n)$$

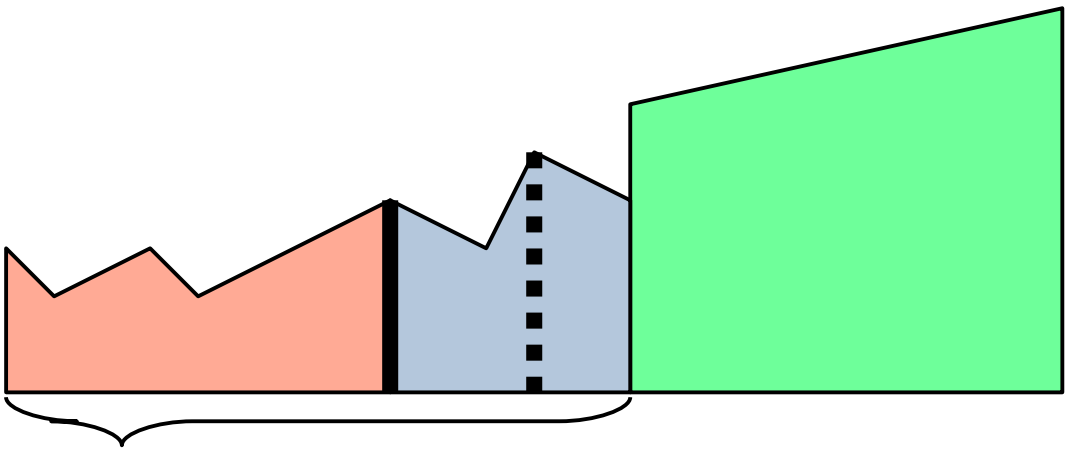
- case `if a[l] ⩽ a[r] then l := l+1`
  - assume `isMax(l', a[l+1 .. r+1])`

    therefore `a[l'] ⩾ a[r]`
  - prove `isMax(l', a[l .. r+1])`

    because `a[l'] ⩾ a[r] ⩾ a[l]`

additional element in range: `a[l]`

Example: Bubble Sort

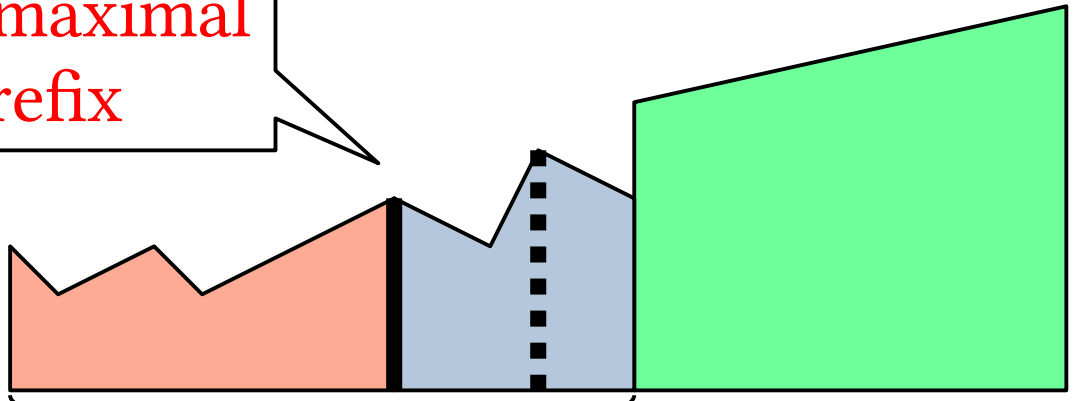


invariant:
sorted & larger
than prefix

summary:
sorted & sorted

summary:
unchanged

Example: Bubble Sort



invariant: maximal wrt. prefix

invariant: sorted & larger than prefix

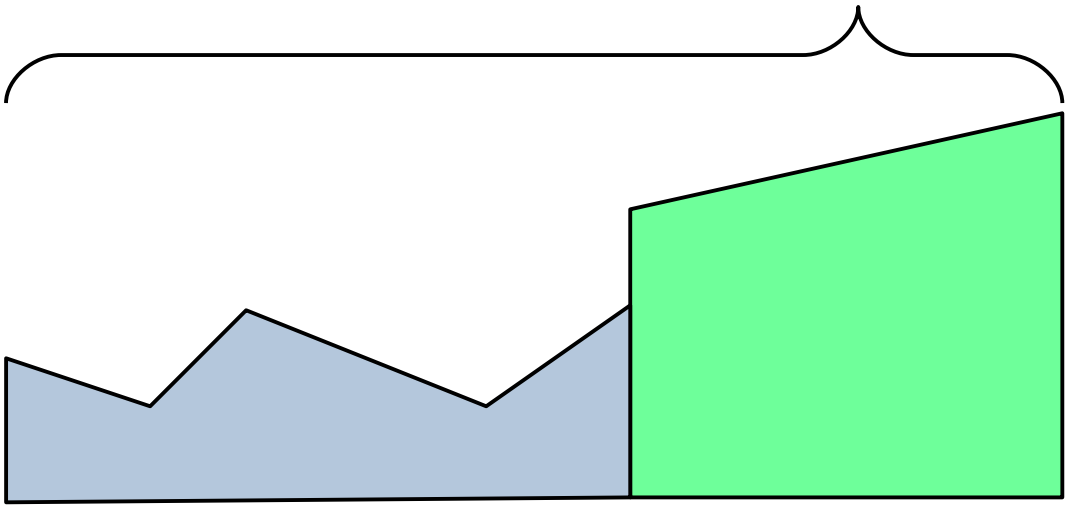
summary: sorted & sorted

summary: bubble up largest intermediate

summary: unchanged

Example: Insertion Sort

summary: overall sorted
(= canonical summary)



invariant and also precondition for contract:
sorted & larger than prefix

Comparison of Sorting Specifications

Bubble Sort

- invariant and summary nicely symmetrical
- work to be done *independent* from work done so far

Insertion Sort

- work to be done depends on sorted suffix
- both approaches essentially the same