Basic Mathematical Techniques for Computer Scientists

(Some) Proof Techniques

November 5, 2012

Recap

Questions?

- Axioms
  - Why we need them
  - As simple as possible
  - Examples: Number theory, Geometry
- Some names
  - Tautology, Contradiction, Contingency
- Logical deductions
  - Rules of replacement
    - Based on equivalences
    - Used to replace parts of propositions
    - Examples: Double Negation, Commutativity, Associativity, De Morgan's Laws
  - Rules of inference
    - Based on implications
    - Used to replace propositions wholesale
    - Examples: Disjunctive Syllogism, Modus Ponens, Modus Tollens

Proof Techniques

Examples

- $\forall a \in \mathbb{N} \;\; 2 \mid a \implies 2 \mid a^2$
  - True or not?
  - Why?
- $\forall a \in \mathbb{N} \;\; 2 \nmid a \implies 2 \nmid a^2$
  - True or not?
  - Why?
- $\forall a, b \in \mathbb{N} \;\; (2 \nmid a \wedge 2 \nmid b) \implies 2 \mid (a + b)$
  - True or not?
  - Why?

Proof Techniques

Direct Proof

- All proofs we saw till now
- Structure matches definition of “proof”
  - Combine axioms and previous theorems
  - In a “linear” fashion
- Many proofs are of this form, but . . .
- . . . there are proofs with other “structures” as well

Proof Techniques

Examples

- $\forall a \in \mathbb{Z} \;\; 5 \nmid a^2 \implies 5 \nmid a$
  - True or not?
  - Why?
- $\forall a \in \mathbb{Z} \;\; 2 \mid a^2 \implies 2 \mid a$
  - True or not?
  - Why?

Proof by Contrapositive

- Based on the following *theorem*
  - $(P \implies Q) \iff (\neg Q \implies \neg P)$
- So to prove $P \implies Q$, we *instead* prove $\neg Q \implies \neg P$
  - From the above theorem, this is enough
- $\neg Q \implies \neg P$ is the *contrapositive* of $P \implies Q$
  - Also: $P \implies Q$ is the *contrapositive* of $\neg Q \implies \neg P$
- Very useful!
  - In many cases, the contrapositive is *much* easier to prove
  - Like in the following examples ...

Proof by Contrapositive

More examples

- $\forall a \in \mathbb{Z}\ \ 2 \mid (a^2 - 4a + 7) \implies 2 \nmid a$

Proof by Contrapositive

More examples

- $\forall a \in \mathbb{N} \ (2^a - 1)$ is prime $\implies a$ is prime

Contraposite and Converse

- Two similar-sounding words, with distinctly different meanings
- $\neg Q \implies \neg P$ is the *contrapositive* of $P \implies Q$
  - Also: $P \implies Q$ is the *contrapositive* of $\neg Q \implies \neg P$
- An implication and its contrapositive are *equivalent*
  - Per above theorem

Contrapositive and Converse

- Two similar-sounding words, with distinctly different meanings
- $\neg Q \implies \neg P$ is the contrapositive of $P \implies Q$
- An implication and its contrapositive are equivalent

- The *converse* of $P \implies Q$ is $Q \implies P$
  - Also: $P \implies Q$ is the converse of $Q \implies P$
- An implication and its converse are *not* equivalent
  - One may be **true** and the other **false**
    - At the same time
    - An implication does **not** always imply its converse
    - Examples?

Proof Techniques

Examples

- $\forall a, b \in \mathbb{Z} \;\; a^2 - 4b \neq 6$
  - True or not?
  - Proof?

- What are prime numbers?
- How many primes numbers are there?
  - Let $p_1, p_2, \ldots, p_n$ be all the primes
  - Consider $a = (\Pi_{i=1}^{n} p_i) + 1$
    - (Shorthand for $a = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$)

- What kind of numbers inhabit the number line?
  - Integers
  - Fractions (Rational numbers)
  - What else?
    - Are there numbers which cannot be expressed as ratios?

Proof Techniques

Proof by Contra*diction*

- Based on the following *inference rule*

$$\frac{\neg \mathrm{P} \implies \text{false}}{\mathrm{P}}$$

- To prove P, prove the following: "$\neg$P implies a falsehood"
- Extremely useful!

Proof Techniques

Examples

- $\forall n \in \mathbb{N} \;\; 4 \mid (5^n - 1)$
  - True or not?
  - Proof?
- The sum of the first n positive integers is $\frac{n(n+1)}{2}$
- Proof?

Proof Techniques

Proof by Induction

- The sum of the first n positive integers is $\frac{n(n+1)}{2}$
- Proof: By *induction* on n.
  1. Express the statement as a predicate:
     $$\forall n \in \mathbb{N}^+ \;\; P(n) \triangleq \sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$
  2. *Basis step:* Show that $P(1)$ is true.
  3. *Induction step:* Prove the following *implication*:
     $\forall n \in \mathbb{N}^+ \;\; P(n) \implies P(n+1)$
  4. Done!

Proof by Induction

More examples

- The sum of the first n *odd* positive integers is n^2
- Proof by induction?

- $\forall n \in \mathbb{N} \;\; 2 \mid (n^2 + n)$
- Proof by induction?

Thank You!