[SQUEAKING]

[RUSTLING]

[CLICKING]

ERIC DEMAINE: All right, let's get started. Welcome back to 6.1200. I am the second of the three lecturers in this class. You can call me Eric. And Brynmor will be on next week. So today we are going to continue our theme of induction and prove some even cooler and stronger forms of induction. Just a recap of where we were last time, as we've seen, we're growing our catalog of different proof techniques of how to prove different types of theorems, almost by like a cookbook. If you want to cook this, here's how you get started. And so here's a brief summary of this.

> If the theorem you want to prove starts with, "there exists something," then a natural way to prove that is by example or by construction. You construct a particular x star and prove that P of x star is true. And if you can do that, then you've proved that there exists an x, where P of x is true. It's straightforward, but it lets you unwrap-if I give you an expression that starts with "exists," then you know your first step is try to figure out an x where this is true.

> And of course, to prove P of x star you probably recursively use this cookbook. If you want to prove a universal, one common way-- if you want to prove for all x, P of x is true, typically your first line is take an arbitrary x. Just give it a name, x. And then prove that P of x is true no matter what x you started with. Therefore, it's true for all of them.

> Come back to induction in a second. If the main thing you want to prove is an implication, P implies Q, this is if P then Q. And I want to remind you that P implies Q is the same thing as not P or Q. We'll use this a bunch today. Then the direct way to prove this, what we call a direct argument, is assume P is true, and then prove Q is true. Because this implication, we only need to prove that Q is true when P is true. If P, then Q.

Or another way to prove that same statement, P implies Q, is what's called the contrapositive. It turns out P implies Q is the same statement-- it's equivalent to not Q implies not P. Remember, this symbol is a negation. Flip true and false. So to do that with a direct argument, we would prove that if not Q is true, then not P is true. In other words, assume not Q, and then prove not P.

This may seem magical. Why is P implies Q the same as not Q implies not P? But it actually follows directly from this equivalence. If you look at not Q implies not P, this is the same thing as-- let me go over here-- not not Q or not P, all right, because it implies-- it's the same thing as taking an or if you negate the first-- the part on the left. And not not Q is the same as Q, OK? So this was not Q implies not P. It's the same thing as. This is the same thing as this. And that is exactly this just by switching the order of the ORs. And so P implies Q is the same thing as not Q implies not P.

So that was contrapositive. There was a related notion of contradiction, where if you want to prove any statement P, you assume that not P is true and then find a contradiction. Prove that in fact false is true, or something is both true and false. All these things are very, very bad because we assume that our axioms are consistent. And so if you can prove false, that means that what you assumed must also be false. And so if not P is false, that's the same thing as saying P is true.

It feels very backwards. Lots of double negatives in there. But that's the nature of contradiction. We try to avoid them when we can, but sometimes it's really the right way to prove something. And the last technique we saw was induction, where if we have a universal quantifier over the natural numbers, we want to prove P of n is true for all natural numbers 0, 1, 2, 3, and so on, then we only need to prove it for some base case, P of 0. And then we need to prove that P of n implies P of n plus 1 for all n. So we'll talk more about induction in a little bit.

Today we're going to add to this list two more proof techniques. One is proof by cases, and the other is strong induction. So proof by cases is just a nice general technique to be aware of. It can be very powerful. Strong induction is going to be an even cooler form of induction. All right, but we'll start today with proof by cases. And we'll start with proof by 2 cases. And then we'll generalize to more than two cases.

So the idea is take any proposition C, and observe that C or not C is a tautology, meaning always true. If C is true, then this whole thing is true because C is true. If C is false, then not C is true. And so this whole thing is true. I'm going to remind you this V symbol is an "or." Whereas, the opposite symbol is an "and." I think the mnemonic here is this looks like a letter A. This looks like a letter O. I've heard some people say this looks like a lowercase r for "or." Anyway, you just remember these things. This is "or." This is "and."

So C or not C is the question, though, is always true. So we call it a tautology, fancy word for being always true. And so what this tells us is that our proposition P-- let's say we want to prove P-- is equivalent to C or not C implies P. So this is saying if C or not C, then P is true. C or not C is just always true. So this is saying if true-- in other words always-- P better be true. So P and this implication are equivalent.

Another way to see that is to rewrite this implication as a negation. So this is like saying not true or P. And so that's just the same thing as P because this is true. OK. Cool. So I want to rewrite this a little bit and say this thing is equivalent to C implies P and not C implies P.

Why is this true? It's like a distributive law. This is saying I want to prove that C implies P, and I want to prove that not C implies P. That's what I wrote over there. That implies that the combination of C and not C implies P. OK, so I claim these are equivalent. One way to verify it is with the truth table, or you can do it with some manipulation.

All right, so we have-- what this is saying is in order to prove P we need to prove that P is true assuming C and prove that P is true assuming not C. And these are the two cases in a proof by cases. Let me write out a little template for you. Let's suppose the theorem we want to prove is P. Theorem means something that's true and that we're about to prove.

And so we usually say proof by cases on the truth value. Of C. So this is for any. Statement C. Proposition is what the word I was looking for. Any Proposition C, it's either true or false. And so we're going to do proof by cases on the truth value of C. Case 1 is that C is true. And case 2 is that C is false.

And so what do we do in each case? Well, in the case that C is true, this means that we get to assume that C is true. And then use that to prove that P is true. And so the missing step in this proof outline or this template is we need to say P is true because some reasons, which we need to fill in. And similarly, in the C is false case, we need to prove P is true for some reasons.

So we need twice as many reasons, but the idea is that maybe assuming C is true makes it easier to prove P is true. Maybe also assuming C is false makes it easier to prove that P is true. So in these boxes here we get to use C. And in here, we get to use not C. And often, this makes proofs easier. But the challenging part is to pick the correct C. What's the right choice of C for this to be true?

And maybe one more line I want to add to this template, which is pretty obvious in the setting but gets much less obvious when you think about more than two cases. So a final step in this proof would be to say C is either true or false because all propositions are either true or false. And so the cases are exhaustive.

So this is also called a proof by exhaustion because we're really tired. Maybe we are also. But the idea is we want to exhaust all possible cases. And if we prove that we captured every possible situation and all of them P is true, then we're done. So that's what we'd like to do. I'm going to give you two examples. First one is very simple. The second one is more interesting. Questions? All right.

So the claim is, this is a general fact, that A implies B or B implies C is a tautology. So this means it's always true. Again, so you can rewrite this as for all A, B, and C, which are either true or false, we have that A implies B or B implies C is true. OK. Fun facts.

Let's prove it. And the proof technique we're going to use by cases, by two cases, namely, on B. B is either true or false. We could try to do a case analysis in terms of A or in terms of C. It turns out B is the right answer here. It will lead to the fewest cases. We'll only need two, intuitively because B is in both of these expressions. So it seems good to split on B because it will impact this one and this one.

OK. So case 1 is that B is true. If B is true, I claim that A implies B is true, which is this first half. Why? In other words, I claim that A implies true is a tautology. I think another-- again, an easy way to see this is to rewrite this implication as not the left-hand side or the right-hand side, not A or true. Well, that's just true. True or anything is true.

So in particular, over here, not A or B is true because we just assumed that B is true. So this tells us that A implies B, or anything, in particular B or C, is also true. So kind of trivial, right? If you assume B is true, then, of course, this is true. And so, of course, the whole thing is true. So easy when you have the correct case. Let's think about the other case. It's not enough to just have one half of the cases. We also need to think about when B is false.

When B is false, I claim that the other term is true. I claim that B implies C is true. This is maybe a little less intuitive. This is saying that false implies C is a tautology, like for any C, false implies it. And this should eventually become intuitive for you when you get used to implies and if then. This is saying if false, which means never, I need C to be true. But if this condition is never true, then I don't care about the right-hand side. If it's if-if pigs fly, then, I don't know, apples are orange or something. That's a true statement because it will never be the case that pigs fly, or at least in the present time.

So another way to see that is to think about, again, not B or C. B is false. So not B is true. And so, of course, true or C is also true. And so that tells us that anything or B implies C is also true. So in other words, this statement, which maybe I'll call P, I'll say in either case P is true. And so I write my little end of proof symbol. This is QED from last time. This means that I have demonstrated the theorem.

Cool. So in one case, this part was trivial. In the other case, this part was trivial because it's an "or." We're happy in either case, and we've done our first proof by cases. Pretty straightforward. Let's do a more surprising result using proof by cases called mutual friends and strangers. This is actually a famous mathematical problem. We're going to solve today a particular case of it, which is suppose you have six people.

And every two of them are either friends or not. And this is an exclusive or, so I'm going to write XOR. You're allowed to be friends or not friends, not both, and not neither. And in the not friends case, I'm also going to call them strangers. So this is like extreme friendship. Either you declare yourself as friends or as knowing each other, or you don't know each other. In that case, you're strangers. You're just never both, and it's always one or the other.

So you can think of this as I can draw a little picture of there are six people represented by circles. You can put smiley faces in them if you want. And maybe I connect them via a white line if they are friends and a dotted line if they're strangers. So let's-- and every two of them have one of these two pictures. Probably missing some. Here. OK, that's them all.

Then I claim no matter what the situation is, which ones are friends, which ones are strangers, there's always either three mutual friends or three mutual strangers. OK. In this example-- hopefully I drew enough. Yeah. These three people are mutual strangers.

They're connected by a triangle of dashed lines, OK? If I drew some other pattern, if they were all solid lines, then I might get the other situation, at least three mutual friends. But it turns out, if you have six people, they're always at least three mutual friends or three mutual strangers. Let's prove this by cases.

Whenever we apply a proof by cases, we need to come up with some proposition C that's either true or false, well, for a proof by two cases, which this will be. And it's a little work in this case to do it. It turns out a useful first step is to pick any person P. So just take the first person or the seventh-- or the fifth person out of six. Doesn't matter which one, but label it P.

So now we have a person to talk about. This is like the proof by example or by construction, right? Overall there, we want to prove an existence. We want to prove existence of three mutual friends or existence of three mutual strangers. So that's a useful step to either construct one. Or in this case, we're actually not doing much for construction. We're just taking an arbitrary x. But that will be enough for this problem.

So let me draw a little circle for P. And it might have some friends, and it might have some strangers. OK. How many of these lines coming out of P are there? Five exactly because there are six people total. P is one of them. So there are five people over here, OK? So turns out useful case strategy is to say either P has at least three friends, or it has less than three friends, right? Either there are three solid lines, like I've drawn here, or there are at least three-- or there are at most two solid lines.

OK. Let's think about this first case. P has at least three friends. Let's give them a name, Q, R, and S. So that's a general picture. Now we're assuming P has three solid lines to three people Q, R, and S. OK. This is not yet a triangle. We haven't solved the problem yet. But if we break into more cases we'll be able to. So case 1A is going to be some two of Q, R, and S are friends.

Suppose, for example, Q and S are friends. Have I found a triangle? Yes, P, Q, and S are mutual friends if this edge is here. Or if this edge is here, then these three people are three mutual friends. Or if this edge is here, these three people or mutual friends. If there's any edge in here that I can draw, any solid line between Q, R, and S, then those two people plus P form three mutual friends. So that case is actually easy. Great. Then P plus those two people are three mutual friends, OK, which was situation one up here. There's always either three mutual friends or three mutual strangers.

OK. So now we need to think about the other cases. Let's go over here. We found one case that was easy, but there's case 1B, which is maybe there aren't two mutual friends. And there's case two, where P does not have at least three friends. But it turns out all of these cases will be easy. So let's do case 1B.

Now, I get to freely choose what case 1 was, and I get to freely choose what case 1A was because whenever I split into cases, I get to choose my proposition C to be anything I want. So this was C in the first case. This was C in the second case. But generally, if you're doing proof by two cases, you have no choice at this point. So case 1A was whatever. Case 1B has to be the negation of this. So case 1B literally is not some 2 of Q, R, S are friends.

But if you think about that for a little bit this is saying Q, R, and S-- let me write this in a couple of steps. No two of Q, R, and S are friends. But that's the same thing as saying Q, R, and S are mutual strangers.

OK. We're using this fact, or this assumption, that every two people are either friends or strangers, always one or the other. So if there's no solid line over here, then all of these are dashed lines. So all three of these are mutual strangers. And there we found our triangle of strangers, OK?

So it turns out case 1A and case 1B are actually just as easy just reversed. So this was situation two. So either we got three mutual friends, or we got three mutual strangers. But we're still inside case 1. We just finished case 1. Now we need to think about case 2. So I'm going to unindent here and go to case 2. Case 2, again, has to be exactly the opposite of this. So P does not have at least three friends. By number of people being an integer, this is saying P has at most two friends. If it doesn't have at least three, it's at most 2 because the number of friends is always an integer.

OK. Great. So case 2 is a negation of case 1. And it turns out that is also kind of easy for asymmetric reason.

Remember, there are six people total. So there's P and five others. So how many strangers is P with? How many people is P a stranger to? Well, it's at least all the others, 5 minus 2. Because at most two of them are friends. The remainder have to be strangers. And so this is 3.

So P having at most two friends is the same thing as P having at least three strangers because there are five other people total. 2 plus 3 is 5. So case 2 is P has at least three strangers. Case 1 was P has at least three friends. These are almost the same. I just have to flip friends versus strangers. So the way I would write this in a proof is this is symmetric to case 1 swapping friends versus strangers. And of course, situation 1 with situation 2.

So case 2 would be P has at least three strangers, Q, R, and S. Case 1A is that some two of Q, R, and S are strangers. Then we conclude that P plus those two are three mutual strangers, which is situation 2. Or case 2B would be no two of Q, R, S are strangers. In other words., Q, R, S are mutual friends. And then we're in situation 1. So case 2 works just like case 1 just swapping the words friends and strangers because they didn't really have any meaning. They were just words. Cool.

So in all cases, we prove the desired result. Either situation 1 or situation 2 happens. This is a particular case of something called Ramsey Theory. What we've just found is that something called R of 3, 3 is at most 6. In general, R of f comma S is the number of people you need in order to guarantee that there's at least f friends or at least S strangers. So we just did at least three friends or at least three strangers. We showed that six people was enough. It turns out six people is exactly the right number. You need six people in order to guarantee at least three friends or three strangers.

If you wanted to guarantee four friends or four strangers, turns out you need 18 people. If you want to guarantee five friends or five strangers, turns out you need somewhere between 43 and 48 people. But we don't know how many. So while this problem was relatively easy, three friends or three strangers, five friends and five strangers already is an unsolved mathematical problem. So that's kind of cool and crazy how easily you get to very difficult problems. Of course, people will try to compute larger numbers too, but we don't have tight bounds, generally.

OK. I want to say one more thing about proof by cases, which is what if we want more than two cases? So more generally, proof by k cases. So instead of just C or not C, let's suppose we have a bunch of propositions, C1 through Ck. And let's suppose that this is a tautology, my favorite word for the day.

So suppose that it's always the case, C1 or C2 or dot, dot, dot, or Ck. One of these things is always true. Then we can follow this template which is suppose we want to prove a theorem that some proposition P is true. Then we'll say a proof by cases, and there's k of them. So I'm just going to write it generically. In case i, is that Ci is true. In other words, we get to assume Ci is true.

And then what we need to do is prove that P is true in that scenario. And P is true because reasons. And then here it's especially important to say that the cases are exhaustive because reasons. And exhaustive here just means that C1 or C2 or up to Ck is a tautology.

So you need to prove that C1 or-- dot, dot, dot, or Ck is always true. That's the meaning of the cases being exhaustive. So there's two parts. One is to prove that each case is OK. The other is to prove that those cases cover everything. So I won't show an example of k cases here. We'll see them in recitation, and so on. But I will tell you a story about one famous proof by cases, which is the Four Color Theorem. I'll illustrate the Four Color Theorem with an example.

So here's a map of the United States. And I've colored all the states, all the regions of this map with four different colors, red, green, blue, yellow, in such a way that if you have two regions that share a positive length boundary, then this color A is different from this color B. It has to be not equal. Otherwise, if you had two red regions next to each other it would be hard to see the boundary. So the colors illustrate the boundaries between all the regions.

Four colors seems to be enough for this map. It's also enough for this map of all the countries. Is it true for all the maps? Turns out, yes, this is called-- for a long time it was called the Four Color Conjecture. And then it became the Four Color Theorem at some date. So Four Color Theorem says you can color the regions of any planar map with four colors so that neighboring regions get different colors. This was first observed and conjectured in 1852 by a guy named Guthrie, who was a student of De Morgan. De Morgan, I think, his name will come up in a moment, famous logician. He actually invented induction as we-- one of the first people to-- he invented the term mathematical induction, at the very least, and really made it more formal.

So a student of him, Guthrie, said, hey, I took all the counties of England. And it turned out I only needed four colors. Is this a theorem? And he asked indirectly De Morgan. And De Morgan said, hey, seems cool. I don't know, maybe. Then the following year, 1853, another mathematician named Kempe proves the theorem. But proved should be in quotes because 11 years later, 1864, Heawood found a bug in that proof. Turns out there were a lot of cases in this proof, and the cases were not exhaustive. So it wasn't done.

Then, 15 years later, 1880, Tait proved the theorem. Then 11 years later, Petersen found a bug in that proof. Again, not all the cases were exhaustive. Then, 85 years later, 1976, Appel and Haken-- or maybe it's Appel, I'm not sure-- proved the theorem. And I think most people consider this an actual proof. But it's a little tricky. Just to give you a sense, this is where my-- I started hearing about the problem. I wasn't alive in 1976, but I heard about it later on.

There are 1,834 cases in this proof. They occupy about a 400-page printout from a computer program. And so this is one of the first mathematical proofs that used a computer to assist in checking all the cases. Because there's so many, 1,834, it's hard to do that by hand and be sure that you didn't make a mistake. So the computer proof, to me, is a little bit more sound. Also apparently checked by hand by Haken's daughter.

Then, five years later, Schmidt found what you could interpret as a bug in this proof, let's say an omission or something, but a missing situation. And then over the next eight years, Appel and Haken fixed all the bugs they could find, that one and some other wording issues, and so on. And then they published it in a book. But a book isn't refereed, so I don't know how many people have read that book. It seems like this proof is maybe correct. It's been many years, and no one has found a bug.

A little bit later, though, in 1996, Robertson, Sanders, Seymour, and Thomas, some of the top graph theorists in the world, found a simpler proof. That proof only has 633 cases. So that's a lot less, maybe three times fewer cases. And also, the length of the paper is shorter, maybe 10 times shorter. So that's progress. But is that proof true? It also used a computer to check the cases.

Finally, in 2005, Werner and Gonthier developed a fully computer-checkable proof using a system called Coq, where you write down every step in the proof. And then the computer just has to check that every mathematical derivation, all the derivations we saw last class, modus ponens, and all those things, are correct. This program has withstood many, many years of scrutiny. So we all believe that it's correct.

And so the fact that you can write the entire proof in this proof language suggests that this really is a true theorem now, thankfully. There won't be more missing cases. I believe that is just an implementation of the Robertson proof. So that one withstood scrutiny. But it's very tedious to write these proofs. And so for the Four Color Theorem, it's worth it, I would say.

All right, so that's just an example of, in general, proofs by cases can involve a zillion cases. It's very annoying, but sometimes that's the best thing we know how to do. Maybe we'll come up with a simpler Four Color Theorem proof at some point, but best we know so far has hundreds of cases. All right, let's go back to induction. At first I want to review induction a little bit, and then we will get a stronger form of it.

So I'm going to call this the induction axiom. This is what we talked about last class. We didn't call it an axiom. And in some setups it is an axiom. We're going to take it as one, something that we just assume is true. Although, as Zach mentioned, in modern times, you usually prove this using other-- using the definition of the natural numbers. But I'll just take it as something is true.

So for any predicate P of n over the natural numbers, if on the one hand P of 0 is true and on the other hand, P of n implies P of n plus 1 for all natural numbers n, then P of n is true for all natural numbers n. This is the magic of induction. You should use this probably in every problem you solve, not every problem, but extremely powerful tool. We're going to use it all the time throughout this class.

I want to give you a visual way of thinking about what's going on with induction, which I call block diagrams. So I'm going to think of a block, like a little box here, that takes as input-- think of it as a procedure. You give it some true propositions on the left, and it produces a true proposition on the right. OK. Or we could think of it as if I give you some proofs of these propositions, then this block will give you a proof of a proposition on the right.

So what's going on with induction is we're given two of these blocks, these two. So you can think of part 1, P of 0 is true, as a block that has no input. So this is what we normally call the base case. So it doesn't need to assume anything. And it just produces for you a proof that P of 0 is true. And the second part here, the induction step, says that if you can prove P of n is true and you plug it into the induction step, then it will give you a proof that P of n plus 1 is true. Saw a bunch of examples of this last time. We assume P of n, and we use that to prove P of n plus 1, OK?

Now, the cool thing about blocks is you can just chain them together. So if we chain, the only block we can place first is this base case because it doesn't need anything to get started. So we start with the base case argument. That produces P of 0. Now we plug this into the step. This step has to work for all n. So in particular, it works for n equals 0. And so we plug that into the step, and we get a P of 1.

We plug P of 1 into the step, so n equals 1. Then we get P of n plus 1, namely, P of 2. And we plug that into the step, and we get P of 3, and so on. So this just gives you some intuition for if I can build an argument for why P of 0 is true and I can build an argument for why if P of n is true, then P of n plus 1 is also true, then I can just repeat that argument over and over with different n, increasing n by 1 each time. And I can use that to prove that all the P of n's are true, OK? This is visual intuition for why this works. Of course, we're not going to actually prove P of n is true for all n, but should be pretty intuitive from that.

Or more abstractly, you can actually think of induction itself as one of these blocks. Let me use another color. So we have, on the one hand a block base which produces P of 0. And we have an induction step, which given P of n, produces P of n plus 1.

So I'm going to think of this as a thing that's true and this as a thing that's true. And then what induction gives me, induction is a block that, given these two facts-- if you can prove each of these things, then it gives me a new fact, which is for all natural numbers n, P of n is true.

So that's the-- instead of having to draw out this infinite length path, induction just does it all at once. It says, oh, I know I can chain these all together forever. Therefore P of n is true for all n, OK? I don't know if that helps, but it's another visual way of thinking about induction. Let's--

All right, let me tell you another equivalent formulation of induction, which I prefer. It starts out the same. Suppose P of 0 is true. The induction step I'm going to phrase slightly differently, almost the same. For all n at least one P of n minus 1 implies P of n. Then, for all natural numbers, P of n.

So the first and last lines are the same. We assume P of 0 is true. We're going to conclude P of n is true for all natural numbers. Here we started at 0, and we wanted to show that P of n implies P of n plus 1. Over here, we're starting at 1 and we're proving that P of n minus 1 implies P of n. These are exactly the same things. I've just shifted the indices by one. So these are identical statements, or equivalent statements.

I like this version. In particular, it will lead into strong induction. But I like this version as a computer scientist because I always want to think about-- what I want to prove P of n, not P of n plus 1. It's confusing to think about proving P of n plus 1. I always want to prove P of n. When n equals 0, OK, that's my base case. I proved that specially. When n is at least 1, I'm not in the base case, and I get to assume that P of n minus 1 is true.

You can think of this like a computer program. Think of a-- proving P of n is like running a computation f of n, or P of n. And I get to recursively call P of n minus 1 in order to compute P of n. n is given to me. This is the one I want to solve. If n is 0, then I solve it one way. If n is bigger than 0 or at least 1, then I recursively call P of n minus 1 or depend on that proof and use it to prove P of n. But you can use either one, whichever is more comfortable to you.

But really, you should use neither, and you should use this stronger form called strong induction. So let's do that. Strong induction just gives you more to work with. So it's in some sense more powerful. Logically, it's identical to induction. You can actually prove it using induction, and we'll do that. Let me first state the theorem.

So if for any natural number this is true, then for any natural number P of n is true, OK? Let me bring this one down to compare. So first thing maybe to notice is that it doesn't seem to be a base case here, which is a little weird. It's just one condition then this. Let's compare the steps, first of all.

Or I guess let's think about the case-- this has to be true for all n. If we think about when n equals 0, that's the missing base case, what this is actually saying is P0 up to P minus 1 implies P of 0. So this is kind of weird notation. I'm abusing the dot, dot, dot a little bit here. And for when n equals 1, this is P of 0. When n equals 2, this is P of 0 and P of 1. When n equals 3, for larger n it's very clear what this dot, dot, dot means. But when n equals 0 it's confusing. So I need to specify. This is defined to be true for n equals 0, OK?

So for n equals 0 what you have to do is prove that true implies P of 0. In other words, P of 0 must be true in all cases, OK? So there's-- but then for larger n, what this is saying is not only do I get to assume P of n minus 1, but I get to assume all the P of i's before P of n. So I would normally say P of i is true for all i less than n. This is what I get to assume. That's probably actually a better way to state this thing.

So with regular induction here, I got to assume that the previous P of n minus 1 was true, and I needed to use that to prove that P of n is true. But actually, if you look at this chain, by the time I'm proving P of 3, I've already proved all the smaller Pi's. So why not assume that. With strong induction, I get to assume that. In order to prove P of n, I get to assume all the Pi's where i is less than n.

Now, when n equals 0, I don't get to assume anything because there are no smaller i's. But when I get to P of 5, I get to assume P0, P1, P2, P3, P4. So I get to assume more, so this only makes my proof easier. OK. To be clear, this is usually proved in cases. Normally, you need to check 0 specially. That might be a base case. Maybe you have to check 1 specially. It depends on your implication argument. Often, this implication assumes that n is at least something, and then you have to prove all the smaller n's to be true specially. But we'll get to examples in a moment.

What I'd like to do first is actually prove that strong induction is true. This is not something you would repeat in your homework. You should just assume strong induction is true. But I think it's instructive to see why it's true as yet another example of induction. So we're going to use regular induction, this version, or actually, I think this version, the induction axiom, to prove strong induction, OK?

Now, this is a situation where we need to define a particular induction hypothesis that's not the obvious one. And this is not at all obvious. But I'm going to define ih of n to be this P of 0 and P of n minus 1. In other words, for all i less than n, P of i. I like that better because it works even when n is 0 because there are no i's less than 0. So that's just true when n is 0.

So this is the thing I want to prove for all n. And how do we do it? Well, as usual, with an induction, we have a base case. Base case is in of 0. So in of 0 is actually literally just true because we defined it to be that way. We say when n equals 0, this dot, dot, dot is true. Or you could say-- this is saying for all i less than 0, where i is a natural number. But there are no natural numbers less than 0, so this is like saying if false, then something. And that's just always true. So this is, by definition, in of 0 is true. Great? Easy base case as usual.

What's the induction step look like? I'm going to-- I get to choose. I could either assume ih of n minus 1 and prove of ih of n. Or I'm going to assume if of n and prove ih of n plus 1. So we want to show ih of n plus 1, assuming ih of n. Cool. So the key thing is we get to assume this is true. The strong induction says if this, then this. So we're assuming the if part. We're assuming that if this implication. And this thing here is exactly ih of n.

So this says ih of n implies P of n. So we know ih of n implies P of n. That's what we get to assume in our theorem statement here. And we just assumed that ih of n is true. Therefore, P of n is true. But P of n was not what we wanted to prove. We wanted to prove ih of n plus 1. So what is ih of n plus 1? Let's just expand out this definition here. It is P of 0 or dot, dot, dot, or P of n minus 1 or P of n because of incremented n by 1. This no longer ends at P of n minus 1. It now ends at P of n.

But this is almost what we had before. This is the induction hypothesis of n. That's this part, or P of n. That's just a formula manipulation. And this we assumed is true, ih of n is true. And P of n we just proved is true. Sorry. I wrote over here, but I meant and everywhere. This is and, and.

See? Even professors get the V's and wedges upside down. So I wrote it correctly here. It's the and of P0 up to Pn minus 1. Here we have the and of P0 up to Pn. And so this is ih of n, which we assumed was true by induction, and P of n, which we just proved using one induction step. Therefore, the and is also true.

And I believe that's the end of the proof, all right? I did a base case. I did a step. Oh, no, not quite the answer. Sorry. There's one more step here, which I will put over here. This is a good illustration in not skipping steps. What did we actually prove?

By induction, we proved induction hypothesis of n is true for all n. So by induction, the regular old induction axiom, for all natural numbers n, induction hypothesis of n is true. Induction hypothesis of n is this thing. But that's not what we wanted to prove. We wanted to prove P of n is true for all of n. But I can do some manipulation to make that what I want.

So this is like saying for all n, let's see. Actually, probably this is nicer. For all natural numbers, ih of n plus 1 is true, OK? This is a shift. It's actually a weaker shift. This includes ih of 0. This should not be greater than or equal to. This should be an element of. This includes 0. This doesn't. This starts at 1, and it goes upwards. But this is nice. So this implies this, right? This is what we've shown. This is a weaker statement because I just threw away ih of 0. ih of 0 wasn't interesting anyway.

ih of 1 includes inside of it-- so it's an and of a bunch of things. But then the last term is P of n. If I take ih of n plus 1, the last term in it is P of n. So it's also anded, but if the and is true, then every term is true. And so, therefore, P of n is true for all n. So this is a final cleanup. After we did induction, we didn't quite get the statement we wanted because we used a different induction hypothesis than just P. And then we needed to show that implied P of n for all n.

But it works. Cool. So now there should be no question about why strong induction is true, assuming you believe this proof. You can draw a diagram. It's a little trickier to do. Maybe I will show you in my handwritten notes here. Here is a block diagram for strong induction. It's harder to draw because you depend on so many things.

When I apply the fourth step here, when I want to conclude P of 4, I assume all the previous P's. So P0, P1, P2, P3, they all feed into this box. In the beginning, it's very similar. I apply a step, I get P of 0. Then I apply that P of 0 to a step. I get P of 1. But then, as I proceed, I'm feeding more and more Pi's into the step, and it gives me one more Pi, OK?

So it's a much more complicated diagram of what's going on under the hood, but from a usage standpoint, it only helps you. When you're trying to prove P of n, you don't just get to assume P of n minus 1. You get to assume all the Pi's where i is less than n. I forgot one part of the Four Color Theorem story, which was when I was growing up, I read a reprint of this article by Martin Gardner, which turned out to be published on April Fools, but I didn't know it at the time.

And in 1975, there was no proof of the Four Color Theorem. Appel and Haken was one year later. So at this point he published a joke saying, in fact, McGregor found this map, which requires five colors. I remember sitting there trying to color it with four colors and always failing. I was like, oh, my gosh. Four Color Theorem isn't true. Or Four Color Conjecture, as it was called then, isn't true. Isn't that amazing? But it was all a lie. In fact, you can four-color that map. But it's a very funny article if you want to read it. It's in the lecture notes, or part of it is there. All sorts of crazy things like, oh, it turns out, if you take e and you raise it to pi times square root of 163, the result is an integer.

## [LAUGHTER]

It's not true, but all sorts of crazy things. Also, chess has a crazy winning move. And-- anyway, let's relive the youth. All right, I think I'd like to, yeah, show you some examples of strong induction. But maybe first I should show you a template for applying induction, strong induction. We'll repeat some of the things that I've said, but I think it's good to have it concrete.

So here is a template. Suppose you want to prove something is true for all natural numbers. So for all natural numbers n, P of n is true. Then here's what the proof will look like by proof by strong induction. So generally, we're assuming P of k for all k less than n. And then we want to show P of n. Or you could shift the numbers by one, but this is my preferred way of thinking about it.

Usually, we prove this by cases, which is the method we just saw. This is why we're pairing proof by cases with strong induction. How do we prove P of n? Well, it might depend. Often, we have some base cases where n is small. So maybe we have to prove P of 0. Maybe we have to prove P of 1. Who knows? Let's say up to P of little b are the base cases. Maybe you have to prove those specially for some reason.

Then we do an induction step. So I'll say by cases here. Induction step we get to assume n is bigger than b because we just proved 0 up to b manually. And then we need to prove, in those scenarios, P of n is true because reasons. But the big thing here is we get to assume, in these reasons we get to use P0, P1, up to P n minus 1.

So that's the big win. And in the base cases, you also get to assume this. But for example, when you're proving P0 you don't really get to assume anything because there are no smaller Pi's. So often, you have to do these specially because the induction step assumes somehow that n is bigger than 0. Sometimes you get lucky, you just need the induction step. But usually you need base cases. Let's see some examples. And this will become much clearer.

So let's play a game called item stacking. Or it's really unstacking. So this is unstacking game. So we're going to start with one stack of n, and then a move splits a stack of S bigger than 1 items into two stacks with a items in one and b items in the other.

And you get to choose these numbers a and b, but you need conservation. So a plus b has to equal S. And we also don't want 0 height stacks. So we need a at least one and b at least one. And so you get to choose a and b however you want so long as there's at least one item in each stack.

So let's take a physical example. I've got lots of blocks here, but I have no audience. So we're just going to demo this myself. In real life, this is actually-- this was a snow day at MIT, and so we're recording after the fact. So all the students-- MIT students have seen it. This is specially for you at OCW.

So when we do a move from S-- so this is-- we have a stack of size S, and we convert it into a stack of size a and a stack of size b. We get a times b points. That's just the definition of the game, a times b points when you split it into a stack of size a and a stack of size b. So how should I maximize my score in this game? What's the best strategy? The game ends when all your stacks have size 1 because you can't make a move on a stack of one item. It has to be greater than 1 items.

So let's try. Here I have a stack of five blocks. And one thing-- maybe I'll try to split it roughly in the middle. So now-- here, I'll rotate this so you can see how it blocks a little bigger. These are five blocks. I split like this. So that's a group of 2 and a group of 3. Product of 2 times 3 is 6. I can do this level of arithmetic. So 6 is our total so far. When I split this one, I get one more point. That's 7. When I split this one, doesn't matter how I do it, I get 2 times 1. So that's two more points. That's 9. And when I split this group, I get one more point. That's 10. OK. So one approach gives me 10 points.

What if-- another natural strategy. That was like splitting in the middle. Another natural strategy is I just take one off each time. So if I take one off here, I get 4 points. If I take one more off, I get 3 more points. That's 7. 4 plus 3 is 7. I take one more off, I get 2 points. That's 9. I take one more off. That's one point. That's 10. Huh. 10 points that way, 10 points the other way as well?

Maybe there's a theorem here. Maybe no matter what I do, I get 10 points. Well, that won't be true. But for five blocks I will always get 10 points. For 6 blocks I will always get-- I don't know-- 15. Some more points. It turns out it doesn't matter what strategy you follow, you always get the same number of points for a given initial stack of size n. Let's prove that with strong induction.

OK. So theorem is for all natural numbers, every strategy for this game starting with the stack, one stack of n items scores-- magic formula is n times n minus 1 over 2. So that's the theorem. And we're going to prove it by strong induction in the straightforward way.

So our induction hypothesis is going to be exactly the theorem statement for a particular n. So I'm going to highlight this statement, everything except the quantifier. And I'll call that P of n. So what I wanted to prove is for all natural numbers n P of n is true. And so that's just going to be our induction hypothesis. We're going to plug that into this template here. Assume that P of k is true for all k less than n, and then prove P of n is true. So let's just try to do that.

So what I would normally write here is assume true-- assume that my theorem is true. Assume P of n is true. Sorry. P of k is true for all k less than n. I would say assume true for all smaller n. OK. We need to do something with the game. We start with a pile of size n. Let's just think about the first move. First move is something. It takes our pile of size n, and it splits it into some piles a and b.

So we don't know what it is. We don't know what a and b are, but we can give them a name. This has to work no matter what a and b are. But let's say consider first move, which we know we start with a pile of size n. And we produce piles of size a and b. And again, a plus b equals n, and a and b are at least 1. But otherwise, we don't know what a and b are.

OK. So we go down here. So we now have a pile of size a, and we have a pile of size b. Again, we don't know how big they are, but they are smaller than b. So I want to claim we are left with two piles. Or we can really think of those as two completely separate games, a and b. We're going to get some points from splitting up. We're going to get some points from splitting up b. They sum together. But these piles don't really interact from here on. We got a times b points from this first step.

We're going to get some points from the pile of size a. We're going to get some points to the pile of size b. How many points do we get? Well, in fact, our induction hypothesis will tell us because a and b are strictly less than n. Why? Because a plus b equals n, and a and b are at least 1. So there's at least 1 in each of a and b. And so the remainder must be strictly less than n. If there's one in a, then there'll be n minus 1 in b. If there's two in a, there'll be n minus 2 in b, in all cases less than n.

Because a and b are less than n, they're not necessarily n minus 1. So we couldn't just use regular induction. But they're less than n. And so by strong induction, by strong induction, we know that P of a is true, and P of b is true. We wrote that up here, some P of k for all k less than n.

So a and b are less than n, so P of a is true, and P of b is true. So that means, from the pile of size a we get a times a minus 1 over 2 points. From the a pile we get b times b minus 1 over 2 points from the b pile. And then, of course, we got a times b points from the first move.

And so now we just need to do some algebra and add up all these points. So the total number of points that we get is a times b plus a times a minus 1 over 2 plus b times b minus 1 over 2. These two were by induction. This was the first move. And now let's just put everything over 2. So this is 2 times a times b plus a squared minus a plus b squared minus b all over 2.

And now, what do I want to get to? This is supposed to equal n times n minus 1 over 2. And what was n? n was a plus b. So what I'd really like to show here is a plus b times a plus b minus 1 over 2. That's my goal. And what I need to do is fill in the in-between. But this is not too hard because, let's see, I see a times b here and a times b here.

In fact, you can just expand this out, and you'll get exactly the same thing here. I think slightly more intuitive is to see, oh, look at this term, this term, and this term. That is a squared plus 2ab plus b squared. That is a plus b squared. And then we have a minus a, minus b over 2. But interject a rule in between. We have a plus b squared minus a plus b over 2. And then these two are the same thing. I think that's pretty clear.

So cool. We did some algebra, and we just computed what we get out of induction. And then boom! We get the answer n times n minus 1 over 2. And it works. How did we know this is the right answer? We were just told that by the theorem. Probably, you would try this for very small n and make a conjecture. Oh, it seems like it's n times n minus 1 over 2. Let's try to prove it. And when you assume the right thing, the proof just works. And it's kind of magical. And that's strong induction.

Again, we need a strong induction here because we need to assume what we wanted for all smaller n because we don't know what a and b are. This has to work for all a and b less than n. So luckily, strong induction gives us that.

All right, I have one more example to tell you about, a slightly more complicated version of the same thing. We're going to use strong induction. Don't need any of these. So let's go. This is the problem called Beat Ordering. I guess somewhat relevant today because it was the Super Bowl. But this is just about any teams of games. Sorry. n teams in some game. And setup is that every two teams play a game, and there are no ties.

One team wins, and the other loses. OK. This is like friends and strangers, where it's either one or the other. But in this case, it's asymmetric. They're not both happy or both sad. One is happy, and one is sad. OK. This is what's called a Round Robin tournament. Most sports are not played this way unless a small number of teams because it's a lot of different teams. It's actually n times n plus 1 over 2 teams games, which is a lot.

All right, so what we would like is what's called a beat ordering. This is an ordering of the teams T1, T2, up to Tn, such that B1 beat-- sorry, T1, T for teams. T1 beats T2. T2 beat T3, and so on. And Tn minus 1 beats Tn. OK. Let's draw a little example.

There's team rock, team scissors, and team paper. OK. Paper beats rock. Rock beats scissors. Scissors beats paper. OK. This is a possible outcome in a three-team tournament. There's not necessarily one best team here. There is no best team. But maybe paper and rock play a game, And. It happens that paper won. Maybe rock plays against scissors, and it happens rock won. And scissors played against paper, and it happens scissors won. OK. You can tell why I named the teams this way.

Then one way I could order these teams is paper, rock, scissors because paper beats rock. Rock beats scissors.

OK. So this is the input. And this is my goal is to produce an ordering like this. But I need to do it for n teams, not just for three. So let's do strong induction to prove that the theorem is a beat ordering always exists.

OK. Theorem. And when I say this always exists, what I really mean is for all n and then for all tournaments of size n there exists a beat order. OK. There exists an ordering of the n teams such that the first one beat the second one, the second one beat the third one, and so on. I should say, for all i Ti beat Ti plus 1.

So we claim this is true. Proof by strong induction. So we're going to assume that this statement is true. Namely, this statement is true for smaller n. And then we're going to prove it for n. OK. Let's pick a team, any team. Call it T. Then I'm going to split everything with respect to t.

So I'm going to define W to be the set of teams that win against T. So this is going to be a set of all teams S where S beat T. So this is 1 versus T. These teams win versus T or 1 versus T. And L is going to be the set of teams that lose against T. So this is the set of teams S where TBS. So this is a loss versus T.

Then, intuitively, what we'd like to do is put the winners first, then put T, then put the losers. I claim that works, OK? But how do I order the winners? How do I order the losers? Well, by induction. I claim the size of W-- this vertical bar means the size of the set-- is less than n. And the size of L is less than n because the size of the winners plus the size of the losers plus 1 equals n.

This is a 1. Why? Because every team is either T, or they won against T, or they lost against T. So this is counting all of the teams. There's T itself, the ones that win against T, the ones that lose against T. Together, that is exactly n. Every team is exactly one of these categories. And there's a plus 1 here. And all of these are nonnegative. Here, W and L might be 0, but there's this plus 1. That means both W and L are strictly less than n. So the induction applies to them.

So by induction. This thing is true for any tournament of size W there exists a bit ordering of W. For every tournament of size L there exists a beat ordering of L. So we get a beat ordering. We get two of them, really. Let's call it W1, W2, dot, dot, dot W size of W. This is for-- this is an ordering of capital W. And we get L1, L2, dot, dot, dot, L size of L as a beat ordering of capital L.

And then, we concatenate. So we claim W1, dot, dot, dot W size of w, then T, then L1, dot, dot, dot L size of L is a beat ordering of all n teams. Again, this is all the teams. All the teams either won against T, or they are T, or they lost against t. And the idea is this part is beat. W1 beats W2, W2 beats W3, and so on, by induction because this is a beat ordering of capital W. Over here, this is a beat ordering of capital L.

And so by induction all these are OK. L1 beat L2. L2 beat so on, dot, dot, dot beat L size of L. The only things we need to check are these two commas. We need to check that W sub big W-- W sub size of W beats T, and T beat L1. Why are those true? By our definition of W and L. Everything in W beat T. So this is by the definition of W. We know that all of these beat T.

So in particular, this one beat T. And we know by the definition of L all of these teams lost against T. In other words, T beats all of these teams. And in particular, T beat L1. And so by combining all these beat statements together, we know that this entire thing is a beat ordering. Each item beats the one right after it. So it's a little more complicated. But again, we're d quite often with strong induction proofs, you apply induction twice.

You have some problem with size n. You split it into two parts. In general, you might split it into many parts. Then you recursively solve the two parts or the many parts, as long as they're strictly smaller than n. By induction, we know they work out. By strong induction, we know they work out. You take those solutions and you combine them in some way. Here, we concatenated with T in the middle.

Over here, we summed them up. We summed up the number of points we got in each one plus the number of points we got in the first step. And in general, you combine them in some way, and you prove that the thing you want to prove holds for size n. And then you get your theorem. So that is the power of strong induction. Thanks.