Verification with Z3

COMPSCI 631

University of Massachusetts Amherst

October 31, 2017

Recap: Calculating Weakest Preconditions

Goal: Answer the question, "does $\{P\}c\{Q\}$ hold"?
Approach: (1) Calculate $\mathrm{wp}(c,Q)$ and (2) verify that $P \Rightarrow \mathrm{wp}(c,Q)$.

$$
\begin{array}{rcl}
wp(\textbf{skip}, Q) & = & Q \\
wp(x := a, Q) & = & Q[x/a] \\
wp(c_1;c_2, Q) & = & wp(c_1, wp(c_2, Q)) \\
wp(\textbf{if } (b) \textbf{ then } c_1 \textbf{ else } c_2, Q) & = & b \Rightarrow wp(c_1, Q) \wedge \neg b \Rightarrow wp(c_2, Q) \\
wp(\textbf{while } b \textbf{ invariant } I \textbf{ do } c, Q) & = & I \wedge (\forall x \cdots . \neg b \wedge I \Rightarrow Q) \wedge (\forall x \cdots . b \wedge I \Rightarrow wp(c, I))
\end{array}
$$

Recap: Calculating Weakest Preconditions

Goal: Answer the question, "does $\{P\}c\{Q\}$ hold"?
Approach: (1) Calculate $\text{wp}(c,Q)$ and (2) verify that $P \Rightarrow \text{wp}(c,Q)$.

$$
\begin{array}{rcl}
wp(\textbf{skip}, Q) & = & Q \\
wp(x := a, Q) & = & Q[x/a] \\
wp(c_1;c_2, Q) & = & wp(c_1, wp(c_2, Q)) \\
wp(\textbf{if } (b) \textbf{ then } c_1 \textbf{ else } c_2, Q) & = & b \Rightarrow wp(c_1, Q) \wedge \neg b \Rightarrow wp(c_2, Q) \\
wp(\textbf{while } b \textbf{ invariant } I \text{ do } c, Q) & = & I \wedge (\forall x \cdots . \neg b \wedge I \Rightarrow Q) \wedge (\forall x \cdots . b \wedge I \Rightarrow wp(c, I))
\end{array}
$$

Example Is $\{y > 15\}\text{x := y + 10}\{x > 20\}$ verifiable?

1. Calculate $\text{wp(x := y + 10, x} > 20)) = y > 10$
2. Verify $\forall y.y > 15 \Rightarrow y > 10$

Satisfiability vs. Validity

The formula $\phi(x)$ is *valid* if it is true for all values of x. We write $\forall x.\phi(x)$ to mean "Is $\phi(x)$ valid?".
The formula $\phi(x)$ is *satisfiable* if it is true for some value of x. We write $\exists x.\phi(x)$ to mean "Is $\phi(x)$ satisfiable?"

Satisfiability vs. Validity

The formula $\phi(x)$ is *valid* if it is true for all values of x. We write $\forall x.\phi(x)$ to mean "Is $\phi(x)$ valid?".
The formula $\phi(x)$ is *satisfiable* if it is true for some value of x. We write $\exists x.\phi(x)$ to mean "Is $\phi(x)$ satisfiable?"
Are the following formulas valid (or not)? Are they satisfiable (or not)?

1. $x > 0 \Rightarrow x + y > 0$

Satisfiability vs. Validity

The formula $\phi(x)$ is *valid* if it is true for all values of x. We write $\forall x.\phi(x)$ to mean "Is $\phi(x)$ valid?".
The formula $\phi(x)$ is *satisfiable* if it is true for some value of x. We write $\exists x.\phi(x)$ to mean "Is $\phi(x)$ satisfiable?"
Are the following formulas valid (or not)? Are they satisfiable (or not)?

1. $x > 0 \Rightarrow x + y > 0$
2. $x > 0 \wedge y > 0 \Rightarrow x + y > 0$

Satisfiability vs. Validity

The formula $\phi(x)$ is *valid* if it is true for all values of x. We write $\forall x.\phi(x)$ to mean "Is $\phi(x)$ valid?".
The formula $\phi(x)$ is *satisfiable* if it is true for some value of x. We write $\exists x.\phi(x)$ to mean "Is $\phi(x)$ satisfiable?"
Are the following formulas valid (or not)? Are they satisfiable (or not)?

1. $x > 0 \Rightarrow x + y > 0$
2. $x > 0 \wedge y > 0 \Rightarrow x + y > 0$
3. $x < 0 \Rightarrow x \cdot x < 0$

Satisfiability vs. Validity

The formula $\phi(x)$ is *valid* if it is true for all values of x. We write $\forall x.\phi(x)$ to mean "Is $\phi(x)$ valid?".
The formula $\phi(x)$ is *satisfiable* if it is true for some value of x. We write $\exists x.\phi(x)$ to mean "Is $\phi(x)$ satisfiable?"
Are the following formulas valid (or not)? Are they satisfiable (or not)?

1. $x > 0 \Rightarrow x + y > 0$
2. $x > 0 \wedge y > 0 \Rightarrow x + y > 0$
3. $x < 0 \Rightarrow x \cdot x < 0$

When we say "verify that $y > 15 \Rightarrow y > 10$" we mean "is $y > 15 \Rightarrow y > 10$ valid?".

Validity and Unsatisfiability

Observation: $\forall x.\phi(x)$ holds if and only if $\exists x.\neg\phi(x)$ does not hold.

Example 1: $\forall y.y > 15 \Rightarrow y > 10$ is valid if and only if $\exists y.\neg(y > 15 \Rightarrow y > 10)$ is unsatisfiable.

Example 2: Let $\phi(x) = x > 10 \Rightarrow x > 20$:

- $\exists x.\phi(x)$ is satisfiable:
  - $\phi(11)$ is true
  - $\phi(0)$ is true (why?)
- $\forall x.\phi(x)$ is not valid. For example, $\phi(11)$ is false.
- $\exists x.\neg\phi(x)$ is satisfiable. For example, $\neg\phi(11)$ is true.

Alternatively, if $\exists x.\neg\phi(x)$ holds, then the value of x that makes $\neg\phi(x)$ true is a *counterexample* that contradicts a claim that $\forall x.\phi(x)$ holds.

Verification with Z3

Goal: Answer the question, "does $\{P\}c\{Q\}$ hold"?

Approach:

1. Calculate $\text{wp}(c,Q)$ and
2. Instead of verifying that $P \Rightarrow \text{wp}(c,Q)$, show that $\neg(P \Rightarrow \text{wp}(c,Q))$ is unsatisfiable.
3. We will check (un-)satisfiability using the Z3 SMT Solver.

Do the Z3 Tutorial (sections 1–4): `https://rise4fun.com/z3/tutorial`

Z3 OCaml API: For the verification assignment, we've written an OCaml library to help you work with Z3. Documentation:
`https://github.com/plasma-umass/ocaml-z3/blob/master/lib/Smtlib.mli`