Bilateral Proofs of Concurrent Programs

Jayadev Misra

Department of Computer Science
University of Texas at Austin

WG 2.3, Jan 2016
Pasadena

Agonizing Reappraisal

- Is it realistic to prove concurrent programs in practice?
- Need to prove only tightly-coupled programs?

  Can they be handled through model-checking?
- Could loose-coupled concurrency become the norm, say through mobile computing?

Agonizing Reappraisal

- Is it realistic to prove concurrent programs in practice?
- Need to prove only tightly-coupled programs?

  Can they be handled through model-checking?
- Could loose-coupled concurrency become the norm, say through mobile computing?

Agonizing Reappraisal

- Is it realistic to prove concurrent programs in practice?
- Need to prove only tightly-coupled programs?

  Can they be handled through model-checking?
- Could loose-coupled concurrency become the norm, say through mobile computing?

Status of Program Design and Verification in Four Decades

- Astounding gains for sequential programming.
- Vast improvement in understanding of concurrent programming.
- Theory and practice lag considerably for the latter, compared to the former.
- Very small concurrent programs proved manually, occasionally.
- Larger concurrent programs proved using model checking. Only bright spot.

Status of Program Design and Verification in Four Decades

- Astounding gains for sequential programming.
- Vast improvement in understanding of concurrent programming.
- Theory and practice lag considerably for the latter, compared to the former.
- Very small concurrent programs proved manually, occasionally.
- Larger concurrent programs proved using model checking. Only bright spot.

Why sequential Programs are more amenable

- Hoare's Proof Theory: Program specification by pre- and postcondition.
- Permits verification of sequential program code for a given specification.
- Proof rules: permit composition of the component specifications, for hierarchical construction.
- Specification used in program construction, instead of source code.
- Concurrent programming lacks a theory of *composable specification*. Pre- and postcondition do not compose for concurrent programs.
- Needed: a scalable theory of composable specification of concurrent programs.

Why sequential Programs are more amenable

- Hoare's Proof Theory: Program specification by pre- and postcondition.
- Permits verification of sequential program code for a given specification.
- Proof rules: permit composition of the component specifications, for hierarchical construction.
- Specification used in program construction, instead of source code.
- Concurrent programming lacks a theory of *composable specification*. Pre- and postcondition do not compose for concurrent programs.
- Needed: a scalable theory of composable specification of concurrent programs.

Motivation for the current work: Commutative, Associative Fold of a bag

- Bag u.

  Commutative, associative binary operator $\oplus$

  Write fold of u as Σu.

- Problem: Replace all elements of u by Σu.

- Strategy: Define f_k that transforms u
  - reduces the size of u by k, and
  - the resulting bag has the same fold as the original bag.

An Orc Program

$$f_1 \quad = \quad get(x);\ get(y);\ put(x \oplus y)$$

$$f_k \quad = \quad f_1 \,[]\, f_{k-1}, \qquad k > 1$$

Given that u has n items initially, $n > 1$, apply f_{n-1}.

- Safety: Finally u has one item, the fold of the original items. Easy.
- Progress: Program terminates. Hard.

  The result does not hold for f_n. There is deadlock.
- No known proof technique for this program.

Observations about the problem

- Desired: Respect the recursive program structure in proof.
- Note interplay between sequential and concurrent aspects.
- Entire code is not available.

Another very difficult program to prove

$$\{x = 0\}$$

$$x := x + 1 \;[]\; x := x + 2$$

$$\{x = 3\}$$

Owicki's Thesis

- Construct annotation of each sequential component.

$$\{x = 0\}$$

$$(\ \{x = 0 \vee x = 2\}\ x := x + 1\ \{x = 1 \vee x = 3\}$$

$$[]\ \ \{x = 0 \vee x = 1\}\ x := x + 2\ \{x = 2 \vee x = 3\})$$

$$\{(x = 1 \vee x = 3) \wedge (x = 2 \vee x = 3)\}$$

$$\{x = 3\}$$

- Show: proofs don't interfere, e.g.,
  given assertions valid in concurrent execution

$$\{(x = 0 \vee x = 2) \wedge (x = 0 \vee x = 1)\}\ \ x := x + 2\ \ \{x = 0 \vee x = 2\}$$
$$\{(x = 0 \vee x = 1) \wedge (x = 0 \vee x = 2)\}\ \ x := x + 1\ \ \{x = 0 \vee x = 1\}$$
$$\ldots$$

Owicki's Thesis

- Construct annotation of each sequential component.

$$\{x = 0\}$$

$$(\ \{x = 0 \lor x = 2\}\ x := x + 1\ \{x = 1 \lor x = 3\}$$

$$[]\ \ \{x = 0 \lor x = 1\}\ x := x + 2\ \{x = 2 \lor x = 3\})$$

$$\{(x = 1 \lor x = 3) \land (x = 2 \lor x = 3)\}$$

$$\{x = 3\}$$

- Show: proofs don't interfere, e.g.,
  given assertions valid in concurrent execution

$$\{(x = 0 \lor x = 2) \land (x = 0 \lor x = 1)\}\ \ x := x + 2\ \ \{x = 0 \lor x = 2\}$$
$$\{(x = 0 \lor x = 1) \land (x = 0 \lor x = 2)\}\ \ x := x + 1\ \ \{x = 0 \lor x = 1\}$$
$$\ldots$$

Assessment

- First real proof technique for concurrent programs.
- Works well for small tightly-coupled components.
- Not scalable.
- Needs program code.
- No notion of a specification.

Rely-Guarantee of Cliff Jones

- Replace non-interference proofs by checks against stable predicates.
- Hoare-like proof rule.
- Limited to safety properties.

Unity by Chandy and Misra

- Simplify program structure: $\mathit{loop}\ \langle g \rightarrow s\rangle\ []\ \mathit{loop}\ \langle g' \rightarrow s'\rangle\ []\ \cdots$

- Each $\langle g \rightarrow s\rangle$ is a guarded action.

- Prove program properties, not assertions at program points:
  - A resource is never granted unless requested.
  - A request for a resource is eventually granted.

- Specification is a set of properties.

- Composition rules for specification are given.

The guard holds as a precondition in concurrent execution.

Limitations of the Unity approach

- Does not support traditional program structure.
- Auxiliary variables needed to capture program control points.

Current Theory: Specification

- Terminal property: postcondition of a program for a given precondition.
- Perpetual property: holds throughout every program execution.

  Similar to invariant.

  - (Safety) once it requests a resource the thread waits until the resource is granted,
  - (Progress) once the resource is granted the thread will eventually release it.
- Specification: Terminal and Perpetual properties.

Summary of the approach

- Create program annotation as before, but with restrictions.
- Annotations are valid even under concurrent execution.
  As in UNITY.
- Bilateral: Derive terminal and perpetual properties from annotations.

  And conversely.
- Composition rules for specifications.

Program Model

- command: Uninterruptible, terminating code,
  e.g.: $x := x - 1$, *put* on a channel.

- action: Guarded command, $b \rightarrow \alpha$,
  e.g.: $x > 0 \rightarrow x := x - 1$, or
  get from a channel, where the guard is implicit.

- f, g :: component: action $\mid$ $f \,[]\, g$ $\mid$ seq $(f_0, f_1, \cdots f_n)$

- program: component executing alone.

Programming Constructs

- seq: Any sequential programming construct that has a proof rule, e.g.:

  $s; t$

  if b **then** s **else** t

  while b **do** s

- Join: $f \; [] \; g$ is commutative, associative.

- Arbitrary hierarchy of sequential and concurrent constructs:

  $(f \; [] \; g); (f' \; [] \; g')$

Program Execution

- Sequential components follow their execution rules.
- Join: starts all components simultaneously.

  Terminates when they all do.
- Program control may reside at multiple program points simultaneously.
- At any moment the action at some control point is executed.
- Every control point is chosen eventually for execution.

Action Execution

- Execution of $b \rightarrow \alpha$ always terminates,

  either effectively or ineffectively.

- Effective execution:
  b is true and α is executed to completion.
  Program control moves past the action.

- Ineffective execution:
  b is *false*.
  Program control remains before the action.

- Evaluation of b is uninterruptible in all cases.

- If b is true: α is executed immediately.

Example: Distributed counter

Program $f = []_j \, f_j$ implements counter ctr.

initially $ctr = 0$

f_j ::

initially $old_j, \; new_j = 0, \; 0$

loop

$new_j := old_j + 1;$

if $[\; ctr = old_j \rightarrow ctr := new_j$

$\mid ctr \neq old_j \rightarrow old_j := ctr \;]$

forever

Show:

Safety: ctr is changed only by incrementation (increased by 1).

Progress: ctr is changed eventually.

Example: Distributed counter

Program $f = [\,]_j\, f_j$ implements counter ctr.

initially $ctr = 0$

f_j ::

  initially $old_j,\ new_j = 0,\ 0$

  loop

    $new_j := old_j + 1;$

    if $[\ ctr = old_j \rightarrow ctr := new_j$

      $|\ ctr \neq old_j \rightarrow old_j := ctr\ ]$

  forever

Show:

Safety: ctr is changed only by incrementation (increased by 1).

Progress: ctr is changed eventually.

Inviolable preconditions of actions

- Find precondition p of each action so that p remains true as long as control remains at the action.

$$\begin{array}{c} (\ \{x = 0 \vee x = 2\}\ x := x + 1\ \{x = 1 \vee x = 3\} \\ [\,]\ \ \{x = 0 \vee x = 1\}\ x := x + 2\ \{x = 2 \vee x = 3\}) \\ \{(x = 1 \vee x = 3) \wedge (x = 2 \vee x = 3)\} \end{array}$$

- Owicki: Check that precondition can not be violated by any concurrent action.
- Unity: Programmer specifies guards for each action.
- In the current theory:
  Unknown concurrent environment.
  General programs: Guards are usually too weak.
  Control flow carries additional information.

Inviolable preconditions of actions

- Find precondition p of each action so that p remains true as long as control remains at the action.

$$
\begin{array}{c}
(\ \{x = 0 \lor x = 2\}\ x := x + 1\ \{x = 1 \lor x = 3\} \\
[]\ \ \{x = 0 \lor x = 1\}\ x := x + 2\ \{x = 2 \lor x = 3\}) \\
\{(x = 1 \lor x = 3) \land (x = 2 \lor x = 3)\}
\end{array}
$$

- Owicki: Check that precondition can not be violated by any concurrent action.

- Unity: Programmer specifies guards for each action.

- In the current theory:
  Unknown concurrent environment.
  General programs: Guards are usually too weak.
  Control flow carries additional information.

Inviolable preconditions of actions

- Find precondition p of each action so that p remains true as long as control remains at the action.

$$
\begin{array}{c}
(\ \{x = 0 \vee x = 2\}\ x := x + 1\ \{x = 1 \vee x = 3\} \\
[]\ \{x = 0 \vee x = 1\}\ x := x + 2\ \{x = 2 \vee x = 3\}) \\
\{(x = 1 \vee x = 3) \wedge (x = 2 \vee x = 3)\}
\end{array}
$$

- Owicki: Check that precondition can not be violated by any concurrent action.

- Unity: Programmer specifies guards for each action.

- In the current theory:
  Unknown concurrent environment.
  General programs: Guards are usually too weak.
  Control flow carries additional information.

Inviolable preconditions of actions

- Find precondition p of each action so that p remains true as long as control remains at the action.

$$
\begin{array}{c}
(\ \{x = 0 \lor x = 2\}\ x := x + 1\ \{x = 1 \lor x = 3\} \\
[]\ \ \{x = 0 \lor x = 1\}\ x := x + 2\ \{x = 2 \lor x = 3\}) \\
\{(x = 1 \lor x = 3) \land (x = 2 \lor x = 3)\}
\end{array}
$$

- Owicki: Check that precondition can not be violated by any concurrent action.

- Unity: Programmer specifies guards for each action.

- In the current theory:
  Unknown concurrent environment.
  General programs: Guards are usually too weak.
  Control flow carries additional information.

Access rights to variables

- x local to f: f has exclusive write-access to x during any execution.
- p local predicate of f: every variable in p is local to f.

Local Annotation

- Annotation of a program in which all predicates are local to the component in which they appear.

- Assert: Given local annotation in which $\{p\}\ b \rightarrow \alpha$, p holds whenever $b \rightarrow \alpha$ is executed.

- Construct local annotation using Hoare-proof rules for seq construct.

- For join, use:

$$\frac{\begin{array}{c}\{r\}\ f\ \{s\} \\ \{r'\}\ g\ \{s'\}\end{array}}{\{r \wedge r'\}\ f\ [\,]\ g\ \{s \wedge s'\}}$$

Local Annotation: Distributed Counter

$$
\begin{array}{l}
f_j :: \\
\quad \textbf{initially} \;\; old_j,\ new_j = 0,\ 0 \\
\quad \{true\} \\
\quad \textbf{loop} \\
\qquad \{true\} \\
\qquad\quad \alpha_j ::\ new_j := old_j + 1; \\
\qquad \{new_j = old_j + 1\} \\
\qquad\quad \textbf{if}\ [\ \ \beta_j ::\ \{new_j = old_j + 1\}\ ctr = old_j \ \rightarrow\ ctr := new_j \ \ \{true\} \\
\qquad\qquad\quad \mid \gamma_j ::\ \{new_j = old_j + 1\}\ ctr \neq old_j \ \rightarrow\ old_j := ctr \ \ \{true\}] \\
\qquad \{true\} \\
\quad \textbf{forever}
\end{array}
$$

Safety Property co

- p co q in component f:

  Effective execution of any action of f in a p-state achieves a q-state.

- In program f: once p holds it continues to hold until q is established.

- As a composition rule:

  p co q holds in f if it holds in every component of f.

Formal definition of co

$$\frac{\begin{array}{c}\{r\}\ f\ \{s\}\\ \text{For every action } b \rightarrow \alpha \text{ with precondition } pre \text{ in the annotation of } f:\\ \{pre \wedge b \wedge p\}\ \alpha\ \{q\}\end{array}}{\{r\}\ f\ \{p\ \mathbf{co}\ q \mid s\}}$$

Special cases of co

- stable p: Once p holds, it continues to hold:

  p co p

- constant e: Value of expression e never changes:

  $(\forall c :: \text{ stable } e = c)$

- invariant p: p always holds:

  initially p and stable p

Distributed Counter, contd.

f_j ::
initially $old_j,\ new_j = 0,\ 0$
$\{true\}$
loop
$\{true\}$
$\alpha_j ::\ new_j := old_j + 1;$
$\{new_j = old_j + 1\}$
if $[\ \beta_j ::\ \{new_j = old_j + 1\}\ ctr = old_j\ \rightarrow\ ctr := new_j\ \ \{true\}$
$\ \ \ |\ \gamma_j ::\ \{new_j = old_j + 1\}\ ctr \neq old_j\ \rightarrow\ old_j := ctr\ \ \{true\}]$
$\{true\}$
forever

Safety: *ctr*'s value is only incremented

- Show: $ctr = m$ co $ctr = m \lor ctr = m + 1$ in f
  prove: $ctr = m$ co $ctr = m \lor ctr = m + 1$ holds in all f_j.

- For each action $b \to \alpha$ with precondition pre, show:

  $$\{pre \land b \land ctr = m\}\ \alpha\ \{ctr = m \lor ctr = m + 1\}$$

- Only β_j may change the value of ctr. So, prove:

  $$\{ctr = m \land new_j = old_j + 1 \land ctr = old_j\}$$
  $$ctr := new_j$$
  $$\{ctr = m \lor ctr = m + 1\}$$

Progress Properties

- Transient: Fundamental property. Compositional.

  transient p: p is false eventually. $\Box\Diamond\neg p$.

- Ensures: p en q
  Once p holds, it continues to hold until q holds; and q holds eventually.

  More useful in practice.
  Defined using transient.

- Leads-to: $p \mapsto q$
  once p holds, q holds eventually.

  Typical property in a specification.
  Defined using ensures.

Progress Properties

- Transient: Fundamental property. Compositional.

  transient p: p is false eventually. $\Box\Diamond\neg p$.

- Ensures: p en q
  Once p holds, it continues to hold until q holds; and q holds eventually.

  More useful in practice.
  Defined using transient.

- Leads-to: $p \mapsto q$
  once p holds, q holds eventually.

  Typical property in a specification.
  Defined using ensures.

Progress Properties

- Transient: Fundamental property. Compositional.

  transient p: p is false eventually. $\Box\Diamond\neg p$.

- Ensures: p en q
  Once p holds, it continues to hold until q holds; and q holds eventually.

  More useful in practice.
  Defined using transient.

- Leads-to: $p \mapsto q$
  once p holds, q holds eventually.

  Typical property in a specification.
  Defined using ensures.

Simplistic Definition of transient p in f: p is false eventually in f

- Each action of f is effectively executed if p is a precondition, and
- its execution establishes $\neg p$.

For every action $b \rightarrow \alpha$ of f with precondition pre :

$$\frac{\begin{array}{c} pre \wedge p \Rightarrow b \\ \{pre \wedge p\}\ \alpha\ \{\neg p\} \end{array}}{\{\}\ f\ \{\text{ transient } p \mid \}}$$

Stronger Rules for transient p

- $f ; g$: either f terminates or p transient in f AND p transient in g.

  Sufficient: f terminates AND p transient in g.

- $f [] g$: p transient in f or g.

- Inheritance: If p transient in ALL components of f, p transient in f.

Stronger Rules for transient p

- $f; g$: either f terminates or p transient in f AND p transient in g.

  Sufficient: f terminates AND p transient in g.

- $f \, [] \, g$: p transient in f or g.

- Inheritance: If p transient in ALL components of f, p transient in f.

Stronger Rules for transient p

- $f; g$: either f terminates or p transient in f AND p transient in g.

  Sufficient: f terminates AND p transient in g.

- $f \, [] \, g$: p transient in f or g.

- Inheritance: If p transient in ALL components of f, p transient in f.

Ensures: p en q

Once p holds, it continues to hold until q holds; and q holds eventually.

- $p \wedge \neg q$ co $p \vee q$
- transient $p \wedge \neg q$

Distributed Counter

- Prove: ctr increases eventually.
- Can not be proved as an ensures property.
- Prove:

  In every step, either ctr increases, or
  the number of old_j that differ from ctr decreases.

- nb: number of old_j such that $ctr \neq old_j$.

  $ctr = m \wedge nb = N$ en $nb < N \vee ctr > m$ in f (E)

Proof strategy

$ctr = m \wedge nb = N$ **en** $nb < N \vee ctr > m$ in f (E)

- To prove (E) in $[]_j\, f_j$: Prove (E) in each f_j.

- To prove (E) in *initialization*; **loop** $body_j$ **forever**:
  Since *initialization* terminates, show (E) in: **loop** $body_j$ **forever**.

- To prove (E) in **loop** $body_j$ **forever**:
  using inheritance prove (E) in $body_j$, .

- To prove (E) in $body_j$, i.e., $new_j := old_j + 1$; **if** $[\beta_j \mid \gamma_j]$:
  Since $new_j := old_j + 1$ terminates, prove (E) in **if** $[\beta_j \mid \gamma_j]$,

- To prove (E) in **if** $[\beta_j \mid \gamma_j]$: prove (E) in β_j and γ_j, i.e.,
  Effective executions of β_j and γ_j establish the postcondition of (E) given its pre-condition.

Proof strategy

$$ctr = m \wedge nb = N \ \ \text{en} \ \ nb < N \vee ctr > m \text{ in } f \qquad \text{(E)}$$

- To prove (E) in $[]_j\, f_j$: Prove (E) in each f_j.

- To prove (E) in $initialization$; **loop** $body_j$ **forever**:
  Since $initialization$ terminates, show (E) in: **loop** $body_j$ **forever**.

- To prove (E) in **loop** $body_j$ **forever**:
  using inheritance prove (E) in $body_j$, .

- To prove (E) in $body_j$, i.e., $new_j := old_j + 1$; **if** $[\beta_j \mid \gamma_j]$:
  Since $new_j := old_j + 1$ terminates, prove (E) in **if** $[\beta_j \mid \gamma_j]$,

- To prove (E) in **if** $[\beta_j \mid \gamma_j]$: prove (E) in β_j and γ_j, i.e.,
  Effective executions of β_j and γ_j establish the postcondition of (E) given its pre-condition.

Proof strategy

$ctr = m \wedge nb = N$ en $nb < N \vee ctr > m$ in f (E)

- To prove (E) in $[]_j f_j$: Prove (E) in each f_j.
- To prove (E) in *initialization*; **loop** $body_j$ **forever**:
  Since *initialization* terminates, show (E) in: **loop** $body_j$ **forever**.
- To prove (E) in **loop** $body_j$ **forever**:
  using inheritance prove (E) in $body_j$, .
- To prove (E) in $body_j$, i.e., $new_j := old_j + 1$; **if** $[\beta_j \mid \gamma_j]$:
  Since $new_j := old_j + 1$ terminates, prove (E) in **if** $[\beta_j \mid \gamma_j]$,
- To prove (E) in **if** $[\beta_j \mid \gamma_j]$: prove (E) in β_j and γ_j, i.e.,
  Effective executions of β_j and γ_j establish the postcondition of (E) given its pre-condition.

Proof strategy

$ctr = m \wedge nb = N$ en $nb < N \vee ctr > m$ in f (E)

- To prove (E) in $[]_j f_j$: Prove (E) in each f_j.

- To prove (E) in *initialization*; **loop** $body_j$ **forever**:
  Since *initialization* terminates, show (E) in: **loop** $body_j$ **forever**.

- To prove (E) in **loop** $body_j$ **forever**:
  using inheritance prove (E) in $body_j$, .

- To prove (E) in $body_j$, i.e., $new_j := old_j + 1$; **if** $[\beta_j \mid \gamma_j]$:
  Since $new_j := old_j + 1$ terminates, prove (E) in **if** $[\beta_j \mid \gamma_j]$,

- To prove (E) in **if** $[\beta_j \mid \gamma_j]$: prove (E) in β_j and γ_j, i.e.,
  Effective executions of β_j and γ_j establish the postcondition of (E) given its pre-condition.

Proof strategy

$$ctr = m \wedge nb = N \;\; \textbf{en} \;\; nb < N \vee ctr > m \text{ in } f \qquad \text{(E)}$$

- To prove (E) in $[]_j f_j$: Prove (E) in each f_j.
- To prove (E) in $initialization$; **loop** $body_j$ **forever**:
  Since $initialization$ terminates, show (E) in: **loop** $body_j$ **forever**.
- To prove (E) in **loop** $body_j$ **forever**:
  using inheritance prove (E) in $body_j$, .
- To prove (E) in $body_j$, i.e., $new_j := old_j + 1$; **if** $[\beta_j \mid \gamma_j]$:
  Since $new_j := old_j + 1$ terminates, prove (E) in **if** $[\beta_j \mid \gamma_j]$,
- To prove (E) in **if** $[\beta_j \mid \gamma_j]$: prove (E) in β_j and γ_j, i.e.,
  Effective executions of β_j and γ_j establish the postcondition of (E) given its pre-condition.

Proof Obligations

Relevant Annotation of f_j:

$$
\begin{array}{l}
\quad\textbf{if}\ \ [\ \beta_j ::\ \{new_j = old_j + 1\}\ ctr = old_j\ \rightarrow\ ctr := new_j\ \ \{true\} \\
\qquad\ \ \mid \gamma_j ::\ \{new_j = old_j + 1\}\ ctr \neq old_j\ \rightarrow\ old_j := ctr\ \ \ \{true\}] \\
\{true\}
\end{array}
$$

Proof Obligations:

$$
\begin{array}{l}
\beta_j ::\ \{ctr = m \wedge nb = N \wedge new_j = old_j + 1 \wedge ctr = old_j\} \\
\qquad\qquad ctr := new_j \\
\qquad \{nb < N \vee ctr > m\}
\end{array}
$$

$$
\begin{array}{l}
\gamma_j ::\ \{ctr = m \wedge nb = N \wedge new_j = old_j + 1 \wedge ctr \neq old_j\} \\
\qquad\qquad old_j := ctr \\
\qquad \{nb < N \vee ctr > m\}
\end{array}
$$

Leads-to

$p \mapsto q$: once p holds, q holds eventually.

- (basis) $\dfrac{p \ \text{en} \ q}{p \mapsto q}$
- (transitivity) $\dfrac{p \mapsto q \ , \ q \mapsto r}{p \mapsto r}$
- (disjunction) For any (finite or infinite) set of predicates S

$$\frac{(\forall p :\ p \in S :\ p \mapsto q)}{(\vee p :\ p \in S :\ p) \mapsto q}$$

Derived Rules: What makes Proofs Practical. For co

$$\mathit{false} \;\; \mathrm{co} \;\; q$$

$$p \;\; \mathrm{co} \;\; \mathit{true}$$

$$\frac{p \;\; \mathrm{co} \;\; q \,,\; p' \;\; \mathrm{co} \;\; q'}{p \wedge p' \;\; \mathrm{co} \;\; q \wedge q'} \qquad \text{(CONJUNCTION)}$$

$$\frac{p \;\; \mathrm{co} \;\; q \,,\; p' \;\; \mathrm{co} \;\; q'}{p \vee p' \;\; \mathrm{co} \;\; q \vee q'} \qquad \text{(DISJUNCTION)}$$

$$\frac{p \;\; \mathrm{co} \;\; q}{p \wedge p' \;\; \mathrm{co} \;\; q} \qquad \text{(LHS STRENGTHENING)}$$

$$\frac{p \;\; \mathrm{co} \;\; q}{p \;\; \mathrm{co} \;\; q \vee q'} \qquad \text{(RHS WEAKENING)}$$

Lightweight Derived Rules for $\mapsto$

1. (implication) $\dfrac{p \Rightarrow q}{p \mapsto q}$

2. (lhs strengthening, rhs weakening)

$$\frac{p \mapsto q}{\begin{array}{c} p' \wedge p \mapsto q \\ p \mapsto q \vee q' \end{array}}$$

3. (cancellation) $\dfrac{p \mapsto q \vee r \,,\; r \mapsto s}{p \mapsto q \vee s}$

Heavyweight Derived Rules for $\mapsto$

1. (PSP) $$\frac{\begin{array}{c} p \mapsto q \\ \text{stable } p' \end{array}}{p \wedge p' \mapsto q \wedge p'}$$

2. (induction) M : Program States $\to W$. $(W, \prec)$ well-founded.

$$\frac{(\forall m :: \ p \ \wedge \ M = m \ \mapsto \ (p \ \wedge \ M \prec m) \ \vee \ q)}{p \ \mapsto \ q}$$

3. (completion) p_i and q_i are predicates; i index over a finite set.

$$\frac{\begin{array}{l} (\forall i :: \\ \quad p_i \ \mapsto \ q_i \vee b \\ \quad q_i \ \text{co} \ q_i \vee b \\ ) \end{array}}{(\forall i :: \ p_i) \ \mapsto \ (\forall i :: \ q_i) \ \vee \ b}$$

Heavyweight Derived Rules for $\mapsto$

1. (PSP) $$\frac{\begin{array}{c} p \mapsto q \\ \text{stable } p' \end{array}}{p \wedge p' \mapsto q \wedge p'}$$

2. (induction) M : Program States $\to W$. $(W, \prec)$ well-founded.

$$\frac{(\forall m :: \ p \wedge M = m \mapsto (p \wedge M \prec m) \vee q)}{p \mapsto q}$$

3. (completion) p_i and q_i are predicates; i index over a finite set.

$$\frac{\begin{array}{l} (\forall i :: \\ \quad p_i \mapsto q_i \vee b \\ \quad q_i \text{ co } q_i \vee b \\ ) \end{array}}{(\forall i :: \ p_i) \mapsto (\forall i :: \ q_i) \vee b}$$

Heavyweight Derived Rules for $\mapsto$

1. (PSP)
$$\frac{\begin{array}{c} p \mapsto q \\ \text{stable } p' \end{array}}{p \wedge p' \mapsto q \wedge p'}$$

2. (induction) M : Program States $\rightarrow W$. $(W, \prec)$ well-founded.
$$\frac{(\forall m :: p \wedge M = m \mapsto (p \wedge M \prec m) \vee q)}{p \mapsto q}$$

3. (completion) p_i and q_i are predicates; i index over a finite set.
$$\frac{\begin{array}{l} (\forall i :: \\ \quad p_i \mapsto q_i \vee b \\ \quad q_i \text{ co } q_i \vee b \\ ) \end{array}}{(\forall i :: p_i) \mapsto (\forall i :: q_i) \vee b}$$

Heavyweight Derived Rules for $\mapsto$

1. (PSP) $$\frac{p \;\mapsto\; q \qquad \text{stable } p'}{p \wedge p' \;\mapsto\; q \wedge p'}$$

2. (induction) M : Program States $\to W$. $(W, \prec)$ well-founded.

$$\frac{(\forall m ::\; p \;\wedge\; M = m \;\mapsto\; (p \;\wedge\; M \prec m) \;\vee\; q)}{p \;\mapsto\; q}$$

3. (completion) p_i and q_i are predicates; i index over a finite set.

$$\frac{(\forall i ::\quad p_i \;\mapsto\; q_i \vee b \qquad q_i \;\text{co}\; q_i \vee b\quad)}{(\forall i ::\; p_i) \;\mapsto\; (\forall i ::\; q_i) \;\vee\; b}$$

Distributed Counter

- Prove in f: ctr increases unboundedly:

  $true \mapsto ctr > C$, for any integer C

- Proved in f: $ctr = m \wedge nb = N \;\; \text{en} \;\; nb < N \vee ctr > m$

- Use definition of $\mapsto$ and its derived rules for the proof.

Distributed Counter, Contd.

$ctr = m \wedge nb = N$ en $nb < N \vee ctr > m$

proven

$ctr = m \wedge nb = N \mapsto nb < N \vee ctr > m$

basis rule of *leads-to*

$ctr = m \wedge nb = N \mapsto ctr = m \wedge nb < N \vee ctr > m$

PSP with $ctr = m$ co $ctr = m \vee ctr = m + 1$

Distributed Counter, Contd.

$ctr = m \wedge nb = N$ en $nb < N \vee ctr > m$

proven

$ctr = m \wedge nb = N \mapsto nb < N \vee ctr > m$

basis rule of *leads-to*

$ctr = m \wedge nb = N \mapsto ctr = m \wedge nb < N \vee ctr > m$

PSP with $ctr = m$ co $ctr = m \vee ctr = m + 1$

Distributed Counter, Contd.

$ctr = m \wedge nb = N \;\; \text{en} \;\; nb < N \vee ctr > m$

proven

$ctr = m \wedge nb = N \;\mapsto\; nb < N \vee ctr > m$

basis rule of *leads-to*

$ctr = m \wedge nb = N \;\mapsto\; ctr = m \wedge nb < N \;\vee\; ctr > m$

PSP with $ctr = m \;\; \text{co} \;\; ctr = m \vee ctr = m + 1$

Apply Induction Rule

$ctr = m \wedge nb = N \;\mapsto\; ctr = m \wedge nb < N \;\vee\; ctr > m$

Induction rule:

$$\frac{(\forall m ::\; p \;\wedge\; M = m \;\mapsto\; (p \;\wedge\; M \prec m) \;\vee\; q)}{p \;\mapsto\; q}$$

Use nb for M and $<$ for $\prec$ to conclude:

$ctr = m \;\mapsto\; ctr > m$

Distributed Counter, Contd.

$ctr = m \wedge nb = N$ en $nb < N \vee ctr > m$
proven

$ctr = m \wedge nb = N \mapsto nb < N \vee ctr > m$
basis rule of *leads-to*

$ctr = m \wedge nb = N$ en $ctr = m \wedge nb < N \vee ctr > m$
PSP with $ctr = m$ co $ctr = m \vee ctr = m + 1$

$ctr = m \mapsto ctr > m$
Induction rule; well-founded order $<$ over natural numbers

$true \mapsto ctr > C$, for any integer C
Induction rule, well-founded order $<$ over natural numbers.

Distributed Counter, Contd.

$ctr = m \wedge nb = N$ en $nb < N \vee ctr > m$

proven

$ctr = m \wedge nb = N \mapsto nb < N \vee ctr > m$

basis rule of *leads-to*

$ctr = m \wedge nb = N$ en $ctr = m \wedge nb < N \vee ctr > m$

PSP with $ctr = m$ co $ctr = m \vee ctr = m + 1$

$ctr = m \mapsto ctr > m$

Induction rule; well-founded order $<$ over natural numbers

$true \mapsto ctr > C$, for any integer C

Induction rule, well-founded order $<$ over natural numbers.