CSE 191, Class Note 08
Computer Sci & Eng Dept
SUNY Buffalo
Outline

1 Mathematical Induction
Suppose we have a ladder of \( n \) rungs. Let’s say we can guarantee two things:

- We can reach the first rung of the ladder.
- If we can reach the \( i \)th rung of the ladder, then we can reach the next (i.e., the \( (i + 1) \)st) rung.

What can we conclude, then?

- We can conclude that we can reach the \( n \)th rung for any \( n \).
Similar to the above argument, we have a proof method called mathematical induction:

- Goal: to prove $P(n)$ is true (where $n$ is a positive integer).
- First step (called the basis step): show $P(1)$ is true.
- Second step (called the inductive step): show $P(k) \rightarrow P(k + 1)$ is true for every positive integer $k$. Here $P(k)$ is called the inductive assumption (or inductive hypothesis).

Clearly, the above method makes sense because from

$$P(1), P(1) \rightarrow P(2), P(2) \rightarrow P(3), \ldots, P(n - 1) \rightarrow P(n)$$

we can easily get $P(n)$. 
First example

Example: Show that, for any positive integer \( n \), \( 2^n > n \).

**Proof:** Basis step: When \( n = 1 \), we have \( 2^n = 2 > 1 = n \). So the proposition is true for \( n = 1 \).

Inductive step: Assume that the proposition is true for \( n = k \) (where \( k \) is a positive integer), i.e., \( 2^k > k \).

Now we prove that it is also true for \( n = k + 1 \), i.e., \( 2^{k+1} > k + 1 \).

From \( 2^k > k \) we get that \( 2^{k+1} = 2 \times 2^k > 2 \cdot k \geq k + 1 \).

This completes the induction proof.
In the first example, we have shown two things:

(a) \(2^1 > 1\);

(b) If \(2^k > k\) for positive integer \(k\), then \(2^{k+1} > k + 1\).

Hence, we have the following statements being true:

(1) \(2^1 > 1\); (This is (a))

(2) If \(2^1 > 1\), then \(2^2 > 2\); (This is (b) when \(k = 1\))

(3) If \(2^2 > 2\), then \(2^3 > 3\); (This is (b) when \(k = 2\))

\[\vdots\]

(n) If \(2^{n-1} > n - 1\), then \(2^n > n\); (This is (b) when \(k = n - 1\))

Putting all of them together, we see that \(2^n > n\).
Example 2: Show that $3 | n^3 - n$ for positive integer $n$.

**Proof:** **Basis step:** When $n = 1$, we have $n^3 - n = 0$. Clearly, $3 | n^3 - n$.

**Inductive step:** Assume that $3 | k^3 - k$ for positive integer $k$. We’ll show that $3 | (k + 1)^3 - (k + 1)$.

It is easy to see $(k + 1)^3 - (k + 1) = k^3 + 3k^2 + 2k = (k^3 - k) + 3(k^2 + k)$.

Since $3 | k^3 - k$, we can write $k^3 - k = 3j$ where $j$ is an integer. So,

$$(k + 1)^3 - (k + 1) = 3j + 3(k^2 + k) = 3(j + k^2 + k)$$

Hence, $3 | (k + 1)^3 - (k + 1)$. 
Understanding second example

In the second example, we have shown two things:

(a) $3 | 1^3 - 1$;
(b) If $3 | k^3 - k$ for positive integer $k$, then $3 | (k + 1)^3 - (k + 1)$.

Hence, we have the following statements being true:

(1) $3 | 1^3 - 1$; (This is (a))
(2) If $3 | 1^3 - 1$, then $3 | 2^3 - 2$; (This is (b) when $k = 1$)
(3) If $3 | 2^3 - 2$, then $3 | 3^3 - 3$; (This is (b) when $k = 2$)

\[ \ldots \]
(n) If $3 | (n - 1)^3 - (n - 1)$, then $3 | n^3 - n$; (This is (b) when $k = n - 1$)

Putting all of them together, we see that $3 | n^3 - n$. 
In the mathematical induction we just studied, the constraint is that \( n \) is a positive integer. In fact, we can have variants:

- \( n \) is a non-negative integer;
- or, \( n \) is a positive integer \( \geq m \).

To deal with the above situations, all we need is:

- adjust the basis step, so that it considers \( n = 0 \) or \( n = m \) instead of \( n = 1 \).
- adjust the inductive step, so that \( P(k) \rightarrow P(k + 1) \) is proved for all non-negative integer \( k \) or all integer \( k \geq m \).
Example for variant

Example:

Suppose that, for a finite set $S$, $|S| = n$. Show that $|P(S)| = 2^n$.

- Note that we cannot consider $n = 1$ in the basis step! Because $S$ could be the empty set and thus $n$ could be 0.
- That means, we have to make sure the above statement is true for all non-negative integer $n$ (not just all positive integer $n$).
- If we consider $n = 1$ in the basis step, then the entire proof ignores the possibility of $n = 0$.
- Similarly, when we do the inductive step, we cannot just prove it for all positive integer $k$. We should prove it for all non-negative integer $k$. 
Example for variant

**Proof: Basis step:** When $n = 0$, $S$ is the empty set. Hence, $P(S) = \{\emptyset\}$, which means $|P(S)| = 1 = 2^0$.

**Inductive step:** Assume that, for all $S$ such that $|S| = k$ (where $k$ is a non-negative integer), $|P(S)| = 2^k$.

Now we show that, for all $S'$ such that $|S'| = k + 1$, $|P(S')| = 2^{k+1}$.

Clearly, all $S'$ such that $|S'| = k + 1$ can be written as $S' = S \cup \{a\}$, where $|S| = k$ and $a$ is not in $S$.

To count $|P(S')|$, i.e., the number of subsets of $S'$, we only need to count:

(a) $|P(S)|$, i.e., the number of subsets of $S$;
By the inductive assumption, we know that $|P(S)| = 2^k$.

(b) The number of subsets of $S'$ that contains $a$.
We note that each subset containing $a$ uniquely corresponds to a subset not containing $a$ (by eliminating $a$ from the subset).
Hence, this number is also $|P(S)| = 2^k$.

We sum up these two numbers and get that $|P(S')| = 2^k + 2^k = 2^{k+1}$. 

We have another important variant called \textit{strong induction}:

- Goal: to prove \( P(n) \) is true (where \( n \) is a positive integer).
- Basis step: show \( P(1) \) is true.
- Inductive step: show \( P(1) \land P(2) \land \cdots \land P(k) \rightarrow P(k+1) \) is true for every positive integer \( k \).

Clearly, the above method makes sense because from \( P(1), P(1) \rightarrow P(2), P(1) \land P(2) \rightarrow P(3), \ldots, P(1) \land P(2) \land \cdots \land P(n-1) \rightarrow P(n) \) we can easily get \( P(n) \).

**Example:**

Show that any positive integer \( n > 1 \) can be written as the product of primes.

Note this is actually part of the \textit{fundamental theorem of arithmetic}. Here we prove it using \textit{strong induction}.

**Proof: Basis step:** Here we consider \( n = 2 \) in stead of \( n = 1 \), because there is a restriction \( n > 1 \).

When \( n = 2 \), since 2 is by itself a prime, the proposition is clearly true.
Example for strong induction

**Inductive step:** Assume every $n$ such that $1 < n \leq k$ (where $k$ is an integer $> 1$) can be written as the product of primes.

Now we show that $k + 1$ can also be written as the product of primes. We consider two cases:

**Case A:** $k + 1$ is a prime. Then we are done.

**Case B:** $k + 1$ is a composite.

- Then there exist positive integers $a > 1$ and $b > 1$ such that $k + 1 = a \cdot b$.
- Since $a > 1$, we know $a \geq 2$, and thus $b \leq (k + 1)/2 < k$.
- By the inductive assumption, $b$ can be written as the product of primes.
- Similarly, $a$ can also be written as the product of primes.
- Combining these two results, we see that $k + 1 = a \cdot b$ can be written as the product of primes.
Understanding example for strong induction

In this example, we have shown two things:
(a) 2 can be written as the product of primes;
(b) If all $n$ such that $1 < n \leq k$ can be written as the product of primes, then $k + 1$ can be written as the product of primes.

Hence, we have the following statements being true:

(1) 2 can be written as the product of primes; (This is (a))

(2) If 2 can be written as the product of primes, then 3 can be written as the product of primes; (This is (b) when $k = 2$)

(3) If 2 and 3 can be written as the product of primes, then 4 can be written as the product of primes; (This is (b) when $k = 3$) . . .

$(n-1)$ If 2, 3, . . . , and $n − 1$ can be written as the product of primes, then $n$ can be written as the product of primes; (This is (b) when $k = n − 1$)

Putting all of them together, we see that $n$ can be written as the product of primes.