CS 173 Lecture B, September 15, 2015

Tandy Warnow

September 16, 2015

CS 173, Lecture B
September 15, 2015
Tandy Warnow

Functions

Notation: $f : A \rightarrow B$ means that f is a function with domain A and co-domain B.
The notation also means that $f(a) \in B$ for all $a \in A$, and that $f(a)$ is defined for every element of A.
The **image** of f, denoted by $f(A)$, is the set of elements of B that are mapped to from A (by f).
When $b \in B$, **pre-image** of b is the set of elements $a \in A$ such that $f(a) = b$. This set may be non-empty (if no element of A is mapped to b) or may have more than one element.
A $1-1$ function never maps two distinct elements of A to the same element of B. In other words, $f(a) \neq f(a')$ for $a \neq a'$ (both in A).
An **onto** function has at least one element in A mapped to every element of B. In other words, $\forall b \in B, \exists a \in A$ such that $f(a) = b$.

Today: Why induction is a valid proof technique

- Induction proofs are valid **for the same reason that a proof by contradiction is valid**.
- Any induction proof can be turned into a (somewhat longer) proof by contradiction.
- Learn how to do them both!

Proofs by contradiction and induction

Theorem: $\forall n \in Z^+, 1 + 2 + \ldots n = n(n+1)/2$
We could do this by induction, but let's do it by contradiction.

Proofs by contradiction and induction

Theorem: $\forall n \in Z^+, 1 + 2 + \ldots + n = n(n+1)/2$
Proof by contradiction. If the statement is not true, then there is at least one $n \in Z^+$ such that $1 + 2 + \ldots + n \neq n(n+1)/2$.
Question:

What can the smallest such n be?

Proofs by contradiction

Theorem: $\forall n \in Z^+, 1 + 2 + \ldots + n = n(n+1)/2$
Proof by contradiction.
Assume the statement is not true. Hence, there must be at least one $n \in Z^+$ such that $1 + 2 + \ldots + n \neq n(n+1)/2$.
Note that $n = 1$ satisfies this equality. Therefore the smallest n such that $1 + 2 + \ldots + n \neq n(n+1)/2$ is at least 2.
Let's call the smallest such value N.

Proofs by contradiction

We are trying to prove that $\forall n \in Z^+, P(n)$, where $P(n) \equiv [1 + 2 + \ldots + n = n(n+1)/2]$.

1. Let N be the smallest value for $n \in Z^+$ such that $\neg P(n)$. Thus, $1 + 2 + \ldots + N \neq N(N+1)/2$.
2. Note that $N \geq 2$ since $P(1)$ is true.
3. Hence $N - 1 \geq 1$, and so $N - 1 \in Z^+$.
4. Therefore, $P(N-1)$ is true, and so

$$1 + 2 + \ldots + (N-1) = (N-1)N/2$$

5. Let's add N to both sides of the equation above. We get:

$$1 + 2 + \ldots + N = (N-1)N/2 + N$$

6. Note that this simplifies to

$$1 + 2 + \ldots + N = N(N+1)/2$$

7. Thus, we have derived a contradiction (compare to (1) above).
8. Therefore, it must be that $\forall n \in Z^+, 1 + 2 + \ldots + n = n(n+1)/2$.

Proof by contradiction

Note the technique. We want to prove a statement of the form

$$\forall n \in Z^+, P(n),$$

where $P(n)$ is a boolean expression (true or false, depending on n).
We suppose the statement is false. Hence, there must be *some* element $n \in Z^+$ such that $P(n)$ is not true.
Since the set $\{n \in Z^+ : \neg P(n)\} \neq \emptyset$, we let N be the **smallest element of the set**. Note that $N - 1 \notin \{n \in Z^+ : \neg P(n)\}$.
If $N - 1 \in Z^+$, then $P(N - 1)$ is true. (Why?)
We then try to use the fact that $P(N - 1)$ *is true to derive that* $P(N)$ *is true.*
If we succeed in showing this, we have derived a contradiction!!

Proof by contradiction

What happens if $N - 1 \notin Z^+$?
Then we cannot argue that $P(N-1)$ is true. And hence the proof falls apart.

Note that $N - 1 \notin Z^+ \equiv [1 \notin \{n \in Z^+ : P(n)\}]$.

This is why we need to do the *base case analysis*.

Another proof by contradiction

Let $F : Z^+ \rightarrow Z^+$ be defined by

- $F(1) = 0$
- $F(n) = 2 + F(n-1)$ if $n \geq 2$

We want to prove that $\forall n \geq 2$, $F(n) \geq n$

Questions:

- Why do we start with $n = 2$ rather than $n = 1$?
- What is the property $P(n)$ for this problem?
- What is $F(3)$? What is $F(4)$?
- Do you think the statement is true for all $n \geq 2$?

Proving $F(n) \geq n$ for all $n \geq 2$ by contradiction

The property $P(n)$ is "$F(n) \geq n$". We wish to show $P(n)$ is true for $n = 2, 3, \ldots$.

Proof by contradiction. Suppose this statement is false. Then there is some $n \geq 2, n \in Z^+$ such that $P(n)$ is not true. Let N be the smallest such n. Hence $P(N)$ is false. **We will derive a contradiction to this statement!**

First - how small can N be? Since $P(2)$ is true (check this!), it must be that $N \geq 3$. Hence $N - 1 \geq 2$.

Since N is the smallest integer $n \geq 2$ for which $P(n)$ is false, $P(N-1)$ must be true.

Proving $F(n) \geq n$ for all $n \geq 2$ by contradiction

The property $P(n)$ is "$F(n) \geq n$". We wish to show $P(n)$ is true for $n = 2, 3, \ldots$.
Since $P(N-1)$ is true, it follows that

$$F(N-1) \geq N-1$$

Now, since $N \geq 3 > 2$, by definition

$$F(N) = 2 + F(N-1)$$

Combining these two statements, we get

$$F(N) \geq 2 + (N-1) = N+1 > N$$

But this means $P(N)$ is true, contradicting our hypothesis.

Connecting proofs by contradiction and induction

We used "proof by contradiction" to show

$$\forall n \geq n_0, P(n)$$

1. We assumed the statement

   $$\forall n \geq n_0, P(n)$$

   is false, and so inferred there must be some smallest number $N \geq n_0$ for which $\neg P(N)$.
2. We showed $P(n_0)$ is true.
3. Hence $N > n_0$, and so $N - 1 \geq n_0$.
4. Since N is the smallest number greater than or equal to n_0 for which $P(N) = F$, it must be that $P(N-1) = T$.
5. We then derived $P(N) = T$, using $P(N-1) = T$.

Note that we have derived a contradiction!

Connecting proofs by contradiction and induction

Note the similarities to proofs by contradiction. To prove that $P(n)$ is true for all $n \geq n_0$, we would

- Show $P(n_0)$ is true
- Show that if $P(K)$ is true (for an arbitrary K) then $P(K+1)$ is true

The reason this works is the same as why the proof by contradiction works.
Proofs by induction are just short ways of doing the proof by contradiction.

Recursively defined sets

Just as functions are often defined recursively, so can sets be. Let's consider some recursively defined sets.

- $S_0 = \emptyset$
- $S_n = S_{n-1} \cup \{n\}$ for $n \geq 1$.

Questions:

1. What is S_1?
2. What is S_2?
3. What is a closed form formula for S_n?
4. Can you prove your formula correct for all n?

Recursively defined set

- $S_0 = \emptyset$
- $S_n = S_{n-1} \cup \{n\}$ for $n \geq 1$.

Theorem: $\forall n \in Z^+$, $S_n = \{x \in Z^+ : x \leq n\}$.
First proof is by contradiction.
Second proof is by induction.

Proof by contradiction

Let $P(n)$ be the boolean statement $[S_n = \{x \in Z^+ : x \leq n\}]$.

1. We verify that $P(1)$ is true, by noting that $S_1 = S_0 \cup \{1\} = \emptyset \cup \{1\} = \{1\}$.
2. Now suppose it is not the case that $\forall n \in Z^+, P(n)$. Let N be the smallest positive integer for which $\neg P(N)$. Note that $N > 1$ since $P(1)$ is true.
3. Hence, $N - 1 \geq 1$. Therefore, $P(N-1)$ must be true, and so
$$S_{N-1} = \{x \in Z^+ : x \leq N - 1\}$$
4. Since $N > 1$, by definition
$$S_N = S_{N-1} \cup \{N\}$$
5. Combining these two statements we get:
$$S_N = \{x \in Z^+ : x \leq N - 1\} \cup \{N\} = \{x \in Z^+ : x \leq N\}$$
And so $P(N)$ is true.

But then this contradicts our hypothesis. Hence the theorem must be true.

Same theorem, now proof by induction

Recall definition of S_n. We let $P(n)$ be the boolean statement $S_n = \{x \in Z^+ : x \leq n\}$.
Theorem: $P(n)$ is true for all $n \in Z^+$
Proof: by induction on n.

- The **base case** is $n = 1$. By definition, $S_1 = S_0 \cup \{1\} = \{1\}$, and so $P(1)$ is true.
- **Inductive hypothesis:** $\exists K \in Z^+$ such that $\forall n \in \{1, 2, \ldots, K\}$, $P(n)$ is true.
- Note $K + 1 \geq 1$, and so by definition $S_{K+1} = S_K \cup \{K + 1\}$.
- By the inductive hypothesis, $S_K = \{1, 2, \ldots, K\}$. Hence $S_{K+1} = \{1, 2, \ldots, K + 1\}$.
- Since K was arbitrary, the statement is true for all $K \geq 1$.

Induction proofs

- Induction proofs are valid **for the same reason that a proof by contradiction is valid**.
- Any induction proof can be turned into a (somewhat longer) proof by contradiction.
- Learn how to do them both!

Next examlet

The next examlet is on Thursday, September 17.
It will have:

- Proof by induction for a recursively defined set
- Proof by contradiction for a recursively defined set

Please remember what your discussion section time is, since you will write it on your examlet page.

Class exercise

Let $F : Z^+ \rightarrow Z$ be defined recursively by

- $F(1) = 3$
- $F(n) = 2F(n-1) + 1$

Prove that $F(n) > 2^{n-1}$ for all $n \in Z^+$.
Do this first by contradiction.
Then do it by induction.
Do this in groups of 4 people. Two people do each type of proof.
Then exchange solutions.

Homework (ungraded): Let A_n, $n \in Z^+ \cup \{0\}$, be defined by $A_0 = \{0\}$, and $A_n = A_{n-1} \cup \{n^2\}$. Prove that $A_n = \{i^2 : 0 \leq i \leq n, i \in Z\}$ for all integers $n \geq 0$. Do this by contradiction, and then do it by induction.