Mathematical Induction

Yih-Kuen Tsay

Department of Information Management
National Taiwan University

The Standard Induction Principle

- Let T be a theorem that we want to prove and suppose that T includes a parameter n whose value can be any natural number.
- Here, natural numbers are positive integers, i.e., 1, 2, 3, ..., excluding 0.
- To prove T, it suffices to prove the following two conditions:
  - T holds for $n = 1$. (Base case)
  - For every $n > 1$, if T holds for $n - 1$, then T holds for n. (Inductive step)
- The assumption in the inductive step that T holds for $n - 1$ is called the *induction hypothesis*.

A Starter

IM NTU

Theorem (2.1)

For all natural numbers x and n, $x^n - 1$ is divisible by $x - 1$.

Proof.

(Note: try to follow the structure of this proof when you do a proof by induction.)

The proof is by induction on n.

Base case: $x - 1$ is trivially divisible by $x - 1$.

Inductive step: $x^n - 1 = x(x^{n-1} - 1) + (x - 1)$. $x^{n-1} - 1$ is divisible by $x - 1$ *from the induction hypothesis* and $x - 1$ is divisible by $x - 1$. Hence, $x^n - 1$ is divisible by $x - 1$. $\square$

Note: a is divisible by b if there exists an integer c such that $a = b \times c$.

Variants of Induction Principle

Theorem

If a statement P, with a parameter n, is true for $n = 1$, and if, for every $n \geq 1$, the truth of P for n implies its truth for $n + 1$, then P is true for all natural numbers.

Theorem (Strong Induction)

If a statement P, with a parameter n, is true for $n = 1$, and if, for every $n > 1$, the truth of P for all natural numbers $< n$ implies its truth for n, then P is true for all natural numbers.

Theorem

If a statement P, with a parameter n, is true for $n = 1$ and for $n = 2$, and if, for every $n > 2$, the truth of P for $n - 2$ implies its truth for n, then P is true for all natural numbers.

Design by Induction: First Glimpse

Problem

Given two sorted arrays $A[1..m]$ and $B[1..n]$ of positive integers, find their smallest common element; returns 0 if no common element is found.

- Assume the elements of each array are in ascending order.
- **Obvious solution**: take one element at a time from A and find out if it is also in B (or the other way around).
- How efficient is this solution?
- Can we do better?

Design by Induction: First Glimpse (cont.)

- There are $m + n$ elements to begin with.
- Can we pick out one element such that either (1) it is the element we look for or (2) it can be ruled out from subsequent searches?
- In the second case, we are left with the same problem but with $m + n - 1$ elements?
- **Idea**: compare the current first elements of A and B.
  1. If they are equal, then we are done.
  2. The smaller one cannot be the smallest common element.

Design by Induction: First Glimpse (cont.)

Below is the complete solution:

Algorithm

function SCE(A, m, B, n) : *integer*;
begin
  if $m = 0$ *or* $n = 0$ **then** $SCE := 0$;
  if $A[1] = B[1]$ **then**
    $SCE := A[1]$;
  else if $A[1] < B[1]$ **then**
      $SCE := SCE(A[2..m], m-1, B, n)$;
  else $SCE := SCE(A, m, B[2..n], n-1)$;
end

Proving vs. Computing

Theorem (2.2)

$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

- This can be easily proven by induction.
- Key steps: $1 + 2 + \cdots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n^2+n+2n+2}{2} = \frac{n^2+3n+2}{2} = \frac{(n+1)(n+2)}{2}$.
- Induction seems to be useful only if we already know the sum.
- What if we are asked to compute the sum of a series?
- Let's try $8 + 13 + 18 + 23 + \cdots + (3 + 5n)$.

Proving vs. Computing (cont.)

- **Idea**: guess and then verify by an inductive proof!
- The sum should be of the form $an^2 + bn + c$.
- By checking $n = 1$, 2, and 3, we get $\frac{5}{2}n^2 + \frac{11}{2}n$.
- Verify this for all n, i.e., the following theorem, by induction.

Theorem (2.3)

$8 + 13 + 18 + 23 + \cdots + (3 + 5n) = \frac{5}{2}n^2 + \frac{11}{2}n.$

Another Simple Example

Theorem (2.4)

If n is a natural number and $1 + x > 0$, then $(1+x)^n \geq 1 + nx$.

- Below are the key steps:

$$\begin{array}{rl} (1+x)^{n+1} & = (1+x)(1+x)^n \\ & \quad \{\text{induction hypothesis and } 1+x>0\} \\ & \geq (1+x)(1+nx) \\ & = 1+(n+1)x+nx^2 \\ & \geq 1+(n+1)x \end{array}$$

- The main point here is that we should be clear about how conditions listed in the theorem are used.

Counting Regions

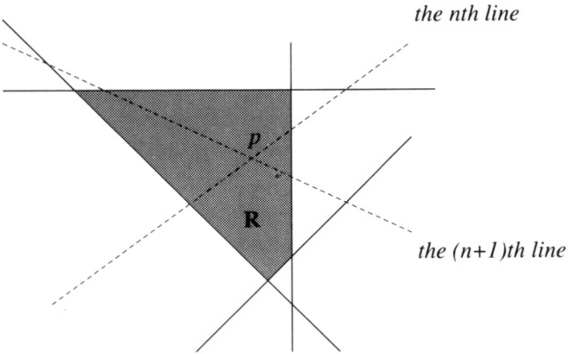

Figure 2.1 $n+1$ lines in general position.

Source: Manber 1989

Counting Regions (cont.)

Theorem (2.5)

The number of regions in the plane formed by n lines in general position is $\frac{n(n+1)}{2} + 1$.

A set of lines are in **general position** if (1) no two lines are parallel and (2) no three lines intersect at a common point.

- We observe that $\frac{n(n+1)}{2} = 1 + 2 + \cdots + n$.
- So, it suffices to prove the following:

Lemma

Adding one more line (the n-th line) to $n-1$ *lines in general position in the plane increases the number of regions by n.*

A Summation Problem

$$\begin{array}{rcl} 1 & = & 1 \\ 3+5 & = & 8 \\ 7+9+11 & = & 27 \\ 13+15+17+19 & = & 64 \\ 21+23+25+27+29 & = & 125 \end{array}$$

Theorem

The sum of row n in the triangle is n^3.

Examine the difference between rows $i+1$ and i ...

Lemma

The last number in row $n+1$ is n^2+3n+1.

A Simple Inequality

Theorem (2.7)

$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^n}<1$, *for all* $n \geq 1$.

- There are at least two ways to select n terms from $n+1$ terms.
  1. $(\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^n})+\frac{1}{2^{n+1}}$.
  2. $\frac{1}{2}+(\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^n}+\frac{1}{2^{n+1}})$.
- The second one leads to a successful inductive proof:

$$\begin{array}{rl} & \frac{1}{2}+(\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^n}+\frac{1}{2^{n+1}}) \\ = & \frac{1}{2}+\frac{1}{2}(\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^{n-1}}+\frac{1}{2^n}) \\ < & \frac{1}{2}+\frac{1}{2} \\ = & 1 \end{array}$$

Euler's Formula

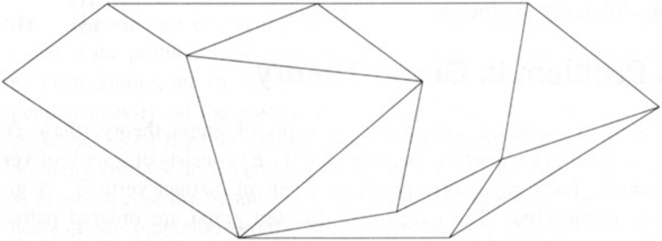

Figure 2.2 A planar map with 11 vertices, 19 edges, and 10 faces.

Source: Manber 1989

Euler's Formula (cont.)

IM NTU

Theorem (2.8)

The number of vertices (V), edges (E), and faces (F) in an arbitrary connected planar graph are related by the formula $V + F = E + 2$.

The proof is by induction on the number of faces.
Base case: graphs with only one face are trees ...

Lemma

A tree with n vertices has $n - 1$ edges.

Inductive step: for a graph with more than one faces, there must be a cycle in the graph. Remove one edge from the cyle ...

Gray Codes

A **Gray code** for n objects is an encoding scheme for naming the n objects such that the n names can be arranged in a *circular* list where *any two adjacent names differ by only one bit*.

Theorem (2.10)

There exist Gray codes of length $\frac{k}{2}$ for any positive even integer k.

Theorem (2.10+)

There exist Gray codes of length $\log_2 k$ for any positive integer k that is a power of 2.

Gray Codes (cont.)

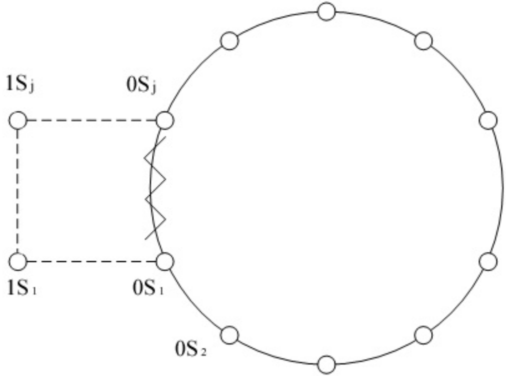

Figure 2.3 Constructing a Gray code of size *2k*

Source: Manber 1989 (adapted)

Note: j in the figure equals $2(k-1)$ and hence $j+2$ equals $2k$.

Gray Codes (cont.)

Theorem (2.11−)

There exist Gray codes of length $\lceil \log_2 k \rceil$ for any positive even integer k.

To generalize, we allow a Gray code to be *open*.

Theorem (2.11)

There exist Gray codes of length $\lceil \log_2 k \rceil$ for any positive integer $k \geq 2$. The Gray codes for the even values of k are closed, and the Gray codes for odd values of k are open.

Gray Codes (cont.)

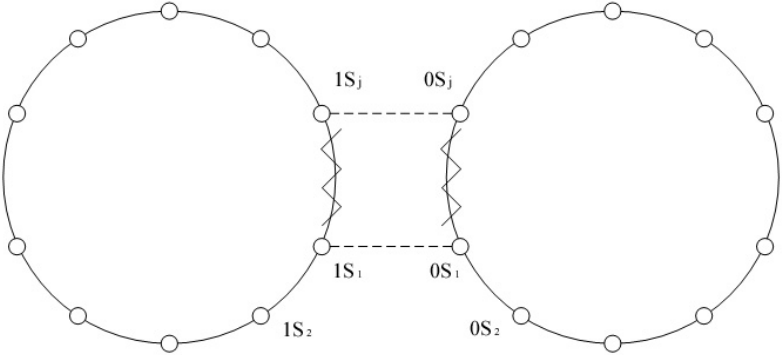

Figure 2.4 Constructing a Gray code from two smaller ones

Source: Manber 1989 (adapted)

Gray Codes (cont.)

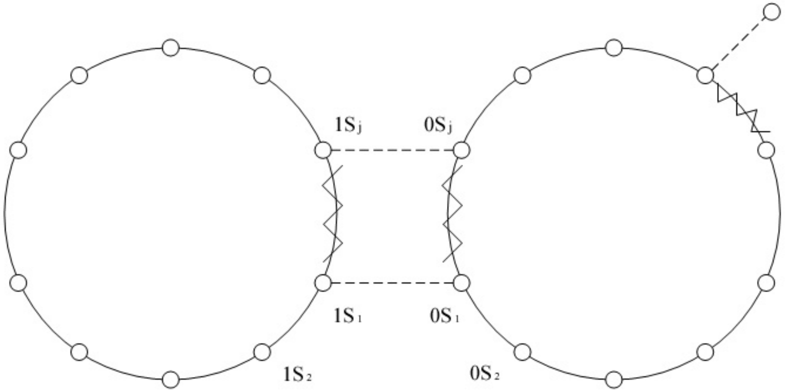

Figure 2.5 Constructing an open Gray code

Source: Manber 1989 (adapted)

Arithmetic vs. Geometric Mean

IM NTU

Theorem (2.13)

If $x_1, x_2, \ldots, x_n$ are all positive numbers, then
$$(x_1 x_2 \cdots x_n)^{\frac{1}{n}} \leq \frac{x_1 + x_2 + \cdots + x_n}{n}.$$

First use the standard induction to prove the case of powers of 2 and then use the reversed induction principle below to prove for all natural numbers.

Theorem (Reversed Induction Principle)

If a statement P, with a parameter n, is true for an infinite subset of the natural numbers, and if, for every $n > 1$, the truth of P for n implies its truth for $n - 1$, then P is true for all natural numbers.

Arithmetic vs. Geometric Mean (cont.)

- For all powers of 2, i.e., $n = 2^k$, $k \geq 1$: by induction on k.
- Base case: $(x_1x_2)^{\frac{1}{2}} \leq \frac{x_1+x_2}{2}$, squaring both sides ....
- Inductive step:

$$
\begin{array}{ll}
 & (x_1x_2\cdots x_{2^{k+1}})^{\frac{1}{2^{k+1}}} \\
= & [(x_1x_2\cdots x_{2^{k+1}})^{\frac{1}{2^k}}]^{\frac{1}{2}} \\
= & [(x_1x_2\cdots x_{2^k})^{\frac{1}{2^k}}(x_{2^k+1}x_{2^k+2}\cdots x_{2^{k+1}})^{\frac{1}{2^k}}]^{\frac{1}{2}} \\
\leq & \frac{(x_1x_2\cdots x_{2^k})^{\frac{1}{2^k}}+(x_{2^k+1}x_{2^k+2}\cdots x_{2^{k+1}})^{\frac{1}{2^k}}}{2}\text{, from the base case} \\
\leq & \frac{\frac{x_1+x_2+\cdots+x_{2^k}}{2^k}+\frac{x_{2^k+1}+x_{2^k+2}+\cdots+x_{2^{k+1}}}{2^k}}{2}\text{, from the Ind. Hypo.} \\
= & \frac{x_1+x_2+\cdots+x_{2^{k+1}}}{2^{k+1}}
\end{array}
$$

Arithmetic vs. Geometric Mean (cont.)

- For all natural numbers: by reversed induction on n.
- Base case: the theorem holds for all powers of 2.
- Inductive step: observe that

$$\frac{x_1 + x_2 + \cdots + x_{n-1}}{n-1} = \frac{x_1 + x_2 + \cdots + x_{n-1} + \frac{x_1+x_2+\cdots+x_{n-1}}{n-1}}{n}.$$

Arithmetic vs. Geometric Mean (cont.)

$$\begin{aligned}
\left(x_1 x_2 \cdots x_{n-1}\left(\tfrac{x_1+x_2+\cdots+x_{n-1}}{n-1}\right)\right)^{\frac{1}{n}} &\leq \frac{x_1+x_2+\cdots+x_{n-1}+\frac{x_1+x_2+\cdots+x_{n-1}}{n-1}}{n} \\
&\quad \text{(from the Ind. Hypo.)} \\
\left(x_1 x_2 \cdots x_{n-1}\left(\tfrac{x_1+x_2+\cdots+x_{n-1}}{n-1}\right)\right)^{\frac{1}{n}} &\leq \frac{x_1+x_2+\cdots+x_{n-1}}{n-1} \\
\left(x_1 x_2 \cdots x_{n-1}\left(\tfrac{x_1+x_2+\cdots+x_{n-1}}{n-1}\right)\right) &\leq \left(\tfrac{x_1+x_2+\cdots+x_{n-1}}{n-1}\right)^{n} \\
\left(x_1 x_2 \cdots x_{n-1}\right) &\leq \left(\tfrac{x_1+x_2+\cdots+x_{n-1}}{n-1}\right)^{n-1} \\
\left(x_1 x_2 \cdots x_{n-1}\right)^{\frac{1}{n-1}} &\leq \left(\tfrac{x_1+x_2+\cdots+x_{n-1}}{n-1}\right)
\end{aligned}$$

Loop Invariants

- An *invariant* at some point of a program is an assertion that holds whenever execution of the program reaches that point.
- Invariants are a bridge between the static text of a program and its dynamic computation.
- An invariant at the front of a while loop is called a *loop invariant* of the while loop.
- A loop invariant is formally established by induction.
  - Base case: the assertion holds right before the loop starts.
  - Inductive step: assuming the assertion holds before the i-th iteration ($i \geq 1$), it holds again after the iteration.

Number Conversion

Algorithm

Algorithm Convert_to_Binary (n);
begin
$\quad t := n;$
$\quad k := 0;$
$\quad$ **while** $t > 0$ **do**
$\qquad k := k + 1;$
$\qquad b[k] := t \bmod 2;$
$\qquad t := t \; div \; 2;$
end

Number Conversion (cont.)

Theorem (2.14)

When Algorithm Convert_to_Binary terminates, the binary representation of n is stored in the array b.

Lemma

If m is the integer represented by the binary array $b[1..k]$, then $n = t \cdot 2^k + m$ is a loop invariant of the while loop.