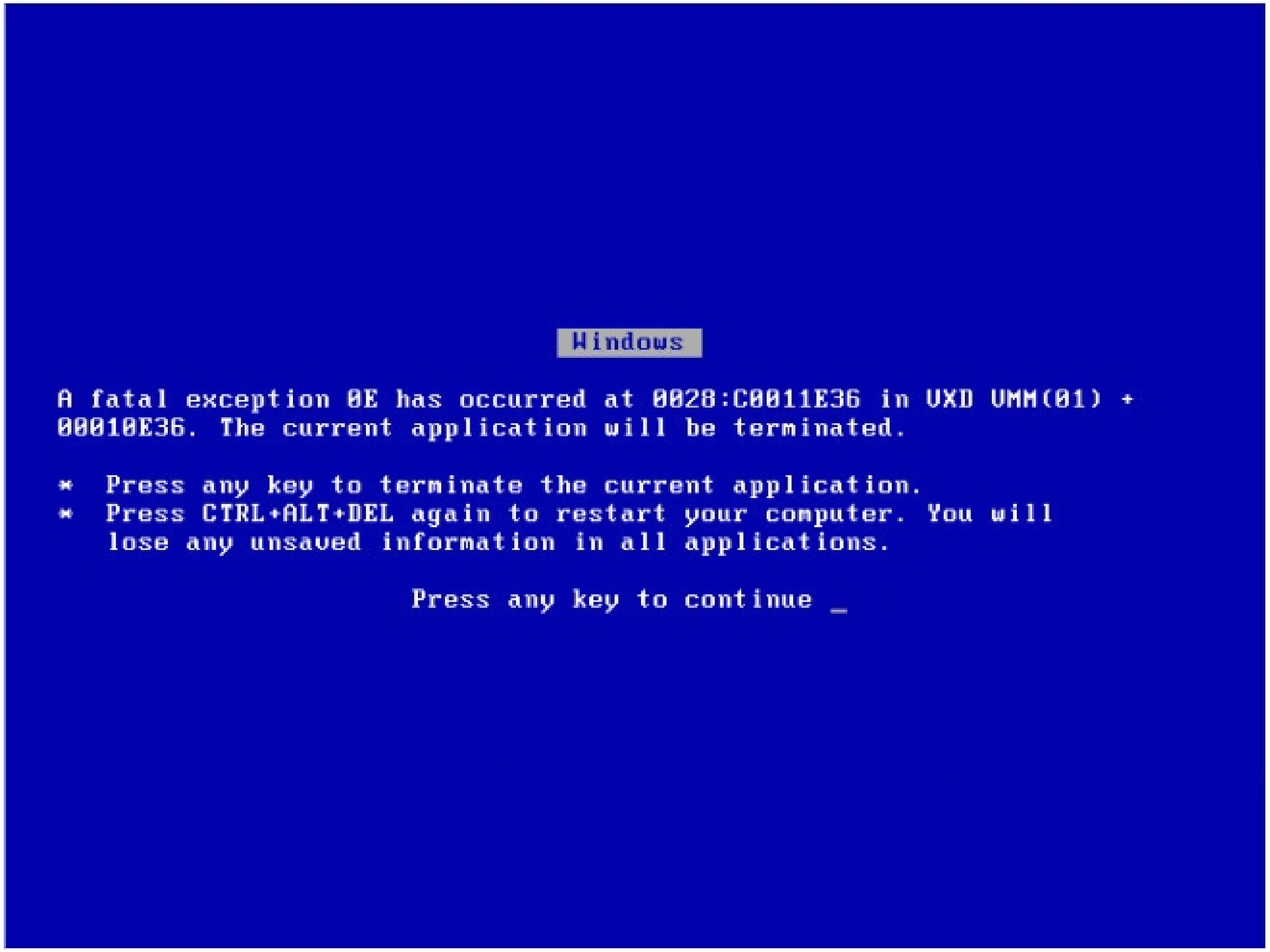
Verifying Programs with Lists [2]

Peter Fontana, Piotr Mardziel

May 6, 2009

[2]... and maybe trees too

Verification (all you need to know)



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.

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

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

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

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

$$\begin{array}{rcl}
\forall x & . & x \rightsquigarrow x \\
\forall x, y, z & . & x \rightsquigarrow y \wedge y \rightsquigarrow z \Rightarrow x \rightsquigarrow z \\
\forall x & . & x \neq \bot \Rightarrow x \rightsquigarrow (x \longrightarrow \mathsf{next}) \\
\forall x, y & . & x \rightsquigarrow y \Rightarrow x = y \vee (x \longrightarrow \mathsf{next}) \\
 & . & \rightsquigarrow y \\
\forall x & . & \bot \rightsquigarrow x \Rightarrow x = \bot
\end{array}$$