

Lecture 5 - January 20

Math Review

Formulating the Model Checking Problem
Describing Implications
Theorems of Propositional Logic

Announcements/Reminders

- **Lab 1** due this Thursday (Jan 23)
- **TA contact information** (on-demand for labs) on eClass
- Office Hours: 3pm to 4pm, Mon/Tue/Wed/Thu

Model Checking Problem


(1) Given module m and some invariant property P :

$$\forall s. s \in \boxed{RG(m)} \Rightarrow P(s)$$

↓
all reachable
states of
the system being
modeled.

(We don't care about unreachable state.) witness of inv. violation

(2) When there's a counter-example: $\exists s. s \in RG(m) \wedge \boxed{\neg P(s)}$

Counter trace \xrightarrow{init} 

$a.length == 10$ $(11) \rightarrow$ SE will not eval. $a[i]$

(1) $i < a.length$ $\&\&$ $a[i] \geq 10$ $\&\&$ $\boxed{i \geq 0}$ ⁻¹

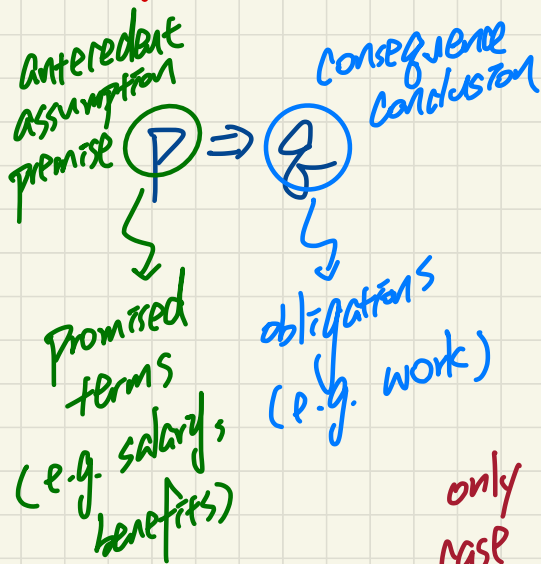
⁻¹
(2) $i \geq 0$ $\&\&$ $a[i] \geq 10$ $\&\&$ $i < a.length$ ¹¹

(A1) Neither (1) nor (2) works all the time.

(A2) For (1), $i \geq 0$ checked too late. e.g. $i == -1$ will trigger AIOBE.

For (2), $i < a.length$ checked too late e.g. $i == 11$ will trigger AIOBE.

Implication \approx Whether a Contract is Honoured



$P \Rightarrow Q$ true if the contract is not breached honoured

only case where \Rightarrow is true non-trivially

(C1) $P = \textcircled{T}$ $Q = \textcircled{T}$

(C2) $P = \textcircled{T}$ $Q = \textcircled{F}$

(C3) $P = \textcircled{F}$ $Q = \textcircled{T}$

(C4) $P = \textcircled{F}$ $Q = \textcircled{F}$

$P \Rightarrow Q$
 \textcircled{T}

\textcircled{F}

\textcircled{T}

only case where \Rightarrow is false

Describing $p \Rightarrow q$

p: snow storm
q: cancel class

enumerates the two scenarios for $p \Rightarrow q$ to be true
 ① p is true and q is true
 ② p is false (so $p = \text{false}$)

q if p, p is sufficient for q

q unless $\neg p$

p	q	$p \Rightarrow q$
true	true	true
true	false	false
false	true	true
false	false	true

given that p is true , q is also true
 p is true but q does not follow that, so \Rightarrow is false

p	q	$p \Rightarrow q$
true	true	true
true	false	false
false	true	true
false	false	true

$\neg q \wedge p$

$$p \Rightarrow q \equiv \neg p \vee q$$

p only if q, q is necessary for p

p	q	$p \Rightarrow q$
true	true	true
true	false	false
false	true	true
false	false	true

knowing that p is true, the only way to make $p \Rightarrow q$ true is when q is true as well.

when p is not true , don't care what q is.

Q. Which of the following expressions
are equivalent to $p \Rightarrow q$

☒ $q \not\equiv p$

☐ $q \text{ only if } p \rightarrow q \Rightarrow p$

To Prove

$$P \stackrel{\text{if}}{\iff} Q \stackrel{\text{only if}}{\iff} Q$$

Need to prove

$$(1) P \leq Q$$

\hookrightarrow

$$\underline{Q \Rightarrow P}$$

$$(2) \underline{P \Rightarrow Q}$$

$$P \stackrel{\text{if}}{\iff} Q$$

$$P \stackrel{\text{only if}}{\iff} Q$$

Example: Inverse, Converse, Contrapositive

De Morgan

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$

$$x > 0 \wedge x \leq 23 \Rightarrow y \geq 23 \vee y < 46$$

Contrapositive

$$p \Rightarrow q \equiv$$

$$\neg q \Rightarrow \neg p$$

Inverse

equational
style
proofs

$$\neg(x > 0 \wedge x \leq 23) \Rightarrow \neg(y \geq 23 \vee y < 46)$$

$$\equiv \{ \text{De Morgan} \}$$

justification

$$x \leq 0 \vee x > 23 \Rightarrow y < 23 \wedge y \geq 46$$

Converse

$$y \geq 23 \vee y < 46 \Rightarrow x > 0 \wedge x \leq 23$$

Contrapositive: converse of inverse

$$y < 23 \wedge y \geq 46 \Rightarrow x \leq 0 \vee x > 23$$

Identity

$$\underline{0} + a = a$$
$$\underline{1} \times a = a$$

Precedence

\neg

\wedge

\vee

\Rightarrow

\equiv

$$\boxed{\neg p \wedge q} \vee r$$

$$\underline{1} \Rightarrow p \equiv p$$

$$\underline{1} \wedge p \equiv p$$

$$\underline{1} \vee p \equiv p$$

Zero

$$\underline{0} \Rightarrow p \equiv \underline{1}$$

$$\underline{0} \wedge p \equiv \underline{0}$$

$$\underline{0} \vee p \equiv p$$

When the zero of \Rightarrow is the antecedent, the value of consequent is fixed.

logical basis of short circuit evaluation.

\mathbb{N}

non-negative

natural numbers

$\hookrightarrow 0, 1, 2, 3, \dots$

\mathbb{Z}

integers

$-\infty, \dots, 0, \dots, +\infty$

Prodr

$$\forall x : R(x) \Rightarrow P(x)$$

$$\nexists x : R(x) \wedge P(x)$$

\exists

TLA+ / PlusCal

Range.

$$\forall (x \in \text{Nat} \rightarrow y \in \text{Int} \Rightarrow P(x))$$

$$\exists x \in \text{Nat}, y \in \text{Int} \wedge P(x)$$