IIT KGP
Dept. of Computer Science & Engineering

CS 30053
Foundations of Computing

Debdeep Mukhopadhyay

Inductive Reasoning

Foreword

- Power of computers come from their ability to repeat the same task
- Computer science uses essentially three problem solving tools:
  - **Data Models:** Abstractions used to describe problems. Like graphs, logic etc. Programming languages, like C, Lisp, Prolog supports various abstractions. E.g. in C we see, char, int, float and even structures, pointers.

Foreword

- **Data Structures:** Sometimes the data models of the language which we are using are unable to handle the data model we wish to represent. For that we study data structures. These are programming language constructs used to represent data models.
- **Algorithm:** Techniques used to obtain solutions by manipulating data as represented by data models, data structures.

The connection with repetition

- Many concepts in data models are repetitions.
  - Like lists: Either empty or is one element followed by another, then another and so on.
  - Iterative Definition
- Recursion: A closely related technique, in which a concept is defined, indirectly or directly by itself
  - Lists is either empty or is an element followed by a list.

First Principle

- A powerful, rigorous technique for proving that a predicate $P(n)$ is true for *every* natural number n, no matter how large.
- Essentially a "domino effect" principle.
- Based on a predicate-logic inference rule:
  $P(0)$
  $\forall n \geq 0\ (P(n) \rightarrow P(n+1))$
  $\therefore \forall n \geq 0\ P(n)$

Outline of an Inductive Proof

- Want to prove $\forall n\ P(n)$…
- *Base case* (or *basis step*): Prove $P(0)$.
- *Inductive step*: Prove $\forall n\ P(n) \rightarrow P(n+1)$.
  - *E.g.* use a direct proof:
  - Let $n \in \mathbf{N}$, assume $P(n)$. (*inductive hypothesis*)
  - Under this assumption, prove $P(n+1)$.
- First Principle of Induction then gives $\forall n\ P(n)$.

Generalizing Induction

- Can also be used to prove $\forall n \geq c\ P(n)$ for a given constant $c \in \mathbf{Z}$, where maybe $c \neq 0$.
  - In this circumstance, the base case is to prove $P(c)$ rather than $P(0)$, and the inductive step is to prove $\forall n \geq c\ (P(n) \rightarrow P(n+1))$.
- Induction can also be used to prove $\forall n \geq c\ P(a_n)$ for an arbitrary series $\{a_n\}$.
- Can reduce these to the form already shown.

Second Principle of Induction

- Characterized by another inference rule:
  $P(0)$

  P is true in *all* previous cases

  $\forall n \geq 0: \overbrace{(\forall 0 \leq k \leq n\ P(k))}^{} \rightarrow P(n+1)$

  $\therefore \forall n \geq 0: P(n)$
- Difference with 1st principle is that the inductive step uses the fact that $P(k)$ is true for *all* smaller $k<n+1$, not just for $k=n$.

Induction Example (1st princ.)

- Prove that the sum of the first n odd positive integers is n^2. That is, prove:

$$\forall n \geq 1: \underbrace{\sum_{i=1}^{n} (2i-1) = n^2}_{P(n)}$$

- Proof by induction.
  - Base case: Let $n=1$. The sum of the first 1 odd positive integer is 1 which equals 1^2. (Cont…)

Example cont.

- Inductive step: Prove $\forall n \geq 1$: $P(n) \rightarrow P(n+1)$.
  - Let $n \geq 1$, assume $P(n)$, and prove $P(n+1)$.

$$\sum_{i=1}^{n+1}(2i-1) = \left(\sum_{i=1}^{n}(2i-1)\right) + (2(n+1)-1)$$

$$= n^2 + 2n + 1 \qquad \textit{By inductive hypothesis P(n)}$$

$$= (n+1)^2$$

Another Induction Example

- Prove that $\forall n > 0$, $n < 2^n$. Let $P(n) = (n < 2^n)$
  - Base case: $P(1) = (1 < 2^1) = (1 < 2) = \mathbf{T}$.
  - Inductive step: For $n > 0$, prove $P(n) \rightarrow P(n+1)$.
    - Assuming $n < 2^n$, prove $n+1 < 2^{n+1}$.
    - Note $n + 1 < 2^n + 1$ (by inductive hypothesis)
      $< 2^n + 2^n$ (because $1 < 2 = 2 \cdot 2^0 \leq 2 \cdot 2^{n-1} = 2^n$)
      $= 2^{n+1}$
    - So $n + 1 < 2^{n+1}$, and we're done.

Example of Second Principle

- Show that every $n>1$ can be written as a product $p_1p_2\ldots p_s$ of some series of s prime numbers. Let $P(n)$="n has that property"
- Base case: $n=2$, let $s=1$, $p_1=2$.
- Inductive step: Let $n\geq 2$. Assume $\forall 2\leq k\leq n$: $P(k)$. Consider $n+1$. If prime, let $s=1$, $p_1=n+1$. Else $n+1=ab$, where $1<a\leq n$ and $1<b\leq n$. Then $a=p_1p_2\ldots p_t$ and $b=q_1q_2\ldots q_u$. Then $n+1=p_1p_2\ldots p_t\,q_1q_2\ldots q_u$, a product of $s=t+u$ primes.

Another 2nd Principle Example

- Prove that every amount of postage of Rs 12 or more can be formed using just Rs 4 and Rs 5 stamps.
- Base case: $12=3(4)$, $13=2(4)+1(5)$, $14=1(4)+2(5)$, $15=3(5)$, so $\forall 12\leq n\leq 15$, $P(n)$.
- Inductive step: Let $n\geq 15$, assume $\forall 12\leq k\leq n$ $P(k)$. Note $12\leq n-3\leq n$, so $P(n-3)$, so add a Rs 4 stamp to get postage for $n+1$.

Can you solve the problem without strong induction?

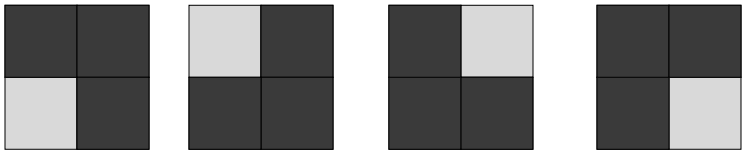
- Intuition:
  - If there are Rs 4 stamps to make stamp worth Rs n, replace one of them by a Rs 5 stamp. You will get stamps worth Rs (n+1)
  - If there are no Rs 4 stamps. Then, all are Rs 5 stamps. As, n ≥ 15, so there must be atleast 3 Rs 5 stamps. So, change any 3 of the Rs 5 stamps to 4 Rs 4 stamps. You again get stamps worth Rs (n+1)

Can you prove without induction?

- A possible proof outline:
  - Any number, n can be expressed as:
    - n=5x or 5x+1 or 5x+2 or 5x+3 or 5x+4
    - If n=5x or 5x+4, nothing is to be done
    - If n=5x+1 <=> n=5(x-1)+6
      <==>n=5(x-2)+4.4. Thus this also satisfies the claim. Except that we have the condition, x≥2 => n ≥16.
    - Likewise, we can complete the remaining cases.

An Interesting Problem

- Let, n be a positive integer. Show that any $2^n x 2^n$ chessboard with one square removed can be tiled using L-shaped pieces, where these pieces cover 3 squares at a time.



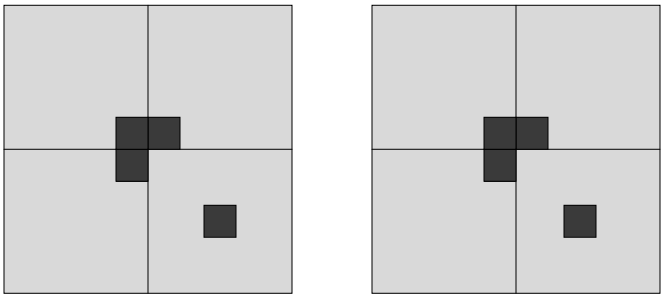
Tiling a 2x2 Chessboard with one square removed

Proof Outline

- Let P(n) be the proposition that any $2^n x 2^n$ chess-board can be tiled, with the L-shaped pieces.
- **Base Step:** From the previous diagram, we know P(1) is true
- **Inductive Step:** Assuming that P(k) is true, we show that P(k+1) is true.

Proof (contd)

- Can you follow the proof? Complete the proof.



The Well Ordering (WO) Property

- Every nonempty set of nonnegative integers has a least element.
- *Prove the division algorithm: if a is an integer and d is a positive integer, then there are unique integers q and r with*

  $0 \leq r < d$ *and* $a=dq+r$

Proof Outline: Form a set S of non-negative integers of the form, a-dq, where q is an integer. Then S is non-empty and so has a least element, $r=a-dq_0$ *(from the well-ordering property)*

- Integer r is non-negative and r<d. Otherwise we can have a smaller element in S
  - e.g. if $r=d+r_0$, then $d+r_0=a-dq_0$
  - then, $r_0=a-(d+1)q_0$ so, $r_0<r$
- Hence, there are integers q and r, with $0 \leq r < d$. Actually, q and r are unique. Can you prove that? Hint: r<d

Infinite Descent

- Used to show that for a propositional function P(n), P(k) is false for all +ve integers k.
- Proof method: Assuming that P(k) is true for at least one integer, k, then from the W.O. principle, there is a smallest integer s, for which P(s)
- The method finds an s'<s, for which P holds. Thus leading to a contradiction.

Example

- Prove $\sqrt{2}$ is irrational.
  - Let $2^{1/2}$=m/n and such solution exists, m,n>0
  - Let, S be the set of the (+ve) denominators of the fractions. So there is an element, N which is the least element of the set. (So, N is the smallest denominator of ratios of two +ve numbers which equal to $2^{1/2}$).
  - Show that, $2^{1/2}$=(2N -M)/(M-N)
  - 1<M/N=$2^{1/2}$<2 => N<M<2N => 0<M-N<N.
  - So, M-N is +ve and also < N. Thus, we have a contradiction.

Why is mathematical Induction valid?

- We know, P(1) is T, P(k)→P(k+1) is T for all +ve integers k.
- Suppose, P(n) does not hold, for some +ve n. So, the set S, which contains the +ve integers which make the proposition invalid is non-empty. Hence, from the W.O principle, there is a least element in the set, say m. So, P(m) is F, but P(m-1) is T.
- But, then using Modus Ponens, P(m) is T!!
- Contradiction, that P(m) is F. So, S must be empty. QED.

A final example

- In a round robin tournament, every player plays every other player exactly once. Each match has a winner or loser. We say that $P_1, P_2,\ldots,P_k$ forms a cycle of length k, if P_1 beats P_2, P_2 beats $P_3,\ldots,P_k$ beats P_1. Prove, that if $k\geq 3$, there must be a cycle of three players.

Proof Outline

- The statement of the proof says, if there is a cycle then…So, we assume we have a cycle and go ahead…
- So, the set S of the +ve integers, for which there is a cycle is not empty. From the W.O principle there has to be a minimum element in the set. Let, it be k.
- So, $P_1, P_2, P_3,\ldots, P_k$ forms a cycle. So, consider P_1, P_2, P_3. If they form a cycle nothing is to be proved. Thus, P_1 must beat P_3. Thus, we can remove P_2 from the cycle of length k and get a cycle of length k-1. Thus, contradicting that k was least.