

Verifying Programs with Lists ²

Peter Fontana, Piotr Mardziel

May 6, 2009

²... and maybe trees too

Verification (all you need to know)

Windows

A fatal exception 0E has occurred at 0028:C0011E36 in UXD UMM(01) + 00010E36. The current application will be terminated.

- * Press any key to terminate the current application.
- * Press CTRL+ALT+DEL again to restart your computer. You will lose any unsaved information in all applications.

Press any key to continue _

Verification (cont.)

- Describe desired program property and show it holds.
 - Proof by exhaustive enumeration not plausible.
 - Derive desired property via derivation rules / axioms.
 - ★ First order logic derivation rules,
 - ★ Hoare Logic derivation rules, and
 - ★ Domain specific axioms: list reachability, integer (in)equalities, etc.

$$\begin{array}{c}
 \frac{\vdash A \quad \vdash B}{\vdash A \wedge B} \quad \frac{\vdash [a/x]A \quad (a \text{ is fresh})}{\vdash \forall x.A} \quad \frac{\vdash \forall x.A}{\vdash [E/x]A} \quad \vdash [a/x]A \\
 \frac{\vdash A}{\vdash B} \quad \frac{\vdash A \Rightarrow B \quad \vdash A}{\vdash B} \quad \frac{\vdash [E/x]A}{\vdash \exists x.A} \quad \frac{\vdash \exists x.A \quad \vdash B}{\vdash B}
 \end{array}$$

$$\frac{}{\vdash \{A\} \text{ skip } \{A\}}$$

$$\frac{\vdash \{A\} c_1 \{B\} \quad \vdash \{B\} c_2 \{C\}}{\vdash \{A\} c_1; c_2 \{C\}}$$

$$\frac{\vdash \{A \wedge b\} c_1 \{B\} \quad \vdash \{A \wedge \neg b\} c_2 \{B\}}{\vdash \{A\} \text{ if } b \text{ then } c_1 \text{ else } c_2 \{B\}}$$

$$\begin{array}{l}
 \forall x \quad \cdot \quad x \rightsquigarrow x \\
 \forall x, y, z \quad \cdot \quad x \rightsquigarrow y \wedge y \rightsquigarrow z \Rightarrow x \rightsquigarrow z \\
 \forall x \quad \cdot \quad x \neq \perp \Rightarrow x \rightsquigarrow (x \rightarrow \text{next}) \\
 \forall x, y \quad \cdot \quad x \rightsquigarrow y \Rightarrow x = y \vee (x \rightarrow \text{next}) \\
 \quad \cdot \quad \rightsquigarrow y \\
 \forall x \quad \cdot \quad \perp \rightsquigarrow x \Rightarrow x = \perp
 \end{array}$$