Shared Variable Proof Methods, Hardware-Assisted Critical Sections

Johannes Åman Pohjola
CSIRO’s Data61 (and UNSW)
Term 2 2021
In the last lecture we introduced the critical section problem, the four properties of critical section solutions, and some solutions for two processes.
In the last lecture we introduced the critical section problem, the four properties of critical section solutions, and some solutions for two processes.

We also introduced the SPIN model checking tool for rigorous analysis of candidate solutions.
In the last lecture we introduced the **critical section** problem, the four properties of critical section solutions, and some solutions for two processes.

We also introduced the **SPIN** model checking tool for rigorous analysis of candidate solutions.

In this lecture, we will introduce a **formal proof** method for verifying safety properties, and apply it to a new kind of critical section solution that relies on hardware support.
Transition Diagrams

Definition

A transition diagram is a tuple \((L, T, s, t)\) where:
- \(L\) is a set of locations (program counter values).
- \(s \in L\) is an entry location.
- \(t \in L\) is an exit location.
- \(T\) is a set of transitions.

A transition is written as \(\ell_i \xrightarrow{g} \ell_j \) where:
- \(\ell_i\) and \(\ell_j\) are locations.
- \(g\) is a guard \(\Sigma \rightarrow B\).
- \(f\) is a state update \(\Sigma \rightarrow \Sigma\).

\[
\begin{align*}
&\ell_0 \\
&\ell_1 \top; i \leftarrow 0 \\
&s \leftarrow 0 \\
&i \leftarrow i + 1 \\
&\text{while } i \neq N \text{ do} \\
&s \leftarrow s + i \\
&i \leftarrow i + 1 \\
&\od \\
&\ell_2
\end{align*}
\]
A **transition diagram** is a tuple \((L, T, s, t)\) where:
- \(L\) is a set of *locations* (program counter values).
- \(s \in L\) is a *entry location*.
- \(t \in L\) is a *exit location*.
- \(T\) is a set of *transitions*. 
Transition Diagrams

Definition

A *transition diagram* is a tuple \((L, T, s, t)\) where:

- \(L\) is a set of *locations* (program counter values).
- \(s \in L\) is a *entry location*.
- \(t \in L\) is a *exit location*.
- \(T\) is a set of *transitions*.

A *transition* is written as \(\ell_i \xrightarrow{g;f} \ell_j\) where:

- \(\ell_i\) and \(\ell_j\) are locations.
- \(g\) is a *guard* \(\Sigma \rightarrow \mathbb{B}\)
- \(f\) is a *state update* \(\Sigma \rightarrow \Sigma\).
Transition Diagrams

Definition

A **transition diagram** is a tuple \((L, T, s, t)\) where:

- \(L\) is a set of *locations* (program counter values).
- \(s \in L\) is a *entry location*.
- \(t \in L\) is a *exit location*.
- \(T\) is a set of *transitions*.

A **transition** is written as \(\ell_i \xrightarrow{g;f} \ell_j\) where:

- \(\ell_i\) and \(\ell_j\) are locations.
- \(g\) is a *guard* \(\Sigma \rightarrow \mathbb{B}\).
- \(f\) is a *state update* \(\Sigma \rightarrow \Sigma\).

```plaintext
i ← 0;
s ← 0;
while \(i \neq N\) do
    s ← s + i;
i ← i + 1
od
```
Transition Diagrams

Definition

A *transition diagram* is a tuple \((L, T, s, t)\) where:

- \(L\) is a set of *locations* (program counter values).
- \(s \in L\) is a *entry location*.
- \(t \in L\) is a *exit location*.
- \(T\) is a set of *transitions*.

A *transition* is written as \(\ell_i \xrightarrow{g;f} \ell_j\) where:

- \(\ell_i\) and \(\ell_j\) are locations.
- \(g\) is a *guard* \(\Sigma \rightarrow \mathbb{B}\).
- \(f\) is a *state update* \(\Sigma \rightarrow \Sigma\).

\[
i \leftarrow 0;
s \leftarrow 0;
\textbf{while } i \neq N \textbf{ do }
  \begin{align*}
s &\leftarrow s + i; \\
i &\leftarrow i + 1
\end{align*}
\textbf{od}
\]
Transition Diagrams

Definition

A *transition diagram* is a tuple \((L, T, s, t)\) where:
- \(L\) is a set of *locations* (program counter values).
- \(s \in L\) is a *entry location*.
- \(t \in L\) is a *exit location*.
- \(T\) is a set of *transitions*.

A *transition* is written as \(\ell_i \xrightarrow{g;f} \ell_j\) where:
- \(\ell_i\) and \(\ell_j\) are locations.
- \(g\) is a *guard* \(\Sigma \rightarrow \mathbb{B}\).
- \(f\) is a *state update* \(\Sigma \rightarrow \Sigma\).

Invariants and Machine Instructions

\[
i \leftarrow 0;
\]
\[
s \leftarrow 0;
\]
\[
\textbf{while } i \neq N \textbf{ do}
\]
\[
s \leftarrow s + i;
\]
\[
i \leftarrow i + 1
\]
\[
\textbf{od}
\]
Transition Diagrams

**Definition**

A *transition diagram* is a tuple \((L, T, s, t)\) where:
- \(L\) is a set of *locations* (program counter values).
- \(s \in L\) is a *entry location*.
- \(t \in L\) is a *exit location*.
- \(T\) is a set of *transitions*.

A *transition* is written as \(\ell_i \xrightarrow{g;f} \ell_j\) where:
- \(\ell_i\) and \(\ell_j\) are locations.
- \(g\) is a *guard* \(\Sigma \rightarrow \mathbb{B}\).
- \(f\) is a *state update* \(\Sigma \rightarrow \Sigma\).

\[\begin{align*}
i &\leftarrow 0; \\
s &\leftarrow 0; \\
\textbf{while } i \neq N &\textbf{ do} \\
&\quad s \leftarrow s + i; \\
&\quad i \leftarrow i + 1 \\
\textbf{od}
\end{align*}\]
Transition Diagrams

Definition

A *transition diagram* is a tuple \((L, T, s, t)\) where:

- \(L\) is a set of *locations* (program counter values).
- \(s \in L\) is a *entry location*.
- \(t \in L\) is a *exit location*.
- \(T\) is a set of *transitions*.

A *transition* is written as \(\ell_i \xrightarrow{g;f} \ell_j\) where:

- \(\ell_i\) and \(\ell_j\) are locations.
- \(g\) is a *guard* \(\Sigma \rightarrow \mathbb{B}\).
- \(f\) is a *state update* \(\Sigma \rightarrow \Sigma\).

\[
\begin{align*}
& i \leftarrow 0; \\
& s \leftarrow 0; \\
& \textbf{while } i \neq N \textbf{ do} \\
& \quad s \leftarrow s + i; \\
& \quad i \leftarrow i + 1 \\
& \textbf{od}
\end{align*}
\]
Transition Diagrams

Definition

A transition diagram is a tuple \((L, T, s, t)\) where:
- \(L\) is a set of locations (program counter values).
- \(s \in L\) is an entry location.
- \(t \in L\) is an exit location.
- \(T\) is a set of transitions.

A transition is written as \(\ell_i \xrightarrow{g; f} \ell_j\) where:
- \(\ell_i\) and \(\ell_j\) are locations.
- \(g\) is a guard \(\Sigma \rightarrow \mathbb{B}\).
- \(f\) is a state update \(\Sigma \rightarrow \Sigma\).

```
i \leftarrow 0;
s \leftarrow 0;
while i \neq N do
    s \leftarrow s + i;
i \leftarrow i + 1
od
```
Floyd Verification

Recall the definition of a Hoare triple for *partial correctness*:

\[
\{ \varphi \} \; P \; \{ \psi \}
\]
Floyd Verification

Recall the definition of a Hoare triple for *partial correctness*:

\[
\{ \varphi \} \quad P \quad \{ \psi \}
\]

This states that if the program \( P \) successfully executes from a starting state satisfying \( \varphi \), the result state will satisfy \( \psi \).
Floyd Verification

Recall the definition of a Hoare triple for \textit{partial correctness}:

$$\{ \varphi \} \ P \ {\psi}$$

This states that if the program \( P \) successfully executes from a starting state satisfying \( \varphi \), the result state will satisfy \( \psi \). Observe that this is a \textit{safety property}.

Verifying Partial Correctness

Given a transition diagram \((L, T, s, t)\):
Floyd Verification

Recall the definition of a Hoare triple for *partial correctness*:

\[ \{ \varphi \} \; P \; \{ \psi \} \]

This states that if the program \( P \) successfully executes from a starting state satisfying \( \varphi \), the result state will satisfy \( \psi \). Observe that this is a *safety property*.

**Verifying Partial Correctness**

Given a transition diagram \((L, T, s, t)\):

1. Associate with each location \( l \in L \) an assertion \( Q(l) : \Sigma \rightarrow \mathbb{B} \).
Floyd Verification

Recall the definition of a Hoare triple for *partial correctness*:

\[ \{ \varphi \} \ P \ \{ \psi \} \]

This states that if the program \( P \) successfully executes from a starting state satisfying \( \varphi \), the result state will satisfy \( \psi \). Observe that this is a *safety property*.

Verifying Partial Correctness

Given a transition diagram \( (L, T, s, t) \):

1. Associate with each location \( \ell \in L \) an assertion \( Q(\ell) : \Sigma \rightarrow \mathbb{B} \).
2. Prove that this *assertion network* is *inductive*, that is: For each transition in \( T \)
   \[ \ell_i \xrightarrow{g;f} \ell_j \] show that:
   \[ Q(\ell_i) \land g \Rightarrow Q(\ell_j) \circ f \]
Floyd Verification

Recall the definition of a Hoare triple for *partial correctness*:

\[ \{ \varphi \} \text{ P } \{ \psi \} \]

This states that if the program \( P \) successfully executes from a starting state satisfying \( \varphi \), the result state will satisfy \( \psi \). Observe that this is a *safety property*.

**Verifying Partial Correctness**

Given a transition diagram \((L, T, s, t)\):

1. Associate with each location \( \ell \in L \) an assertion \( Q(\ell) : \Sigma \rightarrow \mathbb{B} \).
2. Prove that this assertion network is *inductive*, that is: For each transition in \( T \) \( \ell_i \xrightarrow{g;f} \ell_j \) show that:
   \[ Q(\ell_i) \land g \Rightarrow Q(\ell_j) \circ f \]
3. Show that \( \varphi \Rightarrow Q(s) \) and \( Q(t) \Rightarrow \psi \).
Floyd Verification

Recall the definition of a Hoare triple for \textit{partial correctness}:

\[
\{\varphi\} \; P \; \{\psi\}
\]

This states that if the program \( P \) successfully executes from a starting state satisfying \( \varphi \), the result state will satisfy \( \psi \). Observe that this is a \textit{safety property}.

Verifying Partial Correctness

Given a transition diagram \((L, T, s, t)\):

1. Associate with each location \( \ell \in L \) an assertion \( Q(\ell) : \Sigma \rightarrow \mathbb{B} \).

2. Prove that this assertion network is \textit{inductive}, that is: For each transition in \( T \)
   \( \ell_i \xrightarrow{g;f} \ell_j \) show that:

   \[
   Q(\ell_i) \land g \Rightarrow Q(\ell_j) \circ f
   \]

3. Show that \( \varphi \Rightarrow Q(s) \) and \( Q(t) \Rightarrow \psi \).

Johannes will now demonstrate on the previous example
Adding Concurrency

Transition Diagrams

Owicki-Gries Method

Invariants and Machine Instructions

Parallel Composition

Given two processes $P$ and $Q$ with transition diagrams $(L_P, T_P, s_P, t_P)$ and $(L_Q, T_Q, s_Q, t_Q)$, the parallel composition of $P$ and $Q$, written $P \parallel Q$ is defined as

$(L, T, s, t)$ where:

$L = L_P \times L_Q$

$s = s_P s_Q$

$t = t_P t_Q$

$p_i q_i g; f \rightarrow p_j q_i \in T$ if $p_i g; f \rightarrow p_j \in T_P$

$p_i q_i g; f \rightarrow p_i q_j \in T$ if $q_i g; f \rightarrow q_j \in T_Q$
Adding Concurrency

![Transition Diagrams](image)

**Owicki-Gries Method**

**Adding Concurrency**

**Transition Diagrams**

**Invariants and Machine Instructions**
Adding Concurrency

\[ p_0 \quad i = N \quad p_2 \]

\[ x, i \leftarrow n + 1, i + 1 \]

\[ q_0 \quad j = N \quad q_2 \]

\[ x, j \leftarrow m - 1, j + 1 \]

\[ p_0q_0 \quad i = N \quad p_2q_0 \]

\[ x, i \leftarrow n + 1, i + 1 \]

\[ j \leftarrow m - 1, j + 1 \]

\[ p_0q_1 \quad i = N \quad p_2q_1 \]

\[ x, i \leftarrow n + 1, i + 1 \]

\[ j \leftarrow m - 1, j + 1 \]

\[ p_0q_2 \quad i = N \quad p_2q_2 \]

\[ x, i \leftarrow n + 1, i + 1 \]

\[ j \leftarrow m - 1, j + 1 \]
Adding Concurrency

Parallel Composition

Given two processes $P$ and $Q$ with transition diagrams $(L_P, T_P, s_P, t_P)$ and $(L_Q, T_Q, s_Q, t_Q)$, the parallel composition of $P$ and $Q$, written $P \parallel Q$ is defined as $(L, T, s, t)$ where:

- $L = L_P \times L_Q$
- $s = s_Ps_Q$
- $t = t_Pt_Q$
- $p_i q_i \xrightarrow{g;f} p_j q_i \in T$ if $p_i \xrightarrow{g;f} p_j \in T_P$
- $p_i q_i \xrightarrow{g;f} p_i q_j \in T$ if $q_i \xrightarrow{g;f} q_j \in T_Q$
State Space Explosion

If we were SPIN, we would immediately begin exhaustively analysing this large diagram. But human brains don’t have that much storage space.
State Space Explosion

If we were SPIN, we would immediately begin exhaustively analysing this large diagram. But human brains don’t have that much storage space.

**Problem**

Then number of locations and transitions grows exponentially as the number of processes increases.
State Space Explosion

If we were SPIN, we would immediately begin exhaustively analysing this large diagram. But human brains don’t have that much storage space.

Problem

Then number of locations and transitions grows exponentially as the number of processes increases.

We can only use Floyd’s method directly on the parallel composition (product) diagram in the most basic examples.
State Space Explosion

If we were SPIN, we would immediately begin exhaustively analysing this large diagram. But human brains don’t have that much storage space.

Problem

Then number of locations and transitions grows exponentially as the number of processes increases.

We can only use Floyd’s method directly on the parallel composition (product) diagram in the most basic examples.

Our Solution

We will instead use a method that allows us to define only inductive assertion networks for P and Q individually, and, by proving some non-interference properties derive an inductive network for $P \parallel Q$ automatically.

This means we won’t have to draw that large product diagram!
Owicki-Gries Method

Steps
To show $\{\varphi\} P \parallel Q \{\psi\}$:

1. Define local assertion networks $P$ and $Q$ for both processes.
2. Show that they're inductive.
3. For each location $p \in L_P$, show that $P(p)$ is not falsified by any transition of $Q$.
   That is, for each $q \xrightarrow{g} q' \in T_Q$:
   \[ P(p) \land Q(q) \land g \Rightarrow P(p) \circ f \]
4. Vice versa for $Q$.
5. Show that $\varphi \Rightarrow P(s_P) \land Q(s_Q)$ and $P(t_P) \land Q(t_Q) \Rightarrow \psi$.
Owicki-Gries Method

Steps

To show \( \{ \varphi \} P \parallel Q \{ \psi \} \):

1. Define local assertion networks \( P \) and \( Q \) for both processes. Show that they’re inductive.
### Steps

To show $\{\varphi\} P \parallel Q \{\psi\}$:

1. Define local assertion networks $P$ and $Q$ for both processes. Show that they’re inductive.

2. For each location $p \in L_P$, show that $P(p)$ is not falsified by any transition of $Q$. That is, for each $q \xrightarrow{g;f} q' \in T_Q$:
   
   $$P(p) \land Q(q) \land g \Rightarrow P(p) \circ f$$
Owicki-Gries Method

Steps

To show \( \{ \varphi \} \ P \parallel Q \ \{ \psi \} \):

1. Define local assertion networks \( P \) and \( Q \) for both processes. Show that they're inductive.

2. For each location \( p \in L_P \), show that \( P(p) \) is not falsified by any transition of \( Q \). That is, for each \( q \xrightarrow{g;f} q' \in T_Q \):
   \[
P(p) \land Q(q) \land g \Rightarrow P(p) \circ f
   \]

3. Vice versa for \( Q \).
Owicki-Gries Method

Steps

To show \( \{ \varphi \} P \parallel Q \{ \psi \} \):

1. Define local assertion networks \( P \) and \( Q \) for both processes. Show that they’re inductive.
2. For each location \( p \in L_P \), show that \( P(p) \) is not falsified by any transition of \( Q \). That is, for each \( q \xrightarrow{g;f} q' \in T_Q \):
   \[
P(p) \land Q(q) \land g \Rightarrow P(p) \circ f
   \]
3. Vice versa for \( Q \).
4. Show that \( \varphi \Rightarrow P(s_P) \land Q(s_Q) \) and \( P(t_P) \land Q(t_Q) \Rightarrow \psi \).
How does it help?

The Owicki-Gries method generalises to $n$ processes just by requiring more interference freedom obligations.
The Owicki-Gries method generalises to $n$ processes just by requiring more interference freedom obligations.

**Derived Assertion Network**

The automatic assertion network we get for the parallel composition from the Owicki-Gries method is the conjunction of the local assertions at each of the component states.
How does it help?

The Owicki-Gries method generalises to $n$ processes just by requiring more interference freedom obligations.

**Derived Assertion Network**

The automatic assertion network we get for the parallel composition from the Owicki-Gries method is the conjunction of the local assertions at each of the component states.

Given $k$ transitions and $m$ locations per process, using Floyd’s method on the parallel composition of $n$ processes requires us to do $2 + n \cdot k \cdot m^{n-1}$ proofs!
How does it help?

The Owicki-Gries method generalises to $n$ processes just by requiring more interference freedom obligations.

**Derived Assertion Network**

The automatic assertion network we get for the parallel composition from the Owicki-Gries method is the conjunction of the local assertions at each of the component states.

Given $k$ transitions and $m$ locations per process, using Floyd’s method on the parallel composition of $n$ processes requires us to do $2 + n \cdot k \cdot m^{n-1}$ proofs!

The Owicki-Gries method reduces that to $2 + n \cdot k \cdot (1 + (n - 1) \cdot m)$ — merely quadratic in $n$. 
Proving Mutual Exclusion

The Owicki-Gries method can be used to prove properties like Mutual Exclusion.
Proving Mutual Exclusion

The Owicki-Gries method can be used to prove properties like Mutual Exclusion. **How?** Don’t have a postcondition. Instead make the assertions at the critical sections **contradictory** – so that they cannot be true simultaneously.
Proving Mutual Exclusion

The Owicki-Gries method can be used to prove properties like Mutual Exclusion.

**How?** Don’t have a postcondition. Instead make the assertions at the critical sections **contradictory** – so that they cannot be true simultaneously.

**Caution:** Ensure that each transition does not violate the **limited critical reference** rule!
Proving Mutual Exclusion

The Owicki-Gries method can be used to prove properties like Mutual Exclusion.

**How?** Don’t have a postcondition. Instead make the assertions at the critical sections contradictory – so that they cannot be true simultaneously.

**Caution:** Ensure that each transition does not violate the limited critical reference rule!

### Manna-Pnueli Algorithm

<table>
<thead>
<tr>
<th>Manna-Pnueli Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>integer wantp, wantq ← 0, 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>forever do</th>
<th>forever do</th>
</tr>
</thead>
<tbody>
<tr>
<td>p₁</td>
<td>q₁</td>
</tr>
<tr>
<td><strong>non-critical section</strong></td>
<td><strong>non-critical section</strong></td>
</tr>
<tr>
<td>p₂</td>
<td>q₂</td>
</tr>
<tr>
<td>if wantq = −1</td>
<td>if wantp = −1</td>
</tr>
<tr>
<td>then wantp ← −1</td>
<td>then wantq ← 1</td>
</tr>
<tr>
<td>else wantp ← 1</td>
<td>else wantq ← −1</td>
</tr>
<tr>
<td>p₃</td>
<td>q₃</td>
</tr>
<tr>
<td><strong>await</strong> wantq ≠ wantp</td>
<td><strong>await</strong> wantq ≠ −wantp</td>
</tr>
<tr>
<td>p₄</td>
<td>q₄</td>
</tr>
<tr>
<td><strong>critical section</strong></td>
<td><strong>critical section</strong></td>
</tr>
<tr>
<td>p₅</td>
<td>q₅</td>
</tr>
<tr>
<td>wantp ← 0</td>
<td>wantq ← 0</td>
</tr>
</tbody>
</table>

Note: The p₂ and q₂ steps are one atomic step!
Machine Instructions

What about if we had a single machine instruction to swap two values atomically, $XC$?
What about if we had a single machine instruction to swap two values atomically, $XC$?

| bit common $\leftarrow 1$
|---|
| bit tp $\leftarrow 0$
| **forever do**
| $p_1$ _non-critical section_
| **repeat**
| $p_2$ $XC(tp, \text{common})$
| $p_3$ _until_ $tp = 1$
| $p_4$ _critical section_
| $p_5$ $XC(tp, \text{common})$
| bit tq $\leftarrow 0$
| **forever do**
| $q_1$ _non-critical section_
| **repeat**
| $q_2$ $XC(tq, \text{common})$
| $q_3$ _until_ $tq = 1$
| $q_4$ _critical section_
| $q_5$ $XC(tq, \text{common})$
One Big Invariant

Imagine assertion network(s) where every assertion is the same: An invariant.
One Big Invariant

Imagine assertion network(s) where every assertion is the same: An invariant. **Benefit:** We don’t need to prove interference freedom — the local verification conditions already show that the invariant is preserved.
One Big Invariant

Imagine assertion network(s) where every assertion is the same: An invariant. **Benefit:** We don’t need to prove interference freedom — the local verification conditions already show that the invariant is preserved.

**Example (Exchange-based Critical Section Solution)**

Using assertions about the program counters, we can craft an invariant for the XC example!
One Big Invariant

Imagine assertion network(s) where every assertion is the same: An invariant. **Benefit:** We don’t need to prove interference freedom — the local verification conditions already show that the invariant is preserved.

**Example (Exchange-based Critical Section Solution)**

Using assertions about the program counters, we can craft an invariant for the XC example!

\[
\mathcal{I} \equiv (\text{common} \oplus tp \oplus tq) = 1 \land (P@p_4 \Rightarrow tp = 1) \land \\
(Q@q_4 \Rightarrow tq = 1) \land \neg (\text{common} = tp \land \text{common} = tq)
\]

Where \( \oplus \) is exclusive or (xor). Note that this is false at \( p_4q_4 \). So if this invariant is preserved we have mutex.
One Big Invariant

Imagine assertion network(s) where every assertion is the same: An invariant. **Benefit:** We don’t need to prove interference freedom — the local verification conditions already show that the invariant is preserved.

**Example (Exchange-based Critical Section Solution)**

Using assertions about the program counters, we can craft an invariant for the XC example!

\[
\mathcal{I} \equiv (\text{common} \oplus \text{tp} \oplus \text{tq}) = 1 \land (P@p_4 \Rightarrow \text{tp} = 1) \land (Q@q_4 \Rightarrow \text{tq} = 1) \land \neg(\text{common} = \text{tp} \land \text{common} = \text{tq})
\]

Where \( \oplus \) is exclusive or (xor). Note that this is false at \( p_4q_4 \). So if this invariant is preserved we have mutex.

Lets prove mutual exclusion for XC!
What now?

- You now have all you need to complete Assignment 0 (warm-up), due next Thursday.
- I have posted some Promela exercises about XC style solutions we will discuss next week (also due next Thursday).
- Next week: We will examine some more sophisticated critical section solutions for $n$ processes.
- We may also learn about semaphores, time permitting!