Simple Relational Correctness Proofs for Static Analyses and Program Transformations

By Nick Benton

Enrico Steffinlongo

Università Ca' Foscari - Computer science

May 29, 2015

Soundness of Program optimization

Lot of work on functional languages especially in

- formalization
- validation

Few work on imperative programming languages

- seems trivial
- ... but i's not

Some notations

- $\mathbb{V} = \{X, Y, \dots\}$ a set of variables
- $n \in \mathbb{Z}$ a number, $b \in \mathbb{B}$ a boolean literal
- $iop \in \{+, -, \times, \dots\} \subseteq \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ an integer operation
- $bop \in \{<, =, \dots\} \subseteq \mathbb{Z} \times \mathbb{Z} \to \mathbb{B}$ an integer to boolean operation
- $lop \in \{\wedge, \vee, \dots\} \subseteq \mathbb{B} \times \mathbb{B} \to \mathbb{B}$ a logical operation
- $E := n | X | E \ iop \ E$ integer expressions
- $B := b | E \ bop \ E | \texttt{not} \ B | B \ lop \ B$ boolean expressions
- $C := \texttt{skip} | X := E | C; C | \texttt{if} \ B \ \texttt{then} \ C \ \texttt{else} \ C | \texttt{while} \ B \ \texttt{do} \ C$ commands
- $\Game$
- $[\![E]\!]\mathbb{S}$ evaluation
- ddd

$$ss \tag{1}$$

while-Programs

$$\text{(PE-C}\textsc{ond}\text{)}$$

$$\frac{\sqsubseteq \rho}{\hat{v}\rho}$$