Announcements

• Homework 1 is due today
  – Turn it in now

• Homework 2 is posted online
  – Due next Thursday

• Finish Reading Section 1.8 (Proof Methods and Strategy) by next Tuesday
Rules of Inference for Quantifiers

• **Universal Instantiation**
  \[ \forall x \, P(x) \quad \therefore \quad P(c) \]

  If true for all members of a domain, must be true for a particular member.

**Example:**
“All students in this class will receive an A, therefore Pat (who is a student in this class) will receive an A”

• **Universal Generalization**
  \[ P(c) \text{ for an arbitrary } c \quad \therefore \quad \forall x \, P(x) \]

  Under the premise that \( P(c) \) is true for all elements in the \( c \) domain. Given this case, we can take an arbitrary element and show it is true.
Rules of Inference for Quantifiers

- **Existential Instantiation**
  \[ \exists x \, P(x) \quad \therefore P(c) \text{ for some element } c \]
  
  If there exists some element for which \( P(x) \) is true, then there is an element \( c \) in the domain for which it is true.

- **Existential Generalization**
  \[ P(c) \text{ for some element } c \quad \therefore \exists x \, P(x) \]
  
  If we know one element \( c \) in the domain for which \( P(c) \) is true, then we know \( \exists x \, P(x) \) is true.
Quantified Statement Example

Show that the premises “A student in this class has not read the book” and “Everyone in this class passed the first exam” imply “Someone who passed the first exam has not read the book”

C(x) = “x is in this class”
B(x) = “x has read the book”
P(x) = “x passed the first exam”

1. \( \exists x (C(x) \land \neg B(x)) \) Premise
2. \( C(a) \land \neg B(a) \) Existential instantiation from (1)
3. \( C(a) \) Simplification from (2)
4. \( \forall x ((C(x) \rightarrow P(x)) \) Premise
5. \( C(a) \rightarrow P(a) \) Universal instantiation from (4)
6. \( P(a) \) Modus Ponens from (3) and (5)
7. \( \neg B(a) \) Simplification from (2)
8. \( (P(a) \land \neg B(a)) \) Conjunction from (6) and (7)
9. \( \exists x (P(x) \land \neg B(x)) \) Existential generalization from (8)
Proofs of Equivalence

• In order to prove a biconditional statement \( p \leftrightarrow q \), we need to show that
  \( p \rightarrow q \) and \( q \rightarrow p \)
  \[ (p \leftrightarrow q) \equiv [(p \rightarrow q) \land (q \rightarrow p)] \]

• Showing several propositions are equivalent can be done with tautology
  \[ [p_1 \leftrightarrow p_2 \leftrightarrow p_3 \leftrightarrow \ldots \leftrightarrow p_n] \leftrightarrow [(p_1 \rightarrow p_2) \land (p_2 \rightarrow p_3) \land \ldots \land (p_n \rightarrow p_1)] \]

  If the conditionals \( p_1 \rightarrow p_2, p_2 \rightarrow p_3, p_3 \rightarrow p_n, p_n \rightarrow p_1 \) can be shown true, \( p_1, p_2, p_3, \ldots, p_n \) are equivalent

  Easier than \( p_i \rightarrow p_j \) for all \( i \neq j \), \( 1 \leq i \leq n \), and \( 1 \leq j \leq n \).
Example

- **Show that these statements are equivalent**
  - $P_1$: $n$ is even
  - $P_2$: $n-1$ is odd
  - $P_3$: $n^2$ is even

- **Solution:**
  - Need to show that $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$, $p_3 \rightarrow p_1$

- $p_1 \rightarrow p_2$?
  - Direct proof

- $p_2 \rightarrow p_3$?
  - Direct proof

- $p_3 \rightarrow p_1$?
  - Proof by contraposition

I need some volunteers
Example Proofs

• **Show that these statements are equivalent**
  - $P_1$: $n$ is even
  - $P_2$: $n - 1$ is odd
  - $P_3$: $n^2$ is even

• **$P_1 \rightarrow P_2$?**
  - Suppose $n$ is even, therefore $n = 2k$, $n - 1 = 2k - 1 = 2(k - 1) + 1$. Which means $n - 1$ is odd because of the form $2m + 1$ where $m = k - 1$

• **$P_2 \rightarrow P_3$?**
  - Suppose $n - 1$ is odd. Then $n - 1 = 2k + 1$ for some $k$. Hence, $n = 2k + 2$ so $n^2 = (2k+2)(2k+2) = (4k^2 + 4k + 4) = 2(2k^2 + 4k + 2)$, therefore $n^2$ is twice $(2k^2 + 4k + 2)$ therefore is even

• **$P_3 \rightarrow P_1$?**
  - Proof by contraposition $\neg P_1 \Rightarrow \neg P_3$
  - Suppose $n$ is odd, therefore $n = 2k + 1$.
    Therefore $n^2 = (2k+1)(2k+1) = (4k^2 + 4k + 1) = 2(2k^2 + 2k + 1)$
    Therefore $n^2$ is odd $2m + 1$
Suppose I said prove “if n is an integer, then \( n^2 \geq n \)"

\[ p: \text{ n is an integer} \]
\[ q: \text{ } n^2 \geq n \]

What if proving the case for \( p \) as an int is too difficult?

What could I do?
Break it up into cases?
\[ p_1 = \text{ n is an int } > 0 \]
\[ p_2 = \text{ n is an int } < 0 \]
\[ p_3 = \text{ n is an int } = 0 \]
Proof Techniques - proof by cases

Suppose we want to prove a theorem of the form: \((p_1 \lor p_2 \lor ... \lor p_n) \rightarrow q\)

We can prove it in pieces corresponding to the cases, but which must be true?

A: \((p_1 \rightarrow q) \lor (p_2 \rightarrow q) \lor ... \lor (p_n \rightarrow q)\)

B: \((p_1 \rightarrow q) \land (p_2 \rightarrow q) \land ... \land (p_n \rightarrow q)\)
Ask the class

Suppose we want to prove a theorem of the form: \( p_1 \lor p_2 \lor \ldots \lor p_n \rightarrow q \)

We can prove it in pieces corresponding to the cases, but which must be true?

A: \( (p_1 \rightarrow q) \lor (p_2 \rightarrow q) \lor \ldots \lor (p_n \rightarrow q) \)

B: \( (p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \ldots \land (p_n \rightarrow q) \)

C: This class is not fun AND difficult. 😞
Proof Techniques - proof by cases

\[(p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \ldots \land (p_n \rightarrow q)\]

Proof for n=2:

\( (p_1 \lor p_2) \rightarrow q \equiv \neg (p_1 \lor p_2) \lor q \)  
\[\equiv (\neg p_1 \land \neg p_2) \lor q \]  
\[\equiv (\neg p_1 \lor q) \land (\neg p_2 \lor q) \]  
\[\equiv (p_1 \rightarrow q) \land (p_2 \rightarrow q) \]

Defn of →
DeMorgan’s
Distributivity
Defn of →
“if x is a perfect square, and x is even, then x is divisible by 4.”

Formally: \((p \land q) \rightarrow r\)

Contraposition: \(\neg r \rightarrow \neg (p \land q) \equiv \neg r \rightarrow (\neg p \lor \neg q)\)

Suppose x is not divisible by 4. How many cases needed?

Then \(x = 4k + 1\), or \(x = 4k + 2\), or \(x = 4k + 3\).

Now structure looks like \((u_1 \lor u_2 \lor u_3) \rightarrow (\neg p \lor \neg q)\)

Case 1 (&3): \(x = 4k + 1\), odd, corresponds to \(\neg q\)

Case 2: \(x = 4k + 2\), even, so we need to prove it is not a perfect square.
“if $x$ is a perfect square, and $x$ is even, then $x$ is divisible by 4.”

• Subgoal, prove Case 2:

• Case 2: $x = 4k + 2$, even (so we have to show not square).

  But $x = 4k+2 = 2(2k+1)$

  $x$ is the product of 2 and an odd number.
  Assume for sake of contradiction that $x$ is a perfect square
  Then $x = j^2$ for some integer $j$ and $x$ is even, then $j$ is even (Why?)
  Then $j = (2a)$ for some integer $a$ and $j^2 = (2a)^2(2a) = 2(2a^2)$. $x$ is
  the product of 2 and an even number! A contradiction!

• So, $x$ is not a perfect square.
Existence Proofs

Two ways of proving $\exists x \ P(x)$.

Either build one, or show one can be built.

Constructive

Non-constructive

Two examples, both involving $n!$

For the examples, think of $n!$ as a list of factors.
Quantifiers: Existence Proofs

Example: Prove that for all positive integers $n$, there exist $n$ consecutive composite integers.

$\forall n \ (\text{positive integers}), \ \exists x \ \text{so that} \ x, \ x+1, \ x+2, \ \ldots, \ x+n-1 \ \text{are all composite}.$

Proof: Let $n$ be an arbitrary integer.

$(n + 1)! + 2 \ \text{is divisible by} \ 2, \ \therefore \ \text{composite}.$

$(n + 1)! + 3 \ \text{is divisible by} \ 3, \ \therefore \ \text{composite}.$

$(n + 1)! + (n + 1) \ \text{is divisible by} \ n + 1, \ \therefore \ \text{composite}.$
Example: Prove that for all integers n, there exists a prime p so that p > n.

∀n (integer), ∃p so that p is prime, and p > n.

Proof: Let n be an arbitrary integer, and consider n! + 1. If (n! + 1) is prime, we are done since (n! + 1) > n. But what if (n! + 1) is composite?

If (n! + 1) is composite then it has a prime factorization, p_1p_2...p_n = (n! + 1)

Consider the smallest p_i, how small can it be?
Quantifiers: Existence Proofs

∀n (integers), ∃p so that p is prime, and p > n.

Proof: Let n be an arbitrary integer, and consider n! + 1. If (n! + 1) is prime, we are done since (n! + 1) > n. But what if (n! + 1) is composite?

• If (n! + 1) is composite then it has a prime factorization, p_1p_2...p_n = (n! + 1)

• Consider the smallest p_i, and call it p. How small can it be?

• So, p > n, and we are done. BUT WE DON’T KNOW WHAT p IS!!!
Another Example - Largest Prime Number

Prove by contradiction: There is no largest prime number; that is, there are infinitely many prime numbers.

Proof:
Suppose the given conclusion is false; that is, there is a largest prime number $p$. So the prime numbers we have are $2, 3, 5, ..., p$; assume there are $k$ such primes, $p_1, p_2, ..., p_k$.

Let $x$ denote the product of all of these prime numbers plus one:
$x = (2 \times 3 \times 5 \times ... \times p) + 1$. Clearly, $x > p$.

When $x$ is divided by each of the primes $2, 3, 5, ..., p$, we get 1 as the remainder. So $x$ is not divisible by any of the primes. Hence either $x$ must be a prime, or if $x$ is composite then it is divisible by a prime $q \neq p$. In either case, there are more than $k$ primes.

But this contradicts the assumption that there are $k$ primes, so our assumption is false. In other words, there is no largest prime number.

From Discrete Mathematics with Applications, by Thomas Koshy
Group Problem