An Inductive Method for Verifying Properties of a Program

Sungkeun Cho
ROSAEC Workshop
ROPAS, SNU
Motivation

• MSR (Multi-Sector Read) function
  – Copy data from sectors of a flash memory to a buffer

• To verify that MSR code works correctly with an arbitrary size of memory

Model Checking Performance for MSR *

---

if pre-condition is true and program executes
then post-condition is true
An Inductive Method

Base case

\{ x=0 \land \text{pre-cond} \}
program
\{ \text{post-cond} \}

Inductive step
induction hypothesis

\{ x=K \land K\geq 0 \land \text{pre-cond} \}
program
\{ \text{post-cond} \}

proof

\{ x=K+1 \land K\geq 0 \land \text{pre-cond} \}
program
\{ \text{post-cond} \}
Example – While Loop

iteration number of while loop

Base case

\{x=0 \land \text{pre-cond}\}
while(...)\{\ldots\}
\{\text{post-cond}\}

Inductive step

Induction hypothesis

\{x=K \land K\geq0 \land \text{pre-cond}\}
while(...)\{\ldots\}
\{\text{post-cond}\}

proof

\{x=K+1 \land K\geq0 \land \text{pre-cond}\}
while(...)\{\ldots\}
\{\text{post-cond}\}
Example – While Loop

Base case

\{
\begin{align*}
x &= 0 & \text{pre-cond} \\
\text{while}(...)\{\ldots\} \\
\text{post-cond}
\end{align*}
\}

1. show that while condition is false
2. prove this

\begin{align*}
x &= 0 & \text{pre-condition} = \text{true} \\
\text{post-condition} &= \text{true}
\end{align*}
Example – While Loop

**Inductive step**

1. show that while condition is true

\[ \{ x = k + 1 \land k \geq 0 \land \text{pre-cond} \} \]

\[ \text{while}(...) \{ \ldots \} \]

\[ \{ \text{post-cond} \} \]

2. prove this

\[ \{ x = k \land k \geq 0 \land \text{pre-cond} \} \]

\[ \text{while}(...) \{ \ldots \} \]

\[ \{ \text{post-cond} \} \]

3. prove this by induction hypothesis

\[ \{ x = k + 1 \land k \geq 0 \land \text{pre-cond} \} \]

\[ \text{while}(...) \{ \text{body} ; \} \]

\[ \{ \text{post-cond} \} \]

loop unrolling
Summary

• Achievement
  – The pre- and post-conditions of MSR

• Strength
  – Intuitive
    • Easy to apply
    • Easy to understand

• Weakness
  – Take a lot of time
  – Not trustworthy
Future Work

• Mechanize the proof formally
  – Coq
    • Formal proof management
    • Mathematical definitions and theorems
  – Why tool
    • Software verification platform
    • Integrated with many provers
  – Frama-C
    • Extensible platform dedicated to source-code analysis of C software
Thank you.