CS5371
Theory of Computation

Lecture 2: Mathematics Review II
(Proof Techniques)

Some Updates

- Our consultation hours are as follows:

  Kai (資電館741): Tue 1500—1600

  Fri 1400—1500

  Yu-Han (紅樓315): Wed 1500—1700

- There is a link from my homepage to access the course homepage:

  www.cs.nthu.edu.tw/~wkhon

Objectives

- This time, we will look at some examples to demonstrate the following common proof techniques
  - By contradiction
  - By construction
  - By induction
- These techniques often occur in proving theorems in the theory of computation

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

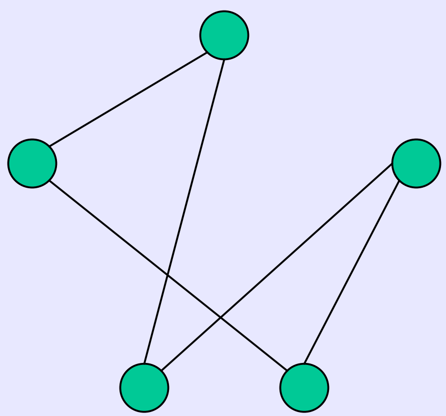
  Thus, there is a contradiction (what is that?)

Proof By Construction

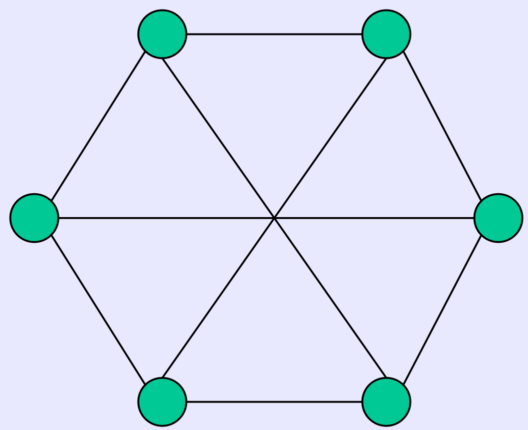
- Many theorem states that a particular type of object exists
- One way to prove is to find a way to construct one such object
- This technique is called proof by construction

By Construction [Example 1]

- Let us define a graph to be k-regular if every vertex of the graph has degree k
- E.g.,



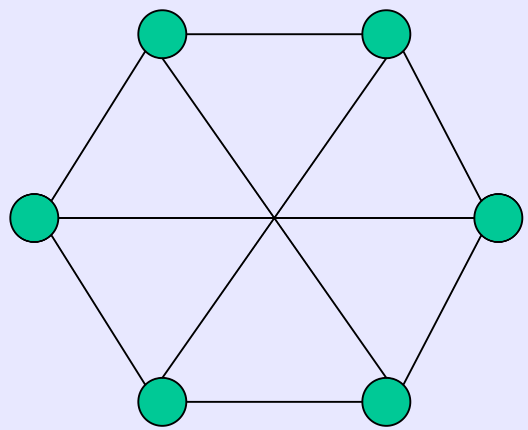
2-regular



3-regular

By Construction

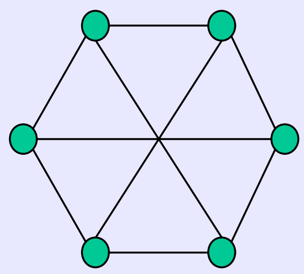
- Theorem: For each even number $n \geq 4$, there exists a 3-regular graph with n vertices.
- How to prove it?



By Construction

- Proof Idea: Arrange the points evenly in a circle, for each vertex, form two edges one with its left neighbor and one with its right neighbor. Also, form an edge with the vertex opposite to it in the circle
- Formal Proof: Label the vertices by 1,2,…, n. The edge set E is the union of
  - $E1 = \{ \{x,x+1\} \mid \text{for } x = 1,2,\dots,n-1 \}$
  - $E2 = \{ \{1,n\} \}$
  - $E3 = \{ \{x, x+(n/2)\} \mid \text{for } x = 1,2,\dots,n/2 \}$

  Then, it is easy to check that the degree of each vertex is exactly 3.



By Construction [Example 2]

- 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

By Induction

- To illustrate how induction works, let us consider the infinite set of natural numbers, {1,2,3,...} and we want to show some property P holds for each element in the set
- One way to do so is:
  - Show P holds for 1 [shorthand: P(1) is true]
  - Show for each $k \geq 1$, if P(k) is true, then P(k+1) is true [shorthand: P(k) → P(k+1) is true]

By Induction

- Then, we can conclude that $P(k)$ is true for all $k \geq 1$ (why?)
  - $P(1)$ is true
  - Because $P(1)$ is true and $P(k) \rightarrow P(k+1)$, then $P(2)$ is true
  - Because $P(2)$ is true and $P(k) \rightarrow P(k+1)$, then $P(3)$ is true
  - …

By Induction

- 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: $P(k) \rightarrow P(k+2)$
- Another example
  - Basis: $P(1)$ is true, $P(2)$ is true, …, $P(2^i)$ is true for all i
  - Inductive step: $P(k) \rightarrow P(k-1)$

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 $n \geq 1$,

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

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

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?

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?

More on Pigeonhole Principle

- Theorem: There exists a number consisted by all 1's (such as 1, 11, 111, …) which is divisible by 1997.
- How to prove?

Next

- Part I: Automata Theory