

Strong Form: Example A (3)

3. 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:

$$P(2) \wedge P(3) \wedge P(4) \wedge \dots \wedge P(k) \text{ is true}$$

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

- $k+1$ is prime, then $P(k+1)$ holds. We are done.
- $k+1$ is a composite.

$k+1$ has two factors u, v , $2 \leq u, v < k+1$ such that $k+1 = u \cdot v$

By the inductive hypothesis $u = \prod_i p_i$, $v = \prod_j p_j$, and p_i, p_j prime

Thus, $k+1 = \prod_i p_i \prod_j p_j$

So, by the strong form of PMI, $P(k+1)$ holds

QED

Induction

Sections 5.1 and 5.2 of Rosen 7th Edition

Spring 2013

CSCE 235 Introduction to Discrete Structures

Course web-page: cse.unl.edu/~cse235

Questions: Piazza

Outline

- Motivation
- What is induction?
 - Viewed as: the Well-Ordering Principle, Universal Generalization
 - Formal Statement
 - 6 Examples
- Strong Induction
 - Definition
 - Examples: decomposition into product of primes, gcd

Motivation

- How can we prove the following proposition?

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

- 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

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

- For an infinite set, we can try to use universal generalization
- Another, more sophisticated way is to use induction

What Is Induction?

- If a statement $P(n_0)$ is true for some nonnegative integer say $n_0=1$
- 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 $n \geq n_0$, that is

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

- The above is the basis of induction, a widely used proof technique and a very powerful one

The Well-Ordering Principle

- Why induction is a legitimate proof technique?
- At its heart, induction is the Well Ordering Principle
- **Theorem:** Principle of Well Ordering. Every nonempty set of nonnegative integers has a least element
- Since, every such has a least element, we can form a basis case (using the least element as the basis case n_0)
- 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

- To look at it in another way, assume that the statements
 - (1) $P(n_0)$
 - (2) $P(k) \Rightarrow P(k+1)$are true. We can now use a form of universal generalization as follows
- Say we choose an element c of the UoD. We wish to establish that $P(c)$ is true. If $c=n_0$, then we are done
- Otherwise, we apply (2) above to get
$$P(n_0) \Rightarrow P(n_0+1), P(n_0+1) \Rightarrow P(n_0+2), P(n_0+2) \Rightarrow P(n_0+3), \dots, P(c-1) \Rightarrow P(c)$$
Via a finite number of steps ($c-n_0$) we get that $P(c)$ is true.
- Because c is arbitrary, the universal generalization is established and
$$\forall n \geq n_0 P(n)$$

Outline

- Motivation
- What is induction?
 - Viewed as: the Well-Ordering Principle, Universal Generalization
 - **Formal Statement**
 - **6 Examples**
- Strong Induction
 - Definition
 - Examples: decomposition into product of primes, gcd

Induction: Formal Definition (1)

- **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 $k+1$: $P(k) \rightarrow P(k+1)$

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

$$\forall n \geq n_0 P(n) \text{ is true}$$

Induction: Formal Definition (2)

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

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

Steps

1. Form the general statement
2. Form and verify the base case (basis step)
3. Form the inductive hypothesis
4. Prove the inductive step

Example A (1)

- Prove that $n^2 \leq 2^n$ for all $n \geq 5$ using induction
- We formalize the statement $P(n) = (n^2 \leq 2^n)$
- Our basis case is for $n=5$. We directly verify that

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

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

- We need now to perform the inductive step

Example A (2)

- Assume $P(k)$ holds (the inductive hypothesis). Thus, $k^2 \leq 2^k$
- Now, we need to prove the inductive step. For all $k \geq 5$,
 $(k+1)^2 = k^2 + 2k + 1 < k^2 + 2k + k$ (because $k \geq 5 > 1$)
 $< k^2 + 3k < k^2 + k \cdot k$ (because $k \geq 5 > 3$)
 $< k^2 + k^2 = 2k^2$
- Using the inductive hypothesis ($k^2 \leq 2^k$), we get
 $(k+1)^2 < 2k^2 \leq 2 \cdot 2^k = 2^{k+1}$
- Thus, $P(k+1)$ holds

Example B (1)

- Prove that for any $n \geq 1$, $\sum_{i=1}^n (i^2) = n(n+1)(2n+1)/6$
- The basis case is easily verified $1^2=1= 1(1+1)(2+1)/6$
- We assume that $P(k)$ holds for some $k \geq 1$, so

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

- We want to show that $P(k+1)$ holds, that is

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

- We rewrite this sum as

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

Example B (2)

- We replace $\sum_{i=1}^k (i^2)$ by its value from the inductive hypothesis

$$\begin{aligned}\sum_{i=1}^{k+1} (i^2) &= \sum_{i=1}^k (i^2) + (k+1)^2 \\ &= k(k+1)(2k+1)/6 + (k+1)^2 \\ &= k(k+1)(2k+1)/6 + 6(k+1)^2/6 \\ &= (k+1)[k(2k+1)+6(k+1)]/6 \\ &= (k+1)[2k^2+7k+6]/6 \\ &= (k+1)(k+2)(2k+3)/6\end{aligned}$$

- Thus, we established that $P(k) \rightarrow P(k+1)$
- Thus, by the principle of mathematical induction we have

$$\forall n \geq 1, \sum_{i=1}^n (i^2) = n(n+1)(2n+1)/6$$

Example C (1)

- Prove that for any integer $n \geq 1$, $2^{2^n} - 1$ is divisible by 3
- Define $P(n)$ to be the statement $3 \mid (2^{2^n} - 1)$
- We note that for the basis case $n=1$ we do have $P(1)$
$$2^{2 \cdot 1} - 1 = 3 \text{ is divisible by } 3$$
- Next we assume that $P(k)$ holds. That is, there exists some integer u such that
$$2^{2^k} - 1 = 3u$$
- We must prove that $P(k+1)$ holds. That is, $2^{2^{(k+1)}} - 1$ is divisible by 3

Example C (2)

- Note that: $2^{2(k+1)} - 1 = 2^2 2^{2k} - 1 = 4 \cdot 2^{2k} - 1$
- The inductive hypothesis: $2^{2k} - 1 = 3u \Rightarrow 2^{2k} = 3u + 1$
- Thus: $2^{2(k+1)} - 1 = 4 \cdot 2^{2k} - 1 = 4(3u + 1) - 1$
 $= 12u + 4 - 1$
 $= 12u + 3$
 $= 3(4u + 1)$, a multiple of 3
- We conclude, by the principle of mathematical induction, for any integer $n \geq 1$, $2^{2n} - 1$ is divisible by 3

Example D

- Prove that $n! > 2^n$ for all $n \geq 4$
- The basis case holds for $n=4$ because $4!=24 > 2^4=16$
- We assume that $k! > 2^k$ for some integer $k \geq 4$ (which is our inductive hypothesis)
- We must prove the $P(k+1)$ holds

$$(k+1)! = k! (k+1) > 2^k (k+1)$$

- Because $k \geq 4$, $k+1 \geq 5 > 2$, thus

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

- Thus by the principal of mathematical induction, we have $n! > 2^n$ for all $n \geq 4$

Example E: Summation

- Show that $\sum_{i=1}^n (i^3) = (\sum_{i=1}^n i)^2$ for all $n \geq 1$
- The basis case is trivial: for $n = 1$, $1^3 = 1^2$
- The inductive hypothesis assumes that for some $n \geq 1$ we have $\sum_{i=1}^k (i^3) = (\sum_{i=1}^k i)^2$
- We now consider the summation for $(k+1)$: $\sum_{i=1}^{k+1} (i^3)$
 $= (\sum_{i=1}^k i)^2 + (k+1)^3 = (k(k+1)/2)^2 + (k+1)^3$
 $= (k^2(k+1)^2 + 4(k+1)^3) / 2^2 = (k+1)^2 (k^2 + 4(k+1)) / 2^2$
 $= (k+1)^2 (k^2 + 4k + 4) / 2^2 = (k+1)^2 (k+2)^2 / 2^2$
 $= ((k+1)(k+2) / 2)^2$
- Thus, by the PMI, the equality holds

Example F: Derivatives

- Show that for all $n \geq 1$ and $f(x) = x^n$, we have $f'(x) = nx^{n-1}$
- Verifying the basis case for $n=1$:

$$\begin{aligned} f'(x) &= \lim_{h \rightarrow 0} (f(x_0+h) - f(x_0)) / h \\ &= \lim_{h \rightarrow 0} ((x_0+h)^1 - (x_0^1)) / h = 1 = 1 \cdot x^0 \end{aligned}$$

- Now, assume that the inductive hypothesis holds for some k , $f(x) = x^k$, we have $f'(x) = kx^{k-1}$
- Now, consider $f_2(x) = x^{k+1} = x^k \cdot x$
- Using the product rule: $f'_2(x) = (x^k)' \cdot x + (x^k) \cdot x'$
- Thus, $f'_2(x) = kx^{k-1} \cdot x + x^k \cdot 1 = kx^k + x^k = (k+1)x^k$

The **Bad** Example: Example G

- Consider the proof for: All of you will receive the same grade
- Let $P(n)$ be the statement: “Every set of n students will receive the same grade”
- Clearly, $P(1)$ is true. So the basis case holds
- Now assume $P(k)$ holds, the inductive hypothesis
- Given a group of k students, apply $P(k)$ to $\{s_1, s_2, \dots, s_k\}$
- Now, separately apply the inductive hypothesis to the subset $\{s_2, s_3, \dots, s_{k+1}\}$
- Combining these two facts, we get $\{s_1, s_2, \dots, s_{k+1}\}$. Thus, $P(k+1)$ holds.
- Hence, $P(n)$ is true for all students

Example G: Where is the Error?

- The mistake is not the basis case: $P(1)$ is true
- Also, it is the case that, say, $P(73) \Rightarrow P(74)$
- So, this is cannot be the mistake
- The error is in $P(1) \Rightarrow P(2)$, which **cannot** hold
- We cannot combine the two inductive hypotheses to get $P(2)$

Outline

- Motivation
- What is induction?
 - Viewed as: the Well-Ordering Principle, Universal Generalization
 - Formal Statement
 - 6 Examples
- **Strong Induction**
 - **Definition**
 - **Examples: decomposition into product of primes, gcd**

Strong Induction

- **Theorem:** Principle of Mathematical Induction (Strong Form)
Given a statement P concerning an integer n ,
suppose
 1. P is true for some particular integer n_0 , $P(n_0)=1$
 2. If $k \geq n_0$ is any integer and P is true for all integers m in the range $n_0 \leq m < k$, then it is true also for kThen, P is true for all integers $n \geq n_0$, i.e.
$$\forall n \geq n_0 P(n) \text{ holds}$$

MPI and its Strong Form

- Despite the name, the strong form of PMI is **not a stronger proof technique** than PMI
- In fact, we have the following Lemma
- **Lemma:** The following are equivalent
 - The Well Ordering Principle
 - The Principle of Mathematical Induction
 - The Principle of Mathematical Induction, Strong Form

Strong Form: Example A (1)

- **Fundamental Theorem of Arithmetic** (page 211): For any integer $n \geq 2$ can be written uniquely as
 - A prime or
 - As the product of primes
- Prove using the strong form of induction to
- **Definition** (page 210)
 - **Prime**: A positive integer p greater than 1 is called prime iff the only positive factors of p are 1 and p .
 - **Composite**: A positive integer that is greater than 1 and is not prime is called composite
- According to the definition, 1 is **not** a prime

Strong Form: Example A (2)

1. Let $P(n)$ be the statement: “ n is a prime or can be written uniquely as a product of primes.”
2. The basis case holds: $P(2)=2$ and 2 is a prime.

Strong Form: Example B (1)

- **Notation:**

- $\gcd(a,b)$: the greatest common divisor of a and b

- Example: $\gcd(27, 15)=3$, $\gcd(35,28)=7$

- $\gcd(a,b)=1 \Leftrightarrow a, b$ are mutually prime

- Example: $\gcd(15,14)=1$, $\gcd(35,18)=1$

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

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

- **Question:** Prove the above lemma using the strong form of induction

Background Knowledge

- Prove that: $\gcd(a,b) = \gcd(a,b-a)$
- Proof: Assume $\gcd(a,b) = k$ and $\gcd(a,b-a) = k'$
 - $\gcd(a,b) = k \Rightarrow k$ divides a and b
 $\Rightarrow k$ divides a and $(b-a) \Rightarrow k$ divides k'
 - $\gcd(a,b-a) = k' \Rightarrow k'$ divides a and $b-a$
 $\Rightarrow k'$ divides a and $a+(b-a)=b \Rightarrow k'$ divides k
 - $(k$ divides $k')$ and $(k'$ divides $k) \Rightarrow k = k'$
 $\Rightarrow \gcd(a,b) = \gcd(a,b-a)$

(Lame) Alternative Proof

- Prove that $\gcd(a,b)=1 \Rightarrow \gcd(a,b-a)=1$
- We prove the contrapositive
 - Assume $\gcd(a,b-a) \neq 1 \Rightarrow \exists k \in \mathbb{Z}, k \neq 1$ k divides a and $b-a \Rightarrow \exists m,n \in \mathbb{Z}$ $a=km$ and $b-a=kn$
 $\Rightarrow a+(b-a)=k(m+n) \Rightarrow b=k(m+n) \Rightarrow k$ divides b
 - $k \neq 1$ divides a and divides $b \Rightarrow \gcd(a,b) \neq 1$
- But, don't prove a special case when you have the more general one (see previous slide..)

Strong Form: Example B (2)

1. Let $P(n)$ be the statement

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

2. Our basis case is when $n=2$ because $a=b=1$.

For $s=1, t=0$, the statement $P(2)$ is satisfied ($sa + tb = 1 \cdot 1 + 1 \cdot 0 = 1$)

3. We form the inductive hypothesis $P(k)$:

- For $k \in \mathbb{N}, k \geq 2$
- For all $i, 2 \leq i \leq k$ $P(a+b=k)$ holds
- For $a, b \in \mathbb{N}, (\gcd(a, b) = 1) \wedge (a + b = k) \exists s, t \in \mathbb{Z}, sa + tb = 1$

4. Given the inductive hypothesis, we prove $P(a+b = k+1)$

We consider three cases: $a=b, a < b, a > b$

Strong Form: Example B (3)

Case 1: $a=b$

- In this case: $\gcd(a,b) = \gcd(a,a)$ *Because $a=b$*
 $= a$ *By definition*
 $= 1$ *See assumption*
- $\gcd(a,b)=1 \Rightarrow a=b=1$
 \Rightarrow We have the basis case,
 $P(a+b)=P(2)$, which holds

Strong Form: Example B (4)

Case 2: $a < b$

- $b > a \Rightarrow b - a > 0$. So $\gcd(a,b) = \gcd(a,b-a) = 1$
- Further: $2 \leq a + (b-a) = (a+b) - a = (k+1) - a \leq k \Rightarrow a + (b-a) \leq k$
- Applying the inductive hypothesis $P(a+(b-a))$
 $(a, (b-a) \in \mathbb{N}) \wedge (\gcd(a, b-a) = 1) \wedge (a + (b-a) = b) \Rightarrow \exists s_0, t_0 \in \mathbb{Z}, s_0 a + t_0 (b-a) = 1$
- Thus, $\exists s_0, t_0 \in \mathbb{Z}$ such that $(s_0 - t_0)a + t_0 b = 1$
- So, for $s, t \in \mathbb{Z}$ where $s = s_0 - t_0$, $t = t_0$ we have $sa + tb = 1$
- Thus, $P(k+1)$ is established for this case

Strong Form: Example B (5)

Case 2: $a > b$

- This case is completely symmetric to case 2
- We use $a-b$ instead of $a-b$
- Because the three cases handle every possibility, we have established that $P(k+1)$ holds
- Thus, by the PMI strong form, the Lemma holds. **QED**

Template

- In order to prove by induction
 - Some mathematical theorem, or
 - $\forall n \geq n_0 P(n)$
- Follow the template
 - 1.State a propositional predicate
 $P(n)$: some statement involving n
 - 2.Form and verify the basis case (basis step)
 - 3.Form the inductive hypothesis (assume $P(k)$)
 - 4.Prove the inductive step (prove $P(k+1)$)

Summary

- Motivation
- What is induction?
 - Viewed as: the Well-Ordering Principle, Universal Generalization
 - Formal Statement
 - 6 Examples
- Strong Induction
 - Definition
 - Examples: decomposition into product of primes, gcd