Class Notes for Lecture 4

Note: Sometimes we will use a predicate as a proposition by assuming implicit universal quantifiers for all unbound variables in the predicate. For example, if we say, "$f_{n+2} = f_{n+1} + f_n$," we mean "$f_{n+2} = f_{n+1} + f_n \; \forall n \in \mathbb{N}$."

Other texts:

- Grimaldi: Discrete and Combinatorial Mathematics
- Truss: Discrete Mathematics for Computer Science

8 Some Warmup Inductions

8.1 Sums of Sequences

An important use of induction is to verify closed-form expressions for sums of sequences.

Theorem 8.1 For any $n \geq 0$, $1 + 2 + 3 + \cdots + n = n(n+1)/2$

What does the left-hand side mean?
The dots ($\cdots$) indicate omitted terms.
Sometimes, it is assumed that the pattern will make it obvious what the missing terms are. (This is the case here).
Frequently, however, the first term after the dots is written as an expression involving its index, and this same expression allows the omitted terms before (and sometimes after) to be computed from their indices.
The obvious pattern above gives exactly n terms, which we consider to be true even in the following special cases:
For $n = 1$, the sum has just one term (1), even though more than one term is explicitly written out.
For $n = 0$, the sum has *no* terms. The sum of no terms is *always* 0.

Proof. Let $P(n)$ be the proposition that the sum of the first n positive integers is $n(n+1)/2$.
BASIS STEP: $P(0)$ is true since $0 = 0(0+1)/2$.
INDUCTIVE STEP: Assume that $P(n)$ holds, i.e.,

$$1 + 2 + 3 + \cdots + n = n(n+1)/2.$$

Add $n+1$ to both sides to get that

$$1 + 2 + 3 + \cdots + n + (n+1) = n(n+1)/2 + (n+1) = (n+1)(n+2)/2.$$

Hence $P(n+1)$ is true. This completes the inductive step and the proof. ∎

This theorem can also be proved without induction. How?

Instead of using dots, we often use Σ notation, which would denote the left-hand side of the theorem either by

$$\sum_{1 \le i \le n} i$$

or (more traditionally) by $\Sigma_{i=1}^{n} i$.

In general, the first style of Σ notation places some predicate on the index variable under the Σ.

$$\sum_{P(i)} f(i)$$

means the sum of all terms $f(i)$ for which $P(i)$ is true.
The second style uses $\Sigma_{i=j}^{k} f(i)$ for $f(j) + f(j+1) + \cdots + f(k)$.

8.2 Angles in A Polygon

Now we look of an example of induction applied to geometry. We are still going to use numbers, but the application is geometric.

Definition 8.2 A **convex polygon** is a polygon such that any straight line between two polygon vertices lies entirely in the polygon.

Lemma 8.3 If we draw a line between two vertices of a convex polygon, it divides the polygon into two convex polygons.

Proof. Sketch. It is "clear" the line divides the convex polygon into two polygons. Each piece is convex because any straight line between two vertices of a piece lies entirely on one side of the dividing line and since it did not leave the original polygon, it must not leave the piece it is in. ∎

Theorem 8.4 The sum of (the measures of the) angles in an n-sided convex polygon is $(n-2)180°$.

Proof. By induction. Let $P(n)$ be the theorem statement (restricted to a particular value of n).
The base case, for $n = 3$, is true from Euclid.
For the inductive step, assume $P(n)$.
To prove $P(n+1)$, consider an $(n+1)$-sided polygon.
Consider three vertices A, B, C that appear consecutively (with B in the middle) on the boundary of the polygon. Draw a line AC. This produces a triangle ABC and a polygon with n vertices.
(We've removed B.)
By the preceding lemma, the smaller polygon is convex and thus, by the induction hypothesis, the sum of its angles is $(n-2)180°$.
We now add in the $180°$ contained in the angles of ABC to find that the total angle sum in the $(n+1)$-vertex polygon is $(n-2)180° + 180° = ((n+1)-2)180°$, which proves $P(n+1)$. ∎

8.3 Courtyard Tiling

When writing an inductive proof, it can sometimes be more convenient to prove a strictly *stronger* statement than the one you want to prove. This is called strengthening the inductive hypothesis. This may seem only to make things more difficult, but this may not be true in the case of induction. Consider what happens to the inductive step. To prove the stronger statement, you must prove the stronger version for $n + 1$. But you also get to assume the stronger version for n. Sometimes, the balance between these two works in your favor, even though what you are now trying to prove is strictly stronger. Note that what is important is that the overall proposition (taken for all n) is stronger than the original one. The strengthened statement may or may not be stronger for any particular n. (It might even be weaker for some n, but usually not). So proving the base case might not be any harder.

Here's another nice example, where you need to strengthen the inductive hypothesis in order to make an inductive proof work.

Consider a $2^k \times 2^k$ square courtyard, $k \geq 1$. We want to tile it using L-shaped tiles consisting of three squares, leaving a particular one of the four center squares untiled (so you can install a birdbath). You don't care what the tile pattern looks like otherwise.

Theorem 8.5 Any 2^k by 2^k courtyard with any central square marked can be tiled with the above type of tile so that only the marked square is left uncovered (for $k \geq 1$).

Proof. Try using induction on k.
The obvious thing to do is to try $Q(k)$ being the statement above.
Base: $k = 1$ is fine, because the part of the courtyard to be tiled is just a single L.
Inductive Step: The obvious thing to try is to split a $2^{k+1} \times 2^{k+1}$ courtyard into four pieces and use the assumed tilings on each of the pieces to paste together a tiling for the whole courtyard.
But if $k > 2$, this gives four isolated empty squares (one in the middle of each piece) and the four center squares all tiled.

It would be better if the left-over squares were in the corners of the four pieces.
That way, we could put the empty corners together and use one additional tile, leaving just one center square empty.
But that's not what the inductive hypothesis gives. ???

On the other hand, we can't just change the hypothesis to say that we can tile except for an arbitrary corner.
This can be proved inductively, but in the end, it doesn't give the result we want (a missing center square, not a corner).

So, try:
$P(k)$: Any $2^k \times 2^k$ courtyard can be tiled leaving any corner square, or any center square, empty.

Base: $P(1)$ is clearly true.
Inductive step:
Given a $2^{k+1} \times 2^{k+1}$ courtyard, use the inductive hypothesis to get four $2^k \times 2^k$ pieces with missing corners.
We must consider two cases:

1. The bigger courtyard is to have a missing center square:
   Then we put the empty corners together in the middle and, as above, cover three of them with one tile.
2. The bigger courtyard is to have a missing corner:
   Then put three of the empty corners together in the middle, and the other in the desired corner.
   Cover the ones in the middle with one tile.

∎

An alternative inductive hypothesis that also works:
$R(k)$: You can tile a $2^k \times 2^k$ courtyard leaving *any* square empty.
A sketch of why:

Given the square to be left empty, divide the courtyard into fourths and tile the piece containing that square so that it is left empty. (This is possible by the inductive hypothesis).
Rely on the inductive hypothesis to tile the other pieces, leaving empty the corner of each piece in the center of the bigger courtyard.
Fill in these corners with one additional tile.

Things to watch for when strengthening an inductive hypothesis:

- It needs to be provable by induction.
  E.g., "can tile any square courtyard with any number of squares missing, with L-shaped tiles", can't be proved by induction, since it isn't even true. (Why not?)
  E.g., "can tile any courtyard with center square missing" can't be proved by induction, since it's too weak for the induction step to go through.
- It needs to imply the result that you really want to prove. E.g., "can tile with corner missing" can be proved by induction, but doesn't imply what we want.
  In other words, strengthening the hypothesis really should make the hypothesis *stronger*.

How do you come up with strengthened hypotheses?
There's no magic formula – it's an art.

8.4 Fallacies

There are several common mistakes made in inductive proofs. The most common is forgetting to prove the base case:

False Theorem 1 All horses are the same color.

Proof. Let $P(n)$ be the proposition that all horses in any set of n horses are the same color.
Clearly, $P(1)$ is true.
Now assume that $P(n)$ is true.
Consider any $n+1$ horses; number these as horses $1, 2, 3, \ldots, n+1$.
The first n of these horses are the same color, and the last n are also the same color.
Since the set of the first n horses and the set of the last n horses overlap, all of the $n+1$ horses are the same color.
This shows that $P(n+1)$ is true and finishes the proof by induction. ∎

This proof is wrong because the inductive step does not work for $n = 1$, i.e. the truth of $P(1)$ does not imply the truth of $P(2)$.

Another common mistake is using an inductive hypothesis that is just too weak.
E.g., in the tiling example, the hypothesis that you can tile with any center square missing.
Another example of this sort is the following variant on the triangle angle-sum example.

False Theorem 2 All *regular* convex polygons with n sides have angles summing to $(n-2)180°$.

Proof. False proof.
The proof is by induction.
Let $P(n)$ be the proposition that all regular convex polygons with n sides have angles summing to $(n-2)180°$.
BASE CASE: $P(3)$ is true since an equilateral triangle has angles summing to $(3-2)180°$.
INDUCTIVE STEP: Assume $P(k)$ to be true, for all $k \leq n$. Consider a regular convex polygon with $n+1$ sides. Consider three vertices A, B, C that appear consecutively on the boundary of the polygon. Draw a line AC. This produces a triangle ABC and a polygon with n vertices (we've removed B). By lemma 2, the smaller polygon is convex and thus, by the induction hypothesis, contains $(n-2)180°$. We now add in the $180°$ contained in the angles of ABC to find that the total angle sum in the $(n+1)$-vertex polygon is $(n-2)180° + 180° = ((n+1)-2)180°$, which proves $P(n+1)$.

This completes the inductive step and hence $P(n)$ is true for all nonnegative integers n.
■

The above proof is wrong because the inductive hypothesis has been invoked wrongly.
The smaller polygon created by line AC is not *regular*.
But this is almost the same proof as our correct one.

9 Induction on Recursive Definitions

A *recursive definition* says how to build something from a simpler version of the same thing.

Two parts:

- Base case(s) that don't depend on anything else
- Combination cases that depend on simpler cases

Note the relationship to a *recursive algorithm.* We will also see a close relation to induction.

In our definitions, we will frequently use the symbol "=" in a special sense that means what appears on the left is defined to be what appears on the right. We expect you to recognize from context which use we intend and, in the definitional case, only to use the statement as a definition and not as an algebraic statement.

Examples:

- The *Factorial function*:
  - $1! = 1$
  - $(n+1)! = (n+1)n!$ for $n \geq 1$.
- Prime numbers (alternative, equivalent definition):
  - 2 is prime
  - $n > 2$ is prime if n is not divisible by any prime less than n.
- The *Fibonacci numbers*:
  - $f_0 = 0$
  - $f_1 = 1$
  - $f_{n+2} = f_{n+1} + f_n$

  Note: 2 base cases, since combination relies on previous two values.

  What is f_4? Well, $f_2 = f_0 + f_1 = 1$, $f_3 = f_1 + f_2 = 2$, so $f_4 = 3$.
- Σ notation (the traditional style):
  - $\Sigma_{i=1}^{0} f(i) = 0$
  - $\Sigma_{i=1}^{n+1} f(i) = \Sigma_{i=1}^{n} f(i) + f(n+1)$.
- A *well formed arithmetic formula* is:
  - A number
  - $(f+g)$, $(f-g)$, $(f*g)$, or (f/g) where f, g are well-formed arithmetic formulae.

You can also have simultaneous recursive definitions:

- Define two functions f and g from $\mathbb{N}$ to $\mathbb{N}$, recursively, by:
  - $f(0) = 1$
  - $g(0) = 1$

- $f(n+1) = f(n) + g(n)$, $n \geq 0$
- $g(n+1) = f(n) \times g(n)$, $n \geq 0$

We must take care that concepts defined by recursive definitions are well-defined.
Examples that aren't well-defined: (In the following examples, the notion being defined always appears on the left-hand side.)

- $f(n) = 2 + f(n-1)$.

  No base case.
- $f(1) = 1$ and $f(n) = 1 + f(n+1)$.

  Still no base case, because $f(n)$ is defined in terms of $f(n+1)$. So for positive integers n other than 1, $f(n)$ is defined in terms of "more complex" cases instead of simpler ones. Note that if we had written $f(n+1) = f(n) - 1$, we would have meant something different (we would be defining $f(n+1)$ in terms of $f(n)$) and f would have been well-defined for all positive integers. Also, note that the first way makes f well-defined for all integers *less than* or equal to 1.
-
  - $f(1) = 1$
  - If n is even, then $f(n) = f(n/2)$.
  - If n is odd, then $f(n) = f(3n+1)$.

  If f is well defined, then $f(n) = 1$ everywhere. But nobody knows if the recursion always terminates (though it's been checked for many numbers).

9.1 Less formal Inductions

The following shows how inductive proofs can fit nicely with recursive definitions:

Example 1 Show $n! \geq 4^{n-2}$ for all $n \geq 2$
BASE CASES: 2 and 3, just check.
(Technically, only 2 is a base – the other is a trivial inductive step.)
INDUCTIVE:
Know $n! \geq 4^{n-2}$. Want $(n+1)! \geq 4^{n-1}$. LHS multiplies by at least 4, RHS by just 4, so the inequality is preserved.

An example of two functions defined together, by recursion:

Example 2 The functions f and g above. Prove the following:

1. If $n \geq 2$ then $f(n)$ is odd.

2. If $n \geq 2$ then $g(n)$ is even.

You can't prove them separately – at least, not the first. So prove the two together by induction. $P(n)$ = conjunction of the two statements. For $n = 2$, show by explicit calculation $(3, 2)$. Inductive step: Assume $f(n)$ odd and $g(n)$ even. Then their sum is odd and product is even, so this is true for $n + 1$ also.

9.2 Addition

Let's do a more careful example: we'll define addition from the Peano axioms.

We define addition:

- $n + 0 = n$ (implicit universal quantification)
- $n + k' = (n + k)'$

This is a *recursive* definition: it lets us compute $n + k$ for any n, k. For example,

$$\begin{aligned} 3 + 2 &= 3 + 1' \\ &= (3 + 1)' \\ &= (3 + 0')' \\ &= ((3 + 0)')' \\ &= (3')' \\ &= 4' \\ &= 5. \end{aligned}$$

Addition is *commutative:* $m + n = n + m$. How can we prove this? It turns out to be helpful to use lemmas. Lemmas are intermediate statements that are proven for use in proving a more important statement (a theorem).

Lemma 9.1 $(\forall n)\ 0 + n = n$

Proof. Let $S = \{n \in \mathbb{N} \mid 0 + n = n\}$ ("The set of all $n \in \mathbb{N}$ such that $0 + n = n$"). We prove $S = \mathbb{N}$.

- $0 \in S$ since $0 + 0 = 0$ by definition of $+$.

- if $x \in S$, so that $0 + x = x$, then

$$\begin{aligned} 0 + x' &= (0 + x)' \quad \text{(definition of +)} \\ &= x', \quad \text{(since } x \in S\text{)} \end{aligned}$$

so $x' \in S$. In other words, $\forall x, (x \in S) \implies (x' \in S)$.

Therefore, by the induction axiom, $S = \mathbb{N}$. ■

Lemma 9.2 $(\forall m, n)\ m' + n = m + n'$.

Proof. We will prove this as follows: fixing m, we prove that $\forall n P(m, n)$. The $(\forall m)(\forall n P(m, n))$ follows by universal generalization. But this is the same as $(\forall m, n)\ P(m, n)$.

Fix m. Let $S = \{n \mid m' + n = m + n'\}$. We prove $S = \mathbb{N}$.

- $0 \in S$, since $m' + 0 = m' = (m + 0)' = m + 0'$
- if $n \in S$, so that $m' + n = m + n'$, then

$$\begin{aligned} m' + n' &= (m' + n)' \quad \text{(definition of +)} \\ &= (m + n')' \quad \text{(true for } n\text{)} \\ &= m + (n')' \quad \text{(definition of +)} \end{aligned}$$

Since $0 \in S$, and $n \in S \implies n' \in S$, the induction axiom proves $S = \mathbb{N}$. ■

Lemma 9.3 $m + n = n + m$

Proof. Let $S = \{n \mid (\forall m) m + n = n + m\}$. We prove $S = \mathbb{N}$.

- $0 \in S$, since $m + 0 = m = 0 + m$ by Lemma 9.1.
- Suppose $n \in S$, so that $(\forall m)\ m + n = n + m$. Then

$$\begin{aligned} m + n' &= (m + n)' \quad \text{(definition)} \\ &= (n + m)' \quad \text{(true for } n\text{)} \\ &= n + m' \quad \text{(definition)} \\ &= n' + m \quad \text{(previous lemma)} \end{aligned}$$

Therefore, $S = \mathbb{N}$ by the induction axiom. ■

10 Other Inductions

Recall the Peano induction rule:

Let $P(n)$ be a predicate, and suppose

- $P(0)$
- $(\forall n)\ (P(n) \implies P(n+1))$.

Then $P(n)$ is true for all natural numbers n.

Plus a simple variation where the lower limit isn't 0, but some other natural number.

Below, we describe two more interesting variations on the induction rule that are also valid for reasoning about natural numbers:

Strong induction and *well-ordering*.

Strong induction is nice because it allows you to use not just $P(n-1)$ when trying to conclude the result for $P(n)$,
but also P of anything else smaller than n,
i.e., $P(0), \ldots, P(n-1)$.

Well-ordering is a restatement of induction that says that every nomempty set of natural numbers has some smallest element.

We will also sketch proofs that these three induction rules are "equivalent".
Thus, they are interchangeable in arguments, though in particular practical cases, one may work out much nicer than the others.

10.1 Picky Axiomatic Remarks

The new induction axioms mention an ordering $<$ on the natural numbers.
The astute, picky student will observe that the Peano axioms don't mention anything about an ordering: they just mention 0 and successor.
We also haven't defined any ordering yet.
We've only defined addition.

If we want to treat these as alternatives to the Peano induction axiom, we will have to add some new notions to the Peano axioms.
This new stuff will include a new symbol $<$, and some new simple axioms like:

- $<$ is a strict total order.
  (Formally: irreflexive, $\neg n < n$;
  antisymmetric, $\neg(m < n \wedge n < m)$;
  transitive, $m < n$, $n < p$ imply $m < p$;
  total: any m, n have either $m < n$ or $n < m$.)
- Every natural number other than 0 is a successor of something,
  i.e., $n \neq 0 \implies \exists m(m' = n)$.
  (Call this its *predecessor*. It must be unique.)
- $0 < n$ for all other n.
- $n < n'$.
- $m < n$ if and only if $m' < n'$.
- $\neg(m < n \wedge n < m + 1)$.
- Etc.

We'll come back to this later.
For now, we'll just continue assuming such basic properties.

11 Strong Induction

11.1 Definition

A variant of induction. To prove $(\forall n \in N)P(n)$

- prove $P(0)$
- prove $((\forall k < n)P(k))$ implies $P(n)$.

Actually, we don't even need the base case.
That's because the second case, when specialized to $n = 0$, says to prove $((\forall k < 0)P(k))$ implies $P(0)$.
But the hypothesis is *vacuously true*, since there's nothing < 0.
So this means you're really forced just to prove the conclusion, $P(0)$, on its own.

But never mind if this is confusing – we'll follow the book and check base cases – they're generally easy anyway.
Another reason for base cases:
Often the first case or first few cases need a different argument from the inductive step.

Again, we can modify this to work from any k instead of 0.

11.2 Fibonacci Examples

Example 3 Recall the Fibonacci numbers:

- $f_0 = 0$
- $f_1 = 1$
- $f_{n+2} = f_{n+1} + f_n$

Theorem 11.1 $f_n \geq (\frac{3}{2})^{n-2}$ for all $n \geq 2$.

Proof. Define $P(n)$ as the predicate above.

It suffices to show for all $n \geq 2$:
$((\forall k, 2 \leq k < n)P(k))$ implies $P(n)$.
(We can omit the base case, since this is *strong* induction (and we will have to deal with the base case differently anyway, since the assumptions become vacuous for that case). You *can't* omit the base case for regular induction.)

But it's convenient to check $P(2)$ and $P(3)$ explicitly in the inductive step.
Or you can regard them as base cases.
At any rate, they use a different argument.

For $n \geq 4$:
Assume $((\forall k, 2 \leq k < n)P(k))$. Show $P(n)$.

By definition, $f_n = f_{n-1} + f_{n-2}$.
Both $n-1$ and $n-2$ are ≥ 2, so we can assume $P(n-1)$ and $P(n-2)$, by the strong inductive hypothesis.
That is, $f_{n-1} \geq (\frac{3}{2})^{n-3}$ and $f_{n-2} \geq (\frac{3}{2})^{n-4}$.

Now, $f_n = f_{n-1} + f_{n-2} \geq (\frac{3}{2})^{n-3} + (\frac{3}{2})^{n-4}$. We want to show that this is $\geq (\frac{3}{2})^{n-2}$.
Dividing all terms by $(\frac{3}{2})^{n-4}$, we see that we need to show:
$\frac{3}{2} + 1 \geq (\frac{3}{2})^2$.
This is easily checked.

The book does a sharper calculation. ∎

Note how we used the inductive hypothesis about *two* earlier cases.

11.3 Fallacies

Another example of a mistake – forgetting to prove enough base cases to make the induction step go through.

False Theorem 3 Every Fibonacci number is even.

Proof. The proof is by strong induction. Let $P(n)$ be the proposition that f_n is even.
BASE: Prove explicitly that $P(0)$ is true – this is because $f_0 = 0$ is even.
INDUCTIVE STEP: Assume $P(k)$ to be true, for all $k < n$.
Consider $f_n = f_{n-1} + f_{n-2}$.
Since f_{n-1} and f_{n-2} are even, by the inductive hypothesis, it follows that f_n is even too.
Hence P_n is true.

This completes the inductive step and hence $P(n)$ is true for all nonnegative integers n. ∎

The above proof is faulty because there were not enough base cases shown explicitly.
The inductive argument doesn't work to show $P(1)$, since f_{-1} is not defined.
We would have to show $P(1)$ explicitly, but of course that doesn't work, since f_1 is odd.

11.4 Number Theory

Definition 11.2 For $a > 0$, we say a *divides* b if there exists an integer t such that $a = bt$. We write $a \mid b$.

- $3 \mid 6$
- $3 \not| 7$

Definition 11.3 $n \geq 2$ is *prime* if the only natural numbers dividing n are 1 and n.

Definition 11.4 $n \geq 2$ is *composite* if $n = ab$ for natural numbers $a, b \neq 1, n$.

Every natural number is either prime or composite. (Why?)

Theorem 11.5 Every natural number ≥ 2 has a prime divisor.

Proof. By strong induction.
BASE CASE: The theorem is true for $n = 2$.

INDUCTIVE STEP: Assuming the theorem true for all k, $2 \leq k < n$, consider the number n. We proceed by cases:

1. n is prime. Then n (a prime) divides n.
2. n is composite. Then $n = ab$ where $2 \leq a < n$. It follows from the inductive hypothesis that a has a prime divisor, ie that $a = pt$ for a prime t. Then $n = ptb$, meaning p divides n.

Since we proved the inductive step for both possible cases, we are done. ∎

Note: we use a base case of 2.

11.5 Ordinary vs. Strong Induction

What is the relationship between the ordinary and strong induction axioms?
It should be clear, intuitively, that the strong induction axiom is at least as powerful as the ordinary one – any proof you can do with weak induction still works based on strong induction.
You only need to invoke the inductive hypothesis for $n - 1$, whereas you're allowed to use all cases smaller than n.

(Remark: This assumes existence of a predecessor, which follows from our basic axioms.)

Though it's not obvious, the strong induction axiom is really *no stronger* than the weak axiom!
That is, any proof you can do based on strong induction can be reformulated so it works just using weak induction.
You just have to use weak induction in a tricky way:
You must strengthen the predicate you prove using weak induction so that it includes information about smaller arguments.

You should be used to strengthening inductive hypotheses...

Suppose P is a predicate such that $(\forall n P(n))$ can be proved using strong induction.

Means: $P(0)$
$(\forall k < n)P(k) \implies P(n)$

Show that we can prove $(\forall n P(n))$ using ordinary induction too. To do so we need to strengthen P so that ordinary induction works:

Define $Q(n) = (\forall k \leq n)P(k)$

Claim: you can prove Q using ordinary induction

Base: $Q(0)$– Same as $P(0)$, we already know this
Inductive step: Show that $Q(n) \implies Q(n+1)$
Show that $(\forall k \leq n)P(k)$ implies $(\forall k \leq n+1)P(k)$
We know this, since $(\forall k \leq n)P(k) \implies P(n+1)$

Claim: $\forall n(Q(n) \implies P(n))$ So, by strengthening P to Q, we have proved P using ordinary induction.

Formally:
If you start with a basic set of axioms – not just Peano, but including ordering axioms and existence of predecessor as above – then adding either induction axiom allows you to prove the other.

Theorem 11.6 Weak induction axiom implies strong induction axiom.

Proof. Suppose we have the weak induction axiom.
This says, for any predicate P, that
$P(0)$ and $(\forall n)(P(n) \implies P(n+1))$
together imply $(\forall n)P(n)$.

What we want to prove is the strong induction axiom, which says:

For any predicate Q,
$Q(0)$ and $(\forall n)(((\forall k < n)Q(k)) \implies Q(n))$
together imply $(\forall n)Q(n)$.

So fix some Q that we'd like to prove using strong induction.
And assume
**
$Q(0)$ and $(\forall n)(((\forall k < n)Q(k)) \implies Q(n))$.
**

We will see how to prove $(\forall n)Q(n)$ using ordinary induction.

The key is to come up with just the right strengthened predicate P
to make an ordinary induction go through.
Here's the clever trick:

Define $P(n)$ as the predicate $(\forall k \leq n)Q(k)$.
Thus, $P(n)$ asserts not only $Q(n)$ for the same argument n, but also for all smaller arguments $k < n$.
We need to strengthen Q in this way to make the induction go through using the weaker principle.

Now check that this definition works. Straightforward, but can be a little hard to keep straight.

In order to apply weak induction, we must show two things:
$P(0)$ and
$(\forall n)(P(n) \implies P(n+1))$.
We'll verify these two, then apply weak induction and see what we get.

$P(0)$:
This says $(\forall k \leq 0)Q(k)$.
That's the same as just $Q(0)$.
But we've assumed this to be true, *** above.

$P(n) \implies P(n+1)$.
(Fix n.)
Assume $P(n)$.
That says $(\forall k \leq n)Q(k)$.
By what we have assumed about Q (*** above), we know that
$((\forall k < n+1)Q(k)) \implies Q(n+1)$.
Therefore we know $Q(n+1)$.
So, we have $(\forall k \leq n+1)Q(k)$.
But this is just $P(n+1)$, as needed.

Now we can apply ordinary induction to P, concluding that $P(n)$ holds for all n.
But $P(n) \implies Q(n)$, so also $Q(n)$ holds for all n. ∎