# Fundamental Theorems of Loop Invariants

Albert Y. C. Lai

Department of Computer Science
University of Toronto

May 25–29, 2008

# Outline

# Background

- State variables $x$, $y$; collectively called $\sigma$.
- Want a program for $x' = f\ x\ y = f\ \sigma$.
- Let's say **while** $g$ **do** $B$ **od** works.

We know the usual proof approach. . .

(assume termination)

**while** $g$ **do** $B$ **od** implements $x' = f\ x\ y$

$\Leftarrow$

$\forall \sigma_0 \cdot f\ \sigma = f\ \sigma_0$ is a loop invariant

$\wedge\ \forall \sigma_0, \sigma \cdot f\ \sigma = f\ \sigma_0 \wedge \neg g \Rightarrow x = f\ \sigma_0$

# The Question

(assume termination)

$$\textbf{while } g \textbf{ do } B \textbf{ od} \text{ implements } x' = f\,x\,y$$

$$\Leftarrow$$

$$\forall \sigma_0 \cdot f\,\sigma = f\,\sigma_0 \text{ is a loop invariant}$$

$$\wedge\ \forall \sigma_0, \sigma \cdot f\,\sigma = f\,\sigma_0 \wedge \neg g \Rightarrow x = f\,\sigma_0$$

Does $f\,\sigma = f\,\sigma_0$ always work?

# Fundamental Theorem of Loop Invariants

(assume termination)

$$\textbf{while } g \textbf{ do } B \textbf{ od} \text{ implements } x' = f\, x\, y$$

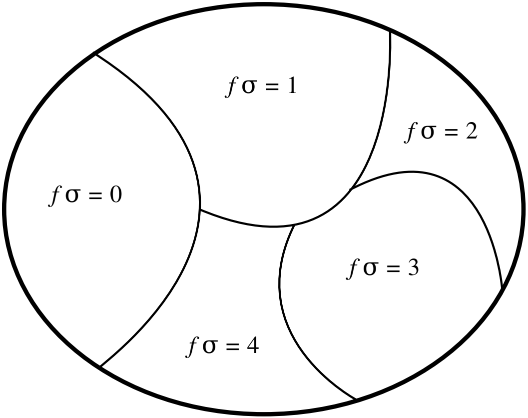
$\Rightarrow$

$$\forall \sigma_0 \cdot f\,\sigma = f\,\sigma_0 \text{ is a loop invariant}$$
$$\wedge\ \forall \sigma_0, \sigma \cdot f\,\sigma = f\,\sigma_0 \wedge \neg g \Rightarrow x = f\,\sigma_0$$

Does $f\,\sigma = f\,\sigma_0$ always work? Yes!

# $f\,\sigma = f\,\sigma_0$ Invariant Visually

Partition state-space by answers. Invariant: Don't cross borders.



# History (circa 1975)

- Several authors noted an easy case for
  **while** $g\,x$ **do** $x{:=}h\,x$ **od** implements $x{:=}f\,x$

# History (circa 1975)

- Several authors noted an easy case for
  **while** $g\ x$ **do** $x := h\ x$ **od** implements $x := f\ x$
- Basu and Misra extended to:
  **while** $g\ x$ **do** $x, y := h\ x\ y$ **od** implements $x' = f\ x$
  But...

Misra

# History (circa 1975)

- Several authors noted an easy case for
  **while** $g\,x$ **do** $x := h\,x$ **od** implements $x := f\,x$
- Basu and Misra extended to:
  **while** $g\,x$ **do** $x, y := h\,x\,y$ **od** implements $x' = f\,x$
  But... must init $y$ before use

Misra

# History (2005 IFIP WG 2.3)

- Misra mentioned the theorem. Audience showed disbelief.
  -  “It’s a theorem! It’s published!"

- Misra mentioned the theorem. Audience showed disbelief.
  -  “It’s a theorem! It’s published!"
  - “Amazing! I’m going to look it up!” 

# History (2005 IFIP WG 2.3)

- Misra mentioned the theorem. Audience showed disbelief.
    -  "It's a theorem! It's published!"
    - "Amazing! I'm going to look it up!" 
- The proof considered execution traces.

# History (2005 IFIP WG 2.3)

- Misra mentioned the theorem. Audience showed disbelief.
  -  "It's a theorem! It's published!"
  - "Amazing! I'm going to look it up!" 
- The proof considered execution traces.
- I tried a proof using refinements, but I made it too complicated.

# History (2005 IFIP WG 2.3)

- Misra mentioned the theorem. Audience showed disbelief.
  -  "It's a theorem! It's published!"
  - "Amazing! I'm going to look it up!" 
- The proof considered execution traces.
- I tried a proof using refinements, but I made it too complicated.
  Dijkstra would not have liked this.

# History (2007)

- Misra visited Toronto.
  “Wouldn’t it be cool to fix my proof and show him!”

# History (2007)

- Misra visited Toronto.
  "Wouldn't it be cool to fix my proof and show him!"
- Ignored some assumptions. Focused on $\Rightarrow$.
  Much simpler.

# History (2007)


- Misra visited Toronto.
  “Wouldn’t it be cool to fix my proof and show him!”
- Ignored some assumptions. Focused on $\Rightarrow$.
  Much simpler.
  Dijkstra would have liked this.

# History (2007)


- Misra visited Toronto.
  "Wouldn't it be cool to fix my proof and show him!"
- Ignored some assumptions. Focused on $\Rightarrow$.
  Much simpler.
  Dijkstra would have liked this.
- The proof today is simpler yet.

# Comparison

**old proof**

- low-level (execution)
  long, informal

**new proof**

- high-level (refinement)
  short, formal

# Comparison

**old proof**

- low-level (execution)
  long, informal
- $B$ deterministic

**new proof**

- high-level (refinement)
  short, formal
- $B$ nondeterministic

# Comparison

## old proof

- low-level (execution)
  long, informal
- $B$ deterministic
- $x' = f\ x$
  $f$ takes $x$ as only input

## new proof

- high-level (refinement)
  short, formal
- $B$ nondeterministic
- $x' = f\ x\ y$
  $f$ may use or ignore $x$,$y$

# Comparison

## old proof

- low-level (execution)
  long, informal
- $B$ deterministic
- $x' = f\ x$
  $f$ takes $x$ as only input
- $y$ for "temp" only
  $g$ cannot read $y$
  $B$ must init $y$ before read

## new proof

- high-level (refinement)
  short, formal
- $B$ nondeterministic
- $x' = f\ x\ y$
  $f$ may use or ignore $x$,$y$
- no restriction on use of $y$

# Outline

# Predicative Programming

$$
\begin{aligned}
\text{specification,program} &= \text{relation between } \sigma \text{ and } \sigma' \\
ok &= \sigma'{=}\sigma \\
B\,.\,C &= \exists\sigma''\cdot B\,\sigma\,\sigma'' \wedge C\,\sigma''\,\sigma' \\
\textbf{if } g \textbf{ then } B \textbf{ else } C &= g{\wedge}B \vee \neg g \wedge C \\
Y \text{ implements } X &= \forall\sigma,\sigma'\cdot X{\Leftarrow}Y
\end{aligned}
$$

# Loops

$$
\begin{aligned}
& \forall \sigma, \sigma' \cdot x' = f\ x\ y \Leftarrow \textbf{while}\ g\ \textbf{do}\ B\ \textbf{od} \\
\wedge\ & \forall \sigma \cdot \exists \sigma' \cdot g \Rightarrow B \\
\wedge\ & \text{loop terminates}
\end{aligned}
$$

$$\Rightarrow$$

$$
\begin{aligned}
\exists W \cdot\quad & \forall \sigma, \sigma' \cdot x' = f\ x\ y \Leftarrow W \Leftarrow \textbf{if}\ g\ \textbf{then}\ B\,.\,W\ \textbf{else}\ ok \\
\wedge\ & \forall \sigma \cdot \exists \sigma' \cdot W\ \sigma\ \sigma'
\end{aligned}
$$

- I just need this much.
- Supported by different definitions.
- Timing included in $B$ and possibly $W$.

# Lemma: $\forall \sigma, \sigma' \cdot f\,\sigma' = f\,\sigma \Leftarrow g \wedge B$

# Lemma: $\forall \sigma, \sigma' \cdot f\,\sigma' = f\,\sigma \Leftarrow g \wedge B$

Proof:

$\top$

# Lemma: $\forall\sigma,\sigma'\cdot f\,\sigma' = f\,\sigma \Leftarrow g \wedge B$

Proof:

$$\top \qquad\qquad x' = f\,\sigma \Leftarrow g \wedge (B\,.\,W)$$

$$\Rightarrow\ \forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g \wedge (B\,.\,W)$$

# Lemma: $\forall \sigma, \sigma' \cdot f\, \sigma' = f\, \sigma \Leftarrow g \wedge B$

Proof:

| | | |
|---|---|---|
| | $\top$ | $x' = f\, \sigma \Leftarrow g \wedge (B\,.\,W)$ |
| $\Rightarrow$ | $\forall \sigma, \sigma' \cdot x' = f\, \sigma \Leftarrow g \wedge (B\,.\,W)$ | sequential |
| $=$ | $\forall \sigma, \sigma' \cdot x' = f\, \sigma \Leftarrow g \wedge (\exists \sigma'' \cdot B\, \sigma\, \sigma'' \wedge W\, \sigma''\, \sigma')$ | |

# Lemma: $\forall\sigma,\sigma'\cdot f\,\sigma' = f\,\sigma \Leftarrow g \wedge B$

Proof:

| | | |
|---|---|---|
| | $\top$ | $x' = f\,\sigma \Leftarrow g \wedge (B\,.\,W)$ |
| $\Rightarrow$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g \wedge (B\,.\,W)$ | sequential |
| $=$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g \wedge (\exists\sigma''\cdot B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma')$ | distribute |
| $=$ | $\forall\sigma,\sigma',\sigma''\cdot x' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma'$ | |

# Lemma: $\forall\sigma,\sigma'\cdot f\,\sigma' = f\,\sigma \Leftarrow g\wedge B$

Proof:

| | | |
|---|---|---|
| | $\top$ | $x' = f\,\sigma \Leftarrow g\wedge(B\,.\,W)$ |
| $\Rightarrow$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g\wedge(B\,.\,W)$ | sequential |
| $=$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g\wedge(\exists\sigma''\cdot B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma')$ | distribute |
| $=$ | $\forall\sigma,\sigma',\sigma''\cdot x' = f\,\sigma \Leftarrow g\wedge B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma'$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow W$ |
| $=$ | $\forall\sigma,\sigma',\sigma''\cdot f\,\sigma'' = f\,\sigma \Leftarrow g\wedge B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma'$ | |

# Lemma: $\forall\sigma,\sigma'\cdot f\,\sigma' = f\,\sigma \Leftarrow g\wedge B$

Proof:

| | | |
|---|---|---|
| | $\top$ | $x' = f\,\sigma \Leftarrow g\wedge(B\,.\,W)$ |
| $\Rightarrow$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g\wedge(B\,.\,W)$ | sequential |
| $=$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g\wedge(\exists\sigma''\cdot B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma')$ | distribute |
| $=$ | $\forall\sigma,\sigma',\sigma''\cdot x' = f\,\sigma \Leftarrow g\wedge B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma'$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow W$ |
| $=$ | $\forall\sigma,\sigma',\sigma''\cdot f\,\sigma'' = f\,\sigma \Leftarrow g\wedge B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma'$ | factor |
| $=$ | $\forall\sigma,\sigma''\cdot f\,\sigma'' = f\,\sigma \Leftarrow g\wedge B\,\sigma\,\sigma'' \wedge(\exists\sigma'\cdot W\,\sigma''\,\sigma')$ | |

# Lemma: $\forall\sigma,\sigma'\cdot f\,\sigma' = f\,\sigma \Leftarrow g \wedge B$

Proof:

| | | |
|---|---|---|
| | $\top$ | $x' = f\,\sigma \Leftarrow g\wedge(B\,.\,W)$ |
| $\Rightarrow$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g\wedge(B\,.\,W)$ | sequential |
| $=$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g\wedge(\exists\sigma''\cdot B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma')$ | distribute |
| $=$ | $\forall\sigma,\sigma',\sigma''\cdot x' = f\,\sigma \Leftarrow g\wedge B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma'$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow W$ |
| $=$ | $\forall\sigma,\sigma',\sigma''\cdot f\,\sigma'' = f\,\sigma \Leftarrow g\wedge B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma'$ | factor |
| $=$ | $\forall\sigma,\sigma''\cdot f\,\sigma'' = f\,\sigma \Leftarrow g\wedge B\,\sigma\,\sigma'' \wedge(\exists\sigma'\cdot W\,\sigma''\,\sigma')$ | $\forall\sigma\cdot\exists\sigma'\cdot W\,\sigma\,\sigma'$ |
| $=$ | $\forall\sigma,\sigma''\cdot f\,\sigma'' = f\,\sigma \Leftarrow g\wedge B\,\sigma\,\sigma''$ | |

# Lemma: $\forall\sigma,\sigma'\cdot f\,\sigma' = f\,\sigma \Leftarrow g\wedge B$

Proof:

| | | |
|---|---|---|
| | $\top$ | $x' = f\,\sigma \Leftarrow g\wedge(B\,.\,W)$ |
| $\Rightarrow$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g\wedge(B\,.\,W)$ | sequential |
| $=$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g\wedge(\exists\sigma''\cdot B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma')$ | distribute |
| $=$ | $\forall\sigma,\sigma',\sigma''\cdot x' = f\,\sigma \Leftarrow g\wedge B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma'$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow W$ |
| $=$ | $\forall\sigma,\sigma',\sigma''\cdot f\,\sigma'' = f\,\sigma \Leftarrow g\wedge B\,\sigma\,\sigma'' \wedge W\,\sigma''\,\sigma'$ | factor |
| $=$ | $\forall\sigma,\sigma''\cdot f\,\sigma'' = f\,\sigma \Leftarrow g\wedge B\,\sigma\,\sigma'' \wedge(\exists\sigma'\cdot W\,\sigma''\,\sigma')$ | $\forall\sigma\cdot\exists\sigma'\cdot W\,\sigma\,\sigma'$ |
| $=$ | $\forall\sigma,\sigma''\cdot f\,\sigma'' = f\,\sigma \Leftarrow g\wedge B\,\sigma\,\sigma''$ | rename |
| $=$ | $\forall\sigma,\sigma'\cdot f\,\sigma' = f\,\sigma \Leftarrow g\wedge B$ | |

# Fundamental Theorem of Loop Invariants

**Definition**

$p$ is a loop invariant $=$ $(\forall \sigma, \sigma' \cdot p\,\sigma' \Leftarrow p\,\sigma \wedge g \wedge B)$

# Fundamental Theorem of Loop Invariants

## Definition

$p$ is a loop invariant $=$ $(\forall \sigma, \sigma' \cdot p\,\sigma' \Leftarrow p\,\sigma \wedge g \wedge B)$

In our case:

$\forall \sigma_0 \cdot f\,\sigma = f\,\sigma_0$ is a loop invariant

# Fundamental Theorem of Loop Invariants

**Definition**

$p$ is a loop invariant $=$ $(\forall \sigma, \sigma' \cdot p\,\sigma' \Leftarrow p\,\sigma \wedge g \wedge B)$

In our case:

$$\begin{array}{ll} & \forall \sigma_0 \cdot f\,\sigma = f\,\sigma_0 \text{ is a loop invariant} \\ = & \forall \sigma_0 \cdot \forall \sigma, \sigma' \cdot f\,\sigma' = f\,\sigma_0 \Leftarrow f\,\sigma = f\,\sigma_0 \wedge g \wedge B \end{array}$$

# Fundamental Theorem of Loop Invariants

**Definition**

$p$ is a loop invariant $=$ $(\forall\sigma,\sigma'\cdot p\,\sigma' \Leftarrow p\,\sigma \wedge g \wedge B)$

In our case:

$$\forall\sigma_0\cdot f\,\sigma = f\,\sigma_0 \text{ is a loop invariant}$$

$$= \quad \forall\sigma_0\cdot \forall\sigma,\sigma'\cdot f\,\sigma' = f\,\sigma_0 \Leftarrow f\,\sigma = f\,\sigma_0 \wedge g \wedge B \qquad \text{context}$$

$$= \quad \forall\sigma_0\cdot \forall\sigma,\sigma'\cdot f\,\sigma' = f\,\sigma \Leftarrow f\,\sigma = f\,\sigma_0 \wedge g \wedge B$$

# Fundamental Theorem of Loop Invariants

**Definition**

$p$ is a loop invariant $=$ $(\forall\sigma,\sigma'\cdot p\,\sigma' \Leftarrow p\,\sigma \wedge g \wedge B)$

In our case:

$$\forall\sigma_0\cdot f\,\sigma = f\,\sigma_0 \text{ is a loop invariant}$$

$$= \quad \forall\sigma_0\cdot \forall\sigma,\sigma'\cdot f\,\sigma' = f\,\sigma_0 \Leftarrow f\,\sigma = f\,\sigma_0 \wedge g \wedge B \qquad \text{context}$$

$$= \quad \forall\sigma_0\cdot \forall\sigma,\sigma'\cdot f\,\sigma' = f\,\sigma \Leftarrow f\,\sigma = f\,\sigma_0 \wedge g \wedge B \qquad \text{factor}$$

$$= \quad \forall\sigma,\sigma'\cdot f\,\sigma' = f\,\sigma \Leftarrow g \wedge B \wedge (\exists\sigma_0\cdot f\,\sigma = f\,\sigma_0)$$

# Fundamental Theorem of Loop Invariants

## Definition

$p$ is a loop invariant $=$ $(\forall \sigma, \sigma' \cdot p\,\sigma' \Leftarrow p\,\sigma \wedge g \wedge B)$

In our case:

$$\forall \sigma_0 \cdot f\,\sigma = f\,\sigma_0 \text{ is a loop invariant}$$

$$= \quad \forall \sigma_0 \cdot \forall \sigma, \sigma' \cdot f\,\sigma' = f\,\sigma_0 \Leftarrow f\,\sigma = f\,\sigma_0 \wedge g \wedge B \qquad \text{context}$$

$$= \quad \forall \sigma_0 \cdot \forall \sigma, \sigma' \cdot f\,\sigma' = f\,\sigma \Leftarrow f\,\sigma = f\,\sigma_0 \wedge g \wedge B \qquad \text{factor}$$

$$= \quad \forall \sigma, \sigma' \cdot f\,\sigma' = f\,\sigma \Leftarrow g \wedge B \wedge (\exists \sigma_0 \cdot f\,\sigma = f\,\sigma_0)$$

$$= \quad \forall \sigma, \sigma' \cdot f\,\sigma' = f\,\sigma \Leftarrow g \wedge B$$

# Fundamental Theorem of Loop Invariants

## Definition

$p$ is a loop invariant $=$ $(\forall \sigma, \sigma' \cdot p\,\sigma' \Leftarrow p\,\sigma \wedge g \wedge B)$

In our case:

$$
\begin{aligned}
& \forall \sigma_0 \cdot f\,\sigma = f\,\sigma_0 \text{ is a loop invariant} && \\
= \;& \forall \sigma_0 \cdot \forall \sigma, \sigma' \cdot f\,\sigma' = f\,\sigma_0 \Leftarrow f\,\sigma = f\,\sigma_0 \wedge g \wedge B && \text{context} \\
= \;& \forall \sigma_0 \cdot \forall \sigma, \sigma' \cdot f\,\sigma' = f\,\sigma \Leftarrow f\,\sigma = f\,\sigma_0 \wedge g \wedge B && \text{factor} \\
= \;& \forall \sigma, \sigma' \cdot f\,\sigma' = f\,\sigma \Leftarrow g \wedge B \wedge (\exists \sigma_0 \cdot f\,\sigma = f\,\sigma_0) && \\
= \;& \forall \sigma, \sigma' \cdot f\,\sigma' = f\,\sigma \Leftarrow g \wedge B && \\
= \;& \text{Lemma} &&
\end{aligned}
$$

# Hehner Told You So

Prove $x' = f\,\sigma \Leftarrow \mathbf{if}\ g\ \mathbf{then}\ B\,.\,x' = f\,\sigma\ \mathbf{else}\ ok$
in the first place?

# Hehner Told You So

Prove $x' = f\,\sigma \Leftarrow \textbf{if } g \textbf{ then } B\,.\,x' = f\,\sigma \textbf{ else } ok$
in the first place?

$$\forall \sigma, \sigma' \cdot x' = f\,\sigma \Leftarrow g \wedge (B\,.\,x' = f\,\sigma)$$

# Hehner Told You So

Prove $x' = f\,\sigma \Leftarrow \textbf{if}\ g\ \textbf{then}\ B\,.\,x' = f\,\sigma\ \textbf{else}\ ok$
in the first place?

$$\forall \sigma, \sigma' \cdot x' = f\,\sigma \Leftarrow g \wedge (B\,.\,x' = f\,\sigma) \qquad \text{sequential}$$

$$= \quad \forall \sigma, \sigma' \cdot x' = f\,\sigma \Leftarrow g \wedge (\exists \sigma'' \cdot B\,\sigma\,\sigma'' \wedge x' = f\,\sigma'')$$

# Hehner Told You So

Prove $x' = f\,\sigma \Leftarrow \textbf{if}\ g\ \textbf{then}\ B\,.\,x' = f\,\sigma\ \textbf{else}\ ok$
in the first place?

$$\forall \sigma, \sigma' \cdot x' = f\,\sigma \Leftarrow g \wedge (B\,.\,x' = f\,\sigma) \qquad \text{sequential}$$

$$= \quad \forall \sigma, \sigma' \cdot x' = f\,\sigma \Leftarrow g \wedge (\exists \sigma'' \cdot B\,\sigma\,\sigma'' \wedge x' = f\,\sigma'') \qquad \text{distribute}$$

$$= \quad \forall \sigma, \sigma', \sigma'' \cdot x' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'' \wedge x' = f\,\sigma''$$

# Hehner Told You So

Prove $x' = f\,\sigma \Leftarrow \mathbf{if}\ g\ \mathbf{then}\ B\,.\,x' = f\,\sigma\ \mathbf{else}\ ok$
in the first place?

| | | |
|---|---|---|
| | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g \wedge (B\,.\,x' = f\,\sigma)$ | sequential |
| $=$ | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g \wedge (\exists\sigma''\cdot B\,\sigma\,\sigma'' \wedge x' = f\,\sigma'')$ | distribute |
| $=$ | $\forall\sigma,\sigma',\sigma''\cdot x' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'' \wedge x' = f\,\sigma''$ | context |
| $=$ | $\forall\sigma,\sigma',\sigma''\cdot f\,\sigma'' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'' \wedge x' = f\,\sigma''$ | |

# Hehner Told You So

Prove $x' = f\,\sigma \Leftarrow \textbf{if } g \textbf{ then } B \,.\, x' = f\,\sigma \textbf{ else } ok$
in the first place?

| | | |
|---|---|---|
| | $\forall\sigma,\sigma' \cdot x' = f\,\sigma \Leftarrow g \wedge (B \,.\, x' = f\,\sigma)$ | sequential |
| $=$ | $\forall\sigma,\sigma' \cdot x' = f\,\sigma \Leftarrow g \wedge (\exists\sigma'' \cdot B\,\sigma\,\sigma'' \wedge x' = f\,\sigma'')$ | distribute |
| $=$ | $\forall\sigma,\sigma',\sigma'' \cdot x' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'' \wedge x' = f\,\sigma''$ | context |
| $=$ | $\forall\sigma,\sigma',\sigma'' \cdot f\,\sigma'' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'' \wedge x' = f\,\sigma''$ | factor |
| $=$ | $\forall\sigma,\sigma'' \cdot f\,\sigma'' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'' \wedge (\exists\sigma' \cdot x' = f\,\sigma'')$ | |

# Hehner Told You So

Prove $x' = f\,\sigma \Leftarrow \textbf{if } g \textbf{ then } B\,.\,x' = f\,\sigma \textbf{ else } ok$
in the first place?

| | | |
|---|---|---|
| | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g \wedge (B\,.\,x' = f\,\sigma)$ | sequential |
| = | $\forall\sigma,\sigma'\cdot x' = f\,\sigma \Leftarrow g \wedge (\exists\sigma''\cdot B\,\sigma\,\sigma'' \wedge x' = f\,\sigma'')$ | distribute |
| = | $\forall\sigma,\sigma',\sigma''\cdot x' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'' \wedge x' = f\,\sigma''$ | context |
| = | $\forall\sigma,\sigma',\sigma''\cdot f\,\sigma'' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'' \wedge x' = f\,\sigma''$ | factor |
| = | $\forall\sigma,\sigma''\cdot f\,\sigma'' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'' \wedge (\exists\sigma'\cdot x' = f\,\sigma'')$ | |
| = | $\forall\sigma,\sigma'\cdot f\,\sigma' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'$ | |

# Hehner Told You So

Prove $x' = f\,\sigma \Leftarrow \textbf{if } g \textbf{ then } B\,.\,x' = f\,\sigma \textbf{ else } ok$
in the first place?

| | | |
|---|---|---|
| | $\forall \sigma, \sigma' \cdot x' = f\,\sigma \Leftarrow g \wedge (B\,.\,x' = f\,\sigma)$ | sequential |
| $=$ | $\forall \sigma, \sigma' \cdot x' = f\,\sigma \Leftarrow g \wedge (\exists \sigma'' \cdot B\,\sigma\,\sigma'' \wedge x' = f\,\sigma'')$ | distribute |
| $=$ | $\forall \sigma, \sigma', \sigma'' \cdot x' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'' \wedge x' = f\,\sigma''$ | context |
| $=$ | $\forall \sigma, \sigma', \sigma'' \cdot f\,\sigma'' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'' \wedge x' = f\,\sigma''$ | factor |
| $=$ | $\forall \sigma, \sigma'' \cdot f\,\sigma'' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'' \wedge (\exists \sigma' \cdot x' = f\,\sigma'')$ | |
| $=$ | $\forall \sigma, \sigma' \cdot f\,\sigma' = f\,\sigma \Leftarrow g \wedge B\,\sigma\,\sigma'$ | |
| $=$ | Lemma | |

Yes!

# Outline

1. The Theorem & History
2. Proof in Predicative Programming
3. Applications
4. Full Versions of The Theorem

# The Theorem Is Useless (A)

## the hard part is inventing the function

$$s' = \Sigma L$$

$$\Leftarrow \quad s{:=}0 \ . \ n{:=}0 \ . \ s' = s + \Sigma L\,[n;..\#L]$$

$$s' = s + \Sigma L\,[n;..\#L]$$

$$\Leftarrow \quad \textbf{while } n \neq \#L \textbf{ do } s := s + L\,n \ . \ n{:=}n{+}1 \textbf{ od}$$

# The Theorem Is Useless (A)

## the hard part is inventing the function

$$s' = \Sigma L$$

$$\Leftarrow \quad s{:=}0 \ . \ n{:=}0 \ . \ s' = s + \Sigma L\,[n;..\#L]$$

The theorem applies here:

$$s' = s + \Sigma L\,[n;..\#L]$$

$$\Leftarrow \quad \textbf{while } n{\neq}\#L \textbf{ do } s := s + L\,n \ . \ n{:=}n{+}1 \textbf{ od}$$

# The Theorem Is Useless (A)

## the hard part is inventing the function

But how did you invent this?

$$s' = \Sigma L$$
$$\Leftarrow \quad s{:=}0 \ . \ n{:=}0 \ . \ s' = s + \Sigma L\,[n;..\#L]$$

The theorem applies here:

$$s' = s + \Sigma L\,[n;..\#L]$$
$$\Leftarrow \quad \textbf{while}\ n{\neq}\#L\ \textbf{do}\ s := s + L\,n \ . \ n{:=}n{+}1\ \textbf{od}$$

# The Theorem Is Useless (B)

## sometimes another invariant is better

Maximum Segment Sum

$$s' = (MAX\ i, j \mid i \le j \le \#L \cdot \Sigma L\,[i;..j])$$

$$\Leftarrow \quad s{:=}0 \,.\, c{:=}0 \,.\, n{:=}0 \,.\, \textbf{while } n \ne \#L \textbf{ do } c := (c + L\,n) \uparrow 0 \,.\, s := s \uparrow c \,.\, n := n+1 \textbf{ od}$$

# The Theorem Is Useless (B)

## sometimes another invariant is better

Maximum Segment Sum

$$s' = (MAX\; i, j \mid i \leq j \leq \#L \cdot \Sigma L[i;..j])$$

$$\Leftarrow \quad s{:=}0 \,.\, c{:=}0 \,.\, n{:=}0 \,.\, \textbf{while}\; n \neq \#L \;\textbf{do}\; c := (c + L\,n) \uparrow 0 \,.\, s := s \uparrow c \,.\, n := n+1 \;\textbf{od}$$

- loop invariant
  $s = (MAX\; i, j \mid i \leq j \leq n \cdot \Sigma L[i;..j])$
  $c = (MAX\; i \mid i \leq n \cdot \Sigma L[i;..n])$
  well-motivated by heuristics

# The Theorem Is Useless (B)

## sometimes another invariant is better

Maximum Segment Sum

$$s' = (MAX\ i, j \mid i \le j \le \#L \cdot \Sigma L\,[i;..j])$$

$$\Leftarrow \quad s{:=}0\,.\,c{:=}0\,.\,n{:=}0\,.\,\mathbf{while}\ n \ne \#L\ \mathbf{do}\ c{:=}(c+L\,n)\uparrow 0\,.\,s{:=}s\uparrow c\,.\,n{:=}n+1\ \mathbf{od}$$

- loop invariant
  $s = (MAX\ i, j \mid i \le j \le n \cdot \Sigma L\,[i;..j])$
  $c = (MAX\ i \mid i \le n \cdot \Sigma L\,[i;..n])$
  well-motivated by heuristics
- loop function
  $s' = s \uparrow (MAX\ j \mid n+1 \le j \le \#L \cdot (c + \Sigma L\,[n;..j]) \uparrow (MAX\ i \mid n+1 \le i \le j \cdot \Sigma L\,[i;..j]))$
  why bother

# The Theorem Is Meaningful

Suggestion for program design, verification, analysis:

- loop invariant from loop function
- loop function from context outside

# The Theorem Is Meaningful

Suggestion for program design, verification, analysis:

- loop invariant from loop function
- loop function from context outside

*Think outside the loop!*

# The Proof Is Meaningful

Two ways to prove a theorem for all programs:

**hairy**

- prove in executions

misses the forest for the trees

**clean**

- prove in refinements
- invoke: refinements faithful to executions

holistic, exploits structures

# Outline

# Full Versions of The Theorem

(assume termination)

$$(\textbf{while } g \textbf{ do } B \textbf{ od} \text{ implements } d \Rightarrow x' = f\ x\ y) \wedge (d \text{ invariant})$$

$$\Rightarrow \quad \forall \sigma_0 \cdot d \wedge f\ \sigma = f\ \sigma_0 \text{ is a loop invariant}$$

$$\wedge\ \forall \sigma, \sigma' \cdot d\ \sigma' \wedge f\ \sigma' = f\ \sigma \Leftarrow d \wedge g \wedge B$$

$$\wedge\ \forall \sigma, \sigma' \cdot (d \Rightarrow x' = f\ \sigma) \Leftarrow g \wedge (B\ .\ d \Rightarrow x' = f\ \sigma)$$

$$\textbf{while } g \textbf{ do } B \textbf{ od} \text{ implements } d \Rightarrow x' = f\ x\ y$$

$$\Rightarrow \quad \forall \sigma_0 \cdot d \Rightarrow f\ \sigma = f\ \sigma_0 \text{ is a loop assertion}$$

Also have proof in weakest preconditions, with $\{d\}\ .\ [x' = f\ x\ y]$