6.1200J/18.062J *Mathematics for Computer Science* Tuesday 13th February, 2024
Massachusetts Institute of Technology, Spring 2024
Z. Abel, B. Chapman, E. Demaine revised Wednesday 14th February, 2024

Lecture 03: Casework and Strong Induction

1 Proof by Cases / Exhaustion

Recall our proof techniques so far:

- Existential by example/construction
  - Theorem: $\exists x.\, P(x)$
  - Method: construct x^*, prove $P(x^*)$
- Universal by instantiation
  - Theorem: $\forall x.\, P(x)$
  - Method: take arbitrary x, prove $P(x)$
- Implication by direct argument
  - Theorem: P IMPLIES Q
  - Method: assume P, prove Q
- Implication by contrapositive
  - Theorem: P IMPLIES Q, aka $\overline{Q}$ IMPLIES $\overline{P}$
  - Method: assume $\overline{Q}$, prove $\overline{P}$
- Contradiction:
  - Theorem: P, aka $\overline{P}$ IMPLIES False
  - Method: Assume $\overline{P}$ and prove false, i.e., prove Q AND $\overline{Q}$ for some proposition Q
- Universal over $\mathbb{N}$ by induction
  - Theorem: $\forall n \in \mathbb{N}.\, P(n)$
  - Method: Prove $P(0)$ and $P(n)$ IMPLIES $P(n+1)$ for every $n \geq 0$.

2 Proof by Cases

For any proposition C, the statement C OR NOT C is a ***tautology***, i.e., always true. So P is equivalent to True IMPLIES P (check truth table for implication), which is equivalent to (C OR NOT C) IMPLIES P, which can be split into (C IMPLIES P) AND (NOT C IMPLIES P). So to prove P, it's enough to show that C implies P AND NOT C implies P.

Template:

Theorem: P is true.

Proof. Proof by cases on the truth value of C:

- **Case 1: Assume *C* is true.** Then P is true because [todo].
- **Case 2: Assume instead that *C* is false.** Then P is true because [todo].

Since C must be either true or false, these two cases are ***exhaustive***, so P is true in all possible cases and is therefore true. □

Example:

Theorem 1. $S :=$ (A IMPLIES B) OR (B IMPLIES C) *is a tautology. In other words, for all values of* $A, B, C \in \{True, False\}$*, the statement* S *is true.*

Proof. Proof by cases: B must be either true or false.

- **Case 1: Assume *B* is true.** Then A IMPLIES B is true, so S is true!
- **Case 2: Assume *B* is false.** Then B IMPLIES C is true, so S is true!

Since S is true in both cases, and these cases are exhaustive, S must be true. □

2.1 A bigger example: Mutual friends/strangers

Say we have a group of 6 people, and every pair is either ***friends*** xor not friends (aka ***strangers***). Friendship is always 2-way, so A is friends with B if and only if B is friends with A.

Theorem 2. *In a group of 6 people, there are always either 3 mutual friends, or 3 mutual strangers (or both).*

Proof. Proof by cases. Pick any person p. Each of the 5 other people are either friends with p or not. We'll consider cases based on whether p has at least 3 friends.

- **Case 1: *p* has at least 3 friends.** Let q, r, s be three of p's friends. We'll consider sub-cases depending on whether any pair from q, r, s are friends with each other:

  - **Case 1a: some pair from q, r, s are friends with each other.** Then these two would, together with p, would be a group of 3 mutual friends!
  - **Case 1b: None of q, r, s are friends with each other.** Then these three form a group of 3 mutual strangers!

- **Case 2, p doesn't have at least 3 friends.** Then p has at most 2 friends and therefore at least 3 strangers. But this is fully symmetric with Case 1: by swapping the words "friends" with "strangers", the same proof as in Case 1 would apply, and would prove the existence of 3 mutual strangers or 3 mutual friends, as needed.

□

This example is part of a field called Ramsey Theory: we define $R(f, s) :=$ the minimum number of people needed to guarantee f mutual friends or s mutual strangers (or both). We just proved $R(3, 3) \leq 6$.

It is known that $R(3, 3) = 6$, $R(4, 4) = 18$, and $43 \leq R(5, 5) \leq 48$, but the exact value is unknown!

3 Proof by Cases, more general

Take any tautology C_1 OR C_2 OR $\cdots$ OR C_k.

Template:

Theorem: P is true.

Proof. Proof by cases:

- **Case 1: Assume C_1 is true.** Then P is true because [todo].
- **Case 2: Assume C_2 is true.** Then P is true because [todo].
- ...
- **Case k: Assume C_k is true.** Then P is true because [todo].

These k cases are **exhaustive** (i.e., C_1 OR $\cdots$ OR C_k is a tautology) because [todo]. □

Famous proof by (lots of) cases:

Proposition 3 (Four Color Theorem)**.** *The regions on any map can be colored with four colors such that no two adjacent regions have the same color.*

Long history...

- 1852: Conjectured by Guthrie in 1853 after noticing 4 colors is enough for countries of England
- 1853: Kempe "proved" the theorem
- 1864: Heawood found a bug :(
- 1880: Tait "proved" the theorem
- 1891: Petersen found a bug :(
- 1976: Appel and Haken "proved" the theorem. This proof had 1834 cases, all checked by computer, and came out to 400 pages printed. Reportedly all checked by hand by Blostein (Haken's daughter)
- 1891: Schmidt found a bug :(
- 1989: Appel and Haken fix bugs, publish full proof in a book (not peer reviewed like journal publications) :)?
- 1996: Robertson, Sanders, Seymour, Thomas, simpler computer-checked proof :), with 633 cases
- 2005: Werner and Gonthier: Formalized proof in Coq, must more reliable tool for computer-verified proofs :):)

Amusing prank: Martin Gardner claimed this map required 5 colors, as an April Fools joke: https://mathworld.wolfram.com/McGregorMap.html.

4 Strong induction

And now for a new version of induction. Recall the induction axiom from last time.

Axiom 1 (Induction axiom)**.** *Suppose $P(n)$ is a predicate with n a natural-number variable. If $P(0)$ is true, and for all $n \in \mathbb{N}$, it holds that $P(n) \implies P(n+1)$, then the proposition*

$$\forall n \in \mathbb{N}, P(n)$$

is true.

(Some people might ask whether this is really an axiom—can't we prove this obvious conclusion from more basic facts? It turns out that something like this is a basic axiom needed to define the natural numbers themselves.)

In a proof by induction, there are two parts: (1) the "base case", which is the proof that $P(0)$ holds, and (2) the "inductive step", which is the proof that $\forall n, P(n) \implies P(n+1)$. Notice that in the inductive step, in order to prove $P(n+1)$ we may *only* assume the truth of $P(n)$. The principle of *strong induction* says that this requirement can be relaxed:

Theorem 4 (Strong induction)**.** *Suppose $P(n)$ is a predicate with n a natural-number variable. Suppose that*

1. *$P(0)$ is true.*
2. *For all $n \in \mathbb{N}$, it holds that*

$$P(0) \wedge P(1) \wedge \ldots P(n) \implies P(n+1).$$

Then it holds that

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

In other words, in proving the inductive step, it is fine to assume the truth of $P(m)$ for any and all m between 0 and n.

At first, it may seem that strong induction is stronger than regular induction. Indeed, if the "regular" version of the inductive step holds, the "strong" version holds as well:

$$(P(n) \implies P(n+1)) \implies (P(0) \wedge P(1) \wedge \ldots P(n) \implies P(n+1)).$$

(Exercise: verify this by unpacking what the implications mean here!)

So anything that can be proved with "regular" induction can be proven with strong induction. But are there propositions that can be proven with strong induction that cannot be proven with regular induction? The answer is NO! Strong induction is in fact *completely equivalent* to regular induction, and the strong induction theorem can easily be *proven* from the Axiom of Induction. You will see more about this on your warm-up exercises tomorrow!

Example 1: stacking blocks Suppose we have a stack of n blocks. Let us play a game, where in each step, we may choose a stack of blocks and split it into two smaller stacks, not necessarily of equal size. Each time we do so, we gain a number of points that is equal to the *product* of the sizes of the two smaller stacks we create. The game ends when all stacks consist of just one block each.

What is the highest score we can attain?

To get a lower bound on this, let us try a very simple-minded strategy: in each step, we will always take the largest stack, and split off one block from it. So, supposing we started with 8 blocks, the strategy would proceed as follows:

1. Split the stack of 8 into $7 + 1$, gaining $7 \cdot 1 = 7$ points.
2. Now split the stack of 7 into $6 + 1$, gaining 6 points.
3. Now split the stack of 6 into $5 + 1$, gaining 5 points.
4. $\ldots$

5. Split the stack of 2 into $1+1$, gaining 1 point. Now all remaining stacks have 1 block in them, so the game terminates.

We can see that the total score we obtained was $7+6+\cdots+2+1=28$.

Very surprisingly, if one tries other, "more intelligent" strategies for this same example of 8 blocks, one will never obtain a value other than 28! Could it be that *all strategies* obtain a value of 28?

The answer is yes, and we will prove it! In fact, we will prove the conclusion in general for *all* n.

Theorem 5. *Any strategy for the block game that starts with* n *blocks will obtain a total of*

$$\sum_{i=1}^{n-1} i = \frac{n(n-1)}{2}$$

points.

(Where did that magical summation formula come from? It can easily be proven with regular induction—do this on your own!)

Proof. We will prove this using strong induction. I'm going to make a small twist and use 1 as the base case, and prove the proposition for all $n \geq 1$. (We could redefine our variable n to make the base case 0 if we wanted to, so this is purely cosmetic.)

Proposition: For all $n \geq 1$, $P(n)$ is the proposition that any strategy for the game starting with n blocks will obtain $n(n-1)/2$ points.

Base case: For $n = 1$, it is clear that we get 0 points since the game immediately terminates. This matches the formula $n(n-1)/2$. It also matches the sum as I have written it: the sum over an empty set of indices is 0.

Strong inductive step: Suppose we start with $n+1$ blocks. Our first step is to split this pile somehow into m_1 and m_2 blocks. Note that m_1 and m_2 are both between 1 and n—empty piles are not allowed! So it's OK that our base case is 1.

Our first claim is that we may now consider what happens to each pile independently. That is, after the first split, the total number of points we gain is just the sum of the number of points we gain from all splits of the first pile, and the number of points we gain from all splits of the second pile. Let us define the notation $F(n, S)$ to mean the number of points gained from splitting an initial pile of n blocks, following a strategy S. Then my claim in this notation is that

$$F(n+1, S) = m_1 \cdot m_2 + F(m_1, S_1) + F(m_2, S_2),$$

where S_1, S_2 are the strategies played on the two separate piles.

Now, the inductive hypothesis tells us that for all $m \leq n$, and for all strategies S', it holds that $F(m, S') = m(m-1)/2$. So we have

$$F(n+1,S) = m_1 \cdot m_2 + m_1(m_1-1)/2 + m_2(m_2-1)/2.$$

We're not quite done: we can still simplify this. Recall that $m_1 + m_2 = n+1$. So we have

$$\begin{aligned}
F(n+1,S) &= \frac{1}{2} \cdot (2m_1m_2 + m_1(m_1-1) + m_2(m_2-1) \\
&= \frac{1}{2} \cdot (2m_1m_2 + m_1^2 - m_1 + m_2^2 - m_2) \\
&= \frac{1}{2} \cdot ((m_1+m_2)^2 - m_1 - m_2) \\
&= \frac{1}{2} \cdot ((m_1+m_2) \cdot (m_1+m_2) - (m_1+m_2)) \\
&= \frac{(m_1+m_2)(m_1+m_2-1)}{2} \\
&= \frac{(n+1)(n+1-1)}{2}.
\end{aligned}$$

This is exactly what we wanted to show! So by strong induction, we are done! □

Example 2: "Beats ordering" Suppose we have a round robin tournament of n players, where every player plays against every other player exactly once. Let's also suppose that each match is a win for one of the players: there are no ties.

Q: Is there an ordering of the n players $p_1, p_2, \ldots, p_n$ such that for all $1 \leq 1 < n$, it holds that p_i beat p_{i+1} in their match?

We call such an ordering a "beats ordering."

As an example, suppose we have 4 players, labeled A, B, C, D, with the following tournament results:

- A beats C, D.
- B beats A, C.
- C beats D.
- D beats B.

Then a possible beats order is $ACDB$. Note that $ABCD$ is *not* a beats order, since A did not beat B.

Claim 6. *A beats order always exists for all n.*

Proof. The proposition $P(n)$ we wish to prove is: for all tournament results on n players, there exists a beats order for the n players. We will show it by strong induction.

First, the base case, $P(0)$: this is obviously true, because an empty list is a beats order for 0 players.

Now, for the *strong* inductive step. Here, we need to use a little bit of ingenuity. Suppose we have a tournament result for $n + 1$ players. Let us choose a player arbitrarily, and call them p'. We know that every other player either won or lost against p', by the assumption that there are no ties. Intuitively, we should put the players that won against p' *before* it in the beats order, and the ones that lost *after* it. So let's try that!

More precisely, let W be the set of players that won against p', and L the set of players that lost. We know that $W \cup L \cup \{p'\}$ is the set of all $n+1$ players. Moreover, we know that W and L have size at most n. (Note: either set could be empty!)

Now, it is time to apply the strong inductive assumption. We can assume that *for all* $m \leq n$, it holds that a tournament result on m players can be arranged in a beats order. So let us take the set W, and generate an ordering $p_1, \ldots, p_{|W|}$ for these players (using only the tournament results between them). Likewise, we may generate an ordering $q_1, \ldots, q_{|L|}$ for L.

Now, we claim that the ordering

$$p_1, \ldots, p_{|W|}, p', q_1, \ldots, q_{|L|}$$

is a beats ordering for the whole set of $n + 1$ players! To see why, let's go back to the definition: we need each player to beat the player immediately to its right. By assumption, this is already known for all players except for the ones next to p': in particular, we have to check that $p_{|W|}$ beats p', and that p' beats q_1. But this is true, since $p_{|W|} \in W$ and $q_1 \in L$! Thus, this is a valid beats ordering for the $n + 1$ players.

Hence, by the principle of strong induction, the proposition is true for all n! □