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.

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

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.

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

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, imaginary numbers.

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

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, imaginary numbers.

(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.

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

(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, imaginary numbers.

(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, imaginary numbers.

(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)

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

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

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 $\mathscr{P}(A) \in \mathscr{P}(A)$?

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.

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.

What can you build with just these two axioms?

YOUR TURN

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

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

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

Lemma

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

?

Lemma

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

?

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

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

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

(domino picture)

APPLICATION

Lemma

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

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

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

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

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

Lemma

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

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

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

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.

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

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

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

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* $s \leqslant i \leqslant n$ $P(i)$ is true, then $P(n+1)$ is true,

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

Lemma

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

Proof.

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

$\square$

(start at 0)

Lemma

All horses are black.

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.

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.

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:

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: $i + j =$

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

```
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:

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

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

$\square$

Theorem

PMI implies WOP

Proof.

$\square$

Next lecture:

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

Important to gets lots of practice doing proofs by induction.

NEXT

Next lecture:

- induction
- correctness of computer code
- relations and functions