EE360T/382C-16 Software Testing

khurshid@ece.utexas.edu

Lecture 3

Last time and today

Discrete math basics

- Review some material from MIT’s 6.042 text
  - https://courses.csail.mit.edu/6.042/spring17/mcs.pdf
- Focus on Section I Proofs in the text
  - Propositions, predicates
  - Logical formulas
  - **Mathematical data types**
  - **Induction**
  - **State machines**

Sets

A set is a collection of objects that are called its elements

Ex: B = { red, blue, yellow } – set of colors

Ex: $C = \{\{a, b\}, \{a, c\}, \{b, c\}\}$ – set of sets

Ex: $D ::= \{ 1, 2, 4, 8, 16, \ldots\}$ – powers of 2

Order of elements is not significant, e.g., $\{x, y\} = \{y, x\}$

There is no notion of an element appearing >1 times, e.g., $\{x, x\} = \{x\}$

Some popular sets

symbol	**set**	**elements**
$\emptyset$	the empty set	none
$\mathbb{N}$	nonnegative integers	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{Z}$	integers	$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$\mathbb{Q}$	rational numbers	$\frac{1}{2},\ -\frac{5}{3},\ 16,$ etc.
$\mathbb{R}$	real numbers	$\pi,\ e,\ -9,\ \sqrt{2},$ etc.
$\mathbb{C}$	complex numbers	$i,\ \frac{19}{2},\ \sqrt{2} - 2i,$ etc.

source: page 98 of https://courses.csail.mit.edu/6.042/spring17/mcs.pdf

Comparing and combining sets

Subset: $S \subseteq T$ if every element in *S* is also is in *T*

Union: $x \in A \cup B$ if and only if $x \in A \vee x \in B$

Intersection: $x \in A \cap B$ if and only if $x \in A \wedge x \in B$

Difference: $x \in A - B$ if and only if $x \in A \wedge x \notin B$

Ex: Let *X* = { 1, 2, 3 } and *Y* = {2, 3, 4}, Then

$$X \cup Y = \{1, 2, 3, 4\}$$
$$X \cap Y = \{2, 3\}$$
$$X - Y = \{1\}$$
$$Y - X = \{4\}$$

Set builder notation

Idea: define a set using a predicate

Ex: $\{ n \in \mathbb{N} . \, n \text{ is a prime and } n = 4k + 1 \text{ for some integer } k \}$

- Elements are: 5, 13, 17, 29, 37, ...

Sequences

A sequence is an ordered list of objects

- Ex: (a, b, c) is a sequence of length 3

A sequence can have repeated elements, e.g., (a, a) is a sequence of length 2

The order of elements matters, e.g., (a, b) and (b, a) are two different sequences

Length 2 sequences are called pairs

Cartesian product

A Cartesian product of sets, S_1 x S_2 x … x S_n, is a set that contains all sequences whose first component is from S_1, second from S_2, and so on

Ex: $\mathbb{N} \times \{a, b\} = \{(0, a), (0, b), (1, a), (1, b), \ldots\}$

Functions

A function assigns an element of a set (domain) to an element of another set (codomain)

$f : A \to B$

- f is a function with domain A and codomain B

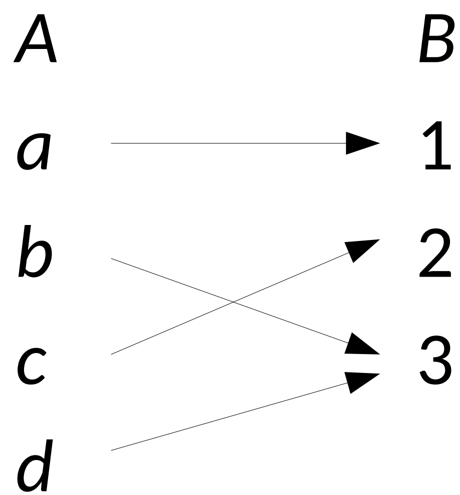
In general, functions may be partial, i.e., for some domain elements the function is not defined

A total function assigns a value to every element of its domain

Binary relations

A binary relation *R* consists of a set *A* (domain), a set *B* (domain), and a subset of *A* x *B* (graph)

- Notation: *a R b* means the pair (*a*, *b*) is in *R*
- A relation can be visualized as a diagram



(By definition) every function is a binary relation

Induction

Induction is a method to show a property holds for all nonnegative integers

The induction principle (ordinary induction) – let P be a predicate on nonnegative integers. If

- $P(0)$ is true, and
- $P(n)$ IMPLIES $P(n + 1)$ for all nonnegative integers n

then

- $P(m)$ is true for all nonnegative integers m

Induction Proof Example

Theorem 5.1.1. For all natural n,

$$1 + 2 + 3 + \ldots + n = n(n + 1)/2 \quad \text{(Eq. 5.1)}$$

Let $P(n)$ be the above predicate. We'll use induction to show $P(n)$ is true for all natural n.

Base case: $P(0)$: $0 = 0\,(0 + 1) / 2$.

Inductive step: Assume $P(n)$. We show $P(n + 1)$, i.e.,

$$1 + 2 + 3 + \ldots + n + (n + 1) = (n + 1)(n + 2)/2$$

Adding $n + 1$ to both sides of Eq. 5.1 gives

$$\begin{aligned} 1 + 2 + 3 + \ldots + n + (n + 1) &= n(n + 1)/2 + (n + 1) \\ &= (n + 1)(n/2 + 1) \\ &= (n + 1)(n + 2)/2, \text{ i.e., } P(n + 1) \end{aligned}$$

Template for induction proofs

1. State the proof uses induction
2. Define an appropriate predicate $P(n)$
3. [Base case] Prove that $P(0)$ is true
4. [Inductive step] Prove that $P(n)$ implies $P(n + 1)$ for every natural n
5. Invoke induction to conclude

A faulty induction proof

False theorem. All horses are the same color

False theorem 5.1.3. In every set of n >= 1 horses, all the horses are the same color

(Use a slight variation on induction since n >= 1)

Bogus proof. $P(n)$: in every set of n horses, all are the same color

Base case: (n = 1). $P(1)$ is certainly true

Inductive step: Assume $P(n)$ is true for some n >= 1, i.e., in every set of n horses, all are the same color.
Consider a set of n + 1 horses: $h_1, h_2, \ldots, h_n, h_{n+1}$

We need to show n + 1 horses are the same color

A faulty induction proof

By our assumption first n horses are the same color:

By our assumption, last n horses are the same color:

So h_1 is the same color as $h_2, \ldots, h_n$ and h_{n+1} is the same color as $h_2, \ldots, h_n$, and therefore all horses are the same color, i.e., $P(n + 1)$

What is the flaw in the argument?

Principle of strong induction

Let P be a predicate on nonnegative integers. If

- $P(0)$ is true, and
- for all natural n, $P(0)$, $P(1)$, …, $P(n)$ together imply $P(n + 1)$,

then $P(m)$ is true for all natural m.

Conceptually, assume a stronger set of hypotheses

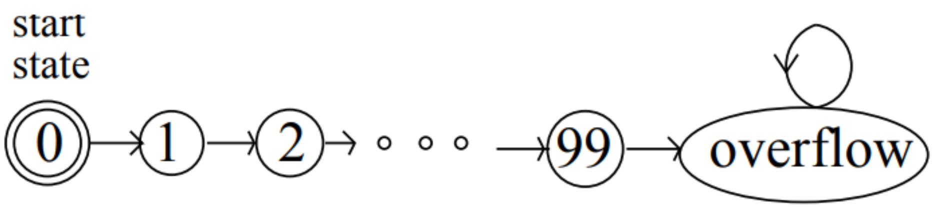
In theory, equivalent to ordinary induction

- A proof by strong induction can be translated into a proof by ordinary induction

State machines

A state machine is a binary relation on a set of states

- The relation is called the transition relation
- One state is called the start state

Example: 

source: page 167 of https://courses.csail.mit.edu/6.042/spring17/mcs.pdf

states = { 0, 1, 2, ..., 99, overflow }

start state = 0

transitions = { $n \rightarrow n + 1 \mid 0 <= n < 99$ } U

{ 99 → overflow, overflow → overflow }

Invariant principle

An execution of a state machine is a possibly infinite sequence of states such that:

- it begins with the start state, and
- if q and r are consecutive states, then $q \to r$

A state is called reachable if it appears in some execution

A preserved invariant is a predicate P on states such that if $P(q)$ and $q \to r$, then $P(r)$

Invariant principle: if a preserved invariant is true for the start state, then it is true for all reachable states

- Induction principle formulated for state machines

A diagonally moving robot

Assume a robot moves on a 2D integer grid and starts at the origin

State of robot is a pair of integer coordinates (x, y)

Start state: (0, 0)

Transitions: $\{(m, n) \rightarrow (m +/- 1, n +/- 1) \mid m, n \text{ in } Z\}$

E.g., after 1 step robot can be in states (1, 1), (1, -1), (-1, 1), (-1, -1)

Q: can the robot reach (1, 0)?

A diagonally moving robot

Even-sum$((m, n))$ ::= $m + n$ is even

Lemma. For any transition $q \to r$, if *Even-sum*(q), then *Even-sum*(r)

- Follows from the definition of transitions. After a transition, the sum of coordinates changes by (+/- 1) + (+/- 1), i.e., by 0, 2, or -2

Theorem. The sum of the coordinates of any state reachable by the robot is even

Proof. By induction on number of transitions robot made. Induction hyp:

$P(n)$ ::= if q is a state reachable in n transitions, then *Even-sum*(q)

A diagonally moving robot

Base case. $P(0)$ is true since (0, 0) is the only state reachable in 0 transitions and 0 + 0 is even

Inductive step. Assume $P(n)$. Let r be any state reachable in $n + 1$ transitions. We show *Even-sum*(r)

Since r is reachable in $n + 1$ transitions, there must be some state q reachable in n transitions with $q \to r$. Since $P(n)$ is true, *Even-sum*(q) holds, so by the lemma, *Even-sum*(r) also holds, i.e., $P(n) \Rightarrow P(n + 1)$

Corollary. The robot can never reach (1, 0)

- By the theorem, robot only reaches positions with coordinates with an even sum and 1 + 0 is odd

Directed graphs

A directed graph G consists of a nonempty set $V(G)$ or vertices and a set $E(G)$ of directed edges

An edge $e = (u, v)$ starts at vertex u (tail) and ends at v (head)

G can be represented using an adjacency matrix A

If G has n vertices v_0, v_1, v_{n-1}, A is an n x n matrix of 0's and 1's

A_{ij} is 1 if there is an edge from i to j and 0 otherwise

?/!