# What is a Proof? (cont'd) & Proof by Induction

## 1 Predicates

Last time we discussed overall structure for proving theorems

- propositions
- definitions
- axioms
- deduction rules

and looked at some toy proofs to demonstrate

Today, we will look at proofs of some less obvious stuff and see how to combine all the proof techniques discussed last time.

### 1.1 What are predicates?

Predicates are similar to propositions but they depend on variables. $P(x, y, z)$ denotes a predicate on variables $x, y, z$. For example, we can define 3 predicates:

- $R(x)$: $x$ is an odd number.
- $Q(x)$: $x > 2$.
- $P(x)$: $x$ is a prime number.

These predicates are *not* propositions, because they can be true or false depending on $x$. When the value of $x$ is not specified, we say $x$ is *unbound*. Predicates are like functions from variables to propositions.

- $P(2)$ is true.
- $R(2)$ is false.
- $P(4) \vee R(3)$ is true.
- $Q(3) \wedge R(4)$ is false.
- $Q(1) \implies R(2)$ is true.

### 1.2 Quantifiers

Many propositions assert that something is true for all or some elements of a given domain (e.g., all numbers). The following quantifiers presume a particular **universe of discourse** has been agreed upon in advance. This is the set of elements values to which we can assign the quantified variables.

**"$\forall$"** means "for all." $\forall x P(x)$ is a statement that is true iff $P(x)$ is true for *every* $x$ in the universe of discourse.

**"$\exists$"** means "there exists." $\exists x P(x)$ is true iff $P(x)$ is true for *at least one* $x$ in the universe of discourse.

**"$\nexists$"** mean "there does not exist" ("there is no").

**"$\exists!$"** means "there exists *exactly* one."

**"$\forall x \in S$"** means "for every $x$ in the set $S$." $(\forall x \in S) P(x)$ is equivalent to $(\forall x)(x \in S \implies P(x))$.

Quantifiers can turn predicates into propositions, e.g.

$$\forall x, P(x) \wedge Q(x) \implies R(x).$$

Note that each appearance of $x$ is associated with the $\forall$ quantifier. A variable associated with a quantifier in this way is said to be *bound*. Since every variable in the above expression is bound, it is a proposition. If $P$, $Q$, and $R$ are the predicates defined above, this proposition says "every prime number greater than 2 is odd" and is true.

**Note:** $\forall x \exists y$ is *different* from $\exists y \forall x$:

- Suppose $S(x, y)$ : means student $x$ will fall asleep in class $y$.
- $\forall y \exists x P(x, y)$ : "In every class, some student will fall asleep."
- $\exists x \forall y P(x, y)$ : "There exists a student who will fall asleep in every class."

What is the universe of discourse above? The set of students.

### 1.3 Deduction rules involving quantifiers

**Reading:** Velleman 2.2, Rosen, p. 173

We've already seen deduction rules for arbitrary propositions. There are others special to propositions with quantifiers.

A first rule deals with negating quantified statements:

- $(\forall x) S(x)$ is equivalent to $\neg(\exists x) \neg S(x)$:
  - $(\forall x) S(x)$ : For all primes $x > 2$, $x$ is odd.
  - $\neg(\exists x) \neg S(x)$ : There is no prime $x > 2$ such that $x$ is not odd.

- $(\exists x)S(x)$ is equivalent to $\neg(\forall x)\neg S(x)$.

There are four main rules for manipulating quantifiers in proofs:

**Universal Generalization UG:** to prove something is true for every $x$ one can show a proof works for arbitrary fixed $x$

**Universal Instantiation UI:** if a statement is true for all $x$, it is true for any one $x$ I want to study.

**Existential Generalization EG:** if have exhibited one $x$, I have proven one exists

**Existential Instantiation EI:** if one exists, I can pick one and use it in the proof.

We'll introduce these as we use them.

Like axioms, these inference rules are really an *agreement* to believe certain inferences. For example, the constructivists (e.g. Brouwer) *reject* the claim that $\neg\forall x \neg P(x)$ implies $\exists x P(x)$. They claim that to prove something exists, you actually have to construct it. Brouwer retracted his most famous theorem after he became a constructivist, since the proof was nonconstructive.

## 2 Predicate reasoning examples

**Reading:** Velleman Chapter 3. Rosen, Section 3.1

We have already been using quantifiers in sloppy ways, or hiding them. Now we can give some examples that use them explicitly and correctly.

### 2.1 Britney's birthdate

This example illustrates: Quantifier reasoning (UG, EI, EG) and cases.

Prove: $\forall n \in N(n^2 + n \text{ is even})$.

| | |
|---|---|
| 1. Fix $n \in N$. | |
| 2. $n^2 + n$ is even. | ??? |
| 3. QED | Universal Generalization (UG) |

UG is the official fancy name for the rule that says, to show something is true for all elements of a set ($\forall$), you pick ("fix") any arbitrary generic element and show it for that. The basic idea is that generate one proof for each possible $x$. The name is hard to remember, don't worry too much about it. Just know how to use it.

The pattern is as follows:

Prove: $\forall x \in X(P(x))$.

| | |
|---|---|
| 1. Fix $x \in X$. | |
| 2. $P(x)$ | |
| 3. QED | Universal Generalization (UG) |

Back to the proof:
To show step 2, can use cases:

Prove: $\forall n \in N(n^2 + n \text{ is even})$.
1. Fix $n \in N$.
2. $n^2 + n$ is even.
    1. If $n$ is odd then $n^2 + n$ is even. ???
    2. If $n$ is even then $n^2 + n$ is even. ???
    3. QED Cases
3. QED

Now fill in steps for the odd case:

1. If $n$ is odd then $n^2 + n$ is even.
    1. Assume $n$ is odd.
    2. $n^2 + n$ is even.
        1. $\exists x \in N(n = 2x + 1)$ Def. of "odd"
        2. Choose $x \in N$, $n = 2x + 1$ Existential Instantiation (EI)
           (If there *exists* one, you can *choose* one.)
        3. $n^2 + n = 4x^2 + 4x + 1 + 2x + 1 = 2(2x^2 + 3x + 1)$
           Algebra
        4. $\exists y \in N(n^2 + n = 2y)$ Existential Generalization (EG)
           (If you *have* one, then one *exists*.)
        5. QED Def. of "even"
    3. QED Implication

Analogously for the "even" case:

2. If $n$ is even then $n^2 + n$ is even.
    1. Assume $n$ is even.
    2. $n^2 + n$ is even.
        1. $\exists x \in N(n = 2x)$ Def. of "even"
        2. Choose $x \in N$, $n = 2x$ EI
        3. $n^2 + n = 4x^2 + 2x = 2(2x^2 + x)$ Algebra
        4. $\exists y \in N(n^2 + n = 2y)$ EG
        5. QED Def. of "even".
    3. QED Implication

Or, condensing a little:

2. If $n$ is even then $n^2 + n$ is even.
    1. Assume $n$ is even.
    2. Choose $x \in N$, $n = 2x$ Def. of "even", EI
    3. $n^2 + n = 4x^2 + 2x = 2(2x^2 + x)$ Algebra
    4. $n^2 + n$ is even. EG, def. of "even"
    5. QED Implication

## 2.2 Proofs by contradiction

Illustrates: Contradiction, more quantifiers.

Prove: $\sqrt{2}$ is irrational.

1. $\sqrt{2}$ rational $\Rightarrow$ *false*
2. QED    Contradiction.

Assume it's rational, play with the definitions, and try to get a contradiction.

Prove: $\sqrt{2}$ is irrational.

1. $\sqrt{2}$ rational $\Rightarrow$ *false*
    1. Assume $\sqrt{2}$ rational.
    2. *false*
        1. Choose $a, b \in N^+$, $\sqrt{2} = \frac{a}{b}$, lowest terms.    Basic properties of rationals, EI
        2. $2b^2 = a^2$    Algebra
        3. $a^2$ is even.    EG, definition of "even"
        4. $a$ is even.    ???
        5. Choose $c \in N$, $a = 2c$.    Definition of "even", EI
        6. $4c^2 = a^2 = 2b^2$    Algebra
        7. $2c^2 = b^2$    Algebra
        8. $b^2$ is even.    EG, definition of "even"
        9. $b$ is even.    ???
        10. $a$ and $b$ aren't in lowest terms.    1.2.4, 1.2.9
        11. QED    1.2.1, 1.2.10, propositional logic
    3. QED    Implication.
2. QED    Contradiction.

There's a little missing piece: Showing that $a$ and $b$ are even, because we know their squares are even. The reason is a general fact, which could itself be proved. Write $P(x)$ for "$x^2$ is even" and $Q(x)$ for "$x$ is even."

Prove: $(\forall x)P(x) \implies Q(x)$

1. $(\forall x)\neg Q(x) \implies \neg P(x)$
    1. Choose $x$    UI
    2. Assume $\neg Q(x)$
    3. $\neg P(x)$
        1. $\neg Q(x)$ means $x$ odd    Def $Q(x)$
        2. so $x^2$ odd    Britney
        3. which means $\neg P(x)$    definition of $P$
        4. QED    UG
    4. QED    Direct proof
2. QED    logical tautology

Alternatively, we could write a proof by contradiction.

Assume: $x \in N$, $x^2$ is even.
Prove: $x$ is even.

| | |
|---|---|
| 1. $x$ is odd $\Rightarrow$ *false* | |
|     1. Assume $x$ is odd. | |
|     2. $x^2$ is odd. | Do a proof like the one in the birthdate example. |
|     3. *false* | Assumption, 1.2.4, Prop. logic |
| 2. QED | Contradiction |

## 2.3 Structured proofs and paragraph proofs

Recall the structured proof just presented to show that $\sqrt{2}$ is irrational. We can compare it to a more typical paragraph proof:

*Proof.* The proof is by contradiction. Assume for purpose of contradiction that $\sqrt{2}$ is rational. Then we can write $\sqrt{2} = a/b$ where $a$ and $b$ are integers and the fraction is in lowest terms. Squaring both sides gives $2 = a^2/b^2$ and so $2b^2 = a^2$. This implies that $a$ is even; that is, $a$ is a multiple of 2. As a result, $a^2$ is a multiple of 4. Because of the equality $2b^2 = a^2$, $2b^2$ must also be a multiple of 4. This implies that $b^2$ is even and so $b$ must be even. But since $a$ and $b$ are both even, the fraction $a/b$ is not in lowest terms. This is a contradiction, and so the assumption that $\sqrt{2}$ is rational must be false. ∎

The paragraph proof contains exactly the same information. Just written differently.

## 2.4 De Morgan's Law

Illustrates: Set theory proof.

Prove: $\forall A, B(\overline{A} \cap \overline{B} = \overline{A \cup B})$

| | |
|---|---|
| 1. Fix $A$, $B$. | |
| 2. $\overline{A} \cap \overline{B} = \overline{A \cup B}$ | ??? |
| 3. QED | UG |

To show two sets are equal, we show that they contain the same elements.

Prove: $\forall A, B(\overline{A} \cap \overline{B} = \overline{A \cup B})$.

| | |
|---|---|
| 1. Fix $A$, $B$. | |
| 2. $\overline{A} \cap \overline{B} = \overline{A \cup B}$ | |
|     1. $\forall x(x \in \overline{A} \cap \overline{B} \Leftrightarrow x \in \overline{A \cup B})$ | |
|         1. Fix $x$. | |
|         2. $x \in \overline{A} \cap \overline{B} \Leftrightarrow x \in \overline{A \cup B}$ | ??? |
|         3. QED | UG |
|     2. QED | Definition of set equality. |
| 3. QED | UG |

Equivalence can be shown by showing two implications, one in each direction:

| | |
|---|---|
| 2. $x \in \overline{A} \cap \overline{B} \Leftrightarrow x \in \overline{A \cup B}$ | |
|     1. $x \in \overline{A} \cap \overline{B} \Rightarrow x \in \overline{A \cup B}$ | ??? |
|     2. $x \in \overline{A \cup B} \Rightarrow x \in \overline{A} \cap \overline{B}$ | ??? |
|     3. QED | Propositional logic |

One direction:

| | |
|---|---|
| 1. $x \in \overline{A} \cap \overline{B} \Rightarrow x \in \overline{A \cup B}$ | |
|     1. Assume $x \in \overline{A} \cap \overline{B}$. | |
|     2. $x \in \overline{A}$, $x \in \overline{B}$ | Definition of intersection. |
|     3. $x \notin A$, $x \notin B$ | Definition of complement. |
|     4. $x \notin A \cup B$ | Definition of union. |
|     5. $x \in \overline{A \cup B}$ | Definition of complement. |
|     6. QED | Implication |

Actually, the union step could be expanded to a little proof by contradiction:
if it is in the union, it's in one of the sets, etc.
The other direction essentially reverses the steps:

| | |
|---|---|
| 2. $x \in \overline{A \cup B} \Rightarrow x \in \overline{A} \cap \overline{B}$ | |
|     1. Assume $x \in \overline{A \cup B}$. | |
|     2. $x \notin A \cup B$ | Complement |
|     3. $x \notin A$, $x \notin B$ | Union |
|     4. $x \in \overline{A}$, $x \in \overline{B}$ | Complement |
|     5. $x \in \overline{A} \cap \overline{B}$ | Intersection |
|     6. QED | Implication |

### 2.5 Counterexamples

Counterexamples are the easiest way to avoid proving a theorem.

Prove: All natural numbers $\geq 2$ are prime.

This turns out to be false. We can show this using a "counterexample", 10. That's all that's needed. Really, we're proving the negation, which says $\exists$ a non-prime $\geq 2$. And this follows just by exhibiting one.

## 3 What we Expect in your Proofs

In practice, people do not write out real proofs about interesting mathematical objects in a completely formal, step-by-step style (unless they are using a computer-aided theorem prover, which really does work step-by-step). Rather, they work more intuitively, skipping a lot of steps. This is a kind of proof sketch.

But it is very important to work *correctly*, so that all the missing steps could really be filled in. It can be very hard to tell (impossible without some training) if a proof sketch is really valid. This course is designed to provide this training.

The basic objective: As in a scientific experiment, it has to be possible for someone else to "replicate" (ie, understand) your proof.

**In your homework, that "someone" should be another 6.042 student.**

In the real world, anything that can be cited can be used without proof. But in homework, where everything we ask you to prove is already known, this defeats the purpose (namely, learning how to prove something that isn't already known).

We don't expect you to reprove arithmetic. Anything from high school math can be used without proof (unless stated otherwise).

Once something has been proved, you can use it again without proof, citing the theorem. Once it has been used so often as to become commonplace, you can even stop citing the theorem.

**Do not introduce any new axioms!**

**When in doubt about whether something can be stated without proof, prove it!**

Elements of a good proof:

- Correctness: first of all, a proof must be correct. Do not introduce more assumptions than the ones already stated in the hypothesis. Do not use unproved 'facts' and beware of logical fallacies.
- Inobvious conclusions are not justified by shortcuts such as "it can be shown that..." and "It is obvious that..." and "any moron can see that...". These phrases save the writer's time, but create a chance for error and consume the reader's time.
- Like a scientific experiment, someone else must be able to "replicate" (i.e. understand) your proof.
- Clarity: a good proof has nice structure, like a good program. It is broken up into separate "lemmas" that prove key intermediate properties.
  - "Top down design" makes it easy to understand the *reasons* why the whole thing works.
  - It also makes it more likely that pieces can be reused.
- Brevity: a proof should be free of wordy arguments and repetitions.
- Generality: a good proof has its pieces presented abstractly and generally. If you give an intermediate fact, state it as generally as you can. This avoids cluttering up a key piece of a proof with unnecessary hypotheses and arguments. It also makes it more likely you can reuse the piece. Again, the analogy to programming holds; a subroutine should be as generally applicable as possible.

This is exactly analogous to what you do in designing programs – make them general and abstract, use subroutines, etc. But there is a difference: in math, proofs are sometimes valued for being deep and hard. This is not much of a consideration in programming: here, the premium is more on how well it works and how easy it is to understand.

Proofs are important. They permit you to convince yourself and others that your reasoning is correct. The insights gained can help you understand why something is true and whether it will stay true when other things change. Proofs are particularly important in computer science and electrical engineering. Bugs have proven costly for Intel, AT&T, and Airbus. A good proof is strong evidence that no bugs exist.

# 4 False Proofs

In your life you will find many false proofs; it is good to know how to find the problem.

If a proof is written carefully, the problem is usually obvious. So false proofs get tricky when they are also sloppy.

What can go wrong?

- Derivation of a new statement by an invalid deduction rule, such as $A \implies B$, and $A$, therefore $C$! This actually appeared in a famous PhD thesis on linear logic. A Stanford student was able to publish a PhD thesis based on his discovery of the error (and conclusion that in fact $C$ was FALSE).
- Unstated axiom. Gauss once said "clearly if a curve enters a region, it has to leave." This was accepted as a proof for a long time; only a century later was it cleared up.
- Misuse of a definition. Using something "obvious" in the *intent* of the definition that doesn't actually arise from the formal definition.

The most common problem is a gap between intuition and formalism.

## 4.1 Example

$$\begin{aligned}
1 &= \sqrt{1} \\
&= \sqrt{(-1)(-1)} \\
&= \sqrt{-1}\sqrt{-1} \\
&= \sqrt{-1}^2 \\
&= -1. \\
\text{So, } 1 &= -1!
\end{aligned}$$

What is wrong?

## 4.2 Some Actual Proofs...

If you make mistakes, you won't be alone!

Rigorous logical proof systems are nice, but no one really has the time or energy to be so careful. We prove things in a less formal way. The objective is to convince everyone that a truly rigorous proof could be built if someone took the time to do it. As a result, even great mathematicians can goof proofs.

- Andrew Wiles recently announced a proof of Fermat's Last Theorem. It was several hundred pages long. It took mathematicians months of hard work to discover it had a fatal flaw (so Wiles produced another proof of several hundred pages; this one seems to have convinced people for now).
- Kempe's invalid "proof" of the Four Color Theorem stood for 10 years (1879–1890)
- Gauss's 1799 Ph.D. thesis is usually referred to as being the first rigorous proof of the Fundamental Theorem of Algebra (every polynomial has a zero over the complex numbers). But it contains quotes like

  > "If a branch of an algebraic curve enters a bounded region, it must necessarily leave it again. ... Nobody, to my knowledge, has ever doubted [this fact]. But if anybody desires it, then on another occasion I intend to give a demonstration which will leave no doubt."

  Fields Medalist Steve Smale writes about this, calling it an "immense gap" in the proof that was not filled in until 1920, more than a hundred years later.
- In 1900 Poincare carelessly claimed a certain very simple topological characterization of the 3-dimensional sphere. Later realizing it was not so obvious, he demoted the claim to the status of a "conjecture" in 1904. The Poincare Conjecture is now one of the biggest open questions in mathematics (two Fields Medals have been given out for partial progress on it).
- In the 1940's Paul Erdos conjectured a certain combinatorial fact about arithmetic progressions (every set of natural numbers of positive density contains arbitrarily long arithmetic progressions), and offered $1000 for a proof or disproof. Endre Szemeredi proved the conjecture in 1972, but the proof was so long and badly written that Erdos was not sure whether to believe it. Finally, Andras Hajnal stepped in and wrote a much clearer version of the same proof, which was eventually published under Szemeredi's name. At some point during the write-up, Hajnal informed Erdos that he was now confident enough of the proof that he was willing to buy it from Szemeredi for $500.
- There's also the story of Newton waiting 20 years to publish the Principia because he didn't see how to prove that one could assume all the mass of a sphere to be concentrated at its center when calculating gravitational attraction. The proof ultimately required the invention of calculus ...

# 5 Inductive proofs

Induction is by far the most important proof method in computer science. Suppose you want to prove something, $P(n)$, is true for all $n \in N$.
$0, 1, 2, \ldots$. You can prove it individually for $0, 1, \ldots$. But that has to stop sometime. The proof method of mathematical induction says that you just need to prove it for 0, then prove "if it's true for $n$ then it's true for $n+1$".

Why does this prove it for all $n \in N$? Perhaps it seems obvious. It seems like dominoes. In fact, it's part of how $N$ is defined. It's usually taken as an assumption (axiom) about $N$:

Induction axiom:

$$[P(0) \wedge \forall n \geq 0(P(n) \Rightarrow P(n+1))] \Rightarrow \forall n(P(n)).$$

Alternatively, you can see it as a deduction rule. The pattern is:

To prove: $\forall n \geq 0(P(n))$
It's enough to show:
1. (Base) $P(0)$
2. (Inductive step) $\forall n \geq 0(P(n) \Rightarrow P(n+1))$

There is a variant if you only want to prove it for $n \geq k$:

To prove: $\forall n \geq k(P(n))$
It's enough to show:
1. (Base) $P(k)$
2. (Inductive step) $\forall n \geq k(P(n) \Rightarrow P(n+1))$

## 5.1 An Example—Sum of Series

This is the canonical first example for induction:

**Lemma 5.1** $\forall n \geq 0(1+2+3+\ldots+n = \frac{n(n+1)}{2})$

Alternatively (and this is better), we can write the LHS in closed form:

$$\sum_{i=1}^{n} i \text{ or } \sum_{1 \leq i \leq n} i$$

Thus, we want to prove:
$\forall n \geq 0(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})$
Let's stop and be sure we know what this summation means. First check boundary cases (always a good idea to see if you understand a definition).

- If $n = 1$, then the sum $1+2+3+\ldots+n = 1$. The sum has one term only. The appearance of 2, 3, and $n$ is misleading!

- If $n = 0$, then $1 + 2 + 3 + \ldots + n = 0$. There are no terms present in the summation.

Now, the induction pattern says:

Prove: $\forall n \geq 0(P(n))$
1. (Base) $P(0)$
2. (Inductive step) $\forall n \geq 0(P(n) \Rightarrow P(n+1))$
3. QED — Induction

Here, we define $P(n)$ to be the predicate $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. In other words:

Prove: $\forall n \geq 0(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})$.
1. (Base) $\sum_{i=1}^{0} i = \frac{0(0+1)}{2}$.
2. (Inductive step) $\forall n \geq 0(\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \Rightarrow \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2})$
3. QED — Induction

The two steps of the proof are called the *base* and the *induction step*.
Usually, the base step is pretty easy to check, but the inductive step can involve some work and creativity.

Whether you give a structured or paragraph style proof, the proof must contain, clearly, all of the following:

1. A statement that the proof is by induction.
2. The definition of the predicate $P(n)$.
3. The proof of the base step, $P(0)$ (or $P(k)$, if we're starting from some other value $k$).
4. The proof of the inductive step, $\forall n \geq 0(P(n) \Rightarrow P(n+1)$

To finish this example:
Base: Easy by definition and arithmetic.

1. (Base) $\sum_{i=1}^{0} i = \frac{0(0+1)}{2}$ $(P(0))$
   1. $\sum_{i=1}^{0} i = 0$ — Definition of summation with no terms
   2. $\frac{0(0+1)}{2} = 0$ — Arithmetic
   3. QED — By 1.1 and 1.2.

Inductive step uses basic logic (UG and implication). What's left is the job of showing that, assuming $P(n)$, we can prove $P(n+1)$.

2. (Inductive step) $\forall n \geq 0(\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \Rightarrow \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2})$
   1. Fix $n \geq 0$.
   2. $\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \Rightarrow \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$
      1. Assume $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
      2. $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$ — ???
      3. QED — Implication
   3. QED — UG

The important job is step 2, showing $P(n+1)$. To do this, we just write out the equation we want to show (for $n+1$), and play around with both sides to try to make them equal. Remember that we are allowed to use the assumption $P(n)$, which is the corresponding equation for $n$. So while we are manipulating the equation for $n+1$, we look for a place to plug in the information for $n$.

2. $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$
    1. $\sum_{i=1}^{n+1} i = (\sum_{i=1}^{n} i) + (n+1)$ — Summation has one extra term.
    2. $(\sum_{i=1}^{n} i) + (n+1) = \frac{n(n+1)}{2} + n + 1$ — Inductive hypothesis $P(n)$ (2.2.1)
    3. $\frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}$ — Algebra
    4. QED — Combining the previous 3 equations.

This worked out nicely because the left hand side (LHS) of the $n+1$ equation was easily expressible in terms of the $n$ equation. Sometimes we'll have to work harder. Also, here the choice of $P(n)$ came directly out of the theorem statement. Sometimes it isn't so obvious.

Also in this example, note that the inductive technique did not help us to come up with the correct expression $\frac{n(n+1)}{2}$ for the summation, but only to prove that it is correct. We'll see how to come up with such sums when we get to the analysis methods section of the course.