Induction

Slides by Christopher M. Bourke
Instructor: Berthe Y. Choueiry

Fall 2007

Computer Science & Engineering 235
Introduction to Discrete Mathematics
Sections 4.1 & 4.2 of Rosen

cse235@cse.unl.edu

How can we prove the following quantified statement?

$$\forall s \in S P(x)$$

Introduction

How can we prove the following quantified statement?

$$\forall s \in S P(x)$$

- For a *finite* set $S = \{s_1, s_2, \ldots, s_n\}$, we can prove that $P(x)$ holds for *each* element because of the equivalence,

$$P(s_1) \wedge P(s_2) \wedge \cdots \wedge P(s_n)$$

Introduction

How can we prove the following quantified statement?

$$\forall s \in S P(x)$$

- For a *finite* set $S = \{s_1, s_2, \ldots, s_n\}$, we can prove that $P(x)$ holds for *each* element because of the equivalence,

$$P(s_1) \wedge P(s_2) \wedge \cdots \wedge P(s_n)$$

- We can use *universal generalization* for infinite sets.

Introduction

How can we prove the following quantified statement?

$$\forall s \in S P(x)$$

- For a *finite* set $S = \{s_1, s_2, \dots, s_n\}$, we can prove that $P(x)$ holds for *each* element because of the equivalence,

$$P(s_1) \wedge P(s_2) \wedge \cdots \wedge P(s_n)$$

- We can use *universal generalization* for infinite sets.
- Another, more sophisticated way is to use *Induction*.

What is Induction?

- If a statement $P(n_0)$ is true for some nonnegative integer; say $n_0 = 1$.

What is Induction?

- If a statement $P(n_0)$ is true for some nonnegative integer; say $n_0 = 1$.
- Also suppose that we are able to prove that *if* $P(k)$ is true for $k \geq n_0$, *then* $P(k+1)$ is also true;

$$P(k) \rightarrow P(k+1)$$

What is Induction?

- If a statement $P(n_0)$ is true for some nonnegative integer; say $n_0 = 1$.
- Also suppose that we are able to prove that *if* $P(k)$ is true for $k \geq n_0$, *then* $P(k+1)$ is also true;

$$P(k) \rightarrow P(k+1)$$

- It follows from these two statements that $P(n)$ is true for all $n \geq n_0$. I.e.

$$\forall n \geq n_0 P(n)$$

What is Induction?

- If a statement $P(n_0)$ is true for some nonnegative integer; say $n_0 = 1$.
- Also suppose that we are able to prove that *if* $P(k)$ is true for $k \geq n_0$, *then* $P(k+1)$ is also true;

$$P(k) \to P(k+1)$$

- It follows from these two statements that $P(n)$ is true for all $n \geq n_0$. I.e.

$$\forall n \geq n_0 P(n)$$

This is the basis of the most widely used proof technique: *Induction*.

The Well Ordering Principle I

Why is induction a legitimate proof technique?

At its heart is the *Well Ordering Principle*.

Theorem (Principle of Well Ordering)

Every nonempty set of nonnegative integers has a least element.

Since every such set has a least element, we can form a *base case*.

We can then proceed to establish that the set of integers $n \geq n_0$ such that $P(n)$ is *false* is actually *empty*.

Thus, induction (both "weak" and "strong" forms) are logical equivalences of the well-ordering principle.

Another View I

To look at it another way, assume that the statements

$$P(n_0) \tag{1}$$
$$P(k) \rightarrow P(k+1) \tag{2}$$

are true. We can now use a form of *universal generalization* as follows.

Say we choose an element from the universe of discourse c. We wish to establish that $P(c)$ is true. If $c = n_0$ then we are done.

Another View II

Otherwise, we apply (2) above to get

$$\begin{aligned} P(n_0) &\Rightarrow P(n_0+1) \\ &\Rightarrow P(n_0+2) \\ &\Rightarrow P(n_0+3) \\ &\cdots \\ &\Rightarrow P(c-1) \\ &\Rightarrow P(c) \end{aligned}$$

Via a finite number of steps $(c - n_0)$, we get that $P(c)$ is true. Since c was arbitrary, the universal generalization is established.

$$\forall n \geq n_0 P(n)$$

Theorem (Principle of Mathematical Induction)

Given a statement P concerning the integer n, suppose

1. *P is true for some particular integer n_0; $P(n_0) = 1$.*
2. *If P is true for some particular integer $k \geq n_0$ then it is true for $k+1$.*

Then P is true for all integers $n \geq n_0$, that is

$$\forall n \geq n_0 P(n)$$

is true.

- Showing that $P(n_0)$ holds for some initial integer n_0 is called the *Basis Step*.
- Showing the implication $P(k) \rightarrow P(k+1)$ for every $k \geq n_0$ is called the *Induction Step*.
- The assumption $P(n_k)$ itself is called the *inductive hypothesis*.
- Together, induction can be expressed as an inference rule.

$$\big(P(n_0) \wedge \forall k \geq n_0 P(k) \rightarrow P(k+1)\big) \rightarrow \forall n \geq n_0 P(n)$$

Example I

Example

Prove that $n^2 \leq 2^n$ for all $n \geq 5$ using induction.

Example I

Example

Prove that $n^2 \leq 2^n$ for all $n \geq 5$ using induction.

We formalize the statement as $P(n) = (n^2 \leq 2^n)$.

Example I

Example

Prove that $n^2 \leq 2^n$ for all $n \geq 5$ using induction.

We formalize the statement as $P(n) = (n^2 \leq 2^n)$.

Our *base case* here is for $n = 5$. We directly verify that

$$25 = 5^2 \leq 2^5 = 32$$

and so $P(5)$ is true and thus the basic step holds.

Example I
Continued

We now perform the induction step and *assume* that $P(k)$ (the inductive hypothesis) is true. Thus,

$$k^2 \leq 2^k$$

Example I

Continued

We now perform the induction step and *assume* that $P(k)$ (the inductive hypothesis) is true. Thus,

$$k^2 \leq 2^k$$

Multiplying by 2 we get

$$2k^2 \leq 2^{k+1}$$

Example I

Continued

We now perform the induction step and *assume* that $P(k)$ (the inductive hypothesis) is true. Thus,

$$k^2 \leq 2^k$$

Multiplying by 2 we get

$$2k^2 \leq 2^{k+1}$$

By a separate proof, we can show that for all $k \geq 5$,

$$2k^2 \geq k^2 + 5k > k^2 + 2k + 1 = (k+1)^2$$

Example I
Continued

We now perform the induction step and *assume* that $P(k)$ (the inductive hypothesis) is true. Thus,

$$k^2 \leq 2^k$$

Multiplying by 2 we get

$$2k^2 \leq 2^{k+1}$$

By a separate proof, we can show that for all $k \geq 5$,

$$2k^2 \geq k^2 + 5k > k^2 + 2k + 1 = (k+1)^2$$

Using transitivity, we get that

$$(k+1)^2 < 2k^2 \leq 2^{k+1}$$

Thus, $P(k+1)$ holds

Example II

Example

Prove that for any $n \geq 1$,

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Example II

Example

Prove that for any $n \geq 1$,

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

The base case is easily verified;

$$1 = 1^2 = \frac{(1+1)(2+1)}{6} = 1$$

Example

Prove that for any $n \geq 1$,

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

The base case is easily verified;

$$1 = 1^2 = \frac{(1+1)(2+1)}{6} = 1$$

Now assume that $P(k)$ holds for some $k \geq 1$, so

$$\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}$$

We want to show that $P(k+1)$ is true; that is, we want to show that

$$\sum_{i=1}^{k+1} i^2 = \frac{(k+1)(k+2)(2k+3)}{6}$$

Example II
Continued

We want to show that $P(k+1)$ is true; that is, we want to show that

$$\sum_{i=1}^{k+1} i^2 = \frac{(k+1)(k+2)(2k+3)}{6}$$

However, observe that this sum can be written

$$\sum_{i=1}^{k+1} i^2 = 1^2 + 2^2 + \cdots k^2 + (k+1)^2 = \sum_{i=1}^{k} i^2 + (k+1)^2$$

Example II
Continued

$$\sum_{i=1}^{k+1} i^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \quad (*)$$

Example II
Continued

$$\begin{aligned}\sum_{i=1}^{k+1} i^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \quad (*)\\ &= \frac{k(k+1)(2k+1)}{6} + \frac{6(k+1)^2}{6}\end{aligned}$$

Nebraska Lincoln

Example II
Continued

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \quad (*) \\
&= \frac{k(k+1)(2k+1)}{6} + \frac{6(k+1)^2}{6} \\
&= \frac{(k+1)\left[k(2k+1)+6(k+1)\right]}{6}
\end{aligned}$$

Example II

Continued

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \qquad (*) \\
&= \frac{k(k+1)(2k+1)}{6} + \frac{6(k+1)^2}{6} \\
&= \frac{(k+1)\left[k(2k+1) + 6(k+1)\right]}{6} \\
&= \frac{(k+1)\left[2k^2 + 7k + 6\right]}{6}
\end{aligned}$$

Example II
Continued

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \quad (*) \\
&= \frac{k(k+1)(2k+1)}{6} + \frac{6(k+1)^2}{6} \\
&= \frac{(k+1)\left[k(2k+1) + 6(k+1)\right]}{6} \\
&= \frac{(k+1)\left[2k^2 + 7k + 6\right]}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6}
\end{aligned}$$

Example II
Continued

Thus we have that

$$\sum_{i=1}^{k+1} = \frac{(k+1)(k+2)(2k+3)}{6}$$

so we've established that $P(k) \rightarrow P(k+1)$.

Thus, by the principle of mathematical induction,

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Example III

Example

Prove that for any integer $n \geq 1$, $2^{2n} - 1$ is divisible by 3.

Example III

Example

Prove that for any integer $n \geq 1$, $2^{2n} - 1$ is divisible by 3.

Define $P(n)$ to be the statement that $3 \mid (2^{2n} - 1)$.

Example III

Example

Prove that for any integer $n \geq 1$, $2^{2n} - 1$ is divisible by 3.

Define $P(n)$ to be the statement that $3 \mid (2^{2n} - 1)$.

Again, we note that the base case is $n = 1$, so we have that

$$2^{2 \cdot 1} - 1 = 3$$

which is certainly divisible by 3.

Example III

Example

Prove that for any integer $n \geq 1$, $2^{2n} - 1$ is divisible by 3.

Define $P(n)$ to be the statement that $3 \mid (2^{2n} - 1)$.

Again, we note that the base case is $n = 1$, so we have that

$$2^{2 \cdot 1} - 1 = 3$$

which is certainly divisible by 3.

We next assume that $P(k)$ holds. That is, we assume that there exists an integer ℓ such that

$$2^{2k} - 1 = 3\ell$$

Example III
Continued

Note that

$$2^{2(k+1)} - 1 = 4 \cdot 2^{2k} - 1$$

Example III
Continued

Note that

$$2^{2(k+1)} - 1 = 4 \cdot 2^{2k} - 1$$

By the inductive hypothesis, $2^{2k} = 3\ell + 1$, applying this we get that

$$\begin{aligned} 2^{2(k+1)} - 1 &= 4(3\ell + 1) - 1 \\ &= 12\ell + 4 - 1 \\ &= 12\ell + 3 \\ &= 3(4\ell + 1) \end{aligned}$$

Example III

Continued

Note that

$$2^{2(k+1)} - 1 = 4 \cdot 2^{2k} - 1$$

By the inductive hypothesis, $2^{2k} = 3\ell + 1$, applying this we get that

$$\begin{aligned} 2^{2(k+1)} - 1 &= 4(3\ell + 1) - 1 \\ &= 12\ell + 4 - 1 \\ &= 12\ell + 3 \\ &= 3(4\ell + 1) \end{aligned}$$

And we are done, since 3 divides the RHS, it must divide the LHS. Thus, by the principle of mathematical induction, $2^{2n} - 1$ is divisible by 3 for all $n \geq 1$.

Example IV

Example

Prove that $n! > 2^n$ for all $n \geq 4$

Example IV

Example

Prove that $n! > 2^n$ for all $n \geq 4$

The base case holds since $24 = 4! > 2^4 = 16$.

Example IV

Example

Prove that $n! > 2^n$ for all $n \geq 4$

The base case holds since $24 = 4! > 2^4 = 16$.

We now make our inductive hypothesis and assume that

$$k! > 2^k$$

for some integer $k \geq 4$

Example IV

Example

Prove that $n! > 2^n$ for all $n \geq 4$

The base case holds since $24 = 4! > 2^4 = 16$.

We now make our inductive hypothesis and assume that

$$k! > 2^k$$

for some integer $k \geq 4$

Since $k \geq 4$, it certainly is the case that $k + 1 > 2$. Therefore, we have that

$$(k + 1)! = (k + 1)k! > 2 \cdot 2^k = 2^{k+1}$$

So by the principle of mathematical induction, we have our desired result.

Example V

Example

Let $m \in \mathbb{Z}$ and suppose that $x \equiv y \pmod{m}$. Then for all $n \geq 1$,

$$x^n \equiv y^n \pmod{m}$$

Example V

Example

Let $m \in \mathbb{Z}$ and suppose that $x \equiv y \pmod{m}$. Then for all $n \geq 1$,

$$x^n \equiv y^n \pmod{m}$$

The base case here is trivial as it is encompassed by the assumption.

Example V

Example

Let $m \in \mathbb{Z}$ and suppose that $x \equiv y \pmod{m}$. Then for all $n \geq 1$,

$$x^n \equiv y^n \pmod{m}$$

The base case here is trivial as it is encompassed by the assumption.

Now assume that it is true for some $k \geq 1$;

$$x^k \equiv y^k \pmod{m}$$

Since multiplication of corresponding sides of a congruence is still a congruence, we have

$$x \cdot x^k \equiv y \cdot y^k \pmod{m}$$

Example V
Continued

Since multiplication of corresponding sides of a congruence is still a congruence, we have

$$x \cdot x^k \equiv y \cdot y^k \pmod{m}$$

And so

$$x^{k+1} \equiv y^{k+1} \pmod{m}$$

$\square$

Example VI

Example

Show that

$$\sum_{i=1}^{n} i^3 = \left(\sum_{i=1}^{n} i\right)^2$$

for all $n \geq 1$.

The base case is trivial since $1^3 = (1)^2$.

The inductive hypothesis will assume that it holds for some $k \geq 1$:

$$\sum_{i=1}^{k} i^3 = \left(\sum_{i=1}^{k} i\right)^2$$

Example VI

Continued

Fact

By another standard induction proof (see the text) the summation of natural numbers up to n is

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

We now consider the summation for $(k+1)$:

$$\sum_{i=1}^{k+1} i^3 = \sum_{i=1}^{k} i^3 + (k+1)^3$$

Example VI
Continued

$$\sum_{i=1}^{k+1} i^3 \quad = \quad \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3$$

Example VI
Continued

$$\begin{aligned}\sum_{i=1}^{k+1} i^3 &= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 \\ &= \frac{(k^2(k+1)^2) + 4(k+1)^3}{2^2}\end{aligned}$$

Example VI
Continued

$$
\begin{aligned}
\sum_{i=1}^{k+1} i^3 &= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 \\
&= \frac{(k^2(k+1)^2) + 4(k+1)^3}{2^2} \\
&= \frac{(k+1)^2\left[k^2+4k+4\right]}{2^2}
\end{aligned}
$$

Example VI

Continued

$$
\begin{aligned}
\sum_{i=1}^{k+1} i^3 &= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 \\
&= \frac{(k^2(k+1)^2) + 4(k+1)^3}{2^2} \\
&= \frac{(k+1)^2\left[k^2+4k+4\right]}{2^2} \\
&= \frac{(k+1)^2(k+2)^2}{2^2}
\end{aligned}
$$

Example VI

Continued

$$\begin{aligned}
\sum_{i=1}^{k+1} i^3 &= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 \\
&= \frac{(k^2(k+1)^2) + 4(k+1)^3}{2^2} \\
&= \frac{(k+1)^2\left[k^2+4k+4\right]}{2^2} \\
&= \frac{(k+1)^2(k+2)^2}{2^2} \\
&= \left(\frac{(k+1)(k+2)}{2}\right)^2
\end{aligned}$$

Example VI
Continued

$$
\begin{aligned}
\sum_{i=1}^{k+1} i^3 &= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 \\
&= \frac{(k^2(k+1)^2) + 4(k+1)^3}{2^2} \\
&= \frac{(k+1)^2\left[k^2+4k+4\right]}{2^2} \\
&= \frac{(k+1)^2(k+2)^2}{2^2} \\
&= \left(\frac{(k+1)(k+2)}{2}\right)^2
\end{aligned}
$$

So by the PMI, the equality holds. $\square$

Example VII

The *Bad* Example

Consider this "proof" that all of you will receive the same grade.

Proof.

Let $P(n)$ be the statement that every set of n students receives the same grade. Clearly $P(1)$ is true, so the base case is satisfied.
Now assume that $P(k-1)$ is true. Given a group of k students, apply $P(k-1)$ to the subset $\{s_1, s_2, \ldots s_{k-1}\}$. Now, separately apply the inductive hypothesis to the subset $\{s_2, s_3, \ldots, s_k\}$. Combining these two facts tells us that $P(k)$ is true. Thus, $P(n)$ is true for all students. $\square$

- The mistake is not the base case, $P(1)$ is true.
- Also, it *is* the case that, say $P(73) \rightarrow P(74)$, so this cannot be the mistake.

- The mistake is not the base case, $P(1)$ is true.
- Also, it *is* the case that, say $P(73) \rightarrow P(74)$, so this cannot be the mistake.

The error is in $P(1) \rightarrow P(2)$ which is certainly not true; we cannot combine the two inductive hypotheses to get $P(2)$.

Strong Induction I

Another form of induction is called the "strong form".

Despite the name, it is *not* a *stronger* proof technique.

In fact, we have the following.

Lemma

The following are equivalent.

- *The Well Ordering Principle*
- *The Principle of Mathematical Induction*
- *The Principle of Mathematical Induction, Strong Form*

Strong Induction II

Theorem (Principle of Mathematical Induction (Strong Form))

Given a statement P concerning the integer n, suppose

1. *P is true for some particular integer n_0; $P(n_0) = 1$.*
2. *If $k > n_0$ is any integer and P is true for all integers l in the range $n_0 \leq l < k$, then it is true also for k.*

Then P is true for all integers $n \geq n_0$; i.e.

$$\forall(n \geq n_0)P(n)$$

is true.

Example

Show that for all $n \geq 1$ and $f(x) = x^n$,

$$f'(x) = nx^{n-1}$$

Example

Show that for all $n \geq 1$ and $f(x) = x^n$,

$$f'(x) = nx^{n-1}$$

Verifying the base case for $n = 1$ is straightforward;

$$f'(x) = \lim_{h \to 0} \frac{f(x_0 + h) - f(x_0)}{h} = \lim_{h \to 0} \frac{(x_0 + h) - x_0}{h} = 1 = 1x^0$$

Example
Continued

Now assume that the inductive hypothesis holds for some k; i.e. for $f(x) = x^k$,

$$f'(x) = kx^{k-1}$$

Example

Continued

Now assume that the inductive hypothesis holds for some k; i.e. for $f(x) = x^k$,

$$f'(x) = kx^{k-1}$$

Now consider $f_2(x) = x^{k+1} = x^k \cdot x$. Using the product rule we observe that

$$f_2'(x) = (x^k)' \cdot x + x^k \cdot (x')$$

Example
Continued

Now assume that the inductive hypothesis holds for some k; i.e. for $f(x) = x^k$,

$$f'(x) = kx^{k-1}$$

Now consider $f_2(x) = x^{k+1} = x^k \cdot x$. Using the product rule we observe that

$$f_2'(x) = (x^k)' \cdot x + x^k \cdot (x')$$

From the inductive hypothesis, the first derivative is kx^{k-1} and the base case gives us the second derivative.

Example

Continued

Now assume that the inductive hypothesis holds for some k; i.e. for $f(x) = x^k$,

$$f'(x) = kx^{k-1}$$

Now consider $f_2(x) = x^{k+1} = x^k \cdot x$. Using the product rule we observe that

$$f_2'(x) = (x^k)' \cdot x + x^k \cdot (x')$$

From the inductive hypothesis, the first derivative is kx^{k-1} and the base case gives us the second derivative. Thus,

$$\begin{aligned} f_2'(x) &= kx^{k-1} \cdot x + x^k \cdot 1 \\ &= kx^k + x^k \\ &= (k+1)x^k \end{aligned}$$

Recall that the Fundamental Theorem of Arithmetic states that any integer $n \geq 2$ can be written as a unique product of primes.

We'll use the strong form of induction to prove this.

Strong Form Example

Fundamental Theorem of Arithmetic

Recall that the Fundamental Theorem of Arithmetic states that any integer $n \geq 2$ can be written as a unique product of primes.

We'll use the strong form of induction to prove this.

Let $P(n)$ be the statement "n can be written as a product of primes."

Clearly, $P(2)$ is true since 2 is a prime itself. Thus the base case holds.

Strong Form Example

Fundamental Theorem of Arithmetic - Continued

We make our inductive hypothesis. Here we assume that the predicate P holds for *all* integers less than some integer $k \geq 2$; i.e. we assume that

$$P(2) \wedge P(3) \wedge \cdots \wedge P(k)$$

is true.

Strong Form Example

Fundamental Theorem of Arithmetic - Continued

We make our inductive hypothesis. Here we assume that the predicate P holds for *all* integers less than some integer $k \geq 2$; i.e. we assume that

$$P(2) \wedge P(3) \wedge \cdots \wedge P(k)$$

is true.

We want to show that this implies $P(k+1)$ holds. We consider two cases.

If $k+1$ is prime, then $P(k+1)$ holds and we are done.

Strong Form Example

Fundamental Theorem of Arithmetic - Continued

We make our inductive hypothesis. Here we assume that the predicate P holds for *all* integers less than some integer $k \geq 2$; i.e. we assume that

$$P(2) \wedge P(3) \wedge \cdots \wedge P(k)$$

is true.

We want to show that this implies $P(k+1)$ holds. We consider two cases.

If $k+1$ is prime, then $P(k+1)$ holds and we are done.

Else, $k+1$ is a composite and so it has factors u, v such that $2 \leq u, v < k+1$ such that

$$u \cdot v = k+1$$

Strong Form Example

Fundamental Theorem of Arithmetic - Continued

We now apply the inductive hypothesis; both u and v are less than $k+1$ so they can both be written as a unique product of primes;

$$u = \prod_i p_i, \quad v = \prod_j p_j$$

Strong Form Example

Fundamental Theorem of Arithmetic - Continued

We now apply the inductive hypothesis; both u and v are less than $k+1$ so they can both be written as a unique product of primes;

$$u = \prod_i p_i, \quad v = \prod_j p_j$$

Therefore,

$$k+1 = \left(\prod_i p_i\right)\left(\prod_j p_j\right)$$

and so by the strong form of the PMI, $P(k+1)$ holds. $\square$

Strong Form Example
GCD

Recall the following.

Lemma

If $a, b \in \mathbb{N}$ are such that $\gcd(a, b) = 1$ then there are integers s, t such that

$$gcd(a, b) = 1 = sa + tb$$

We will prove this using the strong form of induction.

Let $P(n)$ be the statement

$$a, b \in \mathbb{N} \wedge \gcd(a, b) = 1 \wedge a + b = n \Rightarrow \exists s, t \in \mathbb{Z}, as + tb = 1$$

Our base case here is when $n = 2$ since $a = b = 1$.

For $s = 1, t = 0$, the statement $P(2)$ is satisfied since

$$sa + bt = 1 \cdot 1 + 1 \cdot 0 = 1$$

Strong Form Example
GCD

We now form the inductive hypothesis. Suppose $n \in \mathbb{N}, n \geq 2$ and assume that $P(k)$ is true for all k with $2 \leq k \leq n$.

Now suppose that for $a, b \in \mathbb{N}$,

$$\gcd(a, b) = 1 \wedge a + b = n + 1$$

We consider three cases.

Case 1 $a = b$

In this case

$$\begin{array}{rcll} \gcd(a, b) & = & \gcd(a, a) & \text{by definition} \\ & = & a & \text{by definition} \\ & = & 1 & \text{by assumption} \end{array}$$

Therefore, since the $\gcd$ is one, it must be the case that $a = b = 1$ and so we simply have the base case, $P(2)$.

Case 2 $a < b$

Case 2 $a < b$

Since $b > a$, it follows that $b - a > 0$ and so

$$\gcd(a, b) = \gcd(a, b - a) = 1$$

(Why?)

Case 2 $a < b$

Since $b > a$, it follows that $b - a > 0$ and so

$$\gcd(a, b) = \gcd(a, b - a) = 1$$

(Why?)

Furthermore,

$$2 \leq a + (b - a) = n + 1 - a \leq n$$

Since $a + (b - a) \leq n$, we can apply the inductive hypothesis and conclude that $P(n + 1 - a) = P(a + (b - a))$ is true.

This implies that there exist integers s_0, t_0 such that

$$as_0 + (b - a)t_0 = 1$$

Strong Form Example
GCD

Since $a + (b - a) \leq n$, we can apply the inductive hypothesis and conclude that $P(n + 1 - a) = P(a + (b - a))$ is true.

This implies that there exist integers s_0, t_0 such that

$$as_0 + (b - a)t_0 = 1$$

and so

$$a(s_0 - t_0) + bt_0 = 1$$

Since $a + (b - a) \leq n$, we can apply the inductive hypothesis and conclude that $P(n + 1 - a) = P(a + (b - a))$ is true.

This implies that there exist integers s_0, t_0 such that

$$as_0 + (b - a)t_0 = 1$$

and so

$$a(s_0 - t_0) + bt_0 = 1$$

So for $s = s_0 - t_0$ and $t = t_0$ we get

$$as + bt = 1$$

Thus, $P(n + 1)$ is established for this case.

Strong Form Example
GCD

Case 3 $a > b$ This is completely symmetric to case 2; we use $a - b$ instead of $b - a$.

Since all three cases handle every possibility, we've established that $P(n + 1)$ is true and so by the strong PMI, the lemma holds. $\square$