CSE 2001:
Introduction to Theory of Computation

Winter 2013

Suprakash Datta

datta@cse.yorku.ca

Office: CSEB 3043

Phone: 416-736-2100 ext 77875

Course page: http://www.cse.yorku.ca/course/2001

What is a Proof - continued?

“Everybody knows what a mathematical proof is. A proof of a mathematical theorem is a sequence of steps which leads to the desired conclusion. The rules to be followed by such a sequence of steps were made explicit when logic was formalized early in this century, and they have not changed since“

- Giancarlo Rota, The phenomenology of mathematical proof. Synthese, 111: 183-196, 1997

http://www.jstor.org/discover/10.2307/20117627?uid=3739448&uid=2129&uid=2&uid=70&uid=3737720&uid=4&sid=21101181582701

Proof by contradiction - 2

The Pigeonhole Principle

- If n+1 or more objects are placed into n boxes, then there is at least one box containing two or more of the objects

  In a set of any 27 English words, at least two words must start with the same letter

- If n objects are placed into k boxes, then there is at least one box containing $\lceil n/k \rceil$ objects

Proof by induction

Format:

- Inductive hypothesis,
- Base case,
- Inductive step.

Proof by induction

Prove: For any $n \in \mathbf{N}$, n^3-n is divisible by 3.

IH: P(n): For any $n \in \mathbf{N}$, $f(n)=n^3-n$ is divisible by 3.
Base case: P(1) is true, because f(1)=0.
Inductive step:
Assume P(n) is true. Show P(n+1) is true.
Observe that $f(n+1) – f(n) = 3(n^2 + n)$
So f(n+1) – f (n) is divisible by 3.
Since P(n) is true, f(n) is divisible by 3.
So f(n+1) is divisible by 3.
Therefore, P(n+1) is true.
Exercise: give a direct proof.

Recursively defined sets

Close relationship to induction

Example: set of all palindromes

- $\varepsilon \in P$; $\forall a \in \Sigma$, $a \in P$;
- $\forall a \in \Sigma\ \forall x \in P$, $axa \in P$
- No other strings are in P

More definitions

Definition of Σ^*:

- $\varepsilon \in \Sigma^*$;
- $\forall$ a $\in \Sigma$, $\forall$ x $\in \Sigma^*$, xa $\in \Sigma^*$;
- No other strings are in Σ^*.

Exercise

Suppose $\Sigma = \{a,b\}$. Define L as

- $a \in L$;
- $\forall\, x \in L$, $ax \in L$
- $\forall\, x, y \in L$, bxy, xby and xyb are in L
- No other strings are in P

- Prove that this is the language of strings with more a's than b's.