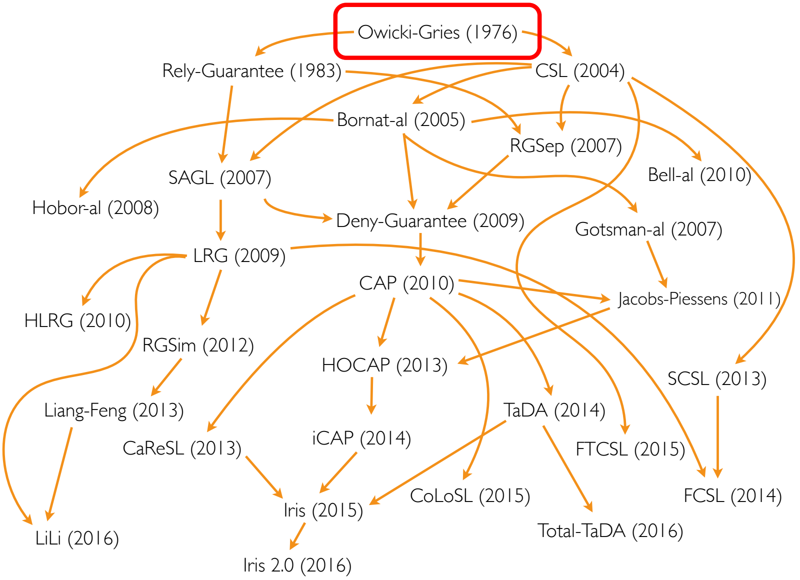
Program logics for weak memory

OGRA: Applying the Owicki-Gries proof method to release-acquire consistency

Ori Lahav Viktor Vafeiadis

31 August 2017



Program logics for concurrent programs (adapted from Ilya Sergey)

Outline

Goals:

- Verify concurrent programs under WMC.
- Investigate which program logics are sound under WMC.

Summary:

- Owicki-Gries is unsound for WMC
  (even without ghost variables and atomic blocks).
- OGRA is a simple weakening of OG that is sound for release/acquire consistency.

Hoare logic (1969)

$$\{P\}\ c\ \{Q\}$$

- P: precondition
- c: program
- Q: postcondition

$$\frac{}{\{P\}\ \textbf{skip}\ \{P\}} \qquad \frac{}{\{P[e/x]\}\ x := e\ \{P\}} \qquad \frac{\{P\}\ c_1\ \{R\} \qquad \{R\}\ c_2\ \{Q\}}{\{P\}\ c_1; c_2\ \{Q\}}$$

$$\frac{\begin{array}{c}\{e \neq 0 \wedge P\}\ c_1\ \{Q\} \\ \{e = 0 \wedge P\}\ c_2\ \{Q\}\end{array}}{\{P\}\ \textbf{if}\ e\ \textbf{then}\ c_1\ \textbf{else}\ c_2\ \{Q\}} \qquad \frac{\{P \wedge e \neq 0\}\ c\ \{P\}}{\{P\}\ \textbf{while}\ e\ \textbf{do}\ c\ \{P \wedge e = 0\}}$$

$$\frac{P_1 \Rightarrow P_2 \qquad \{P_2\}\ c\ \{Q_2\} \qquad Q_2 \Rightarrow Q_1}{\{P_1\}\ c\ \{Q_1\}}$$

Owicki-Gries method (1976)

OG = Hoare logic + rule for parallel composition

$$\frac{\{P_1\}\ c_1\ \{Q_1\} \qquad \{P_2\}\ c_2\ \{Q_2\} \qquad \text{the two proofs are } \textit{non-interfering}}{\{P_1 \wedge P_2\}\ c_1 \parallel c_2\ \{Q_1 \wedge Q_2\}}$$

Non-interference

$R \wedge P \vdash R[u/x]$ for every:

- assertion R in one proof outline
- assignment $x := u$ with precondition P in the other proof outline

$$\begin{array}{c|c} \vdots & \\ \{P\} & \vdots \\ x := u & \{R\} \\ \vdots & \vdots \end{array}$$

Example SB: store buffering

$$
\begin{array}{c}
\{a \neq 0\} \\
\begin{array}{l||l}
\{a \neq 0\} & \{\top\} \\
x := 1 & y := 1 \\
\{x \neq 0\} & \{y \neq 0\} \\
a := y & b := x \\
\{x \neq 0\} & \{y \neq 0 \wedge (a \neq 0 \vee b = x)\}
\end{array} \\
\{a \neq 0 \vee b \neq 0\}
\end{array}
$$

Example SB: store buffering

$$\left\{a \neq 0\right\}$$

$$\begin{array}{l||l}
\left\{a \neq 0\right\} & \left\{\top\right\} \\
x := 1 & y := 1 \\
\left\{x \neq 0\right\} & \left\{y \neq 0\right\} \\
a := y & b := x \\
\left\{x \neq 0\right\} & \left\{y \neq 0 \wedge (a \neq 0 \vee b = x)\right\}
\end{array}$$

$$\left\{a \neq 0 \vee b \neq 0\right\}$$

Standard OG is **unsound** under weak memory!

Example SB: store buffering

$$\left\{a \neq 0\right\}$$

$$\begin{array}{l||l}
\left\{a \neq 0\right\} & \left\{\top\right\} \\
x := 1 & y := 1 \\
\left\{x \neq 0\right\} & \left\{y \neq 0\right\} \\
a := y & b := x \\
\left\{x \neq 0\right\} & \left\{y \neq 0 \land (a \neq 0 \lor b = x)\right\}
\end{array}$$

$$\left\{a \neq 0 \lor b \neq 0\right\}$$

Standard OG is **unsound** under weak memory!

Stronger non-interference condition

$$\frac{\begin{array}{c}\{P_1\}\ c_1\ \{Q_1\} \qquad \{P_2\}\ c_2\ \{Q_2\} \\ \text{the two proofs are non-interfering}\end{array}}{\{P_1 \wedge P_2\}\ c_1 \parallel c_2\ \{Q_1 \wedge Q_2\}}$$

Strong non-interference

$R \wedge P \vdash R[v/x]$ for every:

- assertion R in one proof outline
- assignment $x := u$ with precondition P in the other proof outline
- value v such that $P \wedge R' \wedge u = v$ is satisfiable for some R' above R

$$\begin{array}{c||c} & \vdots \\ \vdots & \{R'\} \\ \{P\} & \vdots \\ x := u & \{R\} \\ \vdots & \vdots \end{array}$$

Example: message passing

$$\{x = 0\}$$

$$\begin{array}{l||l} m := 42 & \textbf{while } x = 0 \textbf{ do skip} \\ x := 1 & a := m \end{array}$$

$$\{a = 42\}$$

Example: message passing

$$
\begin{array}{c}
\{x = 0\} \\
\begin{array}{l||l}
\{\top\} & \{x \neq 0 \Rightarrow m = 42\} \\
m := 42 & \textbf{while } x = 0 \textbf{ do skip} \\
\{m = 42\} & \{m = 42\} \\
x := 1 & a := m \\
\{\top\} & \{a = 42\}
\end{array} \\
\{a = 42\}
\end{array}
$$

Example: read-read coherence (CoRR2)

$$\left\{x = a = b = c = d = 0\right\}$$

$$x := 1 \;\left\|\; x := 2 \;\right\|\; \begin{array}{l} a := x \\ \\ b := x \end{array} \;\left\|\; \begin{array}{l} c := x \\ \\ d := x \end{array}\right.$$

$$\left\{a \neq 1 \lor b \neq 2 \lor c \neq 2 \lor d \neq 1\right\}$$

Example: read-read coherence (CoRR2)

$$\left\{x = a = b = c = d = 0\right\}$$

$$\begin{array}{l||l||l||l}
 & & \left\{\top\right\} & \left\{\top\right\} \\
 & & a := x & c := x \\
\left\{\begin{array}{l} x \neq 1 \wedge \\ a \neq 1 \end{array}\right\} & \left\{\begin{array}{l} x \neq 2 \wedge \\ c \neq 2 \end{array}\right\} & \left\{\top\right\} & \left\{\top\right\} \\
x := 1 & x := 2 & b := x & d := x \\
\left\{\top\right\} & \left\{\top\right\} & \left\{\begin{array}{l} a \neq 1 \vee \\ b \neq 2 \vee \\ x = 2 \end{array}\right\} & \left\{\begin{array}{l} c \neq 2 \vee \\ d \neq 1 \vee \\ x = 1 \end{array}\right\}
\end{array}$$

$$\left\{a \neq 1 \vee b \neq 2 \vee c \neq 2 \vee d \neq 1\right\}$$

Example: read-read coherence (CoRR2)

$$
\begin{array}{c}
\left\{ x = a = b = c = d = 0 \right\} \\
\begin{array}{l||l||l||l}
 & & \{\top\} & \{\top\} \\
 & & a := x & c := x \\
\left\{\begin{array}{l} x \neq 1 \wedge \\ a \neq 1 \end{array}\right\} & \left\{\begin{array}{l} x \neq 2 \wedge \\ c \neq 2 \end{array}\right\} & \{\top\} & \{\top\} \\
x := 1 & x := 2 & b := x & d := x \\
\{\top\} & \{\top\} & \left\{\begin{array}{l} a \neq 1 \vee \\ b \neq 2 \vee \\ x = 2 \end{array}\right\} & \left\{\begin{array}{l} c \neq 2 \vee \\ d \neq 1 \vee \\ x = 1 \end{array}\right\}
\end{array} \\
\left\{ a \neq 1 \vee b \neq 2 \vee c \neq 2 \vee d \neq 1 \right\}
\end{array}
$$

Rely/guarantee-style presentation of OG

OG judgments

$$\mathcal{R}; \mathcal{G} \Vdash \{P\}\ c\ \{Q\}$$

- $\mathcal{R} = \{R_1, \ldots, R_n\}$ (“stable” assertions)
- $\mathcal{G} = \{\{P_1\}x_1 := u_1, \ldots, \{P_n\}x_n := u_n\}$ (guarded assignments)

$$\frac{P \vdash Q}{\{P, Q\}; \emptyset \Vdash \{P\}\ \textbf{skip}\ \{Q\}} \qquad \frac{P \vdash Q[u/x]}{\{P, Q\}; \{\{P\}x := u\} \Vdash \{P\}\ x := u\ \{Q\}}$$

$$\frac{\mathcal{R}_1; \mathcal{G}_1 \Vdash \{P\}\ c_1\ \{R\} \qquad \mathcal{R}_2; \mathcal{G}_2 \Vdash \{R\}\ c_2\ \{Q\}}{\mathcal{R}_1 \cup \mathcal{R}_2; \mathcal{G}_1 \cup \mathcal{G}_2 \Vdash \{P\}\ c_1; c_2\ \{Q\}}$$

$$\frac{\begin{array}{c} \mathcal{R}_1; \mathcal{G}_1 \Vdash \{P_1\}\ c_1\ \{Q_1\} \qquad \mathcal{R}_2; \mathcal{G}_2 \Vdash \{P_2\}\ c_2\ \{Q_2\} \\ P \vdash P_1 \wedge P_2 \qquad Q_1 \wedge Q_2 \vdash Q \\ R \wedge P \vdash R[u/x] \text{ for every} \\ (R \in \mathcal{R}_1 \text{ and } \langle P, x := u\rangle \in \mathcal{G}_2) \text{ or } (R \in \mathcal{R}_2 \text{ and } \langle P, x := u\rangle \in \mathcal{G}_1 \end{array}}{\mathcal{R}_1 \cup \mathcal{R}_2 \cup \{P, Q\}; \mathcal{G}_1 \cup \mathcal{G}_2 \Vdash \{P\}\ c_1 \parallel c_2\ \{Q\}}$$

Rely/guarantee-style presentation of OGRA

OGRA judgments

$$\mathcal{R}; \mathcal{G} \Vdash \{P\}\ c\ \{Q\}$$

- $\mathcal{R} = \{R_1 \upharpoonright c_1, \ldots, R_n \upharpoonright c_n\}$ ("stable" assertions)
- $\mathcal{G} = \{\{P_1\} x_1 := u_1, \ldots, \{P_n\} x_n := u_n\}$ (guarded assignments)

Stability

$R \upharpoonright C$ is *stable* under $\{P\} x := y$ if $R \wedge P \vdash R[v_y / x]$ whenever $C \wedge P \wedge y = v_y$ is satisfiable.

Non-interference

$\mathcal{R}_1; \mathcal{G}_1$ and $\mathcal{R}_2; \mathcal{G}_2$ are *non-interfering* if every $R \upharpoonright C \in \mathcal{R}_i$ is stable under every $\{P\} C \in \mathcal{G}_j$ for $i \neq j$.

Rules of OGRA

Example (Basic assignment rule)

$$\frac{P \vdash Q[y/x]}{\{P \nearrow P, Q \nearrow (P \vee Q)\}; \{\{P\}x := y\} \Vdash \{P\}\ x := y\ \{Q\}}$$

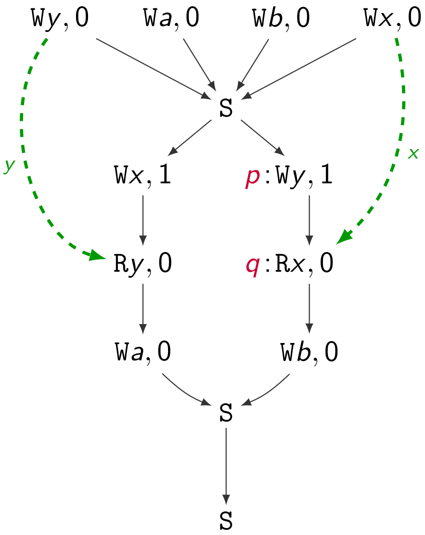
Example (Parallel composition rule)

$$\frac{\begin{array}{c} \mathcal{R}_1; \mathcal{G}_1 \Vdash \{P_1\}\ c_1\ \{Q_1\} \qquad \mathcal{R}_2; \mathcal{G}_2 \Vdash \{P_2\}\ c_2\ \{Q_2\} \\ Q_1 \wedge Q_2 \vdash Q \qquad \mathcal{R}_1; \mathcal{G}_1 \text{ and } \mathcal{R}_2; \mathcal{G}_2 \text{ are non-interfering} \\ \mathcal{R}_1 \cup \mathcal{R}_2 \cup \{Q \nearrow (\mathcal{R}_1^R \vee \mathcal{R}_2^R \vee Q)\} \subseteq \mathcal{R} \end{array}}{\mathcal{R}; \mathcal{G}_1 \cup \mathcal{G}_2 \Vdash \{P_1 \wedge P_2\}\ c_1 \parallel c_2\ \{Q\}}$$

Soundness of OGRA

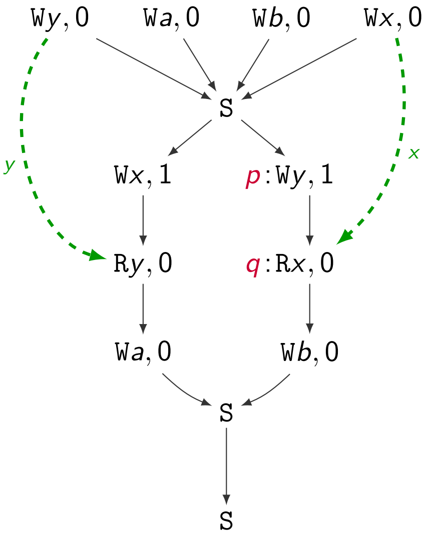
- What is the meaning of Hoare triples?

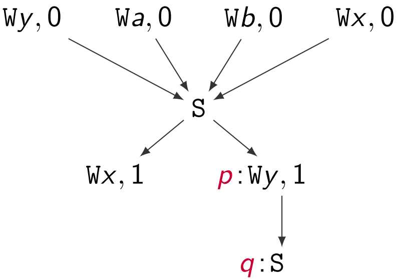
Visible states



$\sigma = \{x \mapsto 1, y \mapsto 1, a \mapsto 0, b \mapsto 0\}$ is visible at $\langle p, q \rangle$

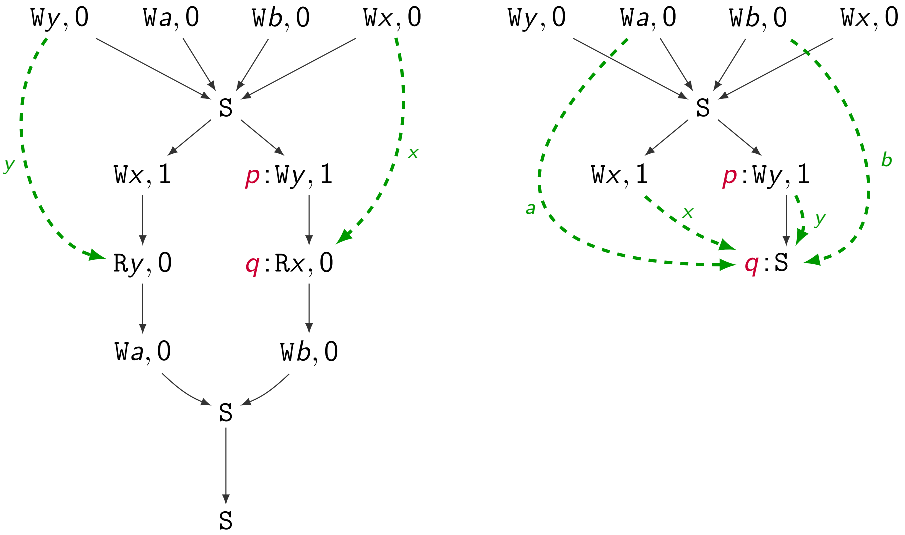
Visible states





$\sigma = \{x \mapsto 1, y \mapsto 1, a \mapsto 0, b \mapsto 0\}$ is visible at $\langle p, q \rangle$

Visible states



$\sigma = \{x \mapsto 1, y \mapsto 1, a \mapsto 0, b \mapsto 0\}$ is visible at $\langle p, q \rangle$

Meaning of Hoare triples

Triple validity

$\{P\}\ c\ \{Q\}$ is *valid* if every state visible at the terminal edge of an RA-consistent execution in $\mathcal{W}(P); [\![c]\!]; \mathbb{S}$ satisfies Q.

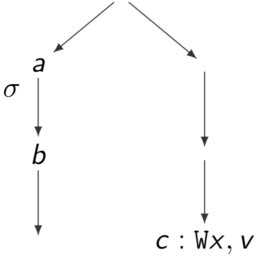
Main steps in soundness proof:

- Study properties of visibility under the RA model.
- Show that edges of consistent executions can be annotated with the assertions from the OG derivation such that every state visible at an edge satisfies its annotation.

Main visibility lemma (simplified)

Lemma

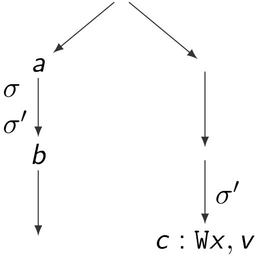
If a state σ becomes visible at $\langle a, b\rangle$ when adding a parallel node $c : \mathtt{W}x\ v$, then some x-variant of σ is visible both at $\langle a, b\rangle$ before adding c, and at every incoming edge to c.



Main visibility lemma (simplified)

Lemma

If a state σ becomes visible at $\langle a, b\rangle$ when adding a parallel node $c : \mathtt{W}x\ v$, then some x-variant of σ is visible both at $\langle a, b\rangle$ before adding c, and at every incoming edge to c.



Stronger assignment rule

$$\{r = 0\}$$

$w := 1$

while $r \neq 1$ **do skip**

$\|$

$r := w$

$r := w$

$$\{r = 1\}$$

Stronger assignment rule

$$\left\{r = 0\right\}$$

$$\begin{array}{l||l}
 & \left\{r = 0\right\} \\
\left\{\top\right\} & r := w \\
w := 1 & \left\{r = 1 \Rightarrow w = 1\right\} \\
\left\{\top\right\} & \\
\textbf{while } r \neq 1 \textbf{ do skip} & r := w \\
\left\{r = 1\right\} & \\
 & \left\{\top\right\}
\end{array}$$

$$\left\{r = 1\right\}$$

Stronger assignment rule

$$\{r = 0\}$$

$\{\top\}$

$w := 1$

$\{\top\}$

while $r \neq 1$ **do skip**

$\{r = 1\}$

$\Bigg\|$

$\{r = 0\}$

$r := w$

$\{r = 1 \Rightarrow w = 1\}$

$r := w \quad \begin{cases} w = 1 & \textit{for } 1 \\ r \neq 1 & \textit{otherwise} \end{cases}$

$\{\top\}$

$$\{r = 1\}$$

Stronger assignment rule

$$
\{r = 0\}
$$

$$
\begin{array}{l|l}
\begin{array}{l}
\{\top\} \\
w := 1 \\
\{\top\} \\
\textbf{while } r \neq 1 \textbf{ do skip} \\
\{r = 1\}
\end{array}
&
\begin{array}{l}
\{r = 0\} \\
r := w \\
\{r = 1 \Rightarrow w = 1\} \\
r := w \quad \begin{cases} w = 1 & \textit{for } 1 \\ r \neq 1 & \textit{otherwise} \end{cases} \\
\{\top\}
\end{array}
\end{array}
$$

$$
\{r = 1\}
$$

$$
\frac{P \vdash Q[y/x] \qquad \{P \upharpoonright P, Q \upharpoonright (P \vee Q)\} \subseteq \mathcal{R} \\ \forall v \in \mathsf{Val}: \qquad P \wedge (y = v) \vdash P_v \qquad P_v \upharpoonright P \in \mathcal{R}}{\mathcal{R}; \{\{P_v\} x := y \mid v \in \mathsf{Val}\} \Vdash \{P\}\ x := y\ \{Q\}}
$$

Modelling fences as RMWs

$$\left\{ f = 0 \right\}$$

$$\begin{array}{l||l} x := 1; & y := 1; \\ \langle f := 10f + 1 \rangle; & \langle f := 10f + 2 \rangle; \\ a := y & b := x \end{array}$$

$$\left\{ a = 1 \lor b = 1 \right\}$$

Modelling fences as RMWs

$$\left\{f = 0\right\}$$

$$
\begin{array}{l||l}
\left\{\begin{array}{l} f \in \{0,2\} \wedge \\ (f = 2 \Rightarrow y = 1) \end{array}\right\} & \left\{\begin{array}{l} f \in \{0,1\} \wedge \\ (f = 1 \Rightarrow x = 1) \end{array}\right\} \\
x := 1; & y := 1; \\
\left\{\begin{array}{l} f \in \{0,2\} \wedge x = 1 \wedge \\ (f = 2 \Rightarrow y = 1) \end{array}\right\} & \left\{\begin{array}{l} f \in \{0,1\} \wedge y = 1 \wedge \\ (f = 1 \Rightarrow x = 1) \end{array}\right\} \\
\langle f := 10f + 1\rangle; & \langle f := 10f + 2\rangle; \\
\left\{\begin{array}{l} f \in \{1,12,21\} \wedge \\ (f = 21 \Rightarrow y = 1) \end{array}\right\} & \left\{\begin{array}{l} f \in \{2,12,21\} \wedge \\ (f = 12 \Rightarrow x = 1) \end{array}\right\} \\
a := y & b := x \\
\left\{\begin{array}{l} f \in \{1,12,21\} \wedge \\ (f = 21 \Rightarrow a = 1) \end{array}\right\} & \left\{\begin{array}{l} f \in \{2,12,21\} \wedge \\ (f = 12 \Rightarrow b = 1) \end{array}\right\}
\end{array}
$$

$$\left\{a = 1 \vee b = 1\right\}$$