Proofcraft

UNSW SYDNEY

COMP4161
Advanced Topics in Software Verification

{}

Gerwin Klein, June Andronick, Miki Tanaka, Johannes Åman Pohjola

T3/2022

Content

- ➜ Foundations & Principles
  - Intro, Lamb[illegible], natural deduction [1,2]
  - Higher Orde[illegible]r (part 1) [2,3[a]]
  - Term rewriti[illegible] [3,4]
- ➜ Proof & Specification Techniques
  - Inductively defined sets, rule induction [4,5]
  - Datatype induction, primitive recursion [5,7]
  - General recursive functions, termination proofs [7[b]]
  - Proof automation, Isar (part 2) [8]
  - Hoare logic, proofs about programs, invariants [8,9]
  - C verification [9,10]
  - Practice, questions, exam prep [10[c]]

---

[a] a1 due; [b] a2 due; [c] a3 due

Last Time

- Sets
- Type Definitions
- Inductive Definiti

Inductive Definitions

How They Work

The Nat Example

$$\frac{n \in N}{n + 1 \in N}$$

- N is the set of na[illegible]ers $\mathbb{N}$
- But why not the [illegible]numbers? $0 \in \mathbb{R}$, $n \in \mathbb{R} \Longrightarrow n + 1 \in \mathbb{R}$
- $\mathbb{N}$ is the **smallest** set that is **consistent** with the rules.

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)

Formally

Rules $\dfrac{a_1 \in X \quad \ldots \quad a_n \in X}{}$ with $a_1, \ldots, a_n, a \in A$

... set $X \subseteq A$

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

Applying rules R to a set B:
$\hat{R}\ B \equiv \{x.\ \exists H.\ (H, x) \in R \wedge H \subseteq B\}$

Example:

$$
\begin{aligned}
R &\equiv \{(\{\}, 0)\} \cup \{(\{n\}, n+1).\ n \in \mathbb{R}\} \\
\hat{R}\ \{3, 6, 10\} &= \{0, 4, 7, 11\}
\end{aligned}
$$

The Set

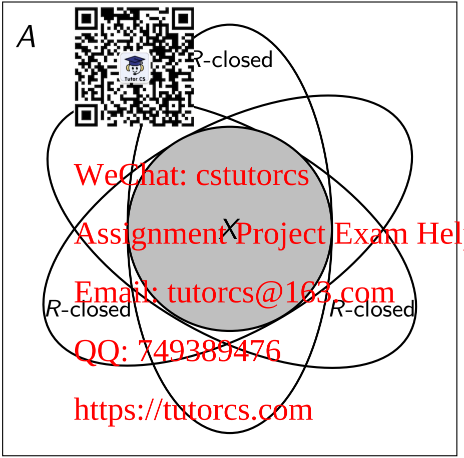
Definition: closed iff $\hat{R}\ B \subseteq B$

Definition: e least R-closed subset of A

This does always exist:

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

Generation from Above



Rule Induction

$$\frac{n \in N}{n + 1 \in N}$$

induces induction principle

$$[\![P\ 0;\ \bigwedge n.\ P\ n \Longrightarrow P\ (n+1)]\!] \Longrightarrow \forall x \in N.\ P\ x$$

In general:

$$\frac{\forall (\{a_1, \ldots a_n\}, a) \in R.\ P\ a_1 \wedge \ldots \wedge P\ a_n \Longrightarrow P\ a}{\forall x \in X.\ P\ x}$$

Why does this work?

$$\frac{\forall(\{a_1, \dots a_n\}, a) \in R.\ P\ a_1 \wedge \dots \wedge P\ a_n \Longrightarrow P\ a}{\forall x \in X.\ P\ x}$$

$$\forall(\{a_1, \dots a_n\}, a) \in R.\ P\ a_1 \wedge \dots \wedge P\ a_n \Longrightarrow P\ a$$

says

$\{x.\ P\ x\}$ is R-closed

but: X is the least R-closed set

hence: $X \subseteq \{x.\ P\ x\}$

which means: $\forall x \in X.\ P\ x$

qed

Rules with side conditions

$$\frac{a_1 \in X \quad \dots \quad a_n \in X \qquad C_1 \quad \dots \quad C_m}{a \in X}$$

Induction scheme:

$$\begin{array}{l} (\forall (\{a_1, \dots a_n\}, a) \in R.\ P\ a_1 \wedge \dots \wedge P\ a_n \wedge \\ \qquad C_1 \wedge \dots \wedge C_m \wedge \\ \qquad \{a_1, \dots, a_n\} \subseteq X \Longrightarrow P\ a) \\ \qquad \Longrightarrow \\ \qquad \forall x \in X.\ P\ x \end{array}$$

X as Fixpoint

How to compute X?

$X = \bigcap\{B \subseteq A.\ B\ R$ [illegible] hard to work with.

Instead: view X as l[illegible]int, X least set with $\hat{R}\ X = X$.

Fixpoints can be approximated by iteration:

$$X_0 = \hat{R}^0\ \{\} = \{\}$$

$$X_1 = \hat{R}^1\ \{\} = \text{rules without hypotheses}$$

$$\vdots$$

$$X_n = \hat{R}^n\ \{\}$$

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

Generation from Below

Does this always work?

Knaster-Tarski Fixpoint Theorem:
Let $(A, \leq)$ be a comp[illegible]e, and $f :: A \Rightarrow A$ a monotone function.
Then the fixpoints of [illegible] form a complete lattice.

Lattice:

Finite subsets have a greatest lower bound (meet) and least upper bound (join).

Complete Lattice:

All subsets have a greatest lower bound and least upper bound.

Implications:

- ➜ least and greatest fixpoints exist (complete lattice always non-empty).
- ➜ can be reached by (possibly infinite) iteration. (Why?)

Exercise

Formalize this lecture in Isabelle:

- Define **closed** f [illegible] $\Rightarrow \alpha$ set) $\Rightarrow \alpha$ set $\Rightarrow$ bool
- Show closed f A [illegible] $B \Longrightarrow$ closed f $(A \cap B)$ if f is monotone (**mono** is predefi[illegible]
- Define **lfpt** f as the intersection of all f-closed sets
- Show that lfpt f is a fixpoint of f if f is monotone
- Show that lfpt f is the least fixpoint of f
- Declare a constant R :: $(\alpha$ set $\times\, \alpha)$ set
- Define $\hat{R}$ :: α set $\Rightarrow \alpha$ set in terms of R
- Show soundness of rule induction using R and lfpt $\hat{R}$

We have learned today ...

- ➜ Formal backgrour tive definitions
- ➜ Definition by inte
- ➜ Computation by i
- ➜ Formalisation in Isabelle