PROOF TECHNIQUES

We look at

- Proof by contradiction
- Proof by construction
- Proof by induction
-
- But we may use some other also..
- For eg., Proof by counter example to disprove a statement…

By Contradiction

- One common way to prove a theorem is to assume that the theorem is false, and then show that this assumption leads to an obviously false consequence (also called a contradiction)
- This type of reasoning is used frequently in everyday life, as shown in the following example

By Contradiction

- Jack sees Jill, who just comes in from outdoor
- Jill looks completely dry
- Jack knows that it is not raining
- Jack's proof:
  - If it *were* raining (the assumption that the statement is false), Jill will be wet.
  - The consequence is: "Jill is wet" AND "Jill is dry", which is obviously false
  - Therefore, it must not be raining

By Contradiction [Example 1]

- Let us define a number is rational if it can be expressed as p/q where p and q are integers; if it cannot, then the number is called irrational
- E.g.,
  - 0.5 is rational because 0.5 = 1/ 2
  - 2.375 is rational because 2.375 = 2375 / 1000

By Contradiction

- Theorem: $\sqrt{2}$ (the square-root of 2) is irrational.
- How to prove?
- First thing is …

  Assume that $\sqrt{2}$ is rational

By Contradiction

- Proof: Assume that $\sqrt{2}$ is rational. Then, it can be written as p/q for some positive integers p and q.
- In fact, we can further restrict that p and q does not have common factor.
  - If D is a common factor of p and q, we use $p' = p/D$ and $q' = q/D$ so that $p'/q' = p/q = \sqrt{2}$ and there is no common factor between p' and q'
- Then, we have $p^2/q^2 = 2$, or $2q^2 = p^2$.

By Contradiction

- Since $2q^2$ is an even number, p^2 is also an even number
  - This implies that p is an even number (why?)
- So, $p = 2r$ for some integer r
- $2q^2 = p^2 = (2r)^2 = 4r^2$
  - This implies $2r^2 = q^2$
- So, q is an even number
- Something wrong happens... (what is it?)

By Contradiction

- We now have: “p and q does not have common factor” AND “p and q have common factor”
  - This is a contradiction
- Thus, the assumption is wrong, so that $\sqrt{2}$ is irrational

By Contradiction [Example 2]

- Theorem (Pigeonhole principle): *A total of n+1 balls are put into n boxes. At least one box containing 2 or more balls.*
- Proof: *Assume "at least one box containing 2 or more balls" is false*
  - That is, each has at most 1 or fewer ball

Consequence: total number of balls $\leq$ n

Thus, there is a contradiction (what is that?)

Proof By Construction

- Many theorem states that a particular type of object exists
- One way to prove is to find a way to construct one such object
- This technique is called proof by construction

- Theorem: There exists a rational number p which can be expressed as q^r, with q and r both irrational.
- How to prove?
  - Find p, q, r satisfying the above condition
- What is the irrational number we just learnt? Can we make use of it?

By Construction

- What is the following value?
  $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$
- If $\sqrt{2}^{\sqrt{2}}$ is rational, then $q = r = \sqrt{2}$ gives the desired answer
- Otherwise, $q = \sqrt{2}^{\sqrt{2}}$ and $r = \sqrt{2}$ gives the desired answer

By Induction

- Normally used to show that all elements in an infinite set have a specified property
- The proof consists of proving two things: The basis, and the inductive step

- Mathematical induction proves that we can climb as high as we like on a ladder, by proving that we can climb onto the bottom rung (the **basis**) and that from each rung we can climb up to the next one (the **inductive step**).

We consider only enumerable or countable sets with a least element [well ordered sets]

1. The **base case**: prove that the statement holds for the first natural number *n*. Usually, *n* = 0 or *n* = 1;
   - rarely, but sometimes conveniently, the base value of *n* may be taken as a larger number, or even as a negative number (the statement only holds at and above that threshold).
2. The **step case** or **inductive step**: assume the statement holds for some natural number *n*, and prove that then the statement holds for *n* + 1.

By Induction [Example 1]

- Let F(k) be a sequence defined as follows:
- $F(1) = 1$
- $F(2) = 1$
- for all $k \geq 3$, $F(k) = F(k-1) + F(k-2)$
- Theorem: For all $n \geq 1$,

  $$F(1)+F(2) + \ldots + F(n) = F(n+2) - 1$$

By Induction

- Let $P(k)$ means "the theorem is true when $n = k$"
- Basis: To show $P(1)$ is true.
  - $F(1) = 1$, $F(3) = F(1) + F(2) = 2$
  - Thus, $F(1) = F(3) - 1$
  - Thus, $P(1)$ is true
- Inductive Step: To show for $k \geq 1$, $P(k) \rightarrow P(k+1)$
  - $P(k)$ is true means: $F(1) + F(2) + \ldots + F(k) = F(k+2) - 1$
  - Then, we have

$$\begin{aligned} & F(1) + F(2) + \ldots + F(k+1) \\ &= (F(k+2) - 1) + F(k+1) \\ &= F(k+3) - 1 \end{aligned}$$

  - Thus, $P(k+1)$ is true if $P(k)$ is true

Variants

- There can be many other types of basis and inductive step, as long as by proving both of them, they can cover all the cases
- For example, to show P is true for all k > 1, we can show
  - Basis: P(1) is true, P(2) is true
  - Inductive step: $P(k) \rightarrow P(k+2)$

Variants

- **Complete (strong) induction:** (in contrast to which the basic form of induction is sometimes known as **weak induction**)
  makes the inductive step easier to prove by using a stronger hypothesis: one proves the statement $P(m + 1)$ under the assumption that $P(n)$ holds for all $n,\ n \leq m$.

Example: forming dollar amounts by coins

- Assume an infinite supply of 4 and 5 dollar coins.
- Prove that any whole amount of dollars greater than 12 can be formed by a combination of such coins.
- In more precise terms, we wish to show that for any amount $n \geq 12$ there exist natural numbers a and b such that $n = 4a + 5b$, where 0 is included as a natural number.
- The statement to be shown true is thus:

$$S(n):\ n \geq 12 \Rightarrow \exists\, a, b \in \mathbb{N}.\ n = 4a + 5b$$

Base case: Show that $S(k)$ holds for $k = 12, 13, 14, 15$.

$$4 \cdot 3 + 5 \cdot 0 = 12$$
$$4 \cdot 2 + 5 \cdot 1 = 13$$
$$4 \cdot 1 + 5 \cdot 2 = 14$$
$$4 \cdot 0 + 5 \cdot 3 = 15$$

The base case holds.

Induction step:
For $j = 12, 13, \dots, 15, \dots, k$ we assume that the theorem is true.

For $j = k + 1$, we show that the theorem is true.

Since for $j = k, k-1, k-2, k-3$ the theorem is true (why?).
So, $k - 3 = 4a + 5b$, for some nonnegative integers a and b.
Since $k + 1 = (k - 3) + 4$,
we have, $k + 1 = 4a + 5b + 4 = 4(a + 1) + 5b$. Q.E.D.

- The following is not a valid proof by induction!

By Induction?

- CLAIM: In any set of h horses, all horses are of the same color.
- PROOF: By induction. Let P(k) means "the claim is true when h = k"
- Basis: P(1) is true, because in any set of 1 horse, all horses clearly are the same color.

By Induction?

- Inductive step:
  - Assume P(k) is true.
  - Then we take any set of k+1 horses.
  - Remove one of them. Then, the remaining horses are of the same color (because P(k) is true).
  - Put back the removed horse into the set, and remove another horse
  - In this new set, all horses are of same color (because P(k) is true).
  - Therefore, all horses are of the same color!
- What's wrong?

Homework

More on Pigeonhole Principle

- Theorem: For any graph with more than two vertices, there exists two vertices whose degree are the same.
- How to prove?