

Review of Proof Techniques

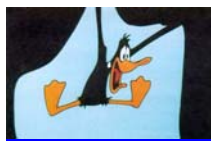
◆ Last Time:

- ⇒ **Proof by counterexample:** Give an example that disproves the given statement. E.g. $\text{PRIMES} \subseteq \text{ODD}$
- ⇒ **Proof by contradiction:** Assume statement is false and show that it leads to a contradiction.
- ⇒ **Proof by construction**
- ⇒ **Proof of set equality** $A = B$: Show $A \subseteq B$ and $B \subseteq A$
- ⇒ **Proof of “X iff Y”** (or $X \Leftrightarrow Y$) statements
- ⇒ “Birdy” technique #1: **Pigeonhole principle**



◆ Today:

- ⇒ **Proof by induction**
- ⇒ “Birdy” technique #2: **Dovetailing**
- ⇒ CS Theoretician’s favorite: **Diagonalization**



Proof Techniques Review:

The Big picture

- ◆ **Proof by contradiction:** Assume statement is false and show that it leads to a contradiction
 - ⇒ E.g.: Prove: Complement of any finite subset of Z is infinite
- ◆ **Proof by construction:** Show that a statement can be satisfied by constructing an object using what is given
 - ⇒ E.g.: Show that for all c , $\exists n_0$ s.t. $n^2 > cn$ for all $n \geq n_0$
- ◆ **Proof of set equality** $A = B$: Show $A \subseteq B$ and $B \subseteq A$
 - ⇒ E.g.: De Morgan’s Law (one of two):
$$A - (B \cap C) = (A - B) \cup (A - C)$$
- ◆ **Proving “X iff Y” statements:** Prove $X \Rightarrow Y$ (“X only if Y”) and $Y \Rightarrow X$ (“X if Y”)
 - ⇒ E.g.: For all real numbers x , show $\lfloor x \rfloor = \lceil x \rceil$ iff $x \in Z$

Review: Avian Technique #1

- ◆ **Pigeonhole principle:** If A and B are finite sets and $|A| > |B|$, then there is no one-to-one function from A to B
 - ⇒ $f : A \rightarrow B$ is one-to-one if for any distinct $x, y \in A$, $f(x) \neq f(y)$
 - ⇒ **Idea:** “more pigeons than pigeonholes” → at least one pigeonhole contains two pigeons.
 - ⇒ E.g. In a room of 13 or more people, at least 2 have same birthmonth
 - ⇒ Proof? By induction on $|B|$
- ◆ What is “Proof by Induction”?



Proof by Induction

- ◆ **Proof by induction** (very common in CS Theory): 2 steps –
 1. **Basis Step:** Show statement is true for some finite value n_0 , typically $n_0 = 0$
 2. **Induction Hypothesis and Induction Step:** Assume statement is true for some fixed but arbitrary $k \geq n_0$. Show it is also true for $k + 1$
- ⇒ **Example:** Show that for all $n \geq 0$, $1 + 2 + \dots + n = n(n+1)/2$



To Infinity and Beyond (with apologies to Disney)

- ◆ **Sizing up sets:** Cardinality of a set and countably infinite sets
- ◆ **Avian Technique #2 – Dovetailing:** Useful for showing union of any finite or countably infinite collection of countably infinite sets is again countably infinite
 - ⇒ A is *countably infinite* if there is a 1-1 correspondence (“bijection”) between \mathbb{N} (the set of natural numbers) and A
 - ⇒ **E.g.** Use dovetailing to show \mathbb{Z} and $\mathbb{N} \times \mathbb{N}$ are both countably infinite
- ◆ **Diagonalization and Uncountable Sets:** See pages 160-163 in the text for a nice introduction and more examples.
 - ⇒ **Example on board:** Power set of \mathbb{N} is uncountable
- ◆ **See Handout #1 for more details...**

Next Class: Enter the finite automaton...

- ◆ **Next time:**
 - ⇒ Finite automata 101
- ◆ **Things to do:**
 - ⇒ Sign up for mailing list if you haven't already
 - ◆ Instructions on website
 - ⇒ Finish Chapter 0 and start Chapter 1
 - ⇒ Work on homework #1