Lecture 7 (9/23)
Outline

- Mathematical proofs (cont., Rosen 1.7, 1.8)
  - How do we write proofs?
  - Contradiction
  - Existence proofs
  - Proofs of equivalence
  - Exhaustive proofs (aka proofs by cases)
  - Uniqueness proofs
  - and...
    - Trivial proofs
    - WLOG
    - Forward/backward reasoning

Proof by contradiction

Exercise: Prove that $\sqrt{2}$ is irrational.

Ideas?

What does it mean to be rational to begin with?

Proof by contradiction [Scratch work]

- *Irrational* means not rational, so our goal is a negative statement. This fact already suggests that a proof by contradiction might be the right choice.

- What would it mean for $\sqrt{2}$ to be rational? $\frac{p}{q} = \sqrt{2}$, where $p, q \neq 0$ are integers.

- In general a fra
- *without loss of generality*, we may assume that p, q are both positive (since $\sqrt{2} > 0$), and that the fraction is in lowest terms (i.e., p, q have no common factors)

- What do we infer by squaring?

Proof by contradiction [Scratch work]

- What do we infer by squaring? That both p, q are even!
- By squaring we obtain that $p^2 = 2q^2$.
- This means that p^2 is even, and therefore $p = 2a$ for some integer a, i.e., p is even.
- By substituting $p = 2a$ we obtain that q^2 and hence q is also even since $2q^2 = 4a^2 \rightarrow q^2 = 2a^2$. Therefore $q = 2b$ for some integer b.

Proof by contradiction [Scratch work]

- So we have shown that p, q have to both be even.
- What does this mean?
  - That they share 2 as a common factor
- Therefore, our assumption that 2 is rational ($\neg p$) leads to the contradiction that
  1. 2 does not divide p, q (lower terms)
  2. p, q are even, so 2 divides both of them
- Thus, $\sqrt{2}$ is rational

Proof by contradiction – $\sqrt{2}$ is irrational

Read carefully the way the proof is also written in Rosen, p. 90, 91

- **Remark:** Writing nice proofs requires practice
- Additional reading: Mathematical writing (sections 1,2,3) `http://jmlr.csail.mit.edu/reviewing-papers/knuth_mathematical_writing.pdf`

Proof by contradiction – Technique

- Suppose we want to prove that p is true.

- For the sake of contradiction, let's assume $\neg p$ is true.

- **Technique:** We prove that $\neg p \rightarrow F$.
    - This achieved by proving $\neg p \rightarrow (r \wedge \neg r)$ for some proposition r

- Practice, practice, practice!

Proof by contradiction

- **Theorem:** If a, b are integers, then $a^2 - 4b \neg 2$.

- **Proof by contradiction (scratch work):** We wish to prove an implication $p \rightarrow q \equiv \neg p \vee q$. The negation is $\neg(p \rightarrow q) \equiv p \wedge \neg q$. In other words we need to assume that there exist two integers a, b such that $a^2 - 4b = 2$.

- That is how we need to start writing our proof.

  "Suppose for the sake of contradiction that there exist two integers a, b such that $a^2 - 4b = 2$."

- The next step is to derive a contradiction based on this logical premise. What observations can we derive from $a^2 - 4b = 2$?

Proof by contradiction

Proof: Suppose for the sake of contradiction that there exist two integers a, b such that $a^2 - 4b = 2$. From this equation we get

$$a^2 = 2(1 + 2b) \tag{1}$$

so a^2 is even, and therefore a is even. This means we can write $a = 2c$ for some integer c. By plugging this expression in Equation 1 and dividing by 2, we obtain $2(c^2 - b) = 1$. Since $c^2 - b$ is an integer, 1 is equal to an even number. Contradiction (i.e., 1 is odd $\wedge$ 1 is even). **QED**

Proof by equivalence

- To prove a biconditional statement (if and only if)

$$p \leftrightarrow q$$

  we need to prove $p \rightarrow q$ and $q \rightarrow p$.

- **Example:** Let n be an integer. Prove that n is odd if and only if (**iff**) n^2 is odd.
  1. One direction is (n is odd $\rightarrow$ n^2 is odd)
  2. The other direction (n^2 is odd $\rightarrow$ n is odd)
     We have already proved both in class.

- How do we prove $p_1 \leftrightarrow p_2 \leftrightarrow p_3$?

Proof by equivalence

- How do we prove $p_1 \leftrightarrow p_2 \leftrightarrow p_3$?
- **Idea 1:** Prove the following:
  1. $p_1 \rightarrow p_2$
  2. $p_2 \rightarrow p_1$
  3. $p_1 \rightarrow p_3$
  4. $p_3 \rightarrow p_1$
  5. $p_2 \rightarrow p_3$
  6. $p_3 \rightarrow p_2$
- **Better idea:** This is not necessary. It is suffices to prove :
  1. $p_1 \rightarrow p_2$
  2. $p_2 \rightarrow p_3$
  3. $p_3 \rightarrow p_1$

Proof by equivalence

- **Example :** Show that these statements about the integer n are equivalent:
  1. p_1 : n is even
  2. p_2 : $n-1$ is odd
  3. p_3 : n^2 is even

  Details on blackboard (see also [Rosen, Example 14, p.92])

- What is an efficient way to prove $p_1 \leftrightarrow \ldots \leftrightarrow p_n$ where $n \geq 2$? (**generalize**)

  Intuition (details in class): Ensure "strong connectivity" when we think of propositions as nodes, and conditionals as arcs

Existence proofs

- **Claim:** Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

  Proof: $1729 = 10^3 + 9^3 = 12^3 + 1^3$ (computer search...)

- **Exercise:** Show that there exist irrational numbers x, y such that x^y is rational.

Existence proofs

- **Exercise:** Show that there exist irrational numbers x, y such that x^y is rational.
- **Scratch work:** Well, the only irrational we have seen so far is $\sqrt{2}$, so let's consider $\sqrt{2}^{\sqrt{2}}$.
  - Well, it is hard to tell. But we know that one of the following two can be true:
    1. $\sqrt{2}^{\sqrt{2}}$ is rational, hence we are done.
    2. $\sqrt{2}^{\sqrt{2}}$ is irrational.
  - But in the latter case, notice that $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$.
    - Therefore we have covered all cases.
      Either $x = y = \sqrt{2}$ or $x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$ have the desired property.
- **Formal proof:** How to write it down? On blackboard and pages 101, 102 Rosen

Proof by exhaustion (aka proof by cases)

- Tautology
  $[(p_1 \vee p_2 \vee \dots p_n) \to q] \leftrightarrow [(p_1 \to q) \wedge (p_2 \to q) \wedge \dots \wedge (p_n \to q)]$

- **Crucial first step:** Identify a **complete list** of possible cases (in principle, they need not be mutually exclusive, but in practice they usually are).

- **Exercises**
  1. Prove that if $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.
  2. Prove that if n is an integer, then $n^2 \geq n$
  3. Let n be an integer. If 3 does not divide n, then 3 divides $n^2 - 1$.

  Solutions on blackboard

Without loss of generality (wlog)

- Example: If three objects are each painted either red or blue, then there must be at least two objects of the same color.

  Proof: Assume without loss of generality that the first object is red. If either of the other two objects is red, we are finished; if not, the other two objects must both be blue and we are still finished.
- Remarks
  1. The *wlog* allows us to cover the symmetric case where the first object is blue.
  2. We will see this again later in class (pigeonhole principle)

Vacuous and Trivial proofs

- Suppose we wish to prove that $p \to q$
  1. If p is always false, then the statement is always true (vacuous proof)
  2. If q is always true, then the statement is again always true (trivial proof)
- Examples
  1. Prove that if n is an integer with $10 \leq n \leq 11$ which is a perfect square, then n is also a perfect cube.
  2. Let $P(n)$ be " if a,b are positive integers with $a \geq b$ then $a^n \geq b^n$, where the domain consists of all nonnegative integers. Show that $P(0)$ is true.
- Proofs on blackboard (see also [Rosen p.88,89])

Uniqueness proofs

- $\exists! x P(x)$
- A uniqueness proof consists typically of two parts
  1. Prove existence of x that has the desired property
  2. Prove that if y has the desired property, then $y = x$
- **Example:** There is a unique function $f : \mathbb{R} \to \mathbb{R}$ such that $f'(x) = 2x$ and $f(0) = 3$.

Proof.

1. Existence: $f(x) = x^2 + 3$ (why?)
2. Uniqueness: If $f_0(x)$ and $f_1(x)$ both satisfy these conditions, then $f_0'(x) = 2x = f_1'(x)$, so they differ by a constant, i.e., there is a C such that $f_0(x) = f_1(x) + C$. Hence, $3 = f_0(0) = f_1(0) + C = 3 + C$. This gives $C = 0$ and so $f_0(x) = f_1(x)$

□

Forward/backward reasoning

- **AM-GM:** Let x, y be two non-negative real numbers. Prove that $\frac{x+y}{2} \geq \sqrt{xy}$.

Backward reasoning.

$$\frac{x+y}{2} \geq \sqrt{xy} \leftrightarrow (\frac{x+y}{2})^2 \geq (\sqrt{xy})^2 \leftrightarrow (x+y)^2 \geq 4xy \leftrightarrow$$
$$(x^2+2xy+y^2) \geq 4xy \leftrightarrow (x^2-2xy+y^2) \geq 0 \leftrightarrow (x-y)^2 \geq 0.$$

- **Remark:** We can use backward reasoning to produce forward reasoning since we used *equivalent* inequalities.
- Details on the blackboard.