CS 19: Discrete Mathematics

Amit Chakrabarti

Proofs by Contradiction

and by Mathematical Induction

Direct Proofs

At this point, we have seen a few examples of mathematical proofs. These have the following structure:

- Start with the given fact(s).
- Use logical reasoning to deduce other facts.
- Keep going until we reach our goal.

Direct Proof: Example

Theorem: $1 + 2 + 3 + \dots + n = n(n+1)/2$.

Proof:

Let $x = 1 + 2 + 3 + \dots + n$. [starting point]

Then $x = n + (n-1) + (n-2) + \dots + 1$. [commutativity]

So, $2x = (n+1) + (n+1) + (n+1) + \dots + (n+1)$

$= n(n+1)$. [add the previous two equations]

So, $x = n(n+1)/2$. [Goal reached !]

Note: each step of the proof is a *grammatical* sentence.

Indirect Proof: Example

Theorem: There are infinitely many primes.

Proof:

Suppose that's not the case.

Then $\exists$ finitely many primes $p_1 < p_2 < \dots < p_n$.

Let $N = p_1p_2 \dots p_n + 1$. Then N is not divisible by any smaller prime number. So N must itself be prime.

But $N > p_n$, the largest prime. Contradiction!

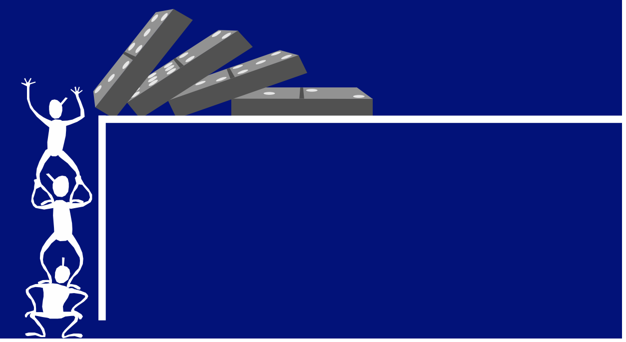
Indirect Proofs

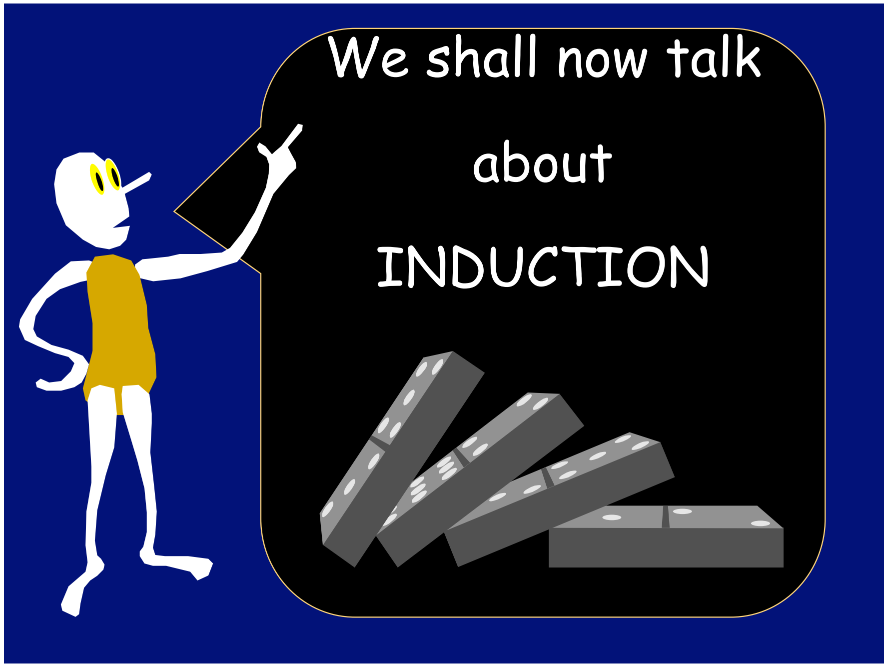
- Instead of starting with the given/known facts, we start by assuming the opposite of what we seek to prove.
- Use logical reasoning to deduce a sequence of facts.
- Eventually arrive at some logical absurdity, e.g. two facts that contradict each other.

a.k.a. "proof by contradiction" or *"reductio ad absurdum"*

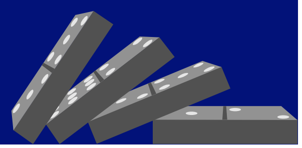
Mathematical Induction

Acknowledgment: The following slides are adapted from
Anupam Gupta's CMU course
"Great Ideas in Theoretical Computer Science"





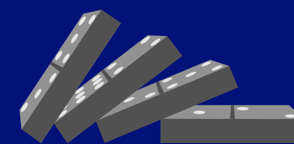
Domino Principle: Line up any number of dominos in a row; knock the first one over and they will all fall.



n dominoes numbered 1 to n

F_k = "the k^{th} domino falls"

If we set them all up in a row then we know that each one is set up to knock over the next one:



For all $1 \le k < n$:

$$F_k \Rightarrow F_{k+1}$$

n dominoes numbered 1 to n

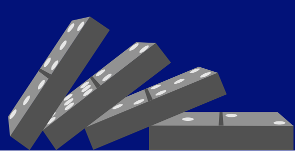
F_k = "the k^{th} domino falls"

For all $1 \le k < n$:

$$F_k \Rightarrow F_{k+1}$$

$F_1 \Rightarrow F_2 \Rightarrow F_3 \Rightarrow \ldots$

$F_1 \Rightarrow$ All Dominoes Fall



n dominoes numbered 0 to n-1

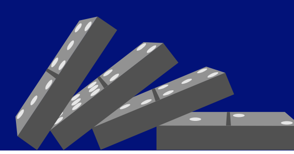
F_k = "the k^{th} domino falls"

For all $0 \le k < n-1$:

$$F_k \Rightarrow F_{k+1}$$

$F_0 \Rightarrow F_1 \Rightarrow F_2 \Rightarrow \ldots$

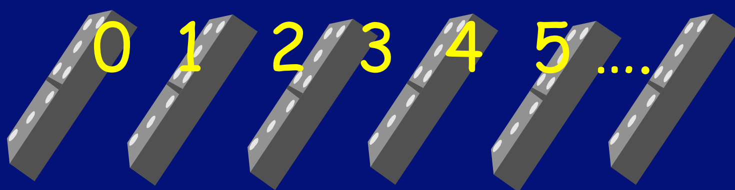
$F_0 \Rightarrow$ All Dominoes Fall



The Natural Numbers

N = { 0, 1, 2, 3, . . .}

One domino for each natural number:



n dominoes numbered 0 to n-1

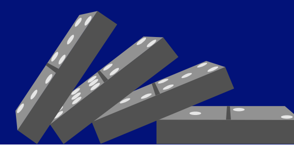
F_k = "the k^{th} domino falls"

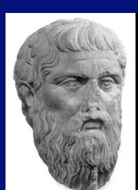
$\forall$ k, $0 \le k < n-1$:

$$F_k \Rightarrow F_{k+1}$$

$F_0 \Rightarrow F_1 \Rightarrow F_2 \Rightarrow \ldots$

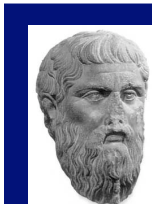
$F_0 \Rightarrow$ All Dominoes Fall





Plato: The Domino Principle works for an infinite row of dominoes

Aristotle: Never seen an infinite number of anything, much less dominoes.



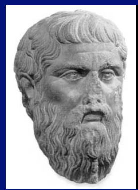
Plato's Dominoes
One for each natural number

An infinite row, 0, 1, 2, … of dominoes,
one domino for each natural number.

Knock the first domino over and they all will fall.

Proof:

Suppose they don't all fall. Let k > 0 be the lowest numbered domino that remains standing. Domino k-1 ≥ 0 did fall, but k-1 will knock over domino k. Thus, domino k must fall and remain standing. Contradiction.



The Infinite Domino Principle

F_k = "the k^{th} domino will fall"

Assume we know that
for every natural number k,

$$F_k \Rightarrow F_{k+1}$$

$F_0 \Rightarrow F_1 \Rightarrow F_2 \Rightarrow \ldots$

$F_0 \Rightarrow$ All Dominoes Fall

Mathematical Induction: statements proved instead of dominoes fallen

Infinite sequence of dominoes.	Infinite sequence of statements: $S_0, S_1, \ldots$
F_k = "domino k fell"	F_k = "S_k proved"

Establish 1) F_0

2) For all k, $F_k \Rightarrow F_{k+1}$

Conclude that F_k is true for all k

Inductive Proof / Reasoning To Prove $\forall k \in N$ (S_k)

Establish "Base Case": S_0

Establish that $\forall k$ $(S_k \Rightarrow S_{k+1})$

$\forall k$ $(S_k \Rightarrow S_{k+1})$:
- Assume hypothetically that S_k for *any* particular k;
- Conclude that S_{k+1}

Inductive Proof / Reasoning To Prove $\forall k \in N$ (S_k)

Establish "Base Case": S_0

Establish that $\forall k$ $(S_k \Rightarrow S_{k+1})$

$\forall k$ $(S_k \Rightarrow S_{k+1})$:
- "Inductive Hypothesis" S_k
- "Induction Step"
  Use I.H. to show S_{k+1}

Inductive Proof / Reasoning
To Prove $\forall k \geq b \ (S_k)$

Establish "Base Case": S_b

Establish that $\forall k \geq b \ (S_k \Rightarrow S_{k+1})$

- Assume $k \geq b$
- "Inductive Hypothesis": Assume S_k
- "Inductive Step": Prove that S_{k+1} follows

Theorem?

The sum of the first n <u>odd</u> numbers is n^2.

Theorem:?

The sum of the first n odd numbers is n^2.

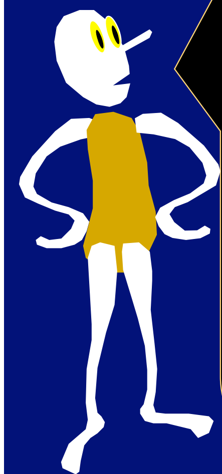
Check on small values:

1	= 1
1+3	= 4
1+3+5	= 9
1+3+5+7	= 16

Theorem:?

The sum of the first n odd numbers is n^2.

The k^{th} odd number is expressed by the formula $(2k - 1)$, when $k>0$.

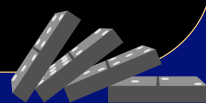


$S_n \equiv$ "The sum of the first n odd numbers is n^2."

Equivalently,

S_n is the statement that:

"$1 + 3 + 5 + (2k-1) + \ldots + (2n-1) = n^2$"



$S_n \equiv$ "The sum of the first n odd numbers is n^2."

"$1 + 3 + 5 + (2k-1) + \ldots + (2n-1) = n^2$"

Trying to establish that: $\forall n \geq 1\ (S_n)$

Assume "Inductive Hypothesis": S_k

(for any particular $k \geq 1$)

$1+3+5+\ldots+(2k-1) = k^2$

Add $(2k+1)$ to both sides.

$1+3+5+\ldots+(2k-1)+(2k+1) = k^2+(2k+1)$

Sum of first k+1 odd numbers $= (k+1)^2$

CONCLUDE: S_{k+1}

$S_n \equiv$ "The sum of the first n odd numbers is n^2."

"$1 + 3 + 5 + (2k-1) + \ldots + (2n-1) = n^2$"

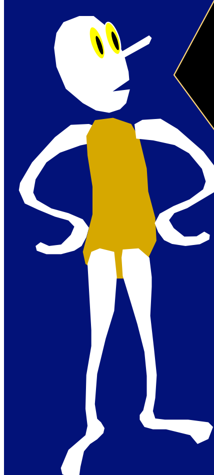
Trying to establish that: $\forall n \geq 1\ (S_n)$

In summary:

1) Establish base case: S_1

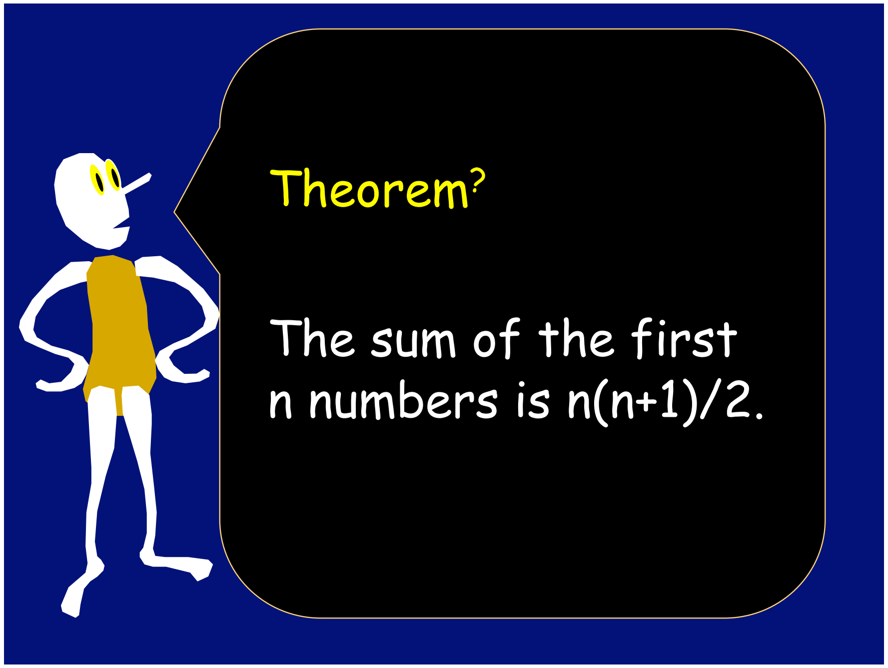
2) Establish domino property: $\forall k \geq 1\ (S_k \Rightarrow S_{k+1})$

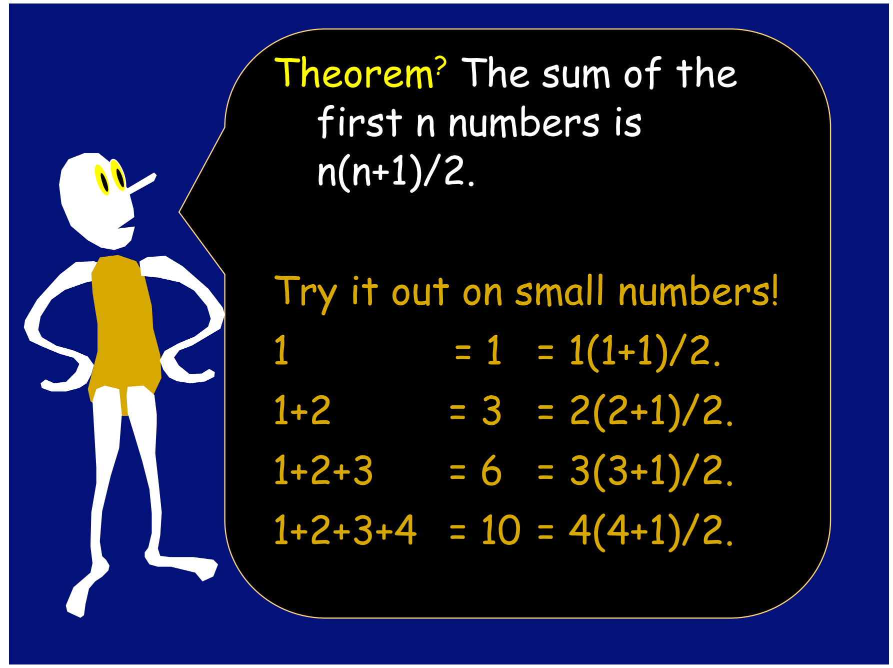
By induction on n, we conclude that: $\forall k \geq 1\ (S_k)$

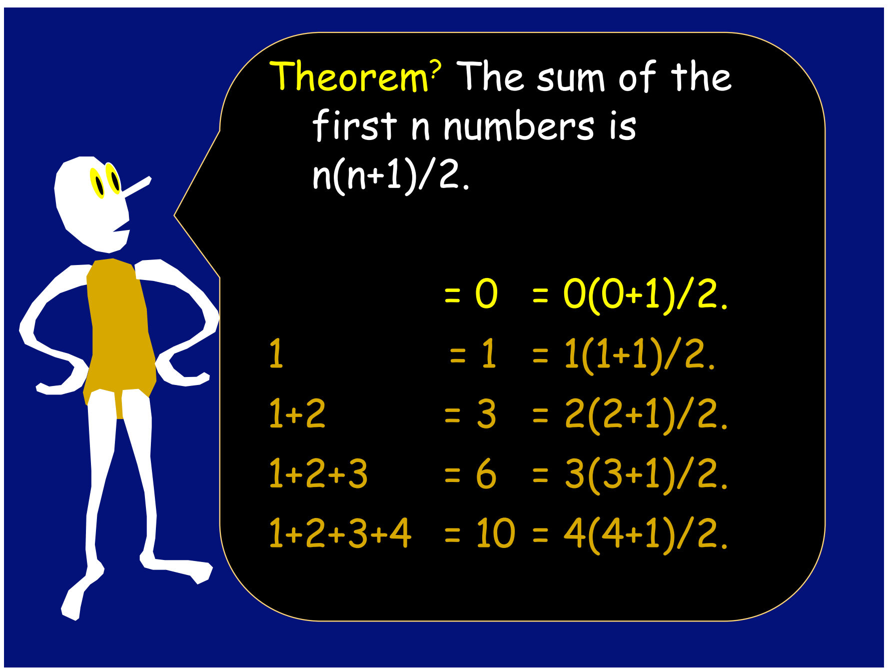


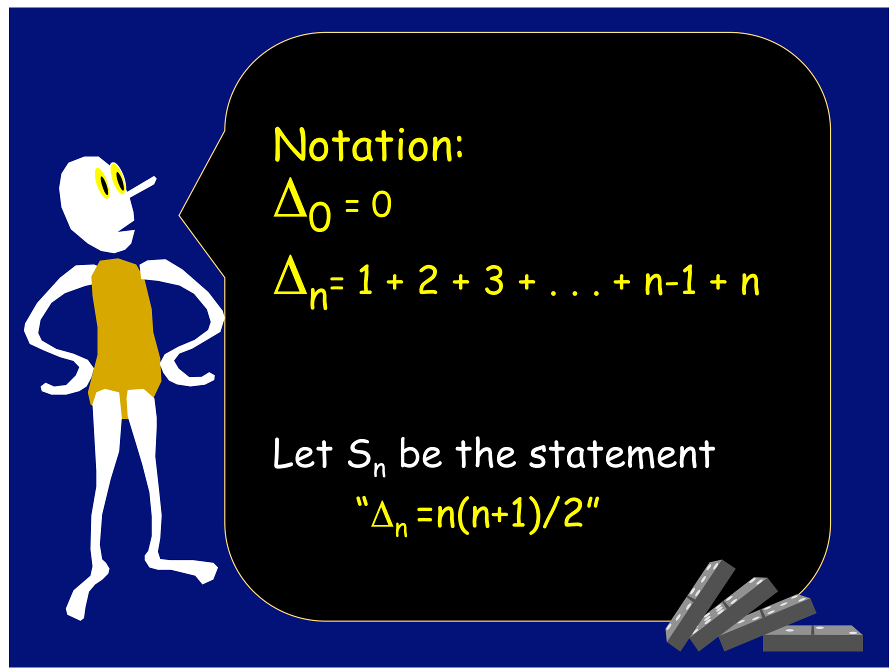
THEOREM:

The sum of the first n odd numbers is n^2.


Theorem?
The sum of the first n numbers is n(n+1)/2.


Theorem? The sum of the first n numbers is n(n+1)/2.
Try it out on small numbers!
1 = 1 = 1(1+1)/2.
1+2 = 3 = 2(2+1)/2.
1+2+3 = 6 = 3(3+1)/2.
1+2+3+4 = 10 = 4(4+1)/2.


Theorem? The sum of the first n numbers is n(n+1)/2.
= 0 = 0(0+1)/2.
1 = 1 = 1(1+1)/2.
1+2 = 3 = 2(2+1)/2.
1+2+3 = 6 = 3(3+1)/2.
1+2+3+4 = 10 = 4(4+1)/2.


Notation:
$\Delta_0 = 0$
$\Delta_n = 1 + 2 + 3 + . . . + n-1 + n$
Let S_n be the statement
"$\Delta_n = n(n+1)/2$"

$S_n \equiv$ "$\Delta_n = n(n+1)/2$"
Use induction to prove $\forall k \geq 0, S_k$

Establish "Base Case": S_0.

Δ_0=The sum of the first 0 numbers = 0.

Setting n=0, the formula gives 0(0+1)/2 = 0.

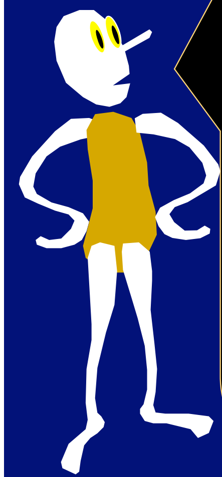
Establish that $\forall k \geq 0, S_k \Rightarrow S_{k+1}$

"Inductive Hypothesis" S_k: $\Delta_k = k(k+1)/2$

$\Delta_{k+1} = \Delta_k + (k+1)$

$= k(k+1)/2 + (k+1)$ [Using I.H.]

$= (k+1)(k+2)/2$ [which proves S_{k+1}]



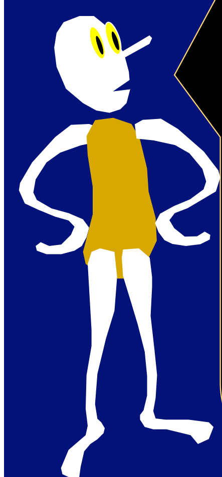
Theorem:

The sum of the first n numbers is n(n+1)/2.

Induction: Other Uses

Not just for proving the validity of algebraic equations.

Induction is a powerful tool that can be used to prove many other sorts of statements.



Theorem?

The set {1,2,3,…,n} has exactly 2^n subsets.

$S_n \equiv$ "{1,2,3,…,n} has exactly 2^n subsets."

Trying to establish that: $\forall n \geq 1\ (S_n)$

Establish "base case": S_1

The set {1} has exactly 2 subsets: { } and {1}.

$2 = 2^1$.

So, S_1 is true.

$S_n \equiv$ "{1,2,3,…,n} has exactly 2^n subsets."

Trying to establish that: $\forall n \geq 1\ (S_n)$

Assume "Inductive Hypothesis": S_k

{1,2,3,…,k} has exactly 2^k subsets.

The subsets of {1,2,3,…,k+1} are

- either subsets of {1,2,3,…,k}
- or $A \cup \{k+1\}$, where $A \subseteq \{1,2,3,\ldots,k\}$

$S_n \equiv$ "{1,2,3,…,n} has exactly 2^n subsets."

Trying to establish that: $\forall n \geq 1\ (S_n)$

Assume "Inductive Hypothesis": S_k

{1,2,3,…,k} has exactly 2^k subsets.

The subsets of {1,2,3,…,k+1} are

- either subsets of {1,2,3,…,k}
  - and there are 2^k of these [by I.H.]
- or $A \cup \{k+1\}$, where $A \subseteq \{1,2,3,\ldots,k\}$
  - and there are 2^k of these. [by I.H.]

$S_n \equiv$ "{1,2,3,…,n} has exactly 2^n subsets."

Trying to establish that: $\forall n \geq 1\ (S_n)$

Assume "Inductive Hypothesis": S_k

{1,2,3,…,k} has exactly 2^k subsets.

The subsets of {1,2,3,…,k+1} are

- either subsets of {1,2,3,…,k}
  - and there are 2^k of these [by I.H.]
- or $A \cup \{k+1\}$, where $A \subseteq \{1,2,3,\ldots,k\}$
  - and there are 2^k of these. [by I.H.]

Together, there are $2^k + 2^k = 2^{k+1}$ subsets.

CONCLUDE: S_{k+1}

In Summary

We have learnt two very important proof techniques today.

- Proof by contradiction
- Proof by mathematical induction.

We shall soon be seeing these on a daily basis. Learn them well!