CS 173, More on Induction

Tandy Warnow

CS 173
More on Induction
Tandy Warnow

Today's Lecture

- Proof by contradiction
- Connection to proof by induction

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

Proofs by contradiction and induction

Theorem: $\forall n \in \mathbb{Z}^+, 1 + 2 + \ldots + n = n(n+1)/2$

Proof by contradiction.

If the statement is not true, then there is at least one $n \in \mathbb{Z}^+$ such that $1 + 2 + \ldots + n \neq n(n+1)/2$.

Question:

What can the smallest such n be?

Proofs by contradiction

Theorem: $\forall n \in \mathbb{Z}^+, 1 + 2 + \ldots + n = n(n+1)/2$

Proof by contradiction.
Let $P(n)$ denote the assertion $1 + 2 + \ldots + n = n(n+1)/2$.

If the theorem isn't true, then $P(n)$ is not true for some $n \in Z^+$.

Note that $P(1)$ is true.

Therefore the smallest n such that $P(n)$ is False must be at least 2.

Let's call the smallest such value N, so that $P(N)$ is False.

Since $N \geq 2$, it follows that $N - 1 \geq 1$ and so $P(N-1)$ is True!

Proofs by contradiction

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

1. We showed $P(1)$ true and we let N be the smallest positive integer n such that $\neg P(n)$. Hence $N \geq 2$ and so $N - 1 \geq 1$.
2. Therefore, $P(N-1)$ is true, and so
$$1 + 2 + \ldots + (N-1) = (N-1)N/2$$
3. We add N to both sides of the equation above, and obtain
$$1 + 2 + \ldots + N = (N-1)N/2 + N$$
4. Note that
$$(N-1)N/2 + N = N(N+1)/2$$
so that $1 + 2 + \ldots + N = N(N+1)/2$
5. Thus, we have derived $P(N)$, contradicting our hypothesis!
6. Therefore, it must be that $\forall n \in \mathbb{Z}^+, 1 + 2 + \ldots + n = n(n+1)/2$.

Proof by contradiction – similar to induction proof

We want to prove $\forall n \in \mathbb{Z}^+, P(n)$
If the "for all" statement is false, then there must be *some* element $n \in \mathbb{Z}^+$ such that $P(n)$ is False.
Let N be the **smallest** positive integer where $P(N)$ is false.

We prove that $P(1)$ is true, so that $N \geq 2$ (and hence $N - 1 \geq 1$).

Since N is the smallest positive integer where $P(N)$ is false, it must be that $P(N-1)$ is true.

We then showed that $P(N-1) \to P(N)$*, and hence derived a contradiction.*

Note the similarity to a proof by induction!

Another proof by contradiction

Let $F : \mathbb{Z}^+ \to \mathbb{Z}^+$ be defined by

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

We want to prove that $\forall n \geq 2$, $F(n) \geq n$
Equivalently, we want to prove that $P(n)$ is true for all $n \geq 2$, where $P(n)$ is the assertion $F(n) \geq n$.

Class exercise:

- Calculate $F(n)$ for $n = 2, 3, 4$.
- Is $P(n)$ true for $n = 1, 2, 3, 4$?

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 false.

Let N be the positive integer s.t. $P(N)$ is false.

We will derive a contradiction to this statement!

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

How small can N be?

Since $P(2)$ is true, 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.

Hence

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

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

Recall the definition of the function $F : \mathbb{Z}^+ \to \mathbb{Z}^+$:

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

We want to prove that $\forall n \geq 2,\ F(n) \geq n$
We assumed N was the smallest positive integer such that $F(N) < N$ and showed

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

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 $P(N)$ is false, it must be that $P(N-1)$ is true.
5. We then derived $P(N)$ is true, which contradicted our hypothesis.

Connecting proofs by contradiction and induction

Note the similarities to proofs by induction.

To prove that $P(n)$ is true for all $n \geq n_0$ *by induction*, we would

- Show $P(n_0)$ is true
- Let N be arbitrary.
- Show that $P(N) \to P(N+1)$

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? (Answer: $S_1 = S_0 \cup \{1\} = \{1\}$)
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: $\forall n \in \mathbb{Z}^+$, $S_n = \{x \in \mathbb{Z}^+ | x \leq n\} = \{1, 2, \ldots, n\}$.

We will prove this two ways:

- First proof is by contradiction.
- Second proof is by induction.

Proof by contradiction

Recall

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

Let $P(n)$ be the Boolean statement "$S_n = \{1, 2, \ldots, n\}$."

What does $P(1)$ assert? Is it true?

What does $P(2)$ assert? Is it true?

Proof by contradiction

Let $P(n)$ be the Boolean statement "$S_n = \{1, 2, \ldots, n\}$."

1. We verified that $P(1)$ is true, by noting that $S_1 = \{1\}$.
2. Now suppose it is not the case that $\forall n \in \mathbb{Z}^+, P(n)$. 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
$$S_{N-1} = \{1, 2, \ldots, N-1\}$$
4. Since $N > 1$, by definition
$$S_N = S_{N-1} \cup \{N\}$$
5. Combining these two statements we get:
$$S_N = \{1, 2, \ldots, N-1\} \cup \{N\} = \{1, 2, \ldots, N\}$$
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 $S_n = \{x \in \mathbb{Z}^+ | x \leq n\}$"

Theorem: $P(n)$ is true for all $n \in \mathbb{Z}^+$
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.
- Let $N \in \mathbb{Z}^+$ be arbitrary.
- **Inductive hypothesis:** $P(N)$ is true.
- Note $N + 1 \geq 2$, and so by definition $S_{N+1} = S_N \cup \{N + 1\}$.
- By the I.H., $S_N = \{1, 2, \ldots, N\}$.
- Hence $S_{N+1} = \{1, 2, \ldots, N\} \cup \{N + 1\} = \{1, 2, \ldots, N + 1\}$.
- Since N was arbitrary, $P(N)$ is true for all $N \geq 1$.

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!

Class exercises

Pick a problem, and do the proof by contradiction and by induction.

Do this in groups of 4 people.

Two people do each type of proof. Then exchange solutions.

Problems

Problem 1: Let $F : \mathbb{Z}^+ \to \mathbb{Z}$ be defined recursively by

- $F(1) = 3$
- $F(n) = 2F(n-1) + 1$ if $n \geq 2$

Prove that $F(n) > 2^{n-1}$ for all $n \in \mathbb{Z}^+$.

Problem 2: Let A_n, $n \in \mathbb{Z}^+ \cup \{0\}$, be defined by

- $A_0 = \{0\}$, and
- $A_n = A_{n-1} \cup \{n^2\}$ if $n \geq 2$.

Prove that $A_n = \{i^2 | 0 \leq i \leq n, i \in \mathbb{Z}\}$ for all integers $n \geq 0$.