CSC006P1M: Design and Analysis of Algorithms
Lecture 02 *(Mathematical Induction)*

Sumit Kumar Pandey

August 10, 2022

Mathematical Induction

The Principle of Mathematical Induction

Let $P(n)$ be a statement which, for each integer n, may be either true or false. To prove $P(n)$ is true for all integers $n \geq 1$, it suffices to prove:

1. $P(1)$ is true.
2. For all $k \geq 1$, $P(k)$ implies $P(k+1)$.

In general,

The Principle of Mathematical Induction

Let $P(n)$ be a statement which, for each integer $n \geq n_0$, may be either true or false. To prove $P(n)$ is true for all integers $n \geq n_0$, it suffices to prove:

1. $P(n_0)$ is true.
2. For all $k \geq n_0$, $P(k)$ implies $P(k+1)$.

Steps in Mathematical Induction

There are three steps to a proof using the principle of mathematical induction

1. (Basis of Induction) Show $P(n_0)$ is true.
2. (Inductive hypothesis) Assume $P(k)$ is true for $k \geq n_0$.
3. (Inductive step) Show that $P(k+1)$ is true on the basis of inductive hypothesis.

The Principle of Mathematical Induction (Strong)

Let $P(n)$ be a statement which, for each integer $n \geq 1$, may be either true or false. To prove $P(n)$ is true for all integers $n \geq 1$, it suffices to prove:

1. $P(1)$ is true.
2. For all $k \geq 1$, if $P(1), P(2), \cdots, P(k)$ implies $P(k+1)$.

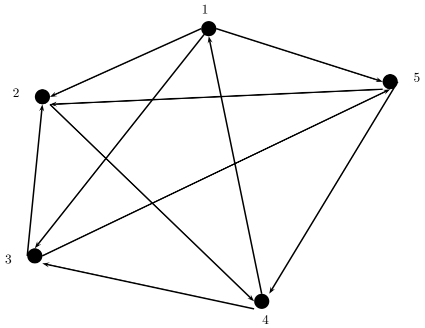
The Principle of Mathematical Induction (Another Version)

Let $P(n)$ be a statement which, for each integer $n \geq 1$, may be either true or false. To prove $P(n)$ is true for all integers $n \geq 1$, it suffices to prove:

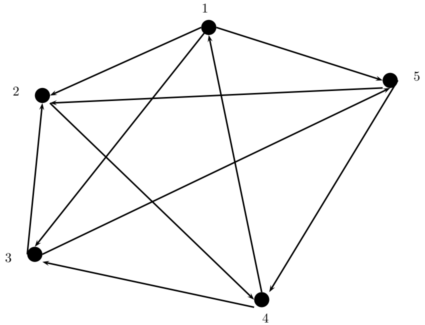
1. $P(n)$ is true for an infinite subset of the natural numbers.
2. If $P(n)$ implies $P(n-1)$.

Example

Every road in Jammu is one-way. Every pair of cities is connected by exactly one direct road. Show that there exists a city which can be reached from every other city either directly or via at most one other city.



Example contd...



There are three cities in the example which satisfy our requirement - City number 2, 3 and 4. City number 1 and 5 cannot be reached from 3 and 2 respectively.

Example contd...

But, how to prove for general n?

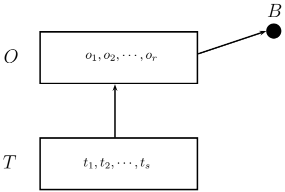
Use Mathematical Induction.

Proof of the Example

Proof:

1. $n = 1$ does not make sense. For $n = 2$, it's obvious.
2. Assume that for $n = k \geq 2$ cities, there exists a city which satisfies the requirement.
3. For $n = k + 1$.
   - Choose any city, say A. Ignore the city A from the graph as well as all roads connected to that city.
   - Now, there will be k cities. By our induction hypothesis, there exists a city, say B, which satisfies the requirement.
   - Consider the rest $k - 1$ cities. We can divide the rest $k - 1$ cities into two sets, say O and T.
   - The set O contains those cities which are directly connected to the city B.
   - The set T contains those cities which are connected to the city B via at most one other city.

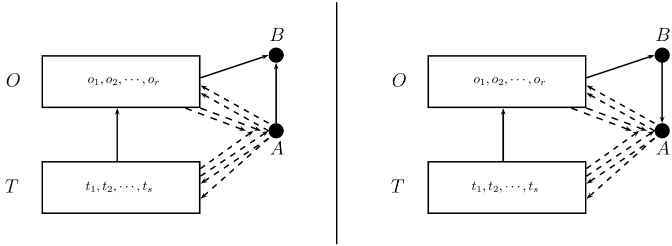
Proof contd...



- Note that B can be reached from any city belonging to the set T via some city in O only.

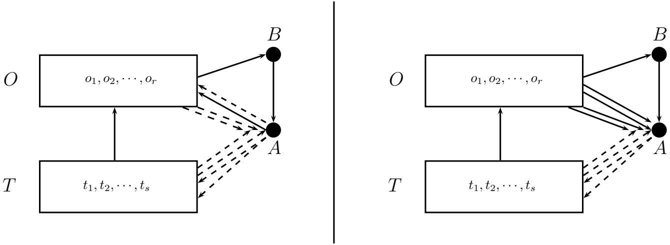
Proof contd...

- Now, consider the city A as well as all connected roads to the other city.
- There can be two choices -
  - First: When there is a direct road from city A to city B. In this case, our desired city will be B.
  - Second: there is a direct road from city B to city A.



Proof contd...

- Now, there are two choices for the second condition also:
  - Case number 1 : When there exists a city in the set O which can be reached from A directly. Then, our desired city is B.
  - Case number 2 : When there does not exist any city in the set O which can be directly reached from A directly. Which means A can be reached from all cities in O directly. In this case, our desired city is A.



Gray Code

Gray Code

- We are given a set of n objects and we want to name them. Each name is represented by a unique string of bits.
- We would like to arrange the names in a circular list such that each name can be obtained from the previous names by changing exactly one bit.
- Such a scheme is called **Gray code**.

Gray Code of Length 2

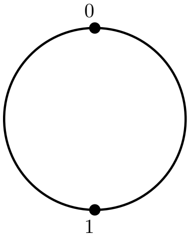


Figure: Gray Code of Length 2

Gray Code of Length 2

1. $0 \rightarrow 0$
2. $1 \rightarrow 1$

Gray Code of Length 4

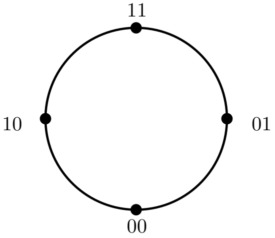


Figure: Gray Code of Length 4

Gray Code of Length 4

1. $0 \rightarrow 00$
2. $1 \rightarrow 01$
3. $2 \rightarrow 11$
4. $3 \rightarrow 10$

Gray Code of Length 3

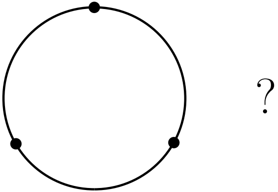


Figure: Gray Code of Length 3

Gray Code of Length 5

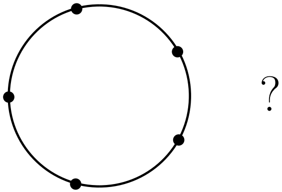


Figure: Gray Code of Length 5

Gray Code of Length 6

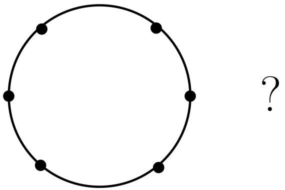


Figure: Gray Code of Length 6

Gray Code of Length 4

- We show how to construct Gray code of length 4 using Gray code of length 2.
- Let the Gray code of length 2 be:
  0 and 1
- Take first string of Gray code of length 2:
  0.
- Now, 0 and 1 are prefixed to the first string:
  00 and 10.
- Take second string of Gray code of length 2:
  1.
- Now, 1 and 0 are prefixed to the second string:
  11 and 01.
- Now, collect all strings in order. We get

$$00, 10, 11, 01$$

Gray Code of Length 6

- We show how to construct Gray code of length 6 using Gray code of length 4.
- Take Gray code of length 4:
  00, 01, 11, 10.
- Take first string of Gray code of length 4: 00.
- Now, 0 and 1 are prefixed to the first string:
  000 and 100.
- Take second string of Gray code of length 4: 01.
- Now, 1 and 0 are prefixed to the second string:
  101 and 001.
- Take rest of the strings of Gray code and prefix them by 0:
  011, 010
- Now, collect all strings in order. We get

$$000, 100, 101, 001, 011, 010$$

Gray Code of Length 8

- We show how to construct Gray code of length 8 using Gray code of length 6.
- Take Gray code of length 6:
  000, 100, 101, 001, 011, 010
- Take first string of Gray code of length 4: 000.
- Now, 0 and 1 are prefixed to the first string:
  0000 and 1000.
- Take second string of Gray code of length 4: 100.
- Now, 1 and 0 are prefixed to the second string:
  1100 and 0100.
- Take rest of the strings of Gray code and prefix them by 0:
  0101, 0001, 0011, 0010
- Now, collect all strings in order. We get

$$0000, 1000, 1100, 0100, 0101, 0001, 0011, 0010$$

Gray Code of Length $2n$

Can we say that, for all $n \geq 2$, a Gray code of length $2n$ can be constructed from a Gray code of length $2n - 2$?

Theorem

There exists a Gray code of length $2n$ for any $n \geq 1$.

Prove it by mathematical induction.

Gray Code of Length $2n$

Theorem

There exists a Gray code of length $2n$ for any $n \geq 1$.

Proof:

- For $n = 1$, the Gray code is: 0, 1.
- Assume that there exists a Gray code for $n = k - 1$, i.e. of length $2k - 2$. Let that Gray code be: $s_1, s_2, \cdots, s_{2k-2}$.
- Construct a code for $n = k$, i.e. of length $2k$ as follows: $0s_1$, $1s_1$, $1s_2$, $0s_2$, $0s_3$, $0s_4$, $\cdots$, $0s_{2k-2}$.
- Now, show that the above code satisfies the criteria for being a Gray code of length $2k$.

Gray Code of Length 8 *Revisited*

A Gray of length 8: $0000, 1000, 1100, 0100, 0101, 0001, 0011, 0010$
The code above requires 4 bits for length 8.
But, we need only 3 bits to map 8 different objects uniquely.

0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Exercise

Can we rearrange the strings above in such a manner so that it forms a Gray code of length 8? If no, why? Else, what's the code?

Thank You