PROFESSOR: Now generally speaking, a proof is going to have seven characteristics that you want to keep in mind. Good proofs are correct-- that's obviously important-- complete-- you've got to have all the details there. All of the key steps have to be there.

They should be clear so we can understand what's going on. Brief is good. You don't want to crush somebody with all the details. You want to get to the key points, and be crisp.

It's really nice if they're elegant. Now, that means clever. It's the mathematician's notion of beauty.

Like you go to the art museum, and the artists will say, wow, that's a beautiful painting. In mathematics, you say, wow, that's an elegant proof. It's crisp, clever, short, to the point.

And it's really the highest compliment you can get from a mathematician, anyway. And there's a lot of judgment that goes into that. Just like in art-- there's judgment over what is great art.

The proof should be well organized. For example, use lemmas the same way you would use subroutines in writing code-- helps to make it clear. And the proof should be in order.

Sometimes you'll see proofs where things are done in a haphazard fashion. All the pieces are there, but they're in the wrong order. Sometimes-- and they teach this in some high schools-- they teach you to do proofs backwards.

And the classic thing there is, say you're trying to prove a equals b. Well, the proof sometimes will start with what you're trying to prove. And then they'll do a bunch of steps. And then you'll end up with 1 equals 1, and you'll write a check, because you went from a equals b to 1 equals 1. And that's, of course, true.

Now, that's not a good thing to do. It can be correct if the implications go this way. Because really, you're starting with a fact-- 1 equals 1-- and deriving a equals b. So if, in fact, the implications work this way, then your proof is right.

But most people, especially as you get farther along, think about it going from top to bottom. So don't use this technique, because it'll confuse people. You're liable to make a mistake. Just start with 1 equals 1 and work your way from there-- top down for being in order.

Now, good proofs are very much like good code. In fact, one of the reasons we care so much about teaching you how to write a good proof in computer science is so that later on, you'll be able to prove that your programs are doing what you expect-- what they're supposed to do. Now, there are many famous examples where programs did not do what they were supposed to do, with disastrous consequences.

The Airbus A300 was one of the first commercial jets totally operated by software. It could take off, fly, and land totally by software. It was a major advance in the airline industry.

The only problem was, that on one of the first flights of the A300, the software accidentally opened the rear door just before landing. And the plane crashed as a result. It was the first plane crash in commercial history because of a software bug.

There's a famous radiation device for cancer patients called the Therac-25. It's famous because it got into a race condition occasionally, which caused the device to just slam the patient with radiation-- so much so, it killed the patient. And they had multiple examples of this, and of course, a lot of lawsuits afterwards.

How many of you all remember the 2000 election? A few of you do. OK, this will probably be the last class that remembers that. But that's where Al Gore was going up against George Bush-- very close election-- all came down to recounting the votes in Florida.

But in fact, Al Gore got negative 16,000 votes in one county because of a software bug in the electronic voting booths, which I think they got rid of a lot of them in the election after that. Because the software was buggy. So poor Al had enough problem which chads and funny business in Florida. But getting negative 16,000 votes certainly didn't help his chances.

Several years ago, a single faulty command in a computer system used by United and American Airlines grounded the entire fleets to both airlines for close to a day. Because they couldn't do anything. They're all run by computer, and the whole thing was screwed up. So there's lots more examples.

We run into this issue all the time at Akamai. Akamai is a company started by MIT folks-- by

myself, and Danny Lewin, and a dozen undergrads in the late 1990s. And we deliver a lot of the content you get on the web-- Facebook, all the search engines. A lot of the stuff you go to comes from our servers.

So we've got to be very careful that we don't have software bugs. Now, in fact we do. And we catch them every once in awhile.

But if we got a bad one, it would bring down all the sites you go to you. You wouldn't be able to go to those sites anymore. And everybody would notice. It would be sort of embarrassing.

Now, this really does matter. And this is going to sound a little scary, but someday-- probably 30, 20 years from now, somewhere in there-- it's possible that all of us, our lives may depend on the software that some of you write.

In fact, to bring this home how scary it is, look at the person sitting next to you. And imagine that in 25 years, your life depends on whether their code does what it's supposed to do-- little scary. That's why we are very motivated to help you learn how to make rock-solid arguments, so you don't have code that fries one of your classmates someday, or puts him in a bad plane situation.

Now unfortunately, writing rock-solid proofs is a very hard thing to do. Even the world's best mathematicians mess them up on a regular basis. In fact, it's estimated that one third of all published proofs have bugs, have flaws, that render the proof incorrect.

The trouble often arises because we get lazy. We don't write down all the details or all the steps. Because, wow, it's clear. Let's just move on.

Now, this can be OK. Not such a good practice, but it dramatically increases the chances of making a mistake. And there's some very famous examples in the math literature from the world's most famous mathematicians.

Gauss-- and we'll talk about Gauss later during the term-- he's one of the most famous mathematicians ever. He wrote his PhD thesis in 1799. And it's usually referred to as the first rigorous proof of the fundamental theorem of algebra.

And that says that every polynomial has a 0 over the complex numbers-- something probably a lot of you learned in high school. You get a polynomial. You can find roots of the polynomial over the complex numbers.

But his thesis contains the following quote, "If a branch of an algebraic curve enters a bounded region, it must necessarily leave again. Nobody, to my knowledge, has ever doubted this fact." Warning signs-- buzzers-- should be going off in your brain.

"But if anybody desires it, then on another occasion, I intend to give a demonstration which will leave no doubt." So he's using something that he believes to be true. He sort of thinks it's clear, that everybody knows it. But he writes this down.

And when you're writing that down, you know there's a problem. And in fact, there's another Fields medalist-- we talked about Fields medals last week-- Stephen Smale writes that this was an immense gap in the proof that was not filled until 1920-- more than 100 years later. So Gauss never could give the proof, and nobody did for over a century more.

Remember the Poincare conjecture from last week? We had Colbert talking about that. In 1900, Poincare claimed it was a simple fact. Four years later, he decided it wasn't so simple, and he demoted his claim to the status of a conjecture. And of course, this became the famous Poincare conjecture, which took another century to solve.

So when you think you see yourself doing this, famous mathematicians do it too, and it catches them. So you want to not try to do that. Now, in fact, just to really bring home the point, we've made a top 10 list of proof techniques you should not use in 6.042.

So everybody go to the handout here. In fact, there's lot of them on the back, too, but on the front page, there's the top 10. So we're going to go through these. These are the ones we've most observed in 6.042 over the years.

Number 10-- proof by throwing in the kitchen sink. The author writes down every theorem known to mankind, and then adds a few more for good measure. Now, this is good, because when you're questioned later-- you're trying to get a better score on your exam-- you say, look, the proof contains all the key facts. They're all here.

And so that does help. You get extra credit if all the facts are there. We are literally seen students copy over their crib sheet, if they got enough time, for a problem they're not knowing how to solve, just to get all of the facts in there.

Number nine-- proof by example-- the author gives the case n equals 2 and suggests it contains most of the ideas of the general proof. In fact, a student before a class was telling me

on one of the homework problems, he talked about it to his non-math friends, and they gave examples, not the proof.

Number eight-- proof by vigorous hand-waving-- one of my favorites-- I get up here and wave my hands. And it must be true.

Number seven-- proof by cumbersome notation-- here the reader gets hopelessly confused, gives up, and says OK. In fact, I once had a grad student, and we called him the encryptor, because he could take the simplest proof and so encrypt it in notation and God knows what, you could never understand the proof and figure out if it was really right or wrong.

That goes well with number six-- proof by exhaustion-- so does throwing in the kitchen sink. Number five-- proof by omission-- you will see that a lot, also by faculty-- "The reader may easily supply the details. The other cases are analogous-- trivial."

Experts use that all the time. You can find a lot of my papers online. "The proof is trivial"-- very bad. Every once in a while, it turned out not to be so trivial.

Number four-- proof by picture-- we've seen those, saw one on Tuesday. Number three-- proof by vehement assertion-- sort of like the hand-waving. The more forceful you are in your argument, the higher you raise your voice, the more intimidating you become, doesn't make it more true.

Number two-- proof by appeal to intuition-- you say, "any moron knows that." Well, you're sort of reluctant to now question it. And then number one-- proof by reference to eminent authority. I saw Fermat on the elevator and he said he had a proof.

I don't think so. Fermat's been dead for over 300 years. And he was not so reliable in the first place. In fact, he has one of the most famous assertions that turned into a conjecture, called Fermat's last theorem. And it was not really a theorem by the time he died.

How many people have heard of Fermat's last theorem? Raise your hand. Yeah, pretty famous. It's the one theorem he proved that actually, he didn't prove. It says, for all n bigger than 2, there does not exist an x, y, and z in the natural numbers plus the positive natural numbers such that x to the n plus y to the n equals z to the n.

Now of course, for n equals 2, that's just the Pythagorean theorem. You can find three, four, and five, when you square them satisfy that. But it says this does not work for any higher

value, any higher power, than 2.

Now in 1637, Fermat wrote in the margin of a block that he had discovered a proof of this result, but the proof was too long to fit in the margin. And so he wasn't going to supply the details there. And he never did supply the details.

And it took 350 years and 100s and 100s of pages. A fellow named Andrew Wiles-- took him personally over 10 years. He more or less locked himself in his room for 10 years, produced 100s of pages, and he finally did prove Fermat's Last Theorem.

So Fermat was right about one thing-- it would not fit in the margin. At least, there's no proof that we know of that would fit in the margin of a book. Any questions on proof technique? We're going to pound a lot on this over the next few weeks.

All right, next we're going to look at a class of puzzles that was very popular in the late 1800s. Now, in these puzzles, you have a grid of letters or numbers. And you've got to slide the letters and numbers around to put them in order.

And so as an example, here's the problem on a three by three grid, or an eight puzzle. You want to find a sequence of moves to go from this configuration. I'll do a three by three case.

I have a here, b here, c, d, e, f. And I've put g and h out of order. And that square is blank, and I can move tiles or letters into it.

I'm going to start here. And I eventually want to get to the configuration where the letters are all in alphabetical order. So g and h are in order. Now, a legal move means you slide a letter into an adjacent blank square.

And you can go in a row or a column.

OK, everybody understand the game, what you're supposed to do? You slide these things. That could go down. That could go across.

How many people played a game like this before? Good, a lot of you. OK, so I need some volunteers who are good at solving puzzles that can do this, have played games like this, that are pretty quick at it.

So I've got it here. Who would like to come down? There are prizes if you can solve this.

What we're going to do is solve this. And see if you can solve it in three minutes. But I need three students to come on down and do this.

Who'd like to volunteer? Who thinks they can handle puzzles under pressure? So you have the g and h out of order. So it's not so hard.

You move the f down there. I don't know, play around like that. So I need some volunteers. Who'd like to come down and do this?

You can win candy. I've got candy here. There's even a prize if you don't make it in three minutes. Who wants some candy? Nobody?

Is there a prize if we don't make it?

What's that?

Is there a prize if we don't make it?

There is. Come on down. All right, now, who's going to help him out? I need a couple more people here just to mess him up, because by himself-- there we go-- good. Anybody else like to come on down? Because if we get three, it really gets hard, because you fight over what moves to make.

Now, what I'd like you all to do is sort of scream out possibilities for him. Like he figures it out there, you scream out, that'll really screw him up. OK, now, you can't pick them up. You've just got to slide them around.

And you can go, and we'll go to 2:56, and see if you can solve it. If you can solve it, you guys get candy. And if you can figure it out out there, let them know.

Slide to the gray area.

No, you can't use the gray area. All right, you've got about two minutes. They have the g and h in order. Everything else is pretty well screwed up, though.

What do you got? A, b, c, d, e, f, h g-- no, no, no, that's where you started, guys. That's not it. It was close, just one was out of order is all. Just one letter at a time. There you go.

I think they need help. We got about a minute ago.

Cannot see anything.

You can't see anything. Well, I don't know if it would help. You want to show them where you are?

This is not looking good.

We're pretty close to the end here, guys. A, b, c, f, e, d, g, h-- g, h is good. F is not so good. All right, you got about 30 seconds.

Whoa, what are you guys doing? One at a time here. One at the time. In fact, I think time is up here.

All right, 2:56. Oh, no, no. That we don't do. No diagonal moves-- no, no, no, no.

All right, well, you guys were good sports, so you do get a prize. It's not the candy, but I have these wonderful plastic Nerd Pride pocket protectors for you. There you go, very good sports. Thank you, well done. All right.

[APPLAUSE]

Now, I was a little cruel to these guys, for a lot of reasons. It's impossible? You think?

[INDISTINCT CHATTER]

Yeah it is impossible. This is impossible to do. Let's see if we can prove it's impossible. Because it doesn't seem so hard, necessarily.

But let's take that as a theorem. There is no sequence of legal moves-- diagonal moves makes this a lot easier-- to invert g and h and also return all the other letters to their original order or position.

Now, to prove this, we're going to use what's called an invariant. It's a very powerful and commonly used concept in computer science, very closely tied to induction, as we'll see. In order to show that your system can never reach a particular special state, it is sufficient to

show there's some property called the invariant that holds at the initial state, and that is preserved by every legal move, and is not present-- does not hold-- in that special state. The idea is, if you get this magic property called the invariant and it holds at the start, and it holds across every step, then the only states you can reach have to have to have the property, be invariant. And if the special state doesn't have that property, you can't reach it.

All right, so there is going to be some property we're going to look for that held at the beginning here-- and the beginning had this set up-- that holds, is preserved, by every move, every legal move, but does not hold in this state. And therefore, you can never reach this state legally. So they were doomed.

So we've got to figure out what that property is. And that's always the trick in analyzing systems or algorithms-- is what's that key property, the invariant property? So to figure out the invariant, we sort of have to look at what happens during a move in this system-- a transition.

Well, there's two kinds of moves. There's a row move. And an example of a row move is you might have a, b, c, d, g, e, f, h.

And I'm going to move the g its row to the blank square. So it would become this state. So g moves rightward into the blank, and the rest stays the same.

Now, when I make a row move, did the relative order of the items change? No. Of course, to be precise, I better define what relative order means, or the natural order. So by the natural order, I mean this ordering-- 1, 2 3, 4, 5, 6, 7, 8, 9.

So if I look at the order here, g moved from 5 to 6, but didn't change order with respect to any of the other guys. Let's state that as a lemma. Because that'll be very useful.

Lemma 1-- a row move does not change the order of the items or the letters. Proof-- well, it's obvious. No, you can't let me get away with that, right? Because I'm not to let you get away with that on homework. That's not so good.

So we've got to be a little more careful in the proof here. Otherwise, we just head down the path to trouble. So let's sort of specify, what does a row move mean-- just get a little bit of math and specification around it.

Well, in a row move, we move an item-- a letter-- from some cell i, whatever i-- it could be anything 1 to 9-- into an adjacent cell. What are the possibilities for the adjacent cell? Plus or

minus 1, yeah, into cell i minus 1 or i plus 1. Nothing else moves.

Hence, the order of the items is preserved.

Because if you're going with i to i plus 1, everything else is in i minus 1 or less, i plus 2 or more. Relative order does not change in this case. And I'll claim that's enough.

You know that I've thought about it a little bit. I've really quantified that i goes to i minus 1 or i plus 1. Nothing else moves. Therefore, we're done. Now, I could've added some more sentences here, like I talked about. But this is probably enough in this case, for this guy.

So in fact, if we only had row moves, there's not much that happens. The order never changes with row moves. So we never get there. But column moves are more interesting.

So as an example of a column move, a, b, c, d, f, h, e, g-- say I move the g up. Then I would get this one-- a, b, c, d, f, g-- because g moved up-- h, e. So g went to there.

Did the ordering change for this move? Yeah. How so? What things changed order? Which pairs of letters changed order?

AUDIENCE: G changed [INAUDIBLE].

PROFESSOR: G changed by three-- moved three in the order. And what letters did it change relative order with?

AUDIENCE: [INAUDIBLE].

AUDIENCE: The two preceding it.

PROFESSOR: Yeah, the two preceding it. g used to be after h and e. Now it's before h and e. All right, so it changed relative order with two items. It changed its position by three. It moved up three in the ordering. And so it changed order with the two in between.

Let's look at another one. Because we're really doing these examples to hunt for an invariant, is what we're trying to do here-- something that will let us prove we can never get to the desired state. Let's look at this one.

a, b, c, d, g, h, e, f goes to-- I'm going to move b down this time-- a, c, d, b, g, h, e, f. So b

moves down. The relative order changes. Which pairs got changed in the relative order?

AUDIENCE: b.

PROFESSOR: b changed with--

AUDIENCE: c and [INAUDIBLE].

PROFESSOR: c and d. b used to be before c and d. when it moves down here, it goes after c and d. Any guess about what Lemma Two is going to be? What happens when we make a column move?

AUDIENCE: [INAUDIBLE].

PROFESSOR: Change the order of--

AUDIENCE: [INAUDIBLE].

PROFESSOR: Good, so a column move changes the order of a guy with the previous two or the next two, which means the relative order of two pairs change. So let's take that as Lemma Two. When we say don't do proof by example, we don't mean don't try examples. Because by trying examples, you find out what you're trying to prove. So that's good to do.

A column move changes the relative order of precisely two pairs of items. So let's prove that. In a column move, we move an item in cell i for some i to a blank spot in cell what?

AUDIENCE: [INAUDIBLE].

PROFESSOR: i minus 3 or i plus 3?

AUDIENCE: [INAUDIBLE].

PROFESSOR: OK, and just to see that, let's draw out the natural order. I've got 1 2, 3, 4, 5, 6, 7, 8, 9. Column moves could be here-- 1 to 4, and 4 to 1, 2 and 5, 3 and 6, 4 and 7, 5 and 8, 6 and 9.

All 12 possible column moves, this works for. They're always separated by 3. And when an item moves three positions, it changes relative order with two other items.

And you can even write down what they are. It's i minus 1, i minus 2, or i plus 1, i plus 2. Those are the guys it changes order with.

All right, we've got two lemmas here. That one's done now. In a row move, order does not

change. In a column move, two pairs of letters get flipped.

That's all you can do with this puzzle now. So can anybody think of something we can work with to get an invariant here-- something that won't change? What we should be focusing on? Yeah.

AUDIENCE: You can only switch two pairs of items at a time. So if you don't have an even number [INAUDIBLE] switch [INAUDIBLE].

PROFESSOR: Yeah, that's good. So really, to focus in on there is, if you have an even number of things out of order to start, you're going to have an even number forever, because you can only change two at a time. That's a great idea. Let's really specify that now, and define that.

A pair of letters or items, call them L1 and L2-- they form an inversion, also known as an inverted pair, if L1 precedes L2 in the alphabet, but L1 appears after L2 in the puzzle. All right, so that is an inversion. So for example, let's see how many inversions do we have in this case?

We've got a, b, c, f, d, g, e, h. How many inversions are there in that state of the puzzle? Yeah?

AUDIENCE: Three.

PROFESSOR: Three, good. And what are they?

AUDIENCE: d is after f.

PROFESSOR: Yeah, d, f is an inversion. e, f is an inversion. And what's the last one?

AUDIENCE: e, g.

PROFESSOR: e, g is an inversion. Yes, so the answer is there's three inversions in this puzzle. And if I keep doing row and column moves to this, what do I know about the parity of the number of inversions?

AUDIENCE: [INAUDIBLE].

PROFESSOR: Will always be odd-- that's sort of interesting. OK, now, how many inverted pairs are there in the start state way back over here? How many inverted pairs here? One inversion.

How many inversions here? Zero. All right, and can you see where we're going to head here now? If I started with one, that's odd. And every time I do a row move or column move, it's going to stay odd. And I can never get here.

Is that clear what we're trying to do? So let's keep doing it. Let's go over here.

All right, so now we'll use Lemma One and Lemma Two create this notion that we only change the number of inversions by an even number. And Lemma Three-- during a move, the number of inversions can only increase by two, decrease by two, or stay the same.

And this proof is pretty easy. There's a couple of cases. In a row move, what happens? How does the number of inversions change in a row move?

AUDIENCE: Stays the same.

PROFESSOR: Stays the same-- no changes-- and that's by Lemma One. Now, in a column move, there's three cases. But we know two pairs change order-- that we know. That's Lemma Two. All right, by Lemma Two, we know that. But the three cases are-- let me start on the next board.

So Case A is that both of the inverted pairs were in order originally, before the column move. What happens to the number of inversions in this case, as a result of the column move?

AUDIENCE: [INAUDIBLE].

PROFESSOR: Goes up by two. Case B is that both pairs were inverted before I made the column move. What happens to the number of inversions in that case?

AUDIENCE: Decreases by two.

PROFESSOR: Decreases by two-- they were in order, so they were inverted. Now when I flop them, they become in order. So inversions drops by two.

And Case C is there's one of each. One of the pairs was inverted. The other wasn't. What happens to the number of inversions in that case?

AUDIENCE: [INAUDIBLE].

PROFESSOR: Yes, stays the same. All right, and we're done. That's what the lemma says-- I can go up by two, down by two, or stay the same.

All right, now a simple corollary of this is that during a move, the parity-- i.e. even or odd of the number of inversions stays the same. It can't change at all. During a move, the parity-- and the parity means even, odd. Sometimes it's called 0, 1, but the evenness and the oddness of the number of inversions does not change.

AUDIENCE: Instead of two pairs you mean one pair, right?

PROFESSOR: Where?

AUDIENCE: [INAUDIBLE] pairs.

PROFESSOR: Oops, I mean one pair's inverted, one pair's not.

AUDIENCE: [INAUDIBLE].

PROFESSOR: No, I mean two pairs change order in a column move. Let's go back and look at that. So I'm doing a column move.

For example, g goes up. g, h changes order. g, e changes order. g changes order with these two guys, so there's two pairs that got flipped.

So in a column move, two pairs reverse their order. If they were in order, they become inverted. If they were inverted, they become in order. Any other questions? Yeah.

AUDIENCE: So we're saying that letters can be numbers in more than one pair?

PROFESSOR: Yes, a letter can be in-- a letter is in seven pairs, because there's seven other letters. And in fact, we're looking at a space of 8 times 7 divided by 2-- 28 pairs of letters. So there could be 28 inversions if they're all out of order. Any other questions?

OK, well, we're getting there. We're almost done. I've got to prove this corollary that during a move, the evenness or oddness of the number of inversions does not change.

And that's because adding or subtracting 2 from a number does not change its parity. It stays odd or stays even. So adding or subtracting 2 does not change the parity.

All right, now we're ready to state the invariant. Anybody tell me what the invariant is going to be? What's the invariant going to be in this system?

AUDIENCE: [INAUDIBLE].

PROFESSOR: Yeah, the parity of the number of inversions is odd, because it starts that way. It's preserved. And it won't hold in the desired end state that we're looking at.

So we can state that as follows. In every state or configuration reachable from the start state, which is a, b, c, d, e, f, h, g-- which are out of order-- the parity of the number of inversions is odd. And the proof will be by induction. And invariant proofs are always by induction.

And the inductive hypothesis-- and this is very typical in a proof by using invariants-- is, so P of n is after any sequence of n moves from the start state-- in fact, just the rest of this is what it is. All right, so our inductive hypothesis is P of n, after any sequence of n moves-- so n is the number of moves you took to get there-- from the start state, the parity of the number of inversions is odd. That is the inductive hypothesis. This is the invariant.

And they become one and the same. And the parameter n is the number of moves you've taken. And that's how you set up a proof using an invariant. It always looks just like this.

OK, so we're doing a proof by induction. We've got the inductive hypothesis. What's the next step?

AUDIENCE: Base case.

PROFESSOR: Base case. And in these circumstances, where the proof by invariant, the base case is always 0. We haven't made any moves yet. Now in this case, if we haven't made moves, the number of inversions in the start state now is 1.

That means the parity is odd, and the hypothesis is satisfied. P of 0 is true, because in any sequence of zero moves, after this-- i.e. in this state-- you've got one inversion. That's odd.

The last step is the inductive step. And here we need to show for any n bigger or equal to 0, we need to show P of n implies p of n plus 1 is true-- the standard thing. So let's look at P n plus 1. That's talking about where we are after a sequence of n plus 1 moves in the puzzle, from the start state.

So let's consider any sequence of n plus 1 moves. And call these moves-- label them by M1 all the way to M n plus 1. Those are the moves we made.

Now, by the inductive hypothesis, because of P n, we know that after the first n moves, the parity is still odd. That's what P n says. That's P n.

After any sequence of n moves from here, the parity of the number of inversions is odd. So we could say by the inductive hypothesis, or we could say by P n, we know that the parity after moves M1 out to M n is odd. Now, by Corollary One-- do we still have Corollary One? [INAUDIBLE]

AUDIENCE: [INAUDIBLE].

PROFESSOR: [INAUDIBLE], yeah, good, we've got Corollary One. During any move, the parity doesn't change. That says from after the nth move to after the n plus 1st move-- one extra move-- doesn't change the parity. So it's still odd.

So next, by Corollary One, we know that the parity of the number of inversions does not change during M n plus 1. Therefore, this implies that the parity after all n plus 1 moves-- these guys-- is odd. It started odd.

It stayed odd after the first n. It stayed odd during the n plus 1st. So it's odd. And that's exactly the statement of P n plus 1.

So we've completed the induction. We've shown that P n implies P n plus 1. All right, so now, any questions so far on this? Yeah.

AUDIENCE: What's the difference between a lemma and a corollary?

PROFESSOR: Really, there's not a lot of difference. Corollary usually is something that's a simple consequence of something else. And the corollary had a pretty short proof. Usually when you see corollary, that's not a 10-page proof there.

A lemma is something that you're going to use as a tool for a bigger thing, often a theorem or another lemma. In fact, now we're going to get to the theorem, which is sort of the final thing-- the thing we're really after. And that's sort of the big deal. And now the proof will be simple, because we've done all these lemmas and corollaries. Any other questions? All right.

In fact, the theorem is up here, right? There is no sequence of legal moves to invert g and h. In other words, the students were screwed. They couldn't do it fairly. So let's prove the theorem now.

The parity of the number of inversions in the desired state-- i.e. in order-- the target state-- is

even. Nothing's out of order. There's zero inversions.

By Lemma Four, the desired state cannot be reached from the start state, because its parity is odd, using legal moves. So we're done. So the proof of the theorem-- by now, it's short, because we did four lemmas, a corollary, and lots of argument.

Could you have solved the puzzle if I allow the blank to be somewhere else at the end? Is the puzzle solvable then? No. Why not? Doesn't impact the parity at all, so you can't do that.

Again, the idea here-- and you'll get some practice in homework-- is you're looking for a property that holds at the beginning, is preserved by every step, but is not present in the target state. Now actually, this puzzle was enormously popular in the late 1880s. In fact there was $1,000 prize offered for anybody who could solve the larger version.

Back then, it was the 15 puzzle, which you can still buy today-- same problem on a 4 by 4 grid-- exactly the same problem. A pair is out of order. You've got to get them in order. You can't do it.

Now, the proof you can't do it is a little harder-- same idea-- one extra idea in it-- one extra lemma. And that's for homework. So you'll go through and see exactly the structure with one extra little trick it.

But back then, I guess most people didn't-- of course, most people didn't realize it wasn't doable. So they could offer this price safely. $1,000 then is probably worth a quarter million dollars today. Any questions on the eight puzzle? Yeah.

AUDIENCE: The inductive steps-- when you said, "by inductive hypothesis," [INAUDIBLE] parity after, shouldn't the first term be M0?

PROFESSOR: Let's see. No, the first move is M1. The second is M2. Now, when I talk about zero moves, that means no moves are taking place. I'm still in the start state.

So a move is a transition between states. So you could have state 0. That's the start state. State one would be the move after move one.

Have I got that right here? So the inductive step, I need to show P0 zero implies P1. P1 implies P2, and so forth. And P n is the parity of inversions after n moves.

So you could have state s0. We didn't label the states here, but you could have state s0. Yeah.

AUDIENCE: So in this problem, we assume that everything should be defined as rows or columns. How do we know when the assumptions are valid?

PROFESSOR: That's a good question. OK, so really, there's two cases. To be really precise, we should have argued there's only two types of moves, a row move and a column move.

And in fact, if you look at what can move into a blank square, there's four guys that can do it-- the guy above, the guy to the right, the guy to the left, and the guy below. Two of those are row moves, two are columns. So that's right-- to really pin down the details, we should have checked those are the only two possible moves.

And if there was a third kind of move that I hadn't considered, this proof would be bogus. That's a good question. Any other questions? OK.

Now, I think probably, you see why the invariants are important. But say that someday, you're building software to run a nuclear reactor. Now, there's a certain state you'd really like to avoid-- meltdown. And you'd like to be able to prove that, in any sequence of moves that happen in your reactor program, you never reach the meltdown state.

Well you'd use invariants to do that. Or if you're building software for an airplane, you'd like to never reach the crash state. Or if you're building a radiation device, you never want to get in the state that fries the patient. So this is an important notion.

So for the rest of the day, we're going to talk about a different kind of induction called strong induction. It's very similar to ordinary induction, but it's a little easier to use when solving certain problems. Now like regular induction, strong induction can be expressed with an axiom. So let me show you the strong induction axiom.

You have a predicate, P n, like before. If P0 is true-- your base case-- and for all n, it's not P n implies P n plus 1, it's P0 and P1 and dot, dot, dot, and P n are all true, then P n plus 1. If this is true for all n, then P n is true for all n.

Now, the only difference between strong induction and ordinary induction that we did last time is this part. In ordinary induction, you're showing that P n implies P n plus 1. In strong induction, you're showing that all these facts put together imply P n plus 1. Now, to show

implication, remember, you get to assume that all these things are true.

So you know how in ordinary induction, we say, "assume P n is true and you're going to prove P n plus 1?" In strong induction, you get to say, "assume P n is true, P n minus 1 is true, dot, dot, dot, P1 is true, and P0 is true. You get to assume a lot more. So it's a stronger proof technique, because it allows you to do more-- or so you would think.

Now in fact, any proof you can do with strong induction, you can do with ordinary induction. It just might be harder. So you can't prove any more with it, but it makes your proofs much easier.

And we're going to do an example in a minute where the proof is much easier by getting to assume all of these things are true in order to prove P n plus 1. Are there any questions about the difference here with strong induction-- that now you get to assume all these are true as part of the inductive step? All right.

Our first example of a strong induction is going to be a simple game. We've got a stack of eight blocks here. Now, in this game, what you're going to do is divide the stack into two sub-stacks. So I just took eight, and split it into three and five.

For that move, you get 15 points-- 3 times 5. Let's write that down.

OK, so this is called the Unstacking Game. And in the first move, we went 8 split to 5 and 3. And that's worth 15 points.

Now in the next move, I'm going to split the stack of five into four and one. And for that, you get 4 points-- 4 times 1. And I keep on going until I have a stacks of height one.

And the last move, I'll be splitting a two into two ones. That'll give me one point. Then I add up all the points, and that's your score. And the goal is to get the most number of points when you add up the entire score.

Now, just so this game is clear, we're going to play it. And I'm going to raise the stakes here. What we're going to do is we're going to have a competition between three members of the class and the TAs.

Now, if the class team wins-- they get more points-- we're going to give everybody in the class candy. And I've got lots of candy here. If the TAs beat you, they get the candy.

AUDIENCE: What if it's a tie?

PROFESSOR: We'll figure that out. We'll come to that later. But you want to win this thing.

So I need some volunteers from the class who think they can do well. Yeah, come on down. You two guys come on down. All right, TAs come on up.

Now, I want you to make some noise if you think your three class reps here can beat the TAs.

[CHEERS AND APPLAUSE]

All right, how many people-- make some noise you think the TAs are going to win.

AUDIENCE: Ooh.

PROFESSOR: Ooh, that's nasty. It must've been a rough recitation last week on Wednesday. All right, so let's see. I think we're going to let the class go first.

This is your stack. Now think about what move you want to make first, because that matters. And you guys can give them some advice if you want, as to the move they should make first. And I'm going to keep score over here.

Oh, OK, they went for the maximum move. That's good. They realized 4 times 4 is 16-- very good. So let's write that up here.

You're Off to a good start. In fact, that's the maximum number of points for the first move, I think-- good job. All right, so here's the class here. And here are the TAs.

And the class went 8 into 4 by 4, and they got 16. Now, the TAs are working hard here, as you can see. And they've got a move. That's a pretty pathetic first move for the TAs. Looking good for the candy for you guys. They got 7 points for the TAs.

Class, what would you like to do for your next move?

AUDIENCE: [INAUDIBLE].

PROFESSOR: You can't start over now-- too late for that.

[SIDE CONVERSATION]

A lot of people counting on you guys.

[SIDE CONVERSATION]

Oh, no, no, one at a time. No, just one. One stack gets split-- either one.

AUDIENCE: [INAUDIBLE].

PROFESSOR: There you go. Oh, well, what do you do now?

[SIDE CONVERSATION]

AUDIENCE: Their strategy's obviously better than ours.

AUDIENCE: Yeah, but we've figured it out already.

AUDIENCE: We're going to lose.

PROFESSOR: The TAs are convinced they're going to lose. Three and one, OK, good, interesting. So we have three and one. That gives you 3 points.

All right, TAs, we need a move. All right, so they've gone six and one-- 6 points. Class, you think you're dead already? So you've gotten three and one now, again, for 3.

So you're up to 22. You're way ahead-- 22 to 13. All right, TAs. They look a little disorganized to me. What do you think?

AUDIENCE: [INAUDIBLE].

PROFESSOR: Another one-- you can tell where they're headed here-- five and one. They have 5 points. They're up to 18. They're 4 behind you.

All right, class. All right, you got 2 points. TAs-- you really think they know how to do this best? I don't know.

AUDIENCE: [INAUDIBLE].

PROFESSOR: Oh, big change in strategy there. All that thinking, and that's what we got. OK, 4 points. Class. All right, they pick up 2 more here. The three just got split into two and one for 2 points.

How are you doing? You've got 19, 22, 24, up to 26. 13, 18, 22-- you're still doing good. TAs

are behind. Let's see what they've got up their sleeves here.

All right, they definitely have a strategy going here. That's 3 points. Ooh, there's not much option left for you guys. Yeah.

[SIDE CONVERSATION]

AUDIENCE: Choose the right.

AUDIENCE: Air blocks.

PROFESSOR: No, no, no, that'll be a 0. All right, that gave you a point-- two went to one and one-- 1 point. Not a lot of choice for you guys either, I guess. There's only one way to split that stack.

All right, 2 points, and your final move for the class and all the candy. You get 1 more point. Let's see what your total is. You've got 22, 24, 26, 27, 28. And the TAs are going to get one last move for the TAs.

All right, and you got 2, 1, 1, 2. That's interesting. 1, 2, 3, 4, 5, 6, 7-- 7 times 8 over 2-- no, that's not right. Did I do that right? Oh, 28-- we got a tie. Oh, geez.

I tell you what-- I'll give you guys one more chance to start over. You've seen that. You've got to beat them. You tied them. You've got to beat them. One more chance here.

[SIDE CONVERSATION]

You got to beat them, though. You got 28. You already tied them.

They came from behind and tied you. You've got to beat them. You got off to a good start, but then they caught up.

[SIDE CONVERSATION]

Now, your class reps had an interesting thought here. They ask, is it possible that any strategy gives 28? Hmm. I wouldn't do that to you, would I?

[LAUGHTER]

Yeah, probably. Any ideas? Can you beat 28? They're already eating the candy.

In fact, you can't beat 28. And you can't do worse than 28, either. Because every strategy

gives 28. So I guess we're going to have to throw it to the class to vote who should get the candy. So if you think your reps really should win this and you should get the candy, make some noise.

[CHEERS AND APPLAUSE]

If you think your TAs should get the candy make some noise.

[CHEERS AND APPLAUSE]

All right, so you get the candy. Here, help pass out the candy here. We've got plenty of bags and baskets. Take it all up on both sides, and pass it out.

[SIDE CONVERSATION]

OK, is everybody getting some candy up there? We should have enough for everybody, unless somebody got really hungry down here in front. OK, so while you're doing that, let's try to prove this theorem.

So the theorem is that all strategies for the n-block game produce the same score. It wasn't a coincidence for 8. And the score, we'll call it S of n for the n-block game. So for example, we're trying to show that S of 8 was 28. So what strategy do you think we're going to use for the proof?

AUDIENCE: Strong induction.

PROFESSOR: Strong induction-- so you want to write that down-- proof by strong induction. What's the next step in a proof by any kind of induction?

AUDIENCE: Base case.

PROFESSOR: Base case-- not yet.

AUDIENCE: The predicate.

PROFESSOR: The predicate-- what's the predicate here? All right, so for the inductive hypothesis, the predicate-- any guesses as to what P of n is going to be?

AUDIENCE: [INAUDIBLE].

PROFESSOR: What's that?

AUDIENCE: n should be 2n minus 1 by 2.

PROFESSOR: Yeah, that's part of it, but we're going to use this as a predicate to start with. You've gone a step ahead there. So I'm going to start with this as being a predicate, because I'm trying to show they're all the same.

And I haven't figured out what the scores going to be. But I think you're already on a good track here for what the score is going to be. Now we do the base case.

So we take n equals 1-- the one-block game. S of 1 is 0. We never took a move. We never got a score. There was only one block. We ended before we started. So that's OK.

And now we have the inductive step. And here we get to assume P1, P2, all the way up to P n, to prove P n plus 1. And so now we look at n plus 1 blocks, because that's we're starting.

So we have n plus 1, and we split it somehow. And it could be any split. We might have K on one side, then n plus 1 minus K on the other side for any K between 1 and n. And let's figure out our score for that scenario.

Well, we get the product of these numbers for the first step. We get K times n plus 1 minus K for the first step. And then as we recurse, and we split up that block of K blocks, how many points do we get for splitting that all the way down?

AUDIENCE: P of K.

PROFESSOR: P of K, because that's the induction. We assume that as part of the induction hypothesis. And how many points do we get for splitting this stack all the way down? Yeah, P of n plus 1 minus K.

And you see why strong induction's coming in handy here? For the TA's strategy, K would be 1. We know P of 1 is 0. And you would just need ordinary induction. This would be P of n.

But for a general strategy, it could be any split. So we need to have all these assumed here. It makes it much easier when using strong induction.

All right, so this is our total score for the game for n plus 1 blocks. And we're trying to show it

just depends on n, and that it doesn't depend on K. Does that depend on K?

Looks like it to me, right? I got K in every single term. So I'm not there. I'm stuck.

You see why I'm stuck? Because I'd like to be able to say that the score I get for the n plus one block game-- this is S n plus 1-- is the same for any sequence of moves. It doesn't even depend on K. But I can't do that.

What do you do when you're stuck with an induction proof? What's one of the tricks?

AUDIENCE: Make it stronger.

PROFESSOR: Make it stronger, which means I get a stronger induction hypothesis. Now, somebody gave me one up there before. How could I strengthen my induction hypothesis here?

AUDIENCE: [INAUDIBLE].

PROFESSOR: Give the formula for S n-- that would make it stronger. I tell you what it is. What's a good guess for the formula here?

AUDIENCE: Factorial.

PROFESSOR: Factorial-- Well, is S of 8 equal 8 factorial? No, not so good.

[SIDE CONVERSATION]

AUDIENCE: n equals n minus 1 over 2.

PROFESSOR: Yeah, that's a better guess-- equals n times n minus 1 over 2. And in fact, what's 8 times 7 over 2? It's 28. It works here.

Let's check another one. What's S of 2?

AUDIENCE: 1.

PROFESSOR: 1-- well, 2 times 1 over 2-- it works. What's S of 3? 2 the first move, then 1 more. 3-- 3 times 2 over 2 is 3-- looks good. So now I've got a stronger induction hypothesis. Not only is it always the same, it is that number is your score.

Let's see if that works. Let's plug that in now. So base case-- let's check it out-- is 1 times 1 minus 1 over 2 equal to 0. Yes.

Let's plug it in here now. P of K would be now K, K minus 1 over 2. This would be n plus 1 minus K, n minus K over 2 plus this one here.

All right, I've got to add all these things up, and see if it equals that expression for n plus 1. Let's do that. All right, I get 2 K n plus 2 K minus 2 K squared. I'm putting all this over 2-- one giant mess over 2 here-- plus K squared minus K plus n squared. Well, let's write it just as n plus 1 times n, minus K n, minus K, minus K n, all over 2.

And now let's cancel. Two K n's here cancel K n, K n. 2K cancels K and K. 2K squared minus 2 K squared cancels K squared. And I forgot, plus K squared from here and here.

So I'm left with n plus 1 times n over 2. That is S n plus 1. And the K disappears.

We've established, now, the stronger induction hypothesis. So not only did we prove that every set of unstackings gives you the same score. We proved the score is, for n blocks, n times n minus 1 over 2.

That's was pretty good for strong induction. It lets you do some pretty powerful things. OK, very good, that's it for today.