Introduction to Software Verification

Orna Grumberg

Lectures Material
winter 2015-16
Lecture 3
Soundness of Hoare proof system (H):

If $\vdash_H \{p\}S\{q\}$ then $\models \{p\}S\{q\}$

Proof:
H* Proof System for Proving termination (full correctness)

We prove $\langle p \rangle S \langle q \rangle$

Example: Assume $x, y \in \mathbb{Z}$

$\langle y \rangle \geq 0$ while $x > 0$ do $x := x - y$ od $\langle \text{true} \rangle$

$\langle y \rangle \geq 0$ while $x > 0$ do $x := x - y$ od $\langle x \leq 0 \rangle$
Well Founded Sets

A set $W$ with a (possibly partial) order $<$
$(W, <)$ is a well founded set if there is no
infinitely decreasing sequences in $W$.
That is, there is no sequence $w_i \in W$ such
that:

$w_0 > w_1 > w_2 > \ldots$
Well Founded Sets - Examples

The partially ordered set $(2^A, \subseteq)$ for $A=\{1,2\}$
Well Founded Sets - Examples

• Naturals with the usual order $<$ (N,$<$) is a well founded set
• Integers with the usual order $<$ is not well founded
• Positive rational numbers with the usual order $<$ is not well founded
• $(2^A,\subseteq)$ for any finite $A$ is well founded
• $(2^A,\subseteq)$ for an infinite $A$ is not well founded
• $\mathbb{N} \times \mathbb{N}$ with the lexicographical order is a well founded set
H* Proof System for Proving Termination (full correctness)

We want to prove $<p>S<q>$

- We choose $(W,\prec)$ to be $(\mathbb{N},\prec)$ with the usual order
- $p(\bar{x},n)$ - an assertion over the naturals and the program variables
- All rules except REP are as in $H$, except that we replace $\{\}$ with $\langle\rangle$
Termination rule for while-statement:

\[
\begin{align*}
p(\bar{x}, n) \land n > 0 & \rightarrow B(\bar{x}) \\
< p(\bar{x}, n) \land n > 0 > S < p(\bar{x}, n-1) > \\
p(\bar{x}, 0) & \rightarrow \neg B(\bar{x}) \\
\frac{< \exists n. p(\bar{x}, n) > \text{ while B do S od} < p(\bar{x}, 0) >}{\quad}
\end{align*}
\]
H* Proof System for Proving Termination (full correctness)

Soundness of the proof system H* :
If $\vdash_{H*} \langle p \rangle S \langle q \rangle$ then $\vdash \langle p \rangle S \langle q \rangle$

Completeness of the proof system H* :
If $\vdash \langle p \rangle S \langle q \rangle$
then $\vdash_{H*} \langle p \rangle S \langle q \rangle$
Completeness proof sketch for the termination rule for while-statement:

If $\not\models \exists n. p(x,n) \ S \ \text{true}$
then $\not\models_{H^*} \exists n. p(x,n) \ S \ \text{true}$

Full completeness proof in [Francez, program verification]
Model Checking

Automated formal verification:

A different approach to formal verification
Formal Verification

Given
- a model of a (hardware or software) system and
- a formal specification

does the system model satisfy the specification?

Not decidable!

To enable automation, we restrict the problem to a decidable one:
- **Finite-state** reactive systems
- **Propositional** temporal logics
Properties in Propositional Temporal Logic - Examples

- **mutual exclusion:**
  always $\neg (cs_1 \land cs_2)$

- **non starvation:**
  always (request $\Rightarrow$ eventually granted)

- **communication protocols:**
  $\neg$ get-message) until send-message
Finite State Systems - Examples

- Hardware designs
- Controllers (elevator, traffic-light)
- Communication protocols (when ignoring the message content)
- High level (abstracted) description of non finite state systems