Lecture 5 - January 24

Math Review

Logical Quantifications: Proof Strategies Exercises

Announcement

- Lab1 Part 2 tutorial videos released
  + ≈ 2 hours
    * $\boxed{\text{debugging}}$ using labels, error trace, state graph
    * PlusCal vs. Auto-Translated TLA+ Predicates
- Optional Textbook for Model Checking and Program Verification
  Logic in Computer Science:
  Modelling and reasoning about systems
  by M. Huth and M. Ryan

Logical Quantifiers: Examples

harder

How to prove $\forall i \bullet \boxed{R(i) \Rightarrow P(i)}$?

(1) Assume $R(\bar{i})$, prove $P(\bar{i})$

(2) Prove $\neg R(\bar{i})$ ($\approx$ empty array)

e.g. $R(\bar{i}) \triangleq \bar{i} < 0 \wedge \bar{i} > 10$

$\Rightarrow P(\bar{i})$

There's no two $\bar{i}$ satisfying disjoint ranges at the same time. F

How to prove $\exists i \bullet R(i) \wedge P(i)$?

(1) Find a witness s.t. $R(\bar{i}) \wedge P(\bar{i})$

How to disprove $\forall i \bullet R(i) \Rightarrow P(i)$?

(1) Give a witness/counter-example : $R(\bar{i}) \wedge \neg P(\bar{i})$

e.g. error trace

How to disprove $\exists i \bullet R(i) \wedge P(i)$?

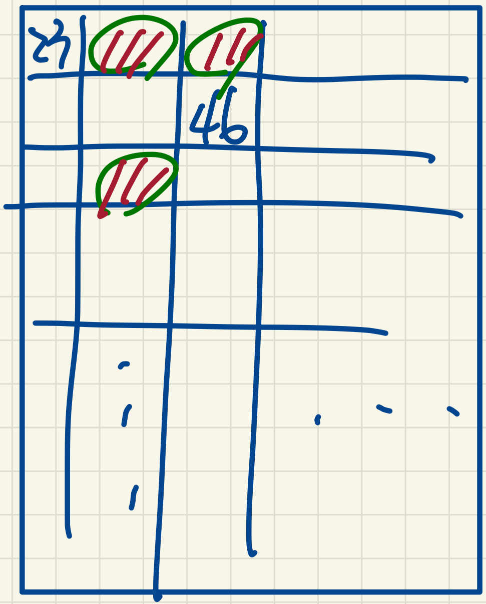
gives some context about $\bar{i}$, might be easier s.t. $P(\bar{i})$ might to be proved false

harder

(1) Show $\neg R(\bar{i})$ ($\approx$ empty array)

(2) $R(\bar{i}) \wedge \neg P(\bar{i}) \rightsquigarrow$ for all $\bar{i}$ satisfying R, they don't satisfy P

Sudoku



$$\underbrace{M}_{\text{model}} \overset{\text{satisfies}}{\models} \underbrace{\phi}_{\text{property}}$$

peg solitaire

$$M \overset{\text{defined as}}{\triangleq} \text{encoding}(\text{board})$$

rules of game

$$M \models \text{no solution}.$$

↳ failed → error trace

rep. the solution

a way to lead to a state

Prove/Disprove Logical Quantifications

- Prove or disprove: $\forall x \bullet \overset{R}{\boxed{(x \in \mathbb{Z} \land 1 \leq x \leq 10)}} \Rightarrow \overset{P}{x > 0}$.

R1 R2 R3 R4

$x \in 1..10$, each > 0

- Prove or disprove: $\forall x \bullet (x \in \mathbb{Z} \land 1 \leq x \leq 10) \Rightarrow x > 1$.

disprove: counter-example: 1

$\underline{1} \in \mathbb{Z} \land 1 \leq \underline{1} \leq 10 \Rightarrow \underline{1} > 1$

$T \Rightarrow F$

F.

- Prove ~~or disprove~~: $\exists x \bullet (x \in \mathbb{Z} \land 1 \leq x \leq 10) \land x > 1$.

witness : 2

- Prove or disprove that $\exists x \bullet (x \in \mathbb{Z} \land 1 \leq x \leq 10) \land x > 10$?

max value is 10 but $10 > 10$ F.

Is the following statement correct:

To

- Prove ~~or disprove~~: $\exists x \bullet (x \in \mathbb{Z} \wedge 1 \leq x \leq 10) \wedge x > 1.$

We can just give a witness $x = 1$.

Not correct! $\because$ $\exists$ is true but

$x = 1$ <u>not</u> a valid witness

$(1 > 1 \equiv F)$.

$$\exists x \cdot \underbrace{x \in \mathbb{Z} \wedge 1 \le x \le 10 \Rightarrow}\ x > 1$$

$$\equiv \quad \exists x \cdot \text{True} \wedge (\qquad\qquad)$$

$\text{True} \wedge P$

$\equiv P.$

Axioms.

$$\forall x \cdot P(x) \equiv \neg \exists x \cdot \neg P(x)$$

$$\exists x \cdot P(x) \equiv \neg \forall x \cdot \neg P(x).$$

Predicate Logic: Exercise 1

$\mathbb{N} = \{0, 1, \ldots, +\infty\}$

Consider the following predicate:

$$\forall x, y \bullet x \in \mathbb{N} \land y \in \mathbb{N} \Rightarrow x * y > 0$$

Choose **all** statements that are **correct**.

1. It is a theorem, provable by (5, 4).
2. It is a theorem, provable by (2, 3).
3. It is not a theorem, witnessed by (5, 0). $\boxed{5 \in \mathbb{N} \land 0 \in \mathbb{N}}$ T $\Rightarrow \boxed{5 * 0 > 0}$ F (F)
4. correct — It is not a theorem, witnessed by (12, −2). inappropriate witness
5. correct — It is not a theorem, $\boxed{\text{witnessed by (12, 13).}}$ (T) $\boxed{12 \in \mathbb{N} \land 13 \in \mathbb{N} \Rightarrow 12 * 13 > 0}$

F

$12 \in \mathbb{N} \land \boxed{-2 \in \mathbb{N}} \Rightarrow 12 * -2 > 0 \equiv$ T

Consider the following predicate:

$$\forall\, x, y \bullet x \in \mathbb{N} \land y \in \mathbb{N} \Rightarrow x * y \cancel{>} 0$$

$\geq$

Choose **all** statements that are **correct**.

x : 0, 1, 2, ..., $+\infty$

y : 0, 1, 2, ..., $+\infty$

Case 1 $\quad x > 0$, $y > 0 \Rightarrow x * y > 0$

$\Rightarrow x * y \geq 0$

Case 2 $\quad x \geq 0$, $y \geq 0$ if one or both is 0

$\Rightarrow x * y = 0 \Rightarrow x * y \geq 0$

- An axiom is assumed to be true, with no need for proofs.
- A theorem is a Boolean expression that requires a proof.

  ↳ lemma

    ↳ sub-theorems to help.

Predicate Logic: Exercise 2

Consider the following predicate:

$$\exists x, y \bullet x \in \mathbb{N} \wedge y \in \mathbb{N} \wedge x * y > 0$$

Choose **all** statements that are **correct**.

T.

$5 \in \mathbb{N} \wedge 4 \in \mathbb{N} \wedge 5 * 4 > 0$

1. It is a theorem, provable by (5, 4).
2. It is a theorem, provable by (2, 3).
3. X It is a theorem, provable by (-2, -3). not a valid witness: $\underbrace{(-2 \in \mathbb{N} \wedge -3 \in \mathbb{N})}_{F} \wedge \underbrace{(-2 * -3 > 0)}_{T}$
4. It is not a theorem, witnessed by (5, 0).
5. It is not a theorem, witnessed by (12, -2).
6. It is not a theorem, witnessed by (12, 13).

F.

Logical Quantifications: Conversions

$R(x)$: $x \in$ 4315_class

$P(x)$: x receives A+

$$\boxed{(\forall X \bullet R(X) \Rightarrow P(X))} \overset{\equiv}{\Leftrightarrow} \neg(\exists X \bullet R(X) \land \neg P(X))$$

Equational Style of Proof.

$\forall x \bullet \underbrace{\boxed{R(x) \Rightarrow P(x)}}_{Q(x)}$

$\equiv$ { Axiom: $\forall x \bullet Q(x) \equiv \neg(\exists x \bullet \neg Q(x))$ }

$\neg(\exists x \bullet \neg(R(x) \Rightarrow P(x)))$

$\equiv$ { Known: $p \Rightarrow q \equiv \neg p \lor q$ }

$\neg(\exists x \bullet \neg(\neg R(x) \lor P(x)))$

$\equiv$ { de Morgan: $\neg(p \lor q) \equiv \neg p \land \neg q$ }

$\neg(\exists x \bullet \neg\neg R(x) \land \neg P(x))$

$\equiv$ { double negation: $\neg\neg p \equiv p$ }

$\neg(\exists x \bullet R(x) \land \neg P(x))$

$$(\exists X \bullet R(X) \land P(X)) \Leftrightarrow \neg(\forall X \bullet R(X) \Rightarrow \neg P(X))$$

De Morgan