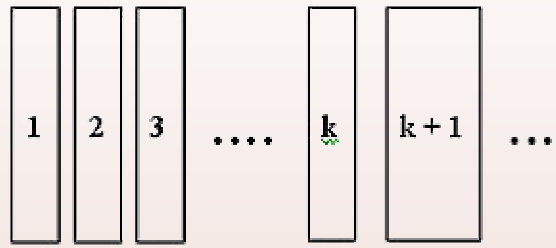
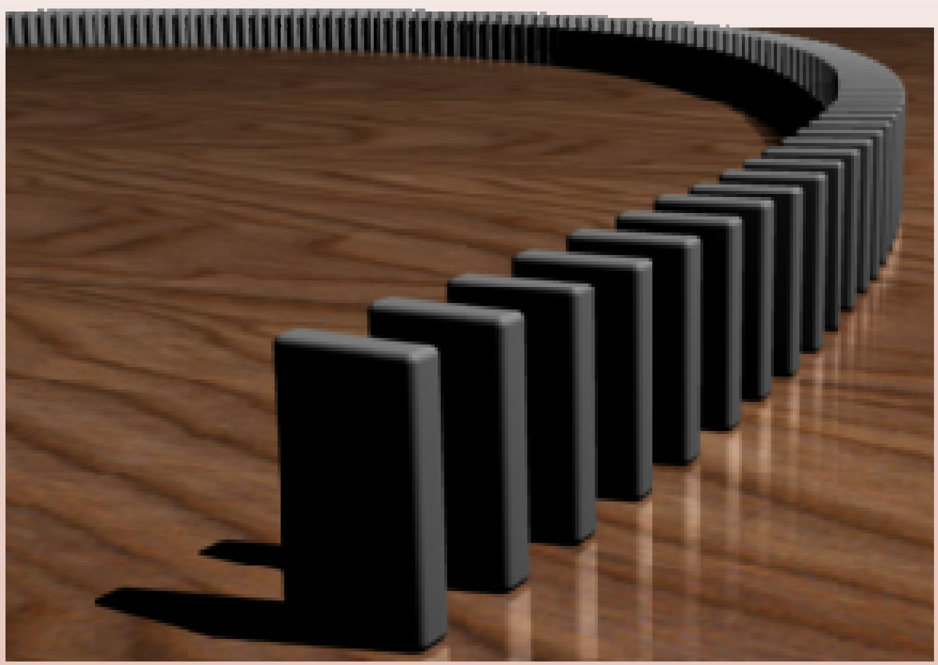
CMSC 250
Discrete Structures

Mathematical Induction

Mathematical Induction

- Used to verify a property of a sequence





Inductive Proof

- Let $P(n)$ be a property that is defined for integers n, and let a be a fixed integer.
- Suppose the following two statements are true.
  - $P(a)$ is true.
  - For all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.
- Then the statement for all integers $n \geq a$, $P(n)$ is true.

Inductive Proofs Must Have

- Base Case (value)
  - Prove base case is true
- Inductive Hypothesis (value)
  - State what will be assumed in this proof
- Inductive Step (value)
  - Show
    - State what will be proven in the next section
  - Proof
    - Prove what is stated in the show portion
    - Must use the Inductive Hypothesis sometime

Prove this statement: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Base Case (n=1): $\sum_{i=1}^{1} i = 1 \quad \frac{n(n+1)}{2} = \frac{1(1+1)}{2} = \frac{2}{2} = 1$

Inductive Hypothesis (n=p): $\sum_{i=1}^{p} i = \frac{p(p+1)}{2}$

Inductive Step (n=p+1):

Show: $\sum_{i=1}^{p+1} i = \frac{(p+1)((p+1)+1)}{2}$

Proof:(in class)

Variations

- 2+4+6+8+…+20 = ???
- If you can use the fact:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

- Rearrange it into a form that works.
- If you can't – you must prove it from scratch

Less Mathematical Example

- If all we had was 2 and 5 cent coins
  - We could make any value greater than 3

- Base Case (n = 4):
- Inductive Hypothesis (n=k):
- Inductive Step (n=k+1):
  - Show
  - Proof

More Examples

- $\forall n \in Z^{\geq 1}, 3 \mid (n^3 - n)$
- $\forall n \in Z^{\geq 0} \sum_{k=0}^{n} 2^k = 2^{n+1} - 1$
- Geometric Progression

$$\forall r \in R^{>1}, \forall a \in R, \forall n \in Z^{\geq 0}, \sum_{j=0}^{n} ar^j = \frac{ar^{n+1} - a}{r - 1}$$

Using Geometric Sequence

$$\sum_{j=0}^{n} ar^{j} = \frac{ar^{n+1} - a}{r - 1}$$

- Find $1 + 3 + 3^2 + \ldots + 3^{m-2}$.

- Find $3^2 + 3^3 + 3^4 + \ldots + 3^m$.

More Examples

- Prove the following for all integers $n \geq 1$.
  - $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$
  - $\displaystyle\sum_{i=1}^{n} i(i!) = (n+1)! - 1$
- Prove the following for all integers $n \geq 2$.

$$\sum_{i=1}^{n-1} i(i+1) = \frac{n(n-1)(n+1)}{3}$$

Another Example

- For all integers $n \geq 1$, $3 \mid \left(2^{2^n} - 1\right)$

Proving Inequalities with Induction

- Inductive Hypothesis
  - Has the form $y<z$
- Inductive Step
  - Needs to prove something of the form $x<z$
- Two methods for the proof part
  - Use whichever you like
  - Book method
    - Substitute "unequals" as long as the signs don't change, or
    - Add unequals to unequals as long as always adding correct sides
  - Transitivity
    - Find a value between (b)
    - Prove that $b < z$
    - Prove that $x < b$

Prove this statement:

$$\forall n \in Z^{\geq 3}, 2n+1 \leq 2^n$$

Base Case (n=3): $LHS: 2(3)+1 = 6+1 = 7$

$RHS: 2^3 = 8 \qquad LHS \leq RHS$

Inductive Hypothesis (n=k): $2k+1 \leq 2^k$

Inductive Step (n=k+1):

Show: $2(k+1)+1 \leq 2^{k+1}$

Proof:

Strong Induction

- Implication changes slightly
  - if true for all lesser elements, then true for current
- $P(i)\ \forall i \in Z\ a \leq i < k \rightarrow P(k)$
- $P(i)\ \forall i \in Z\ a \leq i \leq k \rightarrow P(k+1)$

Regular Induction

- $P(k) \rightarrow P(k+1)$
- $P(k-1) \rightarrow P(k)$

Recurrence Relation Example

- Assume the following definition of a function:

$$a_0 = 1 \qquad a_1 = 1 \qquad a_2 = 3$$

$$\forall k \in Z^{\geq 3}, a_k = a_{k-1} + a_{k-2} - a_{k-3}$$

- Prove the following definition property:

$$\forall n \in Z^{\geq 0}, a_n \in Z^{odd}$$

All integers greater than 1 are divisible by a prime

Base Case (n=2):

$2|2 \quad 2 \in Z^{prime}$

Inductive Hypothesis ($n=i \ \forall i \ 2 \leq i < k$):

$\exists p \in Z^{prime} \ \ p|i$

Inductive Step (n=k):

Show: $\exists p \in Z^{prime} \ \ p|k$

Proof:

Another Example

- Assume the following definition of a recurrence relation

$$a_1 = 0 \quad a_2 = 2$$

$$\forall i \in Z^{\geq 3}, a_i = 3a_{\left\lfloor \frac{i}{2} \right\rfloor} + 2$$

- Prove that all elements in this relation have this property

$$\forall n \in Z^{\geq 1}, a_n \in Z^{even}$$

Well-Ordering Principle

- For any set S of
  – One or more
  – Integers
  – All larger than some value
- S has a least one element

Use this to prove the Quotient Remainder Theorem

- The quotient-remainder theorem said
  - Given
    - Any positive integer n
    - And any positive integer d
  - There exists an r and a q
    - Where $n = dq + r$
    - Where $0 \leq r < d$
    - Which are integers
    - Which are unique

Steps to proving the quotient-remainder theorem

- Define S as the set of all non-negative integers in the form n-dk (all integers k)
- Prove that it is non-empty
- Prove that we can apply the Well-Ordering Principle
- Then it has a least element
- Prove that the least element (r) is:
  - $0 \leq r < d$

Another Example

- For all integers $n \geq 1$, $3 \left| \left(2^{2n} - 1\right) \right.$

Another Example

- For all integers $n \geq 1$, $3 \mid \left(2^{2^n} - 1\right)$

- Counter-example: n=5.

Prove this statement:

$$\forall n \in Z^{\geq 3}, 2n + 1 \leq 2^n$$

Base Case (n=3): $LHS : 2(3) + 1 = 6 + 1 = 7$

$RHS : 2^3 = 8 \qquad LHS \leq RHS$

Inductive Hypothesis (n=k): $2k + 1 \leq 2^k$

Inductive Step (n=k+1):

Show: $2(k+1) + 1 \leq 2^{k+1}$

Proof:

Prove this statement:

$$\forall n \in Z^{\geq 3}, 2n + 1 \leq 2^n$$

Inductive Step (n=k+1):

Show: $2(k+1) + 1 \leq 2^{k+1}$

Proof: $2k + 2 + 1 \leq 2^{k+1} \Rightarrow 2k + 1 + 2 \leq 2^{k+1} \Rightarrow 2k + 1 + 2 \leq 2^k \cdot 2$

$IH \Rightarrow 2(k+1) \leq 2^k \Rightarrow (\text{Multiply by two}) \Rightarrow 4k + 2 \leq 2^k \cdot 2$

New goal: $2k + 1 + 2 < 4k + 2$

$2k + 1 < 4k$

$1 < 2k$

$\frac{1}{2} \leq k$

Which is true since k≥3.

So $2k + 1 + 2 \leq 4k + 2 \leq 2^k \cdot 2$ and $2(k+1) + 1 \leq 2^{k+1}$

Prove this statement:

$$\forall n \in Z^{\geq 0}, 2^n \leq (n+2)!$$

Prove this statement:

$$\forall n \in Z^{\geq 1}, \sum_{i=1}^{n} (3i - 2) > \frac{n(3n-1)}{3}$$

Correctness of Algorithms

- Loop Invariants
  - Pre-conditions
  - Guard condition (so it terminates)
  - Post-conditions
- Loop Invariant Theorem