Week 11 Tutorial

Assignment Preparation; Compactness & Completeness; Hoare Triples

Joe Scott / Jan Gorzny

Prepared based off of the notes of CS245 Instructors, past and present.

17 March 2017

Plan

1. Assignment Preparation
2. Completeness and Compactness
3. Hoare Logic
   - Assignment and Implied Inference Rules
4. The End

Problem 1

Problem

Disprove $\{(\exists x\ P(x)), (\forall x\ (P(x) \to Q(x)))\} \vdash (\forall y Q(y))$

Problem 1

Problem

Disprove $\{(\exists x\ P(x)), (\forall x\ (P(x) \to Q(x)))\} \vdash (\forall y Q(y))$

$dom(\mathcal{I}) = \{a, b\}$
$P = \{(a)\}$
$Q = \{(a)\}$

Problem 2

Problem

Disprove $\{((\forall x\ P(x)) \to (\forall x\ Q(x)))\} \vdash (\forall x(P(x) \to Q(x)))$*: show an unsatisfied interpretation*

Problem 2

Problem

Disprove $\{((\forall x \; P(x)) \rightarrow (\forall x \; Q(x)))\} \vdash (\forall x (P(x) \rightarrow Q(x)))$*: show an unsatisfied interpretation*

false...

Problem 2

Problem

Disprove $\{((\forall x\ P(x)) \to (\forall x\ Q(x)))\} \vdash (\forall x(P(x) \to Q(x)))$*: show an unsatisfied interpretation*

false... Consider $\mathcal{I}$ as

$dom(\mathcal{I}) = \{a, b\}$

$P = \{(a)\}$

$Q = \{\}$

Problem 3

Problem

Disprove $\{((\exists x \; P(x)) \rightarrow (\exists x \; Q(x)))\} \vdash (\forall x(P(x) \rightarrow Q(x)))$*: show an unsatisfied interpretation*

Problem 3

Problem

Disprove $\{((\exists x\ P(x)) \to (\exists x\ Q(x)))\} \vdash (\forall x(P(x) \to Q(x)))$*: show an unsatisfied interpretation*

false...

Problem

Disprove $\{((\exists x\ P(x)) \rightarrow (\exists x\ Q(x)))\} \vdash (\forall x (P(x) \rightarrow Q(x)))$*: show an unsatisfied interpretation*

false... Consider $\mathcal{I}$ as

$dom(\mathcal{I}) = \{a, b\}$

$P = \{(a)\}$

$Q = \{b\}$

Problem 4

Problem

Disprove $\{((\exists x \; P(x)) \wedge (\exists x \; Q(x)))\} \vdash (\exists x(P(x) \wedge Q(x)))$*: show an unsatisfied interpretation*

Problem 4

Problem

Disprove $\{((\exists x\ P(x)) \wedge (\exists x\ Q(x)))\} \vdash (\exists x(P(x) \wedge Q(x)))$*: show an unsatisfied interpretation*

its false..

Problem 4

Problem

Disprove $\{((\exists x\ P(x)) \wedge (\exists x\ Q(x)))\} \vdash (\exists x(P(x) \wedge Q(x)))$*: show an unsatisfied interpretation*

its false.. Consider $\mathcal{I}$ as

$dom(\mathcal{I}) = \{a, b\}$

$P = \{(a)\}$

$Q = \{(b)\}$

Plan

Interpretations

Definition

A sentence ψ is true in an interpretation $\mathcal{I}$, denoted $\mathcal{I} \vDash \psi$, if for every possible sequence of elements in the interpretation, substituting these elements into the variables present in ψ yields a true sentence. Such an interpretation $\mathcal{I}$ is called a satisfying interpretation.

Completeness

Theorem (Godel's Completeness Theorem)

Let Σ be a set of formulas. If Σ is consistent, then it has a satisfying interpretation.

Completeness

Theorem (Godel's Completeness Theorem)

Let Σ be a set of formulas. If Σ is consistent, then it has a satisfying interpretation.

Theorem (Godel's Completeness Theorem - Contrapositive)

If Σ does not have a satisfying interpretation, then Σ is not consistent.

Compactness

Theorem (Compactness Theorem)

A set of sentences Σ has a satisfying interpretation if and only if every finite set of Σ has a satisfying interpretation.

Proof: $\leftarrow$: If Σ has a satisfying interpretation, then every finite subset of Σ has a satisfying interpretation (take the elements of the satisfying interpretation that are used in the finite subset).

Compactness

Theorem (Compactness Theorem)

A set of sentences Σ has a satisfying interpretation if and only if every finite set of Σ has a satisfying interpretation.

Proof: $\leftarrow$: If Σ has a satisfying interpretation, then every finite subset of Σ has a satisfying interpretation (take the elements of the satisfying interpretation that are used in the finite subset).

$\rightarrow$: Suppose to the contrary that every finite subset of Σ has a satisfying interpretation but Σ does not have a satisfying interpretation.
Then by the contrapositive of the Completeness Theorem, Σ is inconsistent.

Compactness

Theorem (Compactness Theorem)

A set of sentences Σ has a satisfying interpretation if and only if every finite set of Σ has a satisfying interpretation.

Proof: $\leftarrow$: If Σ has a satisfying interpretation, then every finite subset of Σ has a satisfying interpretation (take the elements of the satisfying interpretation that are used in the finite subset).

$\rightarrow$: Suppose to the contrary that every finite subset of Σ has a satisfying interpretation but Σ does not have a satisfying interpretation.
Then by the contrapositive of the Completeness Theorem, Σ is inconsistent.

There is a sentence ψ such that $\Sigma \vdash \psi$ and $\Sigma \vdash \neg\psi$.

Compactness

Theorem (Compactness Theorem)

A set of sentences Σ has a satisfying interpretation if and only if every finite set of Σ has a satisfying interpretation.

Proof: $\leftarrow$: If Σ has a satisfying interpretation, then every finite subset of Σ has a satisfying interpretation (take the elements of the satisfying interpretation that are used in the finite subset).

$\rightarrow$: Suppose to the contrary that every finite subset of Σ has a satisfying interpretation but Σ does not have a satisfying interpretation.
Then by the contrapositive of the Completeness Theorem, Σ is inconsistent.

There is a sentence ψ such that $\Sigma \vdash \psi$ and $\Sigma \vdash \neg\psi$.

Each of these derivations is finite.

Compactness Proof - Continued

Let $\Sigma' \subseteq \Sigma$ be the sentences involved in $\Sigma \vdash \psi$ and $\Sigma'' \subseteq \Sigma$ be the sentences involved in $\Sigma \vdash \neg\psi$.

Compactness Proof - Continued

Let $\Sigma' \subseteq \Sigma$ be the sentences involved in $\Sigma \vdash \psi$ and $\Sigma'' \subseteq \Sigma$ be the sentences involved in $\Sigma \vdash \neg\psi$.

Each of Σ', Σ'' is finite; therefore $\Sigma' \cup \Sigma''$ is finite.

Compactness Proof - Continued

Let $\Sigma' \subseteq \Sigma$ be the sentences involved in $\Sigma \vdash \psi$ and $\Sigma'' \subseteq \Sigma$ be the sentences involved in $\Sigma \vdash \neg\psi$.

Each of Σ', Σ'' is finite; therefore $\Sigma' \cup \Sigma''$ is finite.

Furthermore, $\Sigma' \cup \Sigma'' \vdash \psi$ and $\Sigma' \cup \Sigma'' \vdash \neg\psi$.

Compactness Proof - Continued

Let $\Sigma' \subseteq \Sigma$ be the sentences involved in $\Sigma \vdash \psi$ and $\Sigma'' \subseteq \Sigma$ be the sentences involved in $\Sigma \vdash \neg\psi$.

Each of Σ', Σ'' is finite; therefore $\Sigma' \cup \Sigma''$ is finite.

Furthermore, $\Sigma' \cup \Sigma'' \vdash \psi$ and $\Sigma' \cup \Sigma'' \vdash \neg\psi$.

Therefore, $\Sigma' \cup \Sigma''$ is inconsistent. Therefore it has no satisfying interpretation.

Compactness Proof - Continued

Let $\Sigma' \subseteq \Sigma$ be the sentences involved in $\Sigma \vdash \psi$ and $\Sigma'' \subseteq \Sigma$ be the sentences involved in $\Sigma \vdash \neg\psi$.

Each of Σ', Σ'' is finite; therefore $\Sigma' \cup \Sigma''$ is finite.

Furthermore, $\Sigma' \cup \Sigma'' \vdash \psi$ and $\Sigma' \cup \Sigma'' \vdash \neg\psi$.

Therefore, $\Sigma' \cup \Sigma''$ is inconsistent. Therefore it has no satisfying interpretation.

But we assumed that every finite set of Σ has a satisfying interpretation. So we have a contradiction and we're done.

Lowenheim-Skolem Theorem

Theorem

Let A be a sentence of first-order logic such that for any $n \in \mathbb{N}$, $n \geq 1$, there is a domain D and valuation v with at least n elements in D, such that $A^v = 1$. Then A has a domain D' and a valuation v' such that $A^{v'} = 1$ and D' has an infinite number of elements.

Lowenheim-Skolem Theorem

Theorem

Let A be a sentence of first-order logic such that for any $n \in \mathbb{N}$, $n \geq 1$, there is a domain D and valuation v with at least n elements in D, such that $A^v = 1$. Then A has a domain D' and a valuation v' such that $A^{v'} = 1$ and D' has an infinite number of elements.

Proof: For each n, consider the formula

$$B_n : \exists x_1, \ldots, x_n \bigwedge_{1 \leq i < j \leq n} \neg(x_i \approx x_j)$$

Lowenheim-Skolem Theorem

Theorem

Let A be a sentence of first-order logic such that for any $n \in \mathbb{N}$, $n \geq 1$, there is a domain D and valuation v with at least n elements in D, such that $A^v = 1$. Then A has a domain D' and a valuation v' such that $A^{v'} = 1$ and D' has an infinite number of elements.

Proof: For each n, consider the formula

$$B_n : \exists x_1, \ldots, x_n \bigwedge_{1 \leq i < j \leq n} \neg(x_i \approx x_j)$$

Each B_n expresses that a domain satisfying B_n has at least n elements.

Lowenheim-Skolem Theorem

Theorem

Let A be a sentence of first-order logic such that for any $n \in \mathbb{N}$, $n \geq 1$, there is a domain D and valuation v with at least n elements in D, such that $A^v = 1$. Then A has a domain D' and a valuation v' such that $A^{v'} = 1$ and D' has an infinite number of elements.

Proof: For each n, consider the formula

$$B_n : \exists x_1, \dots, x_n \bigwedge_{1 \leq i < j \leq n} \neg(x_i \approx x_j)$$

Each B_n expresses that a domain satisfying B_n has at least n elements.

Let $\Gamma = \{A\} \cup \{B_n | n \geq 1\}$.

Lowenheim-Skolem Theorem - Proof Continued

Let $\Gamma = \{A\} \cup \{B_n | n \geq 1\}$.
Suppose Δ is a finite subset of Γ.

Lowenheim-Skolem Theorem - Proof Continued

Let $\Gamma = \{A\} \cup \{B_n | n \geq 1\}$.
Suppose Δ is a finite subset of Γ.

Consider $k \geq 1$ and $n \leq k$ for all $B_n \in \Delta$.
Since Δ is a finite set, there is some such k.

Lowenheim-Skolem Theorem - Proof Continued

Let $\Gamma = \{A\} \cup \{B_n | n \geq 1\}$.
Suppose Δ is a finite subset of Γ.

Consider $k \geq 1$ and $n \leq k$ for all $B_n \in \Delta$.
Since Δ is a finite set, there is some such k.

By assumption, $\{A, B_k\}$ is satisfiable. Since $B_k \rightarrow B_n$ for all $n \leq k$, Δ is satisfiable.

Lowenheim-Skolem Theorem - Proof Continued

Let $\Gamma = \{A\} \cup \{B_n | n \geq 1\}$.
Suppose Δ is a finite subset of Γ.

Consider $k \geq 1$ and $n \leq k$ for all $B_n \in \Delta$.
Since Δ is a finite set, there is some such k.

By assumption, $\{A, B_k\}$ is satisfiable. Since $B_k \to B_n$ for all $n \leq k$, Δ is satisfiable.

By the compactness theorem, we must have Γ is satisfiable. (every k is finite, and every finite set satisfiable $\implies$ entire formula is satisfiable).

Lowenheim-Skolem Theorem - Proof Continued

Let $\Gamma = \{A\} \cup \{B_n | n \geq 1\}$.
Suppose Δ is a finite subset of Γ.

Consider $k \geq 1$ and $n \leq k$ for all $B_n \in \Delta$.
Since Δ is a finite set, there is some such k.

By assumption, $\{A, B_k\}$ is satisfiable. Since $B_k \to B_n$ for all $n \leq k$, Δ is satisfiable.

By the compactness theorem, we must have Γ is satisfiable. (every k is finite, and every finite set satisfiable $\implies$ entire formula is satisfiable).

That is, there some D' and v' such that $\Gamma^{v'} = 1$. But Γ is infinite; so D' cannot have a finite number of elements.

Plan

Hoare Triple

Assertions of programs take the following form:

1. $(\!|P|\!)$ - a precondition
2. C - a program
3. $(\!|Q|\!)$ - a post condition

That is if a program C satisfies $(\!|P|\!)$ then upon execution, C will satisfy $(\!|Q|\!)$

This is a Hoare Triple.

Proving Correctness

1. $(\!|Assertion|\!)$, precondition
2. Some Code
3. $(\!|ClaimaboutProgram|\!)$, Inference Rule Used
4. More Code
5. $(\!|AnotherClaim|\!)$, Inference Rule
6. More Code
7. ....
8. End Code
9. $(\!|Specification|\!)$, Inference Rule

Correctness

Your proof is partial correct if the proof is valid. Your proof is total correct if the proof is valid and it terminates.

You can not always prove if a program terminates or if it hangs. (The Halting Problem)

Outline

The Assignment Inference Rule

$$
\begin{array}{l|l}
1 & \varnothing \\
\hline
2 & (\!|Q[E/x]|\!)\, x = E\, (\!|Q|\!)
\end{array}
$$

1. $(\!|y = 2|\!)\, x = y\, (\!|x = 2|\!)$
2. $(\!|0 \leq 2|\!)\, x = y\, (\!|x \leq 2|\!)$
3. $(\!|y + 1 = 7|\!)\, x = y + 1\, (\!|x = 7|\!)$

Inference rules of Implication

Precondition Strengthening

$$\begin{array}{l|l} 1 & P \implies P', \quad (\!|P'|\!)\, C\, (\!|Q|\!) \\ \hline 2 & (\!|P|\!)\ C\ (\!|Q|\!) \end{array}$$

Postcondition Weakening

$$\begin{array}{l|l} 1 & Q' \implies Q, \quad (\!|P|\!)\, C\, (\!|Q|\!) \\ \hline 2 & (\!|P|\!)\ C\ (\!|Q'|\!) \end{array}$$

Problem 1

Problem

Prove the partial or total correctness of the following Hoare triple:

1. $(\!|x = n|\!)$
2. $\mathtt{x = x + 1;}$
3. $(\!|x = n + 1|\!)$

Problem 1

Problem

Prove the partial or total correctness of the following Hoare triple:

1. $(\!|x = n|\!)$
2. x = x + 1;
3. $(\!|x = n + 1|\!)$

Consider $f(z) = z + 1$. By eqsubs, $((x = n) \rightarrow (x + 1 = n + 1))$

Problem 1

Problem

Prove the partial or total correctness of the following Hoare triple:

1. $(\!|x = n|\!)$
2. x = x + 1;
3. $(\!|x = n + 1|\!)$

Consider $f(z) = z + 1$. By eqsubs, $((x = n) \rightarrow (x + 1 = n + 1))$

1. $(\!|x = n|\!)$

Problem 1

Problem

Prove the partial or total correctness of the following Hoare triple:

1. $(\!|x = n|\!)$
2. x = x + 1;
3. $(\!|x = n + 1|\!)$

Consider $f(z) = z + 1$. By eqsubs, $((x = n) \rightarrow (x + 1 = n + 1))$

1. $(\!|x = n|\!)$
2. $(\!|x + 1 = n + 1|\!)$ Assignment, Implied

Problem 1

Problem

Prove the partial or total correctness of the following Hoare triple:

1. $(\!|x = n|\!)$
2. x = x + 1;
3. $(\!|x = n + 1|\!)$

Consider $f(z) = z + 1$. By eqsubs, $((x = n) \rightarrow (x + 1 = n + 1))$

1. $(\!|x = n|\!)$
2. $(\!|x + 1 = n + 1|\!)$ Assignment, Implied
3. x = x + 1;

Problem 1

Problem

Prove the partial or total correctness of the following Hoare triple:

1. $(\!| x = n |\!)$
2. x = x + 1;
3. $(\!| x = n + 1 |\!)$

Consider $f(z) = z + 1$. By eqsubs, $((x = n) \to (x + 1 = n + 1))$

1. $(\!| x = n |\!)$
2. $(\!| x + 1 = n + 1 |\!)$ Assignment, Implied
3. x = x + 1;
4. $(\!| x = n + 1 |\!)$ Assignment

Problem 2

Find a precondition, such that the following Hoare triple is satisfied under total correctness:

1. $(\!|??????????|\!)$
2. $\mathrm{x} = \mathrm{x} + 1;$
3. $\mathrm{y} = \mathrm{y} + 2;$
4. $(\!|(x = y)|\!)$

Problem 2

Find a precondition, such that the following Hoare triple is satisfied under total correctness:

1. $(\!|???????????|\!)$
2. x = x + 1;
3. y = y + 2;
4. $(\!|(x = y)|\!)$

Lets try $(\!|x + 1 = y + 2|\!)$

Problem 2

Find a precondition, such that the following Hoare triple is satisfied under total correctness:

1. $(\!|x + 1 = y + 2|\!)$
2. x = x + 1;
3. y = y + 2;
4. $(\!|(x = y)|\!)$

Now let's prove it.

Problem 2

Find a precondition, such that the following Hoare triple is satisfied under total correctness:

1. $(\!| x + 1 = y + 2 |\!)$
2. x = x + 1;
3. y = y + 2;
4. $(\!| (x = y) |\!)$

Now let's prove it.

1. $(\!| x + 1 = y + 2 |\!)$

Problem 2

Find a precondition, such that the following Hoare triple is satisfied under total correctness:

1. $(\!|x + 1 = y + 2|\!)$
2. x = x + 1;
3. y = y + 2;
4. $(\!|(x = y)|\!)$

Now let's prove it.

1. $(\!|x + 1 = y + 2|\!)$
2. x = x + 1;
3. $(\!|x = y + 2|\!)$ Assignment

Problem 2

Find a precondition, such that the following Hoare triple is satisfied under total correctness:

1. $(\!|x + 1 = y + 2|\!)$
2. x = x + 1;
3. y = y + 2;
4. $(\!|(x = y)|\!)$

Now let's prove it.

1. $(\!|x + 1 = y + 2|\!)$
2. x = x + 1;
3. $(\!|x = y + 2|\!)$ Assignment
4. y = y + 2;
5. $(\!|(x = y)|\!)$ Assignment

Problem 2

Find a precondition, such that the following Hoare triple is satisfied under total correctness:

1. $(\!|x + 1 = y + 2|\!)$
2. x = x + 1;
3. y = y + 2;
4. $(\!|(x = y)|\!)$

Now let's prove it.

1. $(\!|x + 1 = y + 2|\!)$
2. x = x + 1;
3. $(\!|x = y + 2|\!)$ Assignment
4. y = y + 2;
5. $(\!|(x = y)|\!)$ Assignment

Plan

The end

Thats it folks. Feel free to hang out and ask questions.

These slides are based off of the tutorial notes and lecture slides provided to you online.
If you want a copy feel free to email me. The are also available on my personal website joe-scott.net

IA Email:

IA	email
Jan Gorzny	jgorzny
Joe Scott	j29scott

Jan and Joe have an office hour Mondays at 3pm in the Tutorial Center in MC.

Instructor Office Hours:

Instructor	Time	Room	Email
Trefler	Tue, Thur 4:00pm	DC 2336	trefler
Rahkooy	Tue, Thur 4:00pm	DC 2302B	hamid.rahkooy