6.1200J/18.062J *Mathematics for Computer Science* Thursday 8th February, 2024
Massachusetts Institute of Technology, Spring 2024
Z. Abel, B. Chapman, E. Demaine revised Saturday 10th February, 2024

Lecture 02: Contradiction and Induction

1 Logical Deduction

- Third component of a proof
- Hardest but also most important component
- Deals with the structure of the proof

Definition 1. *An* inference rule *is a rule for combining true propositions to form other true propositions.*

Examples:

- Modus ponens (can be written many ways)
  - $((P \Rightarrow Q) \text{ AND } P) \Rightarrow Q$
  - $P \Rightarrow Q, P \vdash Q$
  - $$\frac{P \quad P \Rightarrow Q}{Q}$$
- Modus tollens: $((P \Rightarrow Q) \text{ AND NOT } Q) \Rightarrow \text{NOT } P$
- $((P \Rightarrow Q) \text{ AND } (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$
- $((\text{NOT } P) \Rightarrow \text{FALSE}) \Rightarrow P$

You can quickly check e.g. with a truth table that all of the above are sensible rules. As an example, for modus ponens, recall the truth table for $P \Rightarrow Q$:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

There is only one row in which P and $P \Rightarrow Q$ are both True (the first), and in this row, Q is also True.

For this class:

- Each step in a proof should be clear and logical.
- You should state which previously proved propositions are being used.
- Please do not make wild leaps of faith.
- Please do not use "Proof by Intimidation" (P is obvious, Clearly Q, etc.)
- But we are not picky about which inference rules you use, and there is certainly no need to cite an inference rule at every step.
- We are also not picky about precisely which axioms you use; generally basic math you knew before this class is all fair game.
- But if we ask you to prove P, then "I already knew P, so it's an axiom" is not a valid proof...

Today we will explore some basic (but crucial!) proof techniques, and then two powerful techniques: Proof by Contradiction and Proof by Induction.

2 Fundamental proof techniques

2.1 Proving Existence

The most straightforward way to prove that something *exists* is to demonstrate an example! E.g., $\exists n \in \mathbb{N}.\, n \geq 10$ AND isPrime(n).

Proof. We'll show that $n = 17$ satisfies the required condition. This is true because 17 is a prime number and $17 \geq 10$. □

In general, a proof of $\exists x \in S.\, P(x)$ will often look like this:

Proof. We'll show that the value $x =$ [*some specific value*] works. Indeed, for this choice of x, $P(x)$ is true because [*reasons*]. □

2.2 Proving Universality

Can't get away with just a single example, if we need to prove something for *all* members of a set. E.g., $\forall x \in \mathbb{R}.\, x^2 - 6x > -10$.

The strategy: Introduce a *generic/arbitrary* member x of S (i.e., make no assumptions about x other than the fact that $x \in S$), and prove $P(x)$ is true.

Proof. Suppose x is an arbitrary real number. Then $x^2 - 6x + 9 = (x-3)^2$, which is ≥ 0 because the square of every real number is nonnegative. So $x^2 - 6x = (x-3)^2 - 9 \geq -9 > -10$, as needed. □

In general, when proving $\forall x \in S.\, P(x)$,

Proof. Assume x is an arbitrary element of S. Then $P(x)$ is true because [*reasons*]. □

2.3 Proof of an Implication: Direct Method

When proving P IMPLIES Q, the strategy is to *assume* P, and then to prove Q (probably using that assumption).

For example, if n is a multiple of 10, then it is a multiple of 2.

Proof. Assume n is a multiple of 10; in other words, $n = 10k$ for some integer k. This means $n = 2 \cdot (5k)$, and therefore n is equal to 2 times an integer (namely, $5k$) and is therefore a multiple of 2. □

In general,

Proof. Assume P is true. Then Q is also true, because [*reasons*]. □

2.4 Proof of an Implication: Contrapositive

P IMPLIES Q is equivalent to its contrapositive (NOT Q) IMPLIES (NOT P), and the latter is sometimes easier to think about. E.g., assuming n is an integer, (n^2 is even) IMPLIES (n is even).

Proof. The desired theorem is equivalent to its contrapositive (n is odd) IMPLIES (n^2 is odd), so we'll prove *this* implication directly. Assume n is odd, and we'll prove that n^2 is also odd.

Since n is odd, we know $n = 2k+1$ for some integer k. Then $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$, which is one more than a multiple of 2, as required. □

In general, when proving P IMPLIES Q,

Proof. We'll prove the contrapositive, so assume NOT Q is true. Then NOT P is true because [*reasons*]. □

3 Proof by Contradiction

In a *Proof by Contradiction*, you assume the *opposite* of what you want to prove, and you use that assumption to derive a falsehood, or contradiction.

- To prove P by contradiction, you prove the implication (NOT P) $\Rightarrow$ FALSE.
- By our inference rule, this is a valid proof of P!
- Sometimes called an Indirect Proof

For example,

Theorem 1. $\sqrt{2} \notin \mathbb{Q}$

Proof by contradiction. Assume for sake of contradiction that $\sqrt{2} \in \mathbb{Q}$. Write $\sqrt{2}$ as a fraction in lowest terms, i.e. let $a, b \in \mathbb{Z}$ have no common divisors such that:

$$\begin{aligned} \frac{a}{b} &= \sqrt{2} \\ a &= b\sqrt{2} \\ a^2 &= 2b^2 \end{aligned}$$

This tells us that a^2 is even.

By our theorem above, a itself must be even, so we can write $a = 2c$ for some integer c.

$$\begin{aligned} a^2 &= 2b^2 \\ (2c)^2 &= 2b^2 \\ 4c^2 &= 2b^2 \\ 2c^2 &= b^2 \end{aligned}$$

This shows b^2 is even, so with our lemma again, b itself is even. Now a and b share a factor (2). $\Rightarrow\!\!\!\!\!\!\not\Leftarrow$ □

4 Proof Outlining

For many theorems, choosing a proof method can lead to immediate and noticeable progress on constructing the proof, based solely on the requirements of the method. The more precisely you can break down a proof into smaller tasks, the easier it will be to tackle these tasks one at a time, to ensure your proof is complete and correct. As this outlining task becomes faster and more automatic with practice, it will become easier to consider multiple possible approaches to a problem before deciding which one(s) to pursue.

A common proof-writing mistake is to dive headlong into *how to prove* something, while not realizing that you're trying to prove the wrong thing! Spending a bit of time identifying

what needs to be proved, likely using our common proof techniques, will ensure that your "how to prove"-energy is directed at the correct targets. And thankfully, this outlining step can often be started nearly mechanically, based on the form of the theorem being proved and the chosen proof techniques, regardless of the specific concepts or terms used within.

For example, Theorem: "For every integer n, the number n is fooish precisely when $n+1$ is barsome."

What do fooish and barsome mean? Doesn't matter – we can still make significant progress with structuring our proof!

Let's decompose this one step at a time. This theorem has the form $\forall n \in \mathbb{Z}.\, F(n)$ IFF $B(n+1)$. Handling the "$\forall$" makes the outline look like this:

Proof Outline Scratchwork, Step 1. Suppose n is any integer; we must prove $F(n)$ IFF $B(n+1)$. [TODO: prove $F(n)$ IFF $B(n+1)$.] □

Our remaining task is to prove an IFF, and we have a usual strategy for this as well:

Proof Outline Scratchwork, Step 2. Suppose n is any integer; we must show $F(n)$ IMPLIES $B(n+1)$ and $B(n+1)$ IMPLIES $F(n)$.

[TODO: prove $F(n)$ IMPLIES $B(n+1)$.]

[TODO: prove $B(n+1)$ IMPLIES $F(n)$.] □

Now we have some implications, where the usual strategy looks like this:

Proof Outline. Suppose n is any integer; we must show $F(n)$ and $B(n+1)$ both imply each other.

To prove $F(n)$ IMPLIES $B(n+1)$, first assume $F(n)$ is true. [TODO: prove $B(n+1)$.]

To prove $B(n+1)$ IMPLIES $F(n)$, instead assume $B(n+1)$ is true. [TODO: prove $F(n)$.] □

Since the remaining steps require knowing what $F(n)$ and $B(n+1)$ mean and how they relate to each other, this is as far as we can get for now – it's our finished outline!

5 Proof by Induction

Induction is probably the most common and most powerful proof technique in computer science. Let's start with an example to build intuition.

5.1 An Informal Example

Theorem 2. $\forall n \in \mathbb{N}. 1 + 2 + 3 + \cdots + n = n(n+1)/2$.

In order to prove this theorem, we need to verify the predicate $P(n) := 1{+}2{+}3{+}\cdots{+}n = n(n+1)/2$ for every possible natural number n. (Note: including $n = 0$, since the empty sum, by convention, is 0.) Let's investigate:

$$\begin{aligned} 0 &= (0)(1)/2 \\ 1 &= (1)(2)/2 \\ 1+2 &= 3 = (2)(3)/2 \\ 1+2+3 &= 4+5 = 6 = (3)(4)/2 \\ 1+2+3+4 &= 10 = (4)(5)/2 \\ 1+2+3+4+5 &= 15 = (5)(6)/2 \end{aligned}$$

But just checking examples isn't enough!

One possible idea: on the left side, we add 2, then 3, then 4, then 5, etc. Does the right side follow this same pattern?

$$\begin{aligned} P(n): &\quad 1+2+3+\cdots+n &&= (n)(n+1)/2. \\ P(n+1): &\quad 1+2+3+\cdots+n+(n+1) &&= (n+1)(n+2)/2 \end{aligned}$$

On the left side, we got from one sum to the next by adding $n+1$. What about the right side?

$$\frac{(n+1)(n+2)}{2} - \frac{(n)(n+1)}{2} = (n+1) \cdot \frac{(n+2)-n}{2} = (n+1).$$

It's the same! So from each row to the next, we're always adding the same amount on both sides, so the two sides will always stay equal.

This idea of "always adding the same amount to both sides at each step" is not very formal or generalizable, but hopefully it's at least convincing! How can we prove this carefully?

5.2 Digging Deeper

Our "adding n to both sides" argument proves the following: "Assuming $1{+}2{+}\cdots{+}(n{-}1) = (n{-}1)(n)/2$, it follows (by adding n to both sides) that $1{+}2{+}\cdots{+}(n{-}1){+}n = (n)(n{+}1)/2$." In other words, we were able to prove $P(n-1)$ IMPLIES $P(n)$, for every $n \geq 1$. We also noticed that $P(1)$ is true just by looking at it, so here's what we actually proved (left), vs

what we actually want to know (right):

Know all these	Want to prove all these
$P(0)$	$P(0)$
$P(0)$ IMPLIES $P(1)$	$P(1)$
$P(1)$ IMPLIES $P(2)$	$P(2)$
$P(2)$ IMPLIES $P(3)$	$P(3)$
$P(3)$ IMPLIES $P(4)$	$P(4)$
$P(4)$ IMPLIES $P(5)$	$P(5)$
$P(5)$ IMPLIES $P(6)$	$P(6)$
$\vdots$	$\vdots$

This feels like it should be enough, right? We know $P(0)$, and once we know $P(0)$ the implication shows $P(1)$, and from this the next implication proves $P(2)$, and then $P(3)$, and $P(4)$, and all the way down! So they're all true! But again, how can we prove this formally? How can we go from the left column to the right column?

We Know	We Want to Prove
$P(0)$ AND $\forall n \geq 0.\, [P(n)$ IMPLIES $P(n+1)]$	$\forall n \geq 0.\, P(n)$

Turns out, this is exactly what the Induction axiom does for us!

Axiom 1 (Induction)**.** *Let $P(n)$ be a predicate, defined for $n \in \mathbb{N}$. If $P(0)$* AND *$\forall n \in \mathbb{N}.\ P(n) \Rightarrow P(n+1)$, then $\forall n \in \mathbb{N}.\ P(n)$.*

Now, let's see how we use this Induction principle to formally use our theorem.

Proof of Theorem 2 by Induction. Let $P(n)$ be the predicate $1 + 2 + \cdots + n = n(n+1)/2$. We prove $\forall n \in \mathbb{N}.\ P(n)$, by induction on n.

Base case, must show $P(0)$: LHS is 0, RHS is $(0)(1)/2 = 0$, so they're equal.

Inductive step: Let $n \in \mathbb{N}$, and assume $P(n)$ is true; we must show $P(n+1)$. In other words, assume $1 + 2 + \cdots + n = n(n+1)/2$; we must show $1 + 2 + \cdots + n + (n+1) = (n+1)(n+2)/2$. Adding $n+1$ to both sides of $P(n)$ proves that

$$\begin{aligned}(1 + 2 + \cdots + n) + (n+1) &= n(n+1)/2 + (n+1) \\ &= (n+1) \cdot \left(\frac{n}{2} + 1\right) \\ &= (n+1) \cdot \frac{n+2}{2},\end{aligned}$$

which is precisely the statement we needed to show!

Since we've shown $P(0)$ and that $P(n)$ implies $P(n+1)$ for every $n \geq 1$, we conclude by induction that $P(n)$ is true for every $n \in \mathbb{N}$, as desired. □

5.3 Strengthening the Induction Hypothesis

In the preceding proof, the predicate $P(n)$ is what we call the *Induction Hypothesis*. Often (but not always!) this will be the predicate you initially set out to prove.

Here's a setting in which this is not true: Suppose we have a square grid with side length 2^n. Is it possible to use non-overlapping L-trominoes to cover the grid, except for one of the center-most squares?

Let's call $P(n)$ the predicate "it is possible to use non-overlapping L-trominoes to cover a 2^n by 2^n square grid, except for one of the center-most squares".

Theorem 3. $\forall n \in \mathbb{N}.\ P(n)$

What happens if we try to use $P(n)$ as the inductive hypothesis?

- Our base case ($n = 0$) is fine, as the only square is left uncovered.
- But how do we use the inductive hypothesis for the inductive step? Covering a 2^n by 2^n grid doesn't seem to help us cover the 2^{n+1} by 2^{n+1} grid...

Consider $Q(n)$: "it is possible to use non-overlapping L-trominoes to cover *any* $2^{2n} - 1$ squares of a 2^n by 2^n grid".

- $Q(n)$ is *stronger* than $P(n)$
- This actually makes the proof by induction *easier*!

Proof. We prove the stronger claim $\forall n.\ Q(n)$ by induction on n.

Base case ($n = 0$): There is only one square, which is uncovered.

Inductive step: Assume $Q(n)$ for the purposes of induction. Suppose we have a 2^{n+1} by 2^{n+1} grid and wish to leave the square with coordinates (i, j) uncovered. Assume *without loss of generality* that (i, j) is in the top-left quadrant. Place one L-tromino in the middle of the grid to cover one square in each of the other three quadrants. By the inductive hypothesis, we may cover the top-left quadrant, except for (i, j), and we may cover the other three quadrants except for the one square already covered by the middle tromino. Together, this covers the entire grid, except for (i, j).

By induction, $\forall n.\ Q(n).\ P(n)$ is a special case of $Q(n)$, so $\forall n.\ P(n)$. □

Two nice properties of this proof:

- Proof is *constructive*: it not only proves that it is possible to tile the grid; it also gives an algorithm for actually doing it!
- It gives a stronger result: now we can leave any square uncovered, not just one of the center ones.

Takeaway: when doing a proof by induction, if at first you don't succeed, try something harder!

- May seem counterintuitive
- Notice that strengthening the inductive hypothesis also means that the inductive step has a better starting point.
- Finding the right IH can be a bit of an art - sometimes easy, sometimes not.

6.1200J Mathematics for Computer Science

Spring 2024