17 Axiomatic Semantics

Monday, April 22, 2024 12:27 PM

- Hoare Logic

  '69 C.A.R Hoare
  "Tony"

What?: A Formal system of Logic Rules
to reason rigurously about programs

Formal = Mathematical.

Objectives: • Give Meaning to program.
• Prove that a program has certain properties
• Prove correctness of a program

Dijksta, Wirth, Knuth agree

program is a complex mathematical object.

- REVIEW of Mathematical Logic

  Logic: - the mathematics of correct reasoning.
  - "true" - "false"
  - Evaluate sentences / formulas to know whether they are true or false

  - PROPOSITIONAL LOGIC (Boolean Logic)

    - Propositions:
      p q r s

      Propositions are assigned true/false.

      p = true
      q = false
      ⋮

- **Logical Connectives**

  $\wedge \quad \vee \quad \neg \quad \rightarrow$

  the meaning of logical connectives is stated via truth tables:

p	$\neg p$
T	F
F	T

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

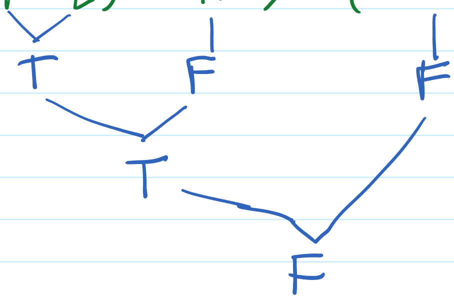
p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

- **Propositional Formulas**

  are evaluated.

$$\boxed{\begin{array}{l} p = T \\ q = F \\ r = T \end{array}}$$

$$((p \vee q) \vee \neg r) \wedge (r \rightarrow q) = F$$



- **Inference Rules.**

  rules of pre-evaluated formulas

Premises → $\dfrac{S_2 \quad S_2 \quad S_3 \ldots S_k}{C_0}$ ← Conclusion

If all S_i are true then C_0 is true.

e.g. $\dfrac{p \wedge q}{p}$ $\qquad \dfrac{p \rightarrow q \quad p}{q}$ $\qquad \dfrac{}{p \vee \neg p}$

modus ponnens

Limitations of propositional Logic:

"All men are mortal, Aristotle is a man therefore Aristotle is mortal"

- PREDICATE LOGIC
  - Objects

    a   b   aristotle

    1   7   garfield

1 7 garfield

- Variables over objects
  X Y Z

- predicates.
  - represent properties or relationships between objects
  - have an "arity": fixed number of arguments

red(a) man(aristotle)

odd(7)

lessthan(1,7) even(X)

$1 < 7$ red(Y)

friend(aristole, Z)

$\left.\begin{array}{l}\text{even}(X)\\ \text{red}(Y)\\ \text{friend}(\text{aristole}, Z)\end{array}\right\}$ variables in predicates

"Ground" Predicates (those without variables) can be assigned True/False.

man(aristotle) true friend(aristotle, garfield) false

red(a) false orange(garfield) True.

- Logical Connectives
  $\wedge \quad \vee \quad \neg \quad \rightarrow \quad \leftrightarrow$

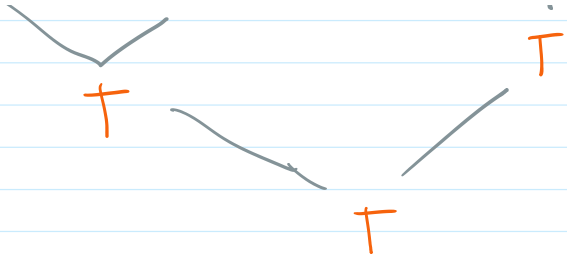
- Quantifiers: to handle variables
  $\forall x(p(X))$:- true if p is ~~true~~ true for every object.
  $\exists x(p(X))$:- true if p is true for at least an object

- Predicate Formulas.
  - Objects, variables, predicates
  - Logical connectives and quantifiers.

objects {a, b}

$$\boxed{\begin{array}{ll} p(a)=T & r(a)=F \\ p(b)=T & r(b)=F \\ q(a)=F & \\ q(b)=T & \end{array}}$$

$$\underbrace{\left(\underbrace{\forall X\, p(x)}_{T} \vee \underbrace{\exists Y\, q(Y)}_{T}\right)}_{T} \wedge \underbrace{\neg \underbrace{\forall x\, r(X)}_{F}}_{T}$$



- Rules of inference.

$$\frac{p(a),\ p(b)}{p(a) \vee p(b)} \qquad \frac{\forall x\ p(x)}{p(c)} \qquad \frac{p(c)}{\exists x\ p(x)}$$

$$\frac{\forall x\ p(x) \to q(x),\quad p(c)}{q(c)}$$

modus ponnens.

– The power of predicate logic.

1) All ~~men~~ are mortal
2) Aristotle is a man

Objects { aristotle, garfield }

$\forall x\ \text{man}(x) \to \text{mortal}(x) \cdot T$

$\text{man}(\text{aristotle}) \cdot T$

plug into modus ponnens

$\text{mortal}(\text{aristotle})$

- HOARE LOGIC

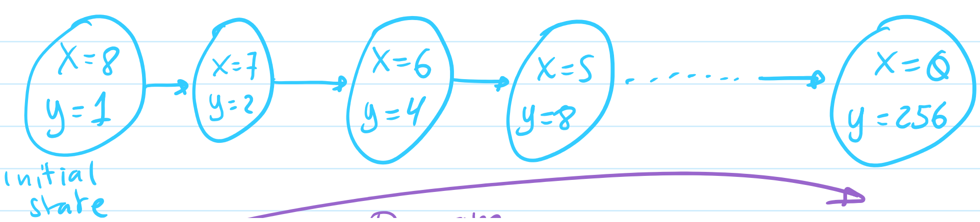
A logic for programs

– Objects:- Program variables and their assignments.

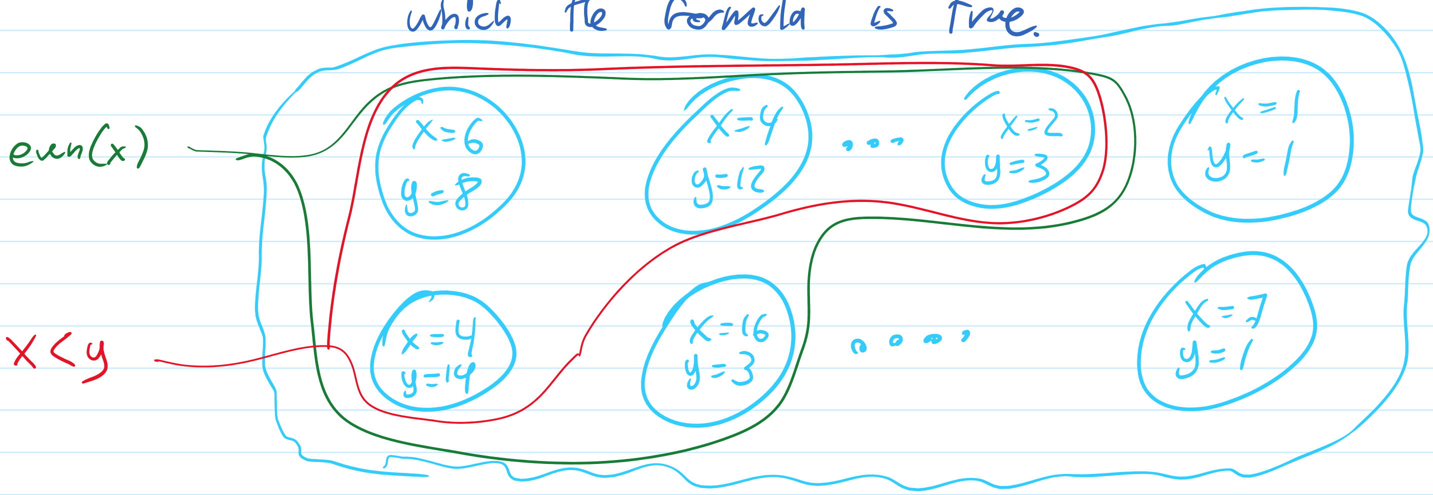
– State:- An assignment of values to variables.

– Program Execution

A sequence of transitions from an initial state to a final state.



- Predicate formulas
  - to talk about states
  - NOT to be evaluated as true or false.
  - Represent the set of all states over which the formula is true.



- Formula in Hoare Logic : "The Hoare triple"

  $\{P\}\ C\ \{Q\}$

  P, Q : predicate formulas

  C : "command" : a piece of program code

  P : "Pre-condition"

  Q : "Post-condition"

In english: If I tell you $\{P\}C\{Q\}$ is true
what I am claiming is that:
"if you execute program C in a state in which P is true, the program will finish ~~in~~ a state in state in which Q is true."

- How is this useful?

  C : your program

  {P} : a formula, spec of the input

  {Q} : a formula, spec of the output

$\{P\}$: a formula, spec of the input
$\{Q\}$: a formula, spec of the output

If you can prove that $\{P\}\,C\,\{Q\}$ is true
then you have proven that the program is correct.

Implications:-
- A program is a mathematical object
- A program can be analysed mathematically
- Use mathematics to prove properties of programs.

Semantics through logic Rules

collection of inference rules :
- assignments
- conditionals
- loops

- Rules of inference in Hoare logic.
  - Axiom of assignment

$$\overline{\{\underbrace{Q_{x \to E}}_{\text{replace every occurance of } x \text{ in } Q \text{ by } E}\}\ x \leftarrow E\ \{Q\}}$$

$$Q' \xrightarrow{x \leftarrow E} Q$$

Example
$$\{?\}\ \overbrace{a}^{x} \leftarrow \overbrace{b-4}^{E}\ \overbrace{\{a>0\}}^{Q}$$

$\{b-4>0\}$

$\{b>4\}\ a \leftarrow b-4\ \{a>0\}$: True.

E.g
$$\{?\}\ a \leftarrow 2*(b-2)\ \{0 \le a \le 10\}$$
$\{0 \le 2 \cdot (b-2) \le 10\}$

$\{0 \le 2\cdot(b-2) \le 10\}$

$\{0 \le 2b-4 \le 10\}$

$\{4 \le 2b \le 14\}$

$\{2 \le b \le 7\}\ a \leftarrow 2*(b-2)\ \{0 \le a \le 10\}$ True.

- Rule of composition

$$\frac{\{P\}\,C_1\,\{R\}, \quad \{R\}\,C_2\,\{Q\}}{\{P\}\,C_1, C_2\,\{Q\}}$$

Example

$\{?\}\ a \leftarrow 3*b-1 \ ;\ b \leftarrow 4*a-22\ \{b > 10\}$

$\{4\cdot a - 22 > 10\}\ b \leftarrow 4*a-22\ \{b > 10\}$

$\{4a > 32\}$

$\{a > 8\}\ b \leftarrow 4*a-22\ \{b > 10\}$ True.

$\{?\}\ a \leftarrow 3*b-1\ \{a > 8\}$

$\{3\cdot b - 1 > 8\}$

$\{3b > 9\}$

$\{b > 3\}\ a \leftarrow 3*b-1\ \{a > 8\}$ True.

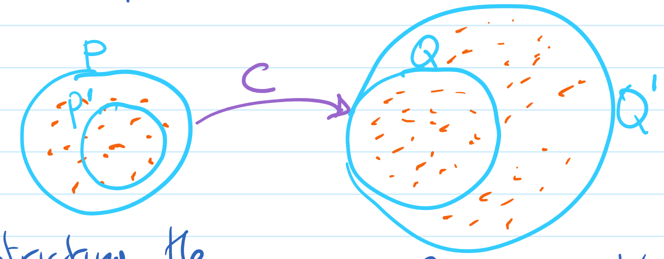
- by rule of composition:

$\{b > 3\}\ a \leftarrow 3*b-1 \ ;\ b \leftarrow 4*a-22\ \{b > 10\}$ True.

- Rule of consequence.

Intuition

suppose $\{P\}\,C\,\{Q\}$ True



Restricting the precondition

- Relaxing the postcondition.

$$\frac{P' \subseteq P, \ \{P\}\, C\, \{Q\}, \ Q \subseteq Q'}{\{P'\}\, C\, \{Q'\}}$$

E.g.

$\{b>4\}\ a \leftarrow b-4\ \{a>0\}$: True.

Restrict the precondition:

$\{b>10\}\ a \leftarrow b-4\ \{a>0\}$: True $\qquad \{b>10\} \subseteq \{b>4\}$

Relax the postcondition

$\{b>4\}\ a \leftarrow b-4\ \{a \geq 0\}$ True $\qquad \{a>0\} \subseteq \{a \leq 0\}$

- Conditional Rule

$$\frac{\{B \wedge P\}\ C_1\ \{Q\}, \ \{\neg B \wedge P\}\ C_2\ \{Q\}}{\{P\}\ \text{IF } B \text{ THEN } C_1 \text{ ELSE } C_2\ \{Q\}}$$