Alignment Completeness for Relational Hoare Logics

Ramana Nagasamudram and Dave Naumann

Stevens Institute of Technology, USA

LICS 29 June 2021

This work was partially supported by NSF award CNS 1718713
and ONR N00014-17-1-2787.

Relational Properties of Programs

$$c \quad \widehat{=} \quad z := x; \textsf{if } x \geq 10 \textsf{ then } z := 2 * z \textsf{ else } z := 3 * x$$
$$c' \quad \widehat{=} \quad z := x; \textsf{if } z \geq 10 \textsf{ then } z := z + z \textsf{ else } z := z + z + z$$

Equiv: from states with the same value for x, get same value for z

$c|c' : x = x' \approx\!> z = z'$

Relational Properties of Programs

$$c \quad \widehat{=} \quad z := x; \mathsf{if}\ x \geq 10\ \mathsf{then}\ z := 2 * z\ \mathsf{else}\ z := 3 * x$$
$$c' \quad \widehat{=} \quad z := x; \mathsf{if}\ z \geq 10\ \mathsf{then}\ z := z + z\ \mathsf{else}\ z := z + z + z$$

Equiv: from states with the same value for x, get same value for z

$c|c' : x = x' \approx> z = z'$ because

- given $x = x'$, after $z := x \mid z := x$ have $x = x' = z = z'$
- at which point $x \geq 10 \iff z' \geq 10$
- for then branch: $z = z' \Rightarrow 2 * z = z' + z'$
- for else branch: $x = x' = z = z' \Rightarrow 3 * x = z' + z' + z'$

Relational Properties of Programs

$$c \quad \widehat{=} \quad z := x; \mathsf{if}\ x \geq 10\ \mathsf{then}\ z := 2 * z\ \mathsf{else}\ z := 3 * x$$
$$c' \quad \widehat{=} \quad z := x; \mathsf{if}\ z \geq 10\ \mathsf{then}\ z := z + z\ \mathsf{else}\ z := z + z + z$$

Equiv: from states with the same value for x, get same value for z

$c|c' : x = x' \approx\!> z = z'$ because

- given $x = x'$, after $z := x \mid z := x$ have $x = x' = z = z'$
- at which point $x \geq 10 \iff z' \geq 10$
- for then branch: $z = z' \Rightarrow 2 * z = z' + z'$
- for else branch: $x = x' = z = z' \Rightarrow 3 * x = z' + z' + z'$

Lockstep aligned conditional rule

$$\frac{\mathcal{R} \Rightarrow e = e' \qquad c|c' : \mathcal{R} \wedge e \approx\!> \mathcal{S} \qquad d|d' : \mathcal{R} \wedge \neg e \approx\!> \mathcal{S}}{\mathsf{if}\ e\ \mathsf{then}\ c\ \mathsf{else}\ d\ \mathsf{fi} \mid \mathsf{if}\ e'\ \mathsf{then}\ c'\ \mathsf{else}\ d'\ \mathsf{fi} : \mathcal{R} \approx\!> \mathcal{S}}$$

One-rule Cook complete RHL

Consider the following RHL rule[1]:

$$\frac{c; d' : \mathcal{R} \rightsquigarrow \mathcal{S} \qquad d' \text{ is renamed copy of } d}{c \mid d : \mathcal{R} \approx\!> \mathcal{S}} \ \textsc{SeqProd}$$

If $c|d : \mathcal{R} \approx\!> \mathcal{S}$ is true then it is provable in HL + SeqProd.

[1] We write $c : P \rightsquigarrow Q$ for the Hoare triple $\{P\}c\{Q\}$

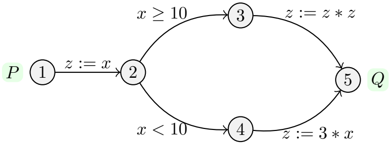
One-rule Cook complete RHL

Consider the following RHL rule[1]:

$$\frac{c; d' : \mathcal{R} \rightsquigarrow \mathcal{S} \qquad d' \text{ is renamed copy of } d}{c \mid d : \mathcal{R} \approx\!> \mathcal{S}} \textsc{SeqProd}$$

If $c|d : \mathcal{R} \approx\!> \mathcal{S}$ is true then it is provable in HL + SeqProd.

Floyd completeness of Hoare logic



$z := x$; if $x \geq 10$ then $z := 2{*}z$ else $z := 3{*}x$

Given a valid annotation, an, for $c : P \rightsquigarrow Q$, there is a HL proof using only judgements derived from an.

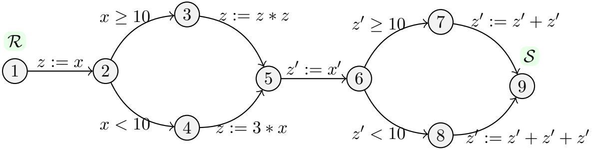
[1] We write $c : P \rightsquigarrow Q$ for the Hoare triple $\{P\}c\{Q\}$

Alignment Completeness

A set of RHL rules is alignment complete, for a given class of product automata, if for any valid annotated product there is a derivation using only the judgements associated with the annotation.

Alignment Completeness

A set of RHL rules is alignment complete, for a given class of product automata, if for any valid annotated product there is a derivation using only the judgements associated with the annotation.

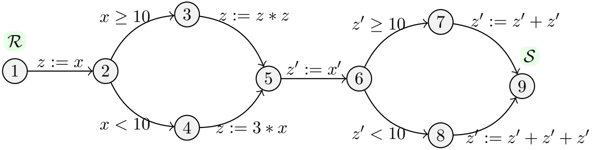


$$\frac{\begin{array}{c} c; d' : \mathcal{R} \rightsquigarrow \mathcal{S} \\ d' \text{ is a renamed copy of } d \end{array}}{c \mid d : \mathcal{R} \approx\!> \mathcal{S}}$$

Thm: HL+SeqProd is alignment complete for sequential products

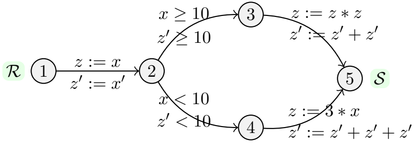
Alignment Completeness

A set of RHL rules is alignment complete, for a given class of product automata, if for any valid annotated product there is a derivation using only the judgements associated with the annotation.



$$\frac{c; d' : \mathcal{R} \rightsquigarrow \mathcal{S} \qquad d' \text{ is a renamed copy of } d}{c \mid d : \mathcal{R} \approx\!> \mathcal{S}}$$

Thm: HL+SeqProd is alignment complete for sequential products



$$\frac{\mathcal{R} \Rightarrow e = e' \qquad c|c' : \mathcal{R} \wedge e \approx\!> \mathcal{S} \qquad d|d' : \mathcal{R} \wedge \neg e \approx\!> \mathcal{S}}{\text{if } e \ldots c \ldots d \mid \text{if } e' \ldots c' \ldots d' : \mathcal{R} \approx\!> \mathcal{S}}$$

Thm: Lockstep rules are alignment complete for lockstep products.