37181: WEEK 3: INDUCTION, CORRECTNESS OF COMPUTER CODE

A/Prof Murray Elder, UTS

Wednesday 14 August 2019

PLAN

- review of end of last lecture
- induction
- correctness of computer code

RECALL

A *set* is a well-defined collection of objects. [1] The objects are called *elements* of the set, or *members* of the set.

[1] Carefully defining what *well-defined* means will take us beyond the scope of this course, into axiomatic set theory and foundations of mathematics.

of $\emptyset$

Let $P(S)$ be the property (of sets) that "S does not contain itself".

$P(\emptyset)$ ~~No.~~ True

$P(\mathbb{N})$

$\mathbb{N}$

$\{0, 1, 2, \ldots$

Let $P(S)$ be the property (of sets) that "S does not contain itself".

For example, $P(\mathbb{N})$ is true because $\mathbb{N}$ contains numbers, it does not contain sets so it cannot contain itself.

Let $P(S)$ be the property (of sets) that "S does not contain itself".

For example, $P(\mathbb{N})$ is true because $\mathbb{N}$ contains numbers, it does not contain sets so it cannot contain itself.

Another example: the *empty set* $\emptyset$ is the set that has no elements, $\emptyset = \{\}$. So it contains nothing so cannot contain itself.

BACK TO THE DEFINITION OF “SET”

Consider the set of all abstract concepts. Call it $\mathscr{A}$. Then A contains things like art, postmodernism, democracy, socialism.

$\mathscr{A}$

BACK TO THE DEFINITION OF "SET"

Consider the set of all abstract concepts. Call it $\mathscr{A}$. Then A contains things like art, postmodernism, democracy, socialism.

(a) Which is true: $\mathscr{A} \in \mathscr{A}$ or $\mathscr{A} \notin \mathscr{A}$?

$P(\mathcal{A})$ False

Consider the set of all abstract concepts. Call it $\mathscr{A}$. Then A contains things like art, postmodernism, democracy, socialism.

(a) Which is true: $\mathscr{A} \in \mathscr{A}$ or $\mathscr{A} \notin \mathscr{A}$?

Let $\mathscr{S} = \{S \mid P(S)\}$ be the set of all sets that do not contain themselves.

$\mathscr{S}$ such that

$\mathscr{S} = \{ \mathbb{N}, \emptyset, \mathbb{Z}, \mathbb{R} \setminus \mathbb{Q}, \mathbb{R}, \mathbb{C}$

Question: Is $\mathscr{S} \in \mathscr{S}$ or not?

BACK TO THE DEFINITION OF "SET"

Consider the set of all abstract concepts. Call it $\mathscr{A}$. Then A contains things like art, postmodernism, democracy, socialism.

(a) Which is true: $\mathscr{A} \in \mathscr{A}$ or $\mathscr{A} \notin \mathscr{A}$?

Let $\mathscr{S} = \{S \mid P(S)\}$ be the set of all sets that do not contain themselves.

So $\mathbb{N} \in \mathscr{S}$ and $\mathscr{A} \notin \mathscr{S}$.

BACK TO THE DEFINITION OF "SET"

Consider the set of all abstract concepts. Call it $\mathscr{A}$. Then A contains things like art, postmodernism, democracy, socialism.

(a) Which is true: $\mathscr{A} \in \mathscr{A}$ or $\mathscr{A} \notin \mathscr{A}$?

Let $\mathscr{S} = \{S \mid P(S)\}$ be the set of all sets that do not contain themselves.

So $\mathbb{N} \in \mathscr{S}$ and $\mathscr{A} \notin \mathscr{S}$.

(b) Which is true: $\mathscr{S} \in \mathscr{S}$ or $\mathscr{S} \notin \mathscr{S}$?

BACK TO THE DEFINITION OF "SET"

Consider the set of all abstract concepts. Call it $\mathscr{A}$. Then A contains things like art, postmodernism, democracy, socialism.

(a) Which is true: $\mathscr{A} \in \mathscr{A}$ or $\mathscr{A} \notin \mathscr{A}$?

Let $\mathscr{S} = \{S \mid P(S)\}$ be the set of all sets that do not contain themselves.

So $\mathbb{N} \in \mathscr{S}$ and $\mathscr{A} \notin \mathscr{S}$.

(b) Which is true: $\mathscr{S} \in \mathscr{S}$ or $\mathscr{S} \notin \mathscr{S}$?

The moral of this story: you cannot define a set using a condition, in general. *i.e.* $\{x \mid P(x)\}$ may not actually be a well-defined collection of objects.

- Let A be a set. Then (axiom)

2. $$\mathscr{P}(A) = \{B \mid B \subseteq A\}$$

is a set. Its called the *power set* of A.

$= \{\phi, \{\phi\}$ $\phi \subseteq \phi$ $\{\phi\} \subseteq$

$A = \{~~1, 2, 3~~\}$?!

$\mathscr{P}(A) = \{\phi, \{1\}, \{2\}, \{3\}, \{1 2\}, \{1 3\}, \{2 3\}, ~~\{1 2 3\}~~ A\}$

Axiom

1. ϕ is a set.

ϕ, $\mathscr{P}(\phi) = \{\phi, \cancel{\{\phi\}}\}$

$\mathscr{P}(\{\phi\}) = \{\phi,$

POWER SET

Let A be a set. Then (axiom)

$$\mathscr{P}(A) = \{B \mid B \subseteq A\}$$

is a set. Its called the *power set* of A.

Questions:

- is $\emptyset \in \mathscr{P}(A)$?
- is $A \in \mathscr{P}(A)$?
- is $\mathscr{P}(A) \in \mathscr{P}(A)$?

POWER SET

Let A be a set. Then (axiom)

$$\mathscr{P}(A) = \{B \mid B \subseteq A\}$$

is a set. Its called the *power set* of A.

Questions:

- is $\emptyset \in \mathscr{P}(A)$?
- is $A \in \mathscr{P}(A)$?
- is $\mathscr{P}(A) \in \mathscr{P}(A)$?

Another axiom: $\emptyset$ is a set.

$\emptyset$ is a set. by Axiom!

By Axiom 2:

$\mathscr{P}(\emptyset) = \{\emptyset\}$

is a set.

By 2, since $\{\emptyset\}$ is a set

$\mathscr{P}(\{\emptyset\})$

$= \{\emptyset, \underline{\{\emptyset\}}\}$

POWER SET

Let A be a set. Then (axiom)

$$\mathscr{P}(A) = \{B \mid B \subseteq A\}$$

is a set. Its called the *power set* of A.

$\mathcal{P}(\mathbb{N})$??

Questions:

- is $\emptyset \in \mathscr{P}(A)$?
- is $A \in \mathscr{P}(A)$?
- is $\mathscr{P}(A) \in \mathscr{P}(A)$?

Another axiom: $\emptyset$ is a set.

What can you build with just these two axioms?

YOUR TURN

- Given $A = \{1, 2, 3\}$ is a set, what is $\mathscr{P}(A)$?

YOUR TURN

- Given $A = \{1, 2, 3\}$ is a set, what is $\mathscr{P}(A)$?

- Prove that if A is a set then $A \subsetneq \mathscr{P}(A)$

$$\begin{array}{r} 121 \\ -16 \\ \hline 105 \end{array}$$

$$11^1 - 4^1 = 7$$

Lemma

For all $n \in \mathbb{N}$, $11^n - 4^n$ is divisible by 7.

?

$$n = 0 \qquad 11^0 - 4^0$$

$$= 1 - 1 = 0 = 7 \cdot 0$$

Lemma

If A is a set of size $n \in \mathbb{N}$, then $\mathscr{P}(A)$ has size 2^n.

?

$A = \emptyset$ size is 0

$\mathscr{P}(\emptyset) = \{\emptyset\}$ size $2^0 = 1$

PMI

Axiom (Principle of mathematical induction)

Let $P(n)$ be a statement about natural numbers. Let $s \in \mathbb{N}$, eg. $s = 0, 1$

Axiom (Principle of mathematical induction)

Let $P(n)$ be a statement about natural numbers. Let $s \in \mathbb{N}$, eg. $s = 0, 1$

If

1. $P(s)$ is true
2. $P(k) \to P(k+1)$ is true for arbitrary $k \geq s$.

$$\frac{\begin{array}{l} P(0) \text{ true} \\ \wedge\ P(0) \to P(1) \end{array}}{\therefore\ P(1)} \qquad \frac{\begin{array}{l} P(1) \\ P(1) \to P(2) \end{array}}{\therefore\ P(3)}$$

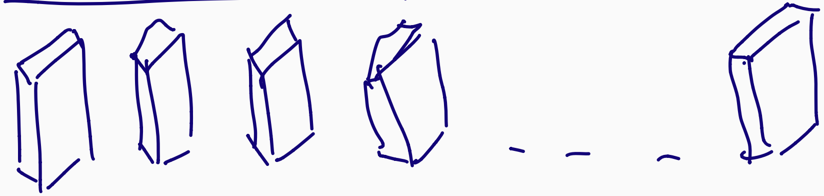
Axiom (Principle of mathematical induction)

Let $P(n)$ be a statement about natural numbers. Let $s \in \mathbb{N}$, eg. $s = 0, 1$

If

1. $P(s)$ is true
2. $P(k) \to P(k+1)$ is true for $k \geqslant s$.

then $P(n)$ is true for all $n \geqslant s$.



(domino picture)

APPLICATION

$$\sum_{i=1}^{\infty} i$$

Lemma

For all $n \in \mathbb{N}, n \geqslant 1$

$$LHS = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} = RHS$$

Proof : Let $P(n)$ be the statement

Lemma

For all $n \in \mathbb{N}, n \geqslant 1$

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Proof.

Let $P(n)$ be the statement that $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

Then $P(1)$:

$LHS = 1$

$RHS = \frac{1(1+1)}{2} = \frac{1 \cdot 2}{2} = 1$

$\therefore LHS = RHS$ ✓

so $P(1)$ is true.

Lemma

For all $n \in \mathbb{N}, n \geqslant 1$

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Proof.

Let $P(n)$ be the statement that $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

$P(1)$ ✓

Suppose $P(k)$ is true.

To show: $P(k+1)$ $LHS = \underbrace{1 + 2 + 3 + \cdots k}_{} + (k+1)$

$= \frac{k(k+1)}{2} + \frac{(k+1)2}{2}$

$= \frac{(k+1)(k+2)}{2}$

$= RHS$

Thus by PMI $P(n)$ is true for all $n \geqslant 1$. $\square$

APPLICATION

Lemma

For all $n \in \mathbb{N}, n \geqslant 1$

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Proof Let $P(n)$ be the statement that

$$1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Then $P(1)$: LHS $= 1^2 = 1$

RHS $= \frac{1(2)(3)}{6} = 1$ ✓✓

Now suppose $P(k)$ is true.

Then $P(k+1)$: LHS $= \underbrace{1^2 + 2^2 + \dots + k^2}$ $+ (k+1)^2$

$$= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \frac{6}{6}$$

$$= \frac{(k+1)\left[k(2k+1) + 6(k+1)\right]}{6}$$

$$= \frac{(k+1)}{6}\left[2k^2 + k + 6k + 6\right]$$

$$= \frac{(k+1)}{6}\left((k+2)(2k+3)\right)$$

$$= \text{RHS}$$

$$= \frac{k(k+1)(2k+1)}{6} + (k+1) \cdot \frac{6}{6}$$

Lemma

For all $n \in \mathbb{N}, n \geqslant 1$

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Proof.

Let $P(n)$ be the statement that

Lemma

For all $n \in \mathbb{N}, n \geqslant 1$

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Proof.

Let $P(n)$ be the statement that

$P(1)$

Assume $P(k)$. Then $P(k+1)$:

Thus by PMI $P(n)$ is true for all $n \geqslant 1$. $\square$

Lemma

For all $n \in \mathbb{N}$, $11^n - 4^n$ is divisible by 7.

Pf Let $P(n)$ statement "$7 \mid (11^n - 4^n)$"

$P(0)$: $11^0 - 4^0 = 1 - 1 = 0 = 7 \cdot 0$

So $P(0)$ is true.

Assume $P(k)$ is true. $\rightarrow 11^k - 4^k = 7p$ some $p \in \mathbb{Z}$.

Then $P(k+1)$: $11^{k+1} - 4^{k+1}$

$= 11 \cdot 11^k - 4 \cdot 4^k$

$$= (7+4)\,11^k - 4\cdot 4^k$$
$$= 7\cdot 11^k + 4\left(11^k - 4^k\right)$$
$$= 7\cdot 11^k + 4\cdot(7p)$$
$$= 7\left(11^k + 4p\right)$$

$\therefore$ $\underline{P(k+1)}$ is true.

By PMI, true for all $n \geq 0$ $\square$

Lemma

For all $n \in \mathbb{N}$, $11^n - 4^n$ is divisible by 7.

Proof.

Let $P(n)$ be the statement that

Lemma

For all $n \in \mathbb{N}$, $11^n - 4^n$ is divisible by 7.

Proof.

Let $P(n)$ be the statement that

Thus by PMI $P(n)$ is true for all $n \geqslant 0$. $\square$

Lemma

If A is a set of size $n \in \mathbb{N}$, then $\mathscr{P}(A)$ has size 2^n.

Proof.

Let $P(n)$ be the statement that if $|A| = n$ then $|\mathscr{P}(A)| = 2^n$

$P(0)$: If $|A| = 0$, $A = \emptyset$
then $\mathscr{P}(\emptyset) = \{\emptyset\}$
$|\mathscr{P}(\emptyset)| = 1 = 2^0$
$\therefore P(0)$ is true.

~~Thus by PMI $P(n)$ is true for all $n \geq 0$.~~ □

Assume $P(k)$.

Then $P(k+1)$:

Suppose $A = \{a_1, a_2, \ldots a_{k+1}\}$

$\mathcal{P}(A)$ is the set of all subsets

For every subset of A, ask:

is $a_1 \in A$ or not?

$\emptyset$ $\{a_2\}$ $\{a_2, a_3\}$ $\{a_1\}$ $\{a_1, a_2\}$

$\{a_3, a_4\}$ $\{a_1, a_3, a_4\}$

2^k

$\{a_2 a_3 \ldots a_{k+1}\}$ A

2^k size k

$$2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$$

Lemma

For all $n \in \mathbb{N}$, if $n \geqslant \square$ then (some statement).

Proof.

Let $P(n)$ be the statement $\boxed{}$

Then $P(\square)$ is true since $\boxed{}$

Assume $P(k)$ for $k \geqslant \square$. Then

$\boxed{}$

Thus by PMI $P(n)$ is true for all $n \geqslant \square$. $\square$

STRONGER VERSION (OR IS IT?)

PMI is equivalent to the following: Let $s \in \mathbb{N}$.

If

- $P(s)$ is true and
- if *for all* $s \leqslant i \leqslant n$ $P(i)$ is true, then $P(n+1)$ is true,

PMI is equivalent to the following: Let $s \in \mathbb{N}$.

If

- $P(s)$ is true and
- if *for all* $s \leqslant i \leqslant k$ $P(i)$ is true, then $P(k + 1)$ is true,

then $P(n)$ is true for all $n \in \mathbb{Z}, n \geqslant s$.

EG

Lemma

For all $n \in \mathbb{N}, n > 1$ if n is not prime then some prime number p divides n.

Proof.

Let $p(n)$ statement $n > 1$ and
n prime or $\exists\, p$ prime
$p \mid n$.

$p(2)$: 2 is prime ✓

Assume $p(2)$ $p(3)$ ... $p(k)$ all true

$p(k+1)$: either $k+1$ is prime or not

If $k+1$ is prime, $P(k+1)$ is true ✓

Else $\exists\ a, b \in \mathbb{Z}\ a, b > 1$

$k+1 = a \cdot b$.

Since $2 \leq a \leq k$, $P(a)$ is true

so either a prime

or $a = q \cdot c$ q prime

$k+1 = q \cdot c \cdot b$ ...

p .

Lemma

For all $n \in \mathbb{N}, n > 1$ if n is not prime then some prime number p divides n.

Proof.

Let $P(n)$ be the statement that either n is prime or some prime divides n.

$\square$

Lemma

For all $n \in \mathbb{N}$, $n! \geqslant 2^{n-1}$

Proof.

Let $P(n)$ be the statement that

$P(0)$ $0!$ 2^{-1}

$\square$

(start at 0)

EG

Lemma

All horses are black.

Proof: Let $p(n)$ statements that for any collection of n horses, they are all black.

$p(0)$: suppose $p(0)$ false.

Lemma

All horses are black.

Proof.

Let $P(n)$ be the statement that

$\square$

PAUSE

CORRECTNESS OF COMPUTER CODE

We say a procedure/computer program/(~~algorithm~~) is correct if

- It stops after a finite number of steps..
- The output claimed to be produced by the algorithm is what is promised.

We say a procedure/computer program/(algorithm) is correct if

- It stops after a finite number of steps..
- The output claimed to be produced by the algorithm is what is promised.

Wikipedia: In computer science, a *loop invariant* is a property of a program loop that is true before (and after) each iteration.

It is a logical assertion, sometimes checked within the code by an assertion call. Knowing its invariant(s) is essential in understanding the effect of a loop.

CORRECTNESS OF COMPUTER CODE

Here is a fragment of slightly useless code.

```
int j = 9;
for(int i=0; i<10; i++)
    j--;
```

(1) terminates

$i' = i+1$

$j' = j-1$

There is no output, but we will use this to illustrate loop invariant. Something that is true at the start, and remains true after each iteration, so is true at the end also.

i	j	$i+j$
0	9	9
⋮	⋮	

Loop invariant:

$L(i,j)$: $i + j = 9$

If $i+j=9$, $i' = i+1$, $j' = j-1$, $i'+j' = i+1+j-1$

$i+j=9$

Here is a fragment of slightly useless code.

```
int j = 9;
for(int i=0; i<10; i++)
   j--;
```

There is no output, but we will use this to illustrate loop invariant. Something that is true at the start, and remains true after each iteration, so is true at the end also.

Termination: for loop

Loop invariant: $i+j=9$

CORRECTNESS OF COMPUTER CODE

Here is a fragment of slightly useless code.

```
int j = 9;
for(int i=0; i<10; i++)
   j--;
```

There is no output, but we will use this to illustrate loop invariant. Something that is true at the start, and remains true after each iteration, so is true at the end also.

Termination:

Loop invariant: $i + j =$

input: x, d pos integers

```
q=0;
r=x;
while(r>=d)
  r=r-d;
  q++;
return (q,r)
```

$r' = r - d$

$q' = q + 1$

Loop invariant:

$x = q \cdot d + r$ → $0 \le r < d$

True at start? $0 \cdot d + x = x$

Suppose $x = qd + r$ before 1 step of while

After:

$q' = q + 1$

$r' = r - d$

$q'd + r' = (q+1)d + r - d$

$= qd + d + r - d$

$= qd + r = x$

```
q=0;
r=x;
while(r>=d)
  r=r-d;
  q++;
return (q,r)
```

Termination:

Loop invariant:

EXAMPLE FROM WIKIPEDIA

```
int max(int n,const int a[]) {
    int m = a[0];
    // m equals the maximum value in a[0...0]
    int i = 1;
    while (i != n) {
        // m equals the maximum value in a[0...i-1]
        if (m < a[i])
            m = a[i];
        // m equals the maximum value in a[0...i]
        ++i;
        // m equals the maximum value in a[0...i-1]
    }
    // m equals the maximum value in a[0...i-1], and i==n
    return m;
}
```

Termination:

Loop invariant:

Euclidean algorithm: $a, b \in \mathbb{Z}_+$ (for simplicity) and $a \neq 0 \vee b \neq 0$.

The steps are:

1. Start with (a, b) such that $a \geqslant b$. (ie. put them in order).
2. While $b \neq 0$,

   compute the remainder $0 \leqslant r < b$ of a divided by b.

   set $a = b, b = r$ (and thus $a \geqslant b$ again).
3. Return a

Euclidean algorithm: $a, b \in \mathbb{Z}_+$ (for simplicity) and $a \neq 0 \vee b \neq 0$.

The steps are:

1. Start with (a, b) such that $a \geqslant b$. (ie. put them in order).
2. While $b \neq 0$,

   compute the remainder $0 \leqslant r < b$ of a divided by b.

   set $a = b, b = r$ (and thus $a \geqslant b$ again).
3. Return a

Termination:

Loop invariant:

WOP AND PMI

More practice on loop invariants in the homework and worksheet.

Finally, so far in this course, we have asked you to *accept* two “facts” or axioms:

WOP:

PMI:

Axiom: true without following from any other fact.

Theorem

WOP implies PMI

Proof.

Assume $P(0)$ and $(P(k) \to P(k+1))$ are both true. Define

$$S = \{i \in \mathbb{N} \mid P(i) \text{ is false}\}.$$

$\square$

WOP AND PMI

Theorem

PMI implies WOP

Proof.

$\square$

NEXT

Next lecture:

- Relations
- Functions
- one-to-one
- onto
- bijection

Important to gets lots of practice doing proofs by induction.