UNSW SYDNEY

COMP4161
Advanced Topics in Software Verification

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

T3/2022

Content

➜ Foundations & Principles

- Intro, Lambda [illegible] atural deduction [1,2]
- Higher Order [illegible] part 1) [2,3[a]]
- Term rewriting [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 Definition

Inductive Definitions

How They Work

The Nat Example

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

The Nat Example

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

➜ N is the set of natu… s $\mathbb{N}$

The Nat Example

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

- ➜ N is the set of natu[illegible]s $\mathbb{N}$
- ➜ But why not the se[illegible]mbers? $0 \in \mathbb{R}$, $n \in \mathbb{R} \implies n+1 \in \mathbb{R}$

The Nat Example

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

- ➜ N is the set of natu[illegible]s $\mathbb{N}$
- ➜ But why not the se[illegible]mbers? $0 \in \mathbb{R}$, $n \in \mathbb{R} \implies n+1 \in \mathbb{R}$
- ➜ $\mathbb{N}$ is the **smallest** set that is **consistent** with the rules.

The Nat Example

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

- ➜ N is the set of natu[illegible]s $\mathbb{N}$
- ➜ But why not the se[illegible]mbers? $0 \in \mathbb{R}$, $n \in \mathbb{R} \implies n+1 \in \mathbb{R}$
- ➜ $\mathbb{N}$ is the **smallest** set that is **consistent** with the rules.

Why the smallest set?

The Nat Example

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

- ➜ N is the set of natu[illegible]s $\mathbb{N}$
- ➜ But why not the se[illegible]mbers? $0 \in \mathbb{R}$, $n \in \mathbb{R} \implies n+1 \in \mathbb{R}$
- ➜ $\mathbb{N}$ 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.

The Nat Example

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

- ➜ N is the set of natu[illegible]s $\mathbb{N}$
- ➜ But why not the se[illegible]mbers? $0 \in \mathbb{R}$, $n \in \mathbb{R} \implies n+1 \in \mathbb{R}$
- ➜ $\mathbb{N}$ 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 $\frac{a_1 \in X \quad \ldots \quad a_n \in X}{a \in X}$ with $a_1, \ldots, a_n, a \in A$

e set $X \subseteq A$

Formally:

Formally

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

e set $X \subseteq A$

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

Applying rules R to a set B:

Formally

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

e set $X \subseteq A$

Formally: set of rules $R \subseteq A$ 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:

Formally

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

e set $X \subseteq A$

Formally: set of rules $R \subseteq$? 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:

$$R \equiv \{(\{\}, 0)\} \cup \{(\{n\}, n+1).\ n \in \mathbb{R}\}$$

$\hat{R}\ \{3, 6, 10\} =$

Formally

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

e set $X \subseteq A$

Formally: set of rules $R \subseteq A$ 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:

$$R \equiv \{(\{\}, 0)\} \cup \{(\{n\}, n+1).\ n \in \mathbb{R}\}$$

$$\hat{R}\ \{3, 6, 10\} = \{0, 4, 7, 11\}$$

The Set

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

The Set

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

Definition e least R-closed subset of A

This does always exist:

The Set

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

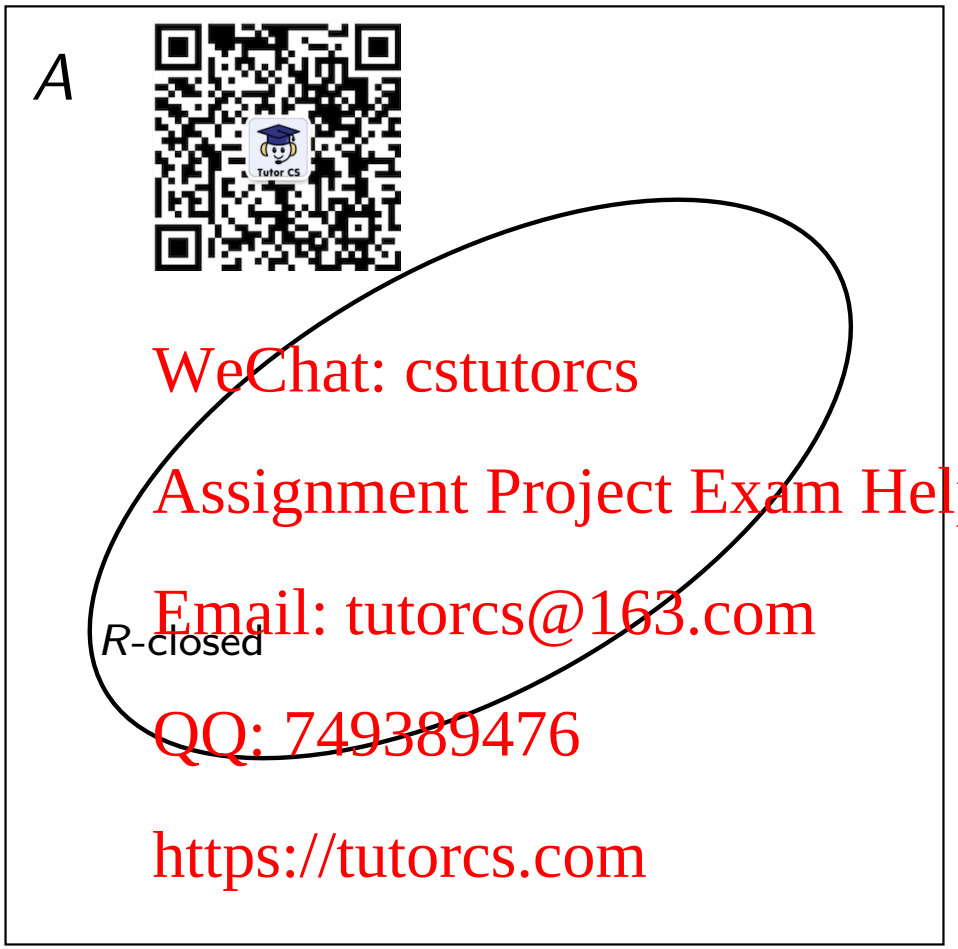
Definition $\hat{R}^*$ is the least R-closed subset of A

This does always exist:

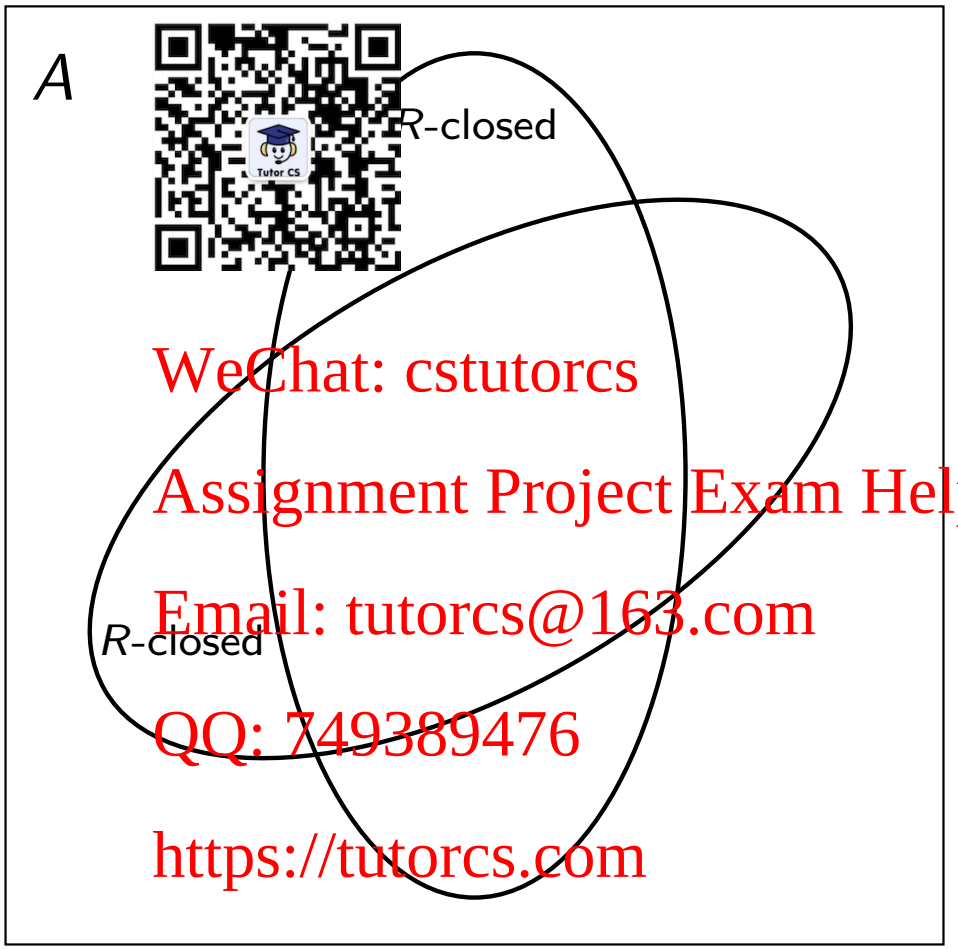
Fact: $X = \bigcap \{B \subseteq A.\ B \text{ is } R\text{-closed}\}$

Generation from Above

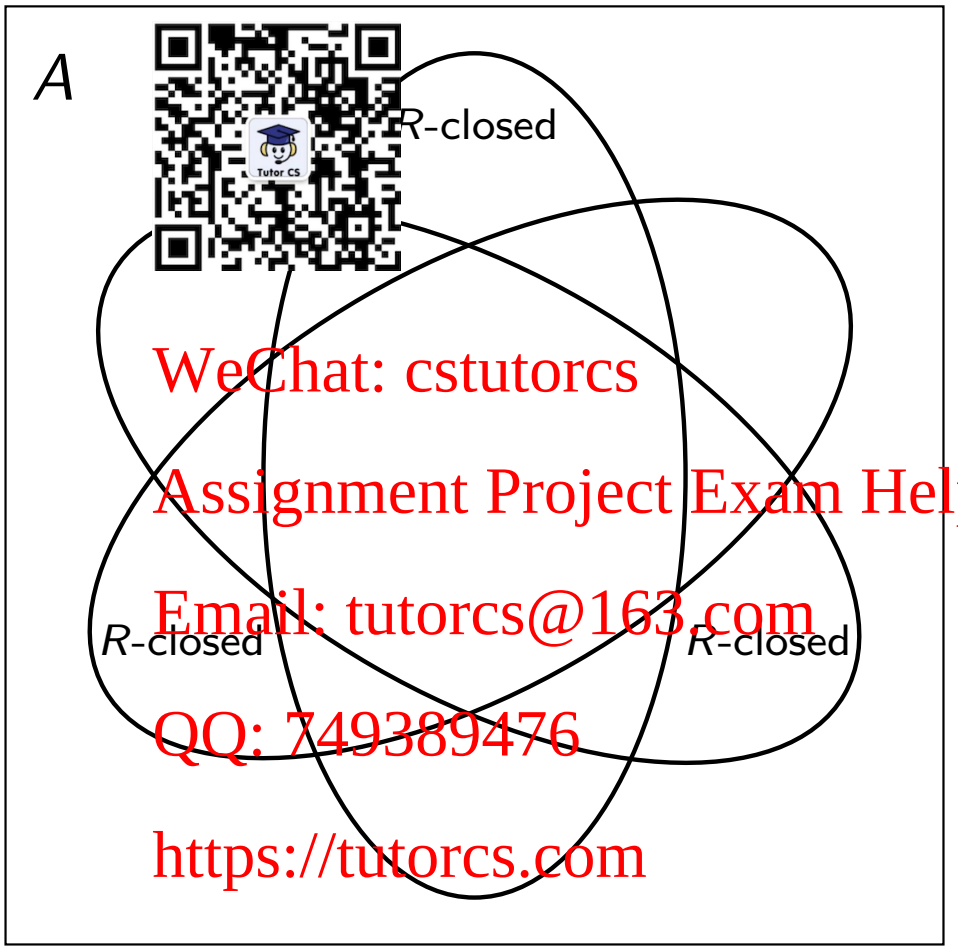
Generation from Above



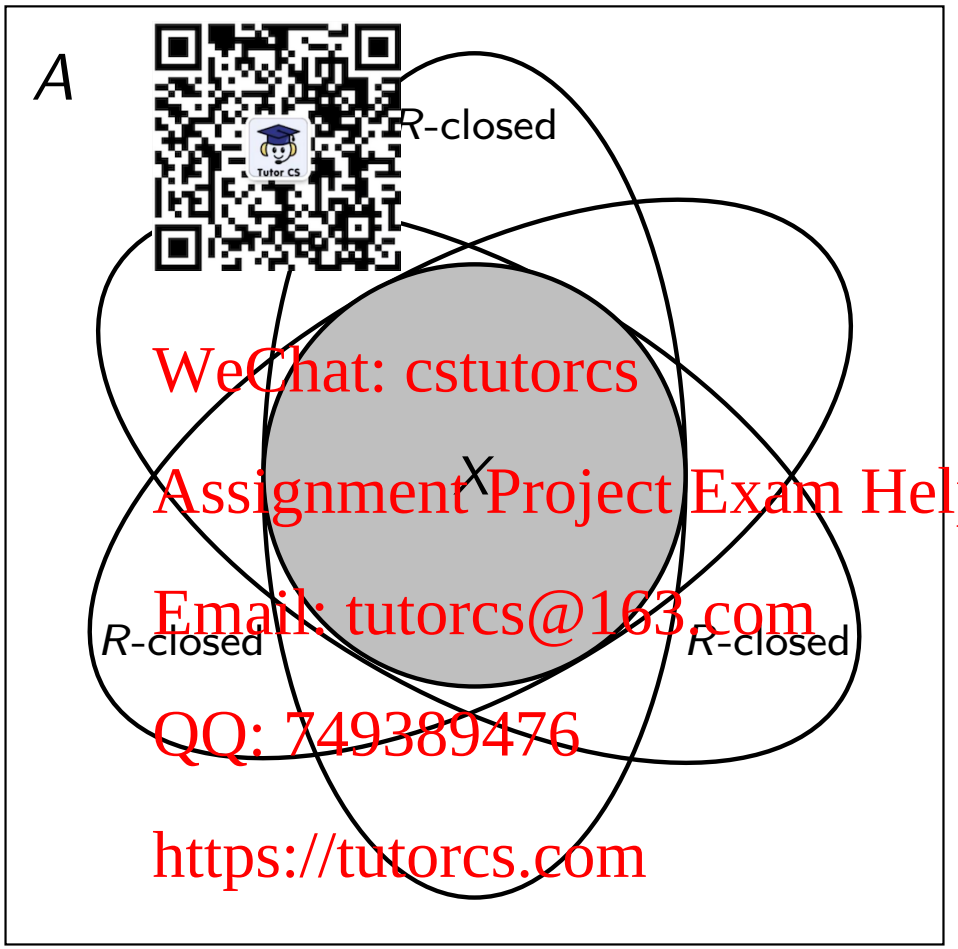
Generation from Above



Generation from Above



Generation from Above



Rule Induction

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

duction principle

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

Rule Induction

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

duction 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?

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

says

Why does this work?

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

says

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

but:

Why does this work?

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

says

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

but: X is the least R-closed set

hence:

Why does this work?

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

says

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

but: X is the least R-closed set

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

which means:

Why does this work?

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

says

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

but: X is the least R-closed set

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

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

Why does this work?

$$\frac{\forall(\{a_1, \ldots a_n\}, a) \in R.\ P\ a_1 \wedge \ldots \wedge P\ a_n \Longrightarrow P\ a}{\forall(\{a_1, \ldots a_n\}, a) \in R.\ P\ a_1 \wedge \ldots \wedge P\ a_n \Longrightarrow P\ a} \quad \text{says} \quad \{x.\ P\ x\} \text{ is } R\text{-closed}$$

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

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

Rules with side conditions

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

ion scheme:

$$(\forall(\{a_1, \ldots a_n\}, a) \in R.\ P\ a_1 \wedge \ldots \wedge P\ a_n \wedge C_1 \wedge \ldots \wedge C_m \wedge \{a_1, \ldots, a_n\} \subseteq X \Longrightarrow P\ a) \Longrightarrow \forall x \in X.\ P\ x$$

X as Fixpoint

How to compute X?

X as Fixpoint

How to compute X?

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

Instead:

X as Fixpoint

How to compute X?

$X = \bigcap\{B \subseteq A.\ B\ R -$ [redacted] rd to work with.

Instead: view X as lea[redacted], X least set with $\hat{R}\ X = X$.

X as Fixpoint

How to compute X?

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

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

Fixpoints can be approximated by iteration:

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

X as Fixpoint

How to compute X?

$X = \bigcap\{B \subseteq A.\ B\ R -$ ard to work with.

Instead: view X as lea , 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 as Fixpoint

How to compute X?

$X = \bigcap\{B \subseteq A.\ B\ R - $  rd to work with.

Instead: view X as lea , 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 as Fixpoint

How to compute X?

$X = \bigcap\{B \subseteq A.\ B\ R - $  ard to work with.

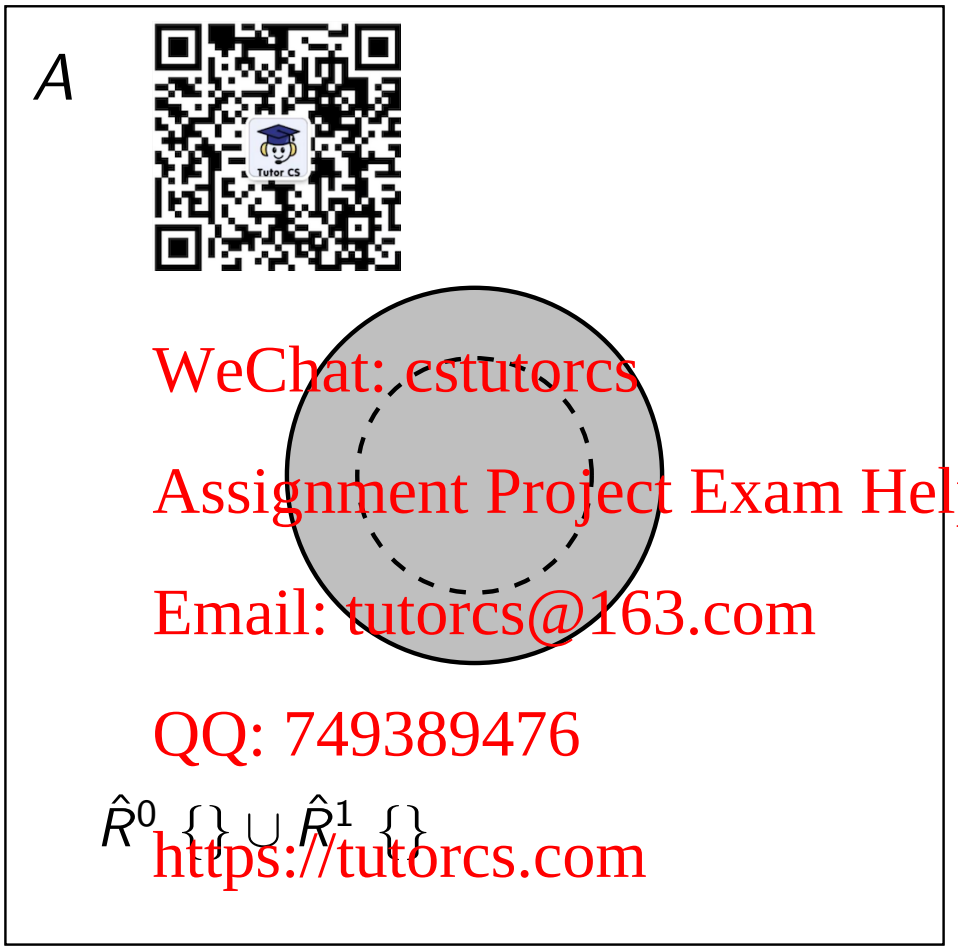
Instead: view X as lea , X least set with $\hat{R}\ X = X$.

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

Generation from Below



Generation from Below

Generation from Below

Does this always work?

Knaster-Tarski Fixpoint Theorem:

Let $(A, \leq)$ be a comple[redacted] and $f :: A \Rightarrow A$ a monotone function. Then the fixpoints of f[redacted] a complete lattice.

Does this always work?

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

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

Does this always work?

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

Does this always work?

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

Does this always work?

Knaster-Tarski Fixpoint Theorem:
Let $(A, \leq)$ be a complete lattice and $f :: A \Rightarrow A$ a monotone function.
Then the fixpoints of f again 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 A : (α set) $\Rightarrow$ α set $\Rightarrow$ bool
- Show closed f A $\wedge$ $\Longrightarrow$ closed f $(A \cap B)$ if f is monotone (**mono** is predefined)
- 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 :: (α set $\times$ α) set
- Define $\hat{R}$ :: α set $\Rightarrow$ α set in terms of R
- Show soundness of rule induction using R and lfpt $\hat{R}$

We have learned today ...

- ➜ Formal background [illegible] definitions
- ➜ Definition by inters[illegible]
- ➜ Computation by ite[illegible]
- ➜ Formalisation in Isabelle