COMP 4161
NICTA Advanced Course

Advanced Topics in Software Verification

Simon Winwood, Toby Murray, June Andronick, Gerwin Klein

Content
- Intro & motivation, getting started with Isabelle
- Foundations & Principles
  - Lambda Calculus
  - Higher Order Logic, natural deduction
  - Term rewriting
- Proof & Specification Techniques
  - Inductively defined sets, rule induction
  - Datatypes, recursion, induction
  - Calculational reasoning, mathematics style proofs
  - Hoare logic, proofs about programs

Last Time
- More confluence
- Knuth-Bendix Algorithm, Waldmeister
- More Isar: forward, backward, obtain, abbreviations, moreover
- Specification techniques: Sets
Example

\[ <\text{skip}, \sigma> \longrightarrow \sigma \]
\[ <x := e, \sigma> \longrightarrow \sigma[x \mapsto v] \]
\[ <c_1, \sigma> \longrightarrow \sigma' \quad <c_2, \sigma'> \longrightarrow \sigma'' \]
\[ <c_1, c_2, \sigma> \longrightarrow \sigma'' \]
\[ [b] \sigma = \text{False} \quad \langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma' \]
\[ [b] \sigma = \text{True} \quad \langle \text{while } b \text{ do } c, \sigma \rangle \longrightarrow \sigma'' \]

Slide 5

What does this mean?

- \( <c, \sigma> \longrightarrow \sigma' \) fancy syntax for a relation \( (c, \sigma, \sigma') \in E \)
- relations are sets: \( E : (\text{com} \times \text{state} \times \text{state}) \) set
- the rules define a set inductively

But which set?

Slide 6

Simpler Example

\[ 0 \in \mathbb{N} \quad n \in \mathbb{N} \rightarrow n + 1 \in \mathbb{N} \]

Why the smallest set?

- Objective: no junk. Only what must be in \( X \) shall be in \( X \).
- Gives rise to a nice proof principle (rule induction)
- Alternative (greatest set) occasionally also useful: coinduction

Slide 7

Formally

Rules \( \frac{a_1 \in X \ldots a_n \in X}{a \in X} \) with \( a_1, \ldots, a_n, a \in A \)

define set \( X \subseteq A \)

Formally: set of rules \( R \subseteq A \times A \) \( (R, X \) possibly infinite)

Applying rules \( R \) to a set \( B \): \( R B = \{ x : \exists H. (H, x) \in R \land H \subseteq B \} \)

Example:

\[ R = \{ (\{\}, 0) \cup (\{(n), n + 1\}, n \in \mathbb{N}) \} \]
\[ R \{3, 6, 10\} = \{0, 4, 7, 11\} \]

Slide 8
The Set

Definition: \( B \) is \( R \)-closed iff \( R B \subseteq B \)

Definition: \( X \) is the least \( R \)-closed subset of \( A \)

This does always exist:

Fact: \( X = \bigcap \{ B \subseteq A. B \text{ \( R \)-closed} \} \)

Slide 9

Generation from Above

Rule Induction

\[
\begin{align*}
0 & \in N \\
n & \in N \\
n + 1 & \in N \\
\end{align*}
\]

induces induction principle

\[ [ P 0; \bigwedge n. P n \implies P (n + 1) ] \implies \forall x \in X. P x \]

In general:

\[
\forall \{(a_1, \ldots, a_n), a\} \in R. P a_1 \land \ldots \land P a_n \implies P a
\]

\[
\forall x \in X. P x
\]

Slide 11

Why does this work?

\[
\forall \{(a_1, \ldots, a_n), a\} \in R. P a_1 \land \ldots \land P a_n \implies P a
\]

\[
\forall x \in X. P x
\]

\[
\forall \{(a_1, \ldots, a_n), a\} \in R. P a_1 \land \ldots \land P a_n \implies P a
\]

\[
\forall x \in X. P x
\]

says

\[
\{ x, P x \} \text{ is \( R \)-closed}
\]

but: \( X \) is the least \( R \)-closed set

hence:

\[
X \subseteq \{ x, P x \}
\]

which means:

\[
\forall x \in X. P x
\]

\[ \text{qed} \]

Slide 12
Rules with side conditions

\[ a_1 \in X \quad \ldots \quad a_n \in X \quad C_1 \quad \ldots \quad C_m \]

\[ a \in X \]

induction scheme:

\[ \forall \left( \{a_1, \ldots, a_n \}, a \right) \in R. P \ a_1 \land \ldots \land P \ a_n \land \]

\[ C_1 \land \ldots \land C_m \land \]

\[ \{a_1, \ldots, a_n \} \subseteq X \implies P \ a \]

\[ \implies \]

\[ \forall x \in X. P \ x \]

Slide 13

X as Fixpoint

How to compute X?

\[ X = \cap \{B \subseteq A. B \ R \text{ - closed}\} \text{ hard to work with.} \]

Instead: view X as least fixpoint, X least set with \( \hat{R} X = X \).

Fixpoints can be approximated by iteration:

\[ X_0 = R^0 \{} = \{} \]

\[ X_1 = R^1 \{} = \text{rules without hypotheses} \]

\[ \vdots \]

\[ X_n = R^n \{} \]

\[ X_\omega = \bigcup_{n \in \mathbb{N}} (R^n \{}) = X \]

Slide 14

Generation from Below

\[ \hat{R} \{} \cup R^1 \{} \cup R^2 \{} \cup \ldots \]

Slide 15

DEMO: inductive definitions

Slide 16
We have seen today ...

- Sets in Isabelle
- Inductive Definitions
- Rule induction
- Fixpoints