First order Logic (Predicate Logic) and Methods of Proof
• Introduction

• Terminology:
  – Propositional functions; arguments; arity; universe of discourse

• Quantifiers
  – Definition; using, mixing, negating them
Consider the following argument: “Everyone who has green eyes is not to be trusted. Bill has green eyes. Therefore Bill is not to be trusted”

Is the argument valid? Can we capture this with propositional Logic?

Two propositions such as “Bill has green eyes” and “Jeff has green eyes” would have to be symbolized by $p$ and $q$. Through both propositions are about green eyes, there is no means to relate these propositions.

Propositional logic is Not that powerful enough to capture the above.

We need “First order logic” which is propositional logic + more!!!
Consider the statements:

\[ x > 3, \ x = y + 3, \ x + y = z \]

The symbols >, +, = denote relations between \( x \) and 3, \( x \), \( y \), and 4, and \( x \), \( y \), and \( z \), respectively.

These relations may hold or not hold depending on the values that \( x \), \( y \), and \( z \) may take.

A **predicate** is a property that is affirmed or denied about the subject (in logic, we say ‘variable’ or ‘argument’) of a statement.

Consider the statement : ‘\( x \) is greater than 3’

- ‘\( x \)’ is the subject
- ‘is greater than 3’ is the predicate
Propositional Functions (1)

• To write in Predicate Logic ‘$x$ is greater than 3’
  – We introduce a functional symbol for the **predicate** and
  – Put the subject as an **argument** (to the functional symbol): $P(x)$

• Terminology
  – $P(x)$ is a statement
  – $P$ is a predicate or propositional function
  – $x$ as an argument
Propositional Functions (2)

• Examples:
  – Father(x): unary predicate
  – Brother(x,y): binary predicate
  – Sum(x,y,z): ternary predicate
  – P(x,y,z,t): n-ary predicate
Propositional Functions (3)

- **Definition**: A statement of the form $P(x_1,x_2,\ldots, x_n)$ is the value of the propositional symbol $P$.
- **Here**: $(x_1,x_2,\ldots, x_n)$ is an $n$-tuple and $P$ is a predicate
- **We can think of a propositional function as a function that**
  - Evaluates to true or false
  - Takes one or more arguments
  - Expresses a predicate involving the argument(s)
  - Becomes a proposition when values are assigned to the arguments
Propositional Functions: Example

Let $Q(x,y,z)$ denote the statement ‘$x^2+y^2=z^2$’

– What is the truth value of $Q(3,4,5)$?  
  $Q(3,4,5)$ is true

– What is the truth value of $Q(2,2,3)$?  
  $Q(2,3,3)$ is false

– How many values of $(x,y,z)$ make the predicate true?  
  There are infinitely many values that make the proposition true, how many right triangles are there?
Consider the statement ‘$x > 3$’, does it make sense to assign to $x$ the value ‘blue’?

Intuitively, the **universe of discourse** is the set of all things we wish to talk about; that is the set of all objects that we can sensibly assign to a variable in a propositional function.

What would be the universe of discourse for the propositional function below be:

‘$x > 3$’
Universe of Discourse: Multivariate functions

• Each variable in an n-tuple (i.e., each argument) may have a different universe of discourse
• Consider an n-ary predicate $P$:
  \[ P(r,g,b,c) = \text{‘The rgb-values of the color c is (r,g,b)’} \]
• Example, what is the truth value of
  – $P(255,0,0,\text{red})$
  – $P(0,0,255,\text{green})$
• What are the universes of discourse of $(r,g,b,c)$?
Quantifiers: Introduction

- The statement ‘$x>3$’ is not a proposition
- It becomes a proposition
  - When we assign values to the argument: ‘4>3’ is false, ‘2<3’ is true, or
  - When we quantify the statement
- Two quantifiers
  - Universal quantifier $\forall$
    the proposition is true for all possible values in the universe of discourse
  - Existential quantifier $\exists$
    the proposition is true for some value(s) in the universe of discourse
• **Definition**: The universal quantification of a predicate $P(x)$ is the proposition ‘$P(x)$ is true for all values of $x$ in the universe of discourse.’ We use the notation: $\forall x \ P(x)$, which is read ‘for all $x$’.  

• If the universe of discourse is finite, say $\{n_1, n_2, \ldots, n_k\}$, then the universal quantifier is simply the conjunction of the propositions over all the elements

\[
\forall x \ P(x) \iff P(n_1) \land P(n_2) \land \ldots \land P(n_k)
\]
Universal Quantifier: Example 1

• Express the statements:
  – “Every MT student must take a discrete mathematics course.”
    \[ \forall x \ Q(x) \rightarrow P(x) \]
  – “Everybody must take a discrete mathematics course or be an MT student.”
    \[ \forall x \ ( P(x) \lor Q(x) ) \]
  – “Everybody must take a discrete mathematics course and be an MT student.”
    \[ \forall x \ ( P(x) \land Q(x) ) \]
Universal Quantifier: Example 2

- Express the statement: ‘for every $x$ and every $y$, $x+y>10$’
- Answer:
  - Let $P(x,y)$ be the statement $x+y>10$
  - Where the universe of discourse for $x$, $y$ is the set of integers
  - The statement is: $\forall x \; \forall y \; P(x,y)$
Existential Quantifier: Definition

- **Definition**: The existential quantification of a predicate $P(x)$ is the proposition ‘There exists a value $x$ in the universe of discourse such that $P(x)$ is true.’ We use the notation: $\exists x P(x)$, which is read ‘there exists $x$’.

- If the universe of discourse is finite, say $\{n_1, n_2, \ldots, n_k\}$, then the existential quantifier is simply the conjunction of the propositions over all the elements

$$\exists x P(x) \iff P(n_1) \lor P(n_2) \lor \ldots \lor P(n_k)$$
Existential Quantifier: Example 1

- Let $P(x,y)$ denote the statement ‘$x+y=5$’
- What does the expression $\exists x \ \exists y \ P(x,y)$ mean?
- Which universe(s) of discourse make it true?
Existential Quantifier: Example 2

• Express the statement: ‘there exists a real solution to $ax^2+bx-c=0$’

• Answer:
  – Let $P(x)$ be the statement $x= (-b\pm\sqrt{(b^2-4ac)})/2a$
  – Where the universe of discourse for $x$ is the set of real numbers.
    Note here that $a$, $b$, $c$ are fixed constants.
  – The statement can be expressed as $\exists x P(x)$

• What is the truth value of $\exists x P(x)$?
  – It is false. When $b^2<4ac$, there are no real number $x$ that can satisfy the predicate

• What can we do so that $\exists x P(x)$ is true?
  – Change the universe of discourse to the complex numbers, $\mathbb{C}$
In general, when are quantified statements true or false?

<table>
<thead>
<tr>
<th>Statement</th>
<th>True when...</th>
<th>False when...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\forall x \ P(x)$</td>
<td>$P(x)$ is true for every $x$</td>
<td>There is an $x$ for which $P(x)$ is false</td>
</tr>
<tr>
<td>$\exists x \ P(x)$</td>
<td>There is an $x$ for which $P(x)$ is true</td>
<td>$P(x)$ is false for every $x$</td>
</tr>
</tbody>
</table>
Existential and universal quantifiers can be used together to quantify a propositional predicate. For example:

$$\forall x \exists y P(x,y)$$

is perfectly valid

Alert:
- The quantifiers must be read from left to right
- The order of the quantifiers is important
- $$\forall x \exists y P(x,y)$$ is not equivalent to $$\exists y \forall x P(x,y)$$
Mixing quantifiers (2)

• Consider
  - \(\forall x \exists y \text{ Loves}(x,y)\): Everybody loves somebody
  - \(\exists y \forall x \text{ Loves}(x,y)\): There is someone loved by everyone

• The two expressions do not mean the same thing

• \((\exists y \forall x \text{ Loves}(x,y)) \rightarrow (\forall x \exists y \text{ Loves}(x,y))\) but the converse does not hold

• However, you can commute similar quantifiers
  - \(\forall x \forall y P(x,y)\) is equivalent to \(\forall y \forall x P(x,y)\) (thus, \(\forall x,y P(x,y)\))
  - \(\exists x \exists y P(x,y)\) is equivalent to \(\exists y \exists x P(x,y)\) (thus \(\exists x,y P(x,y)\))
Mixing Quantifiers: Truth values

<table>
<thead>
<tr>
<th>Statement</th>
<th>True when...</th>
<th>False when...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\forall x \forall y , P(x,y)$</td>
<td>$P(x,y)$ is true for every pair $x,y$</td>
<td>There is at least one pair $x,y$ for which $P(x,y)$ is false</td>
</tr>
<tr>
<td>$\forall x \exists y , P(x,y)$</td>
<td>For every $x$, there is a $y$ for which $P(x,y)$ is true</td>
<td>There is an $x$ for which $P(x,y)$ is false for every $y$</td>
</tr>
<tr>
<td>$\exists x \forall y , P(x,y)$</td>
<td>There is an $x$ for which $P(x,y)$ is true for every $y$</td>
<td>For every $x$, there is a $y$ for which $P(x,y)$ is false</td>
</tr>
<tr>
<td>$\exists x \exists y , P(x,y)$</td>
<td>There is at least one pair $x,y$ for which $P(x,y)$ is true</td>
<td>$P(x,y)$ is false for every pair $x,y$</td>
</tr>
</tbody>
</table>
• Express, in predicate logic, the statement that there is an infinite number of integers

• Answer:

  – Let $P(x, y)$ be the statement that $x < y$
  – Let the universe of discourse be the integers, $\mathbb{Z}$
  – The statement can be expressed by the following

    \[ \forall x \exists y \ P(x, y) \]
Express the *commutative law of addition* for $R$

We want to express that for every pair of reals, $x, y$, the following holds: $x + y = y + x$

Answer:

- Let $P(x, y)$ be the statement that $x + y$
- Let the universe of discourse be the reals, $R$
- The statement can be expressed by the following

$$\forall x \forall y \ (P(x, y) \iff P(y, x))$$

Alternatively, $\forall x \forall y \ (x + y = y + x)$
Mixing Quantifiers: Example (3)

• Express the multiplicative law for nonzero reals $R \setminus \{0\}$
• We want to express that for every real number $x$, there exists a real number $y$ such that $xy = 1$
• Answer: $\forall x \exists y (xy = 1)$
Does commutativity for substraction hold over the reals?
That is: does \( x-y = y-x \) for all pairs \( x, y \) in \( \mathbb{R} \)?
Express using quantifiers

\[ \forall x \forall y (x-y = y-x) \]
Mixing Quantifiers: Example (5)

• Express the statement as a logical expression: “There is a number $x$ such that when it is added to any number, the result is that number and if it is multiplied by any number, the result is $x$” as a logical expression

• Let $P(x,y)$ be the expression “$x+y=y$”

• Let $Q(x,y)$ be the expression “$xy=x$”

• The universe of discourse is $\mathbb{N},\mathbb{Z},\mathbb{R},\mathbb{Q}$ (but not $\mathbb{Z}^+$)

• Then the expression is:

$$\exists x \ \forall y \ P(x,y) \land Q(x,y)$$

Alternatively:

$$\exists x \ \forall y \ (x+y=y) \land (xy = x)$$
Binding Variables

• When a quantifier is used on a variable \( x \), we say that \( x \) is **bound**

• If no quantifier is used on a variable in a predicate statement, the variable is called **free**

• Examples
  – In \( \exists x \forall y P(x, y) \), both \( x \) and \( y \) are bound
  – In \( \forall x P(x, y) \), \( x \) is bound but \( y \) is free

• A statement is called a **well-formed formula**, when all variables are properly quantified
The set of all variables bound by a common quantifier is called the **scope** of the quantifier.

For example, in the expression $\exists x, y \forall z P(x, y, z, c)$

- What is the scope of existential quantifier?
- What is the scope of universal quantifier?
- What are the bound variables?
- What are the free variables?
- Is the expression a well-formed formula?
• We can use negation with quantified expressions as we used them with propositions

• **Lemma:** Let $P(x)$ be a predicate. Then the followings hold:

\[ \neg (\forall x \ P(x)) \equiv \exists x \ \neg P(x) \]
\[ \neg (\exists x \ P(x)) \equiv \forall x \ \neg P(x) \]

• This is essentially the quantified version of De Morgan’s Law (when the universe of discourse is finite, this is exactly De Morgan’s Law)
### Negation: Truth

#### Truth Values of Negated Quantifiers

<table>
<thead>
<tr>
<th>Statement</th>
<th>True when...</th>
<th>False when...</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\neg \exists x \ P(x) \equiv \forall x \ \neg P(x)$</td>
<td>$P(x)$ is false for every $x$</td>
<td>There is an $x$ for which $P(x)$ is true</td>
</tr>
<tr>
<td>$\neg \forall x \ P(x) \equiv \exists x \ \neg P(x)$</td>
<td>There is an $x$ for which $P(x)$ is false</td>
<td>$P(x)$ is true for every $x$</td>
</tr>
</tbody>
</table>
• Logic is more precise than English
• Transcribing English into Logic and vice versa can be tricky
• When writing statements with quantifiers, usually the correct meaning is conveyed with the following combinations:
  Use $\forall$ with $\Rightarrow$
  $\forall x \ Lion(x) \Rightarrow Fierce(x)$: Every lion is fierce
  $\forall x \ Lion(x) \land Fierce(x)$: Everyone is a lion and everyone is fierce
  Use $\exists$ with $\land$
  $\exists x \ Lion(x) \land Vegan(x)$: Holds when you have at least one vegan lion
  $\exists x \ Lion(x) \Rightarrow Vegan(x)$: Holds when you have vegan people in the universe of discourse (even though there is no vegan lion in the universe of discourse)
More exercises (1)

• Rewrite the following expression, pushing negation inward:

\[ \neg \forall x (\exists y \forall z P(x,y,z) \land \exists z \forall y P(x,y,z)) \]

• Answer:

\[ \exists x (\forall y \exists z \neg P(x,y,z) \lor \forall z \exists y \neg P(x,y,z)) \]
More Exercises (2)

- Let $P(x,y)$ denote ‘$x$ is a factor of $y$’ where
  - $x \in \{1,2,3,\ldots\}$ and $y \in \{2,3,4,\ldots\}$
- Let $Q(x,y)$ denote:
  - \( \forall x,y \ [P(x,y) \rightarrow (x=y) \lor (x=1)] \)
- Question: When is $Q(x,y)$ true?
Proofs with Quantifiers

- Rules of inference can be extended in a straightforward manner to quantified statements.
- **Universal Instantiation:** Given the premise that $\forall x P(x)$ and $c \in UoD$ (where $UoD$ is the universe of discourse), we conclude that $P(c)$ holds.
- **Universal Generalization:** Here, we select an arbitrary element in the universe of discourse $c \in UoD$ and show that $P(c)$ holds. We can therefore conclude that $\forall x P(x)$ holds.
- **Existential Instantiation:** Given the premise that $\exists x P(x)$ holds, we simply give it a name, $c$, and conclude that $P(c)$ holds.
- **Existential Generalization:** Conversely, we establish that $P(c)$ holds for a specific $c \in UoD$, then we can conclude that $\exists x P(x)$ holds.
Natural Deduction

Four more inference rules are introduced in predicate logic, apart from the ones discussed in propositional logic:

1) $\forall$ Introduction ($\forall$I)  
   \[
   \frac{F(x) \ {x \ arbitrary}}{\forall x \ F(x)}
   \]

2) $\forall$ Elimination ($\forall$E)  
   \[
   \frac{\forall x \ F(x)}{F(p) \ {p \ particular \ or \ arbitrary}}
   \]

3) $\exists$ Introduction ($\exists$I)  
   \[
   \frac{F(p) \ {p \ particular}}{\exists x \ F(x)}
   \]

4) $\exists$ Elimination ($\exists$E)  
   \[
   \frac{\exists x \ F(x) \ , \ F(x) \ |- \ A \ {x \ arbitrary}}{A}
   \]
Examples:

1. \( \exists x \ P(x) \rightarrow S \quad \vdash \quad \forall x \ ( P(x) \rightarrow S ) \)

   Sol.

   \[
   \begin{align*}
   P(x) \quad (x \text{ arbitrary}) & \quad \{EI\} \\
   \exists x P(x) & \quad \{EI\} \\
   P(x) \rightarrow \exists x P(x) & \quad \{EI\} \\
   \exists x P(x) \rightarrow S & \quad \{CIR\} \\
   \hline
   P(x) \rightarrow S \quad (x \text{ arbitrary}) & \quad \{\forall I\} \\
   \forall x (P(x) \rightarrow S) & \quad \{\forall I\}
   \end{align*}
   \]

2. \( S \rightarrow \forall x \ Q(x) \quad \vdash \quad \forall x \ ( S \rightarrow Q(x) ) \)

   Sol.

   \[
   \begin{align*}
   S & \quad \rightarrow E \\
   S \rightarrow \forall x Q(x) & \quad \{\forall E\} \\
   \forall x Q(x) & \quad \{\forall E\} \\
   Q(p) \quad (p \text{ arbitrary}) & \quad \{\forall E\} \\
   S \rightarrow Q(p) \quad (p \text{ arbitrary}) & \quad \{\rightarrow I\} \\
   S \rightarrow Q(p) \quad (p \text{ arbitrary}) & \quad \{\forall I\} \\
   \forall x (S \rightarrow Q(p)) & \quad \{\forall I\}
   \end{align*}
   \]
Proofs with Quantifiers: Example (1)

• Show that “A car in the garage has an engine problem” and “Every car in the garage has been sold” imply the conclusion “A car has been sold has an engine problem”

• Let
  – \( G(x) \): “\( x \) is in the garage”
  – \( E(x) \): “\( x \) has an engine problem”
  – \( S(x) \): “\( x \) has been sold”

• Let \( \text{UoD} \) be the set of all cars

• The premises are as follows:
  – \( \exists x \ (G(x) \land E(x)) \)
  – \( \forall x \ (G(x) \rightarrow S(x)) \)

• The conclusion we want to show is: \( \exists x \ (S(x) \land E(x)) \)
Proofs with Quantifiers: Example

1. \( \exists x \ (G(x) \land E(x)) \)
   \( 1^{st} \) premise

2. \( (G(c) \land E(c)) \)
   Existential instantiation of (1)

3. \( G(c) \)
   Simplification of (2)

4. \( \forall x \ (G(x) \to S(x)) \)
   \( 2^{nd} \) premise

5. \( G(c) \to S(c) \)
   Universal instantiation of (4)

6. \( S(c) \)
   Modus ponens on (3) and (5)

7. \( E(c) \)
   Simplification from (2)

8. \( S(c) \land E(c) \)
   Conjunction of (6) and (7)

9. \( \exists x \ (S(x) \land E(x)) \)
   Existential generalization of (8)

QED
Types of Proofs

- Trivial proofs
- Vacuous proofs
- Direct proofs
- Proof by Contrapositive (indirect proof)
- Proof by Contradiction (indirect proof, aka refutation)
- Proof by Cases (sometimes using WLOG)
- Proofs of equivalence
- Existence Proofs (Constructive & Nonconstructive)
- Uniqueness Proofs
Trivial Proofs (1)

- Conclusion holds without using the premise
- A trivial proof can be given when the conclusion is shown to be (always) true.
- That is, if $q$ is true, then $p \rightarrow q$ is true
- Examples
  - Prove ‘If $x > 0$ then $(x+1)^2 - 2x \geq x^2$’
Proof. It is easy to see:

\[(x+1)^2 - 2x\]

\[= (x^2 + 2x +1) -2x\]

\[= x^2 +1\]

\[\geq x^2\]

Note that the conclusion holds \textit{without} using the hypothesis.
Vacuous Proofs

• If the premise p is false
• Then the implication \( p \rightarrow q \) is always true
• A vacuous proof is a proof that relies on the fact that no element in the universe of discourse satisfies the premise (thus the statement exists in vacuum in the UoD).
• Example:
  – If \( x \) is a prime number divisible by 16, then \( x^2 < 0 \)
• No prime number is divisible by 16, thus this statement is true (counter-intuitive as it may be)
Most of the proofs we have seen so far are direct proofs.

In a direct proof:
- You assume the hypothesis $p$, and
- Give a direct series (sequence) of implications
- Using the rules of inference
- As well as other results (proved independently)
- To show that the conclusion $q$ holds.
Proof by Contrapositive (indirect proof)

• Recall that \((p \to q) \equiv (\neg q \to \neg p)\)
• This is the basis for the proof by contraposition
  – You assume that the conclusion is false, then
  – Give a series of implications to show that
  – Such an assumption implies that the premise is false
• Example
  – Prove that if \(x^3 < 0\) then \(x < 0\)
Proof by Contrapositive: Example

- The contrapositive is “if \( x \geq 0 \) then \( x^3 \geq 0 \)”
- Proof:
  1. If \( x = 0 \) \( \rightarrow \) \( x^3 = 0 \geq 0 \)
  2. If \( x > 0 \) \( \rightarrow \) \( x^2 > 0 \) \( \rightarrow \) \( x^3 > 0 \)

QED
Proof by Contradiction

• To prove a statement \( p \) is true
  – you may assume that it is false
  – And then proceed to show that such an assumption leads a contradiction with a known result

• In terms of logic, you show that
  – for a known result \( r \),
  – \((\neg p \rightarrow (r \land \neg r))\) is true
  – Which yields a contradiction \( c = (r \land \neg r) \) cannot hold

• Example: \( \sqrt{2} \) is an irrational number
Proof by Contradiction: Example

- Let $p$ be the proposition ‘$\sqrt{2}$ is an irrational number’
- Assume $\neg p$ holds, and show that it yields a contradiction
- $\sqrt{2}$ is rational

$$\sqrt{2} = \frac{a}{b}, \ a, b \in \mathbb{R} \text{ and } a, b \text{ have no common factor}$$ \hspace{1cm} \text{(proposition r)}

\text{Definition of rational numbers}

$$2 = \frac{a^2}{b^2}$$ \hspace{1cm} \text{Squaring the equation}

$$\rightarrow (2b^2 = a^2) \rightarrow (a^2 \text{ is even}) \rightarrow (a = 2c)$$ \hspace{1cm} \text{Algebra}

$$\rightarrow (2b^2 = 4c^2) \rightarrow (b^2 = 2c^2) \rightarrow (b \text{ is even})$$ \hspace{1cm} \text{Algebra}

$$\rightarrow (a, b \text{ are even}) \rightarrow (a, b \text{ have a common factor } 2) \rightarrow \neg r$$

$$\rightarrow (\neg p \rightarrow (r \land \neg r)), \text{ which is a contradiction}$$

So, $\neg p$ is false) $\rightarrow$ (p is true), which means $\sqrt{2}$ is irrational
Proof by Cases

• Sometimes it is easier to prove a theorem by
  – Breaking it down into cases and
  – Proving each one separately
• Example:
  – Let $n \in \mathbb{Z}$. Prove that $9n^2 + 3n - 2$ is even
Proof by Cases: Example

- Observe that $9n^2 + 3n - 2 = (3n+2)(3n-1)$
- $n$ is an integer $\rightarrow (3n+2)(3n-1)$ is the product of two integers
- **Case 1:** Assume $3n+2$ is even
  - $\rightarrow 9n^2 + 3n - 2$ is trivially even because it is the product of two integers, one of which is even
- **Case 2:** Assume $3n+2$ is odd
  - $\rightarrow 3n+2-3$ is even $\rightarrow 3n-1$ is even $\rightarrow 9n^2 + 3n - 2$ is even because one of its factors is even
Types of Proofs

• Trivial proofs
• Vacuous proofs
• Direct proofs
• Proof by Contrapositive (indirect proof)
• Proof by Contradiction (indirect proof, aka refutation)
• Proof by Cases (sometimes using WLOG)
• Proofs of equivalence
• Existence Proofs (Constructive & Nonconstructive)
• Uniqueness Proofs
Proofs By Equivalence (Iff)

• If you are asked to show an equivalence
  \[ p \leftrightarrow q \text{ “if an only if”} \]
• You must show an implication in both directions
• That is, you can show (independently or via the same technique) that
  \( (p \rightarrow q) \) and \( (q \rightarrow p) \)
• Example
  – Show that \( x \) is odd iff \( x^2+2x+1 \) is even
Example (iff)

$x$ is odd $\iff x = 2k + 1, \, k \in \mathbb{Z}$
$\iff x + 1 = 2k + 2$
$\iff x + 1 = 2(k + 1)$
$\iff x + 1$ is even
$\iff (x + 1)^2$ is even
$\iff x^2 + 2x + 1$ is even

by definition
algebra
factoring
by definition

Since $x$ is even iff $x^2$ is even

algebra

QED
Existence Proofs

• A **constructive existence proof** asserts a theorem by providing a specific, concrete example of a statement
  – Such a proof only proves a statement of the form $\exists x P(x)$ for some predicate $P$.
  – It does not prove the statement for all such $x$

• A **nonconstructive existence proof** also shows a statement of the form $\exists x P(x)$, but does not necessarily need to give a specific example $x$.
  – Such a proof usually proceeds by contradiction:
    • Assume that $\neg \exists x P(x) \equiv \forall x \neg P(x)$ holds
    • Then get a contradiction
Uniqueness Proofs

• A uniqueness proof is used to show that a certain element (specific or not) has a certain property.

• Such a proof usually has two parts

  1. A proof of existence: $\exists x P(x)$
  2. A proof of uniqueness: if $x \neq y$ then $\neg P(y)$

• Together we have the following:

  $$\exists x ( P(x) \land (\forall y (x \neq y \rightarrow \neg P(y))))$$
Counter Examples

- Sometimes you are asked to **disprove** a statement.
- In such a situation you are actually trying to prove the **negation** of the statement.
- With statements of the form $\forall x \ P(x)$, it suffices to give a **counter example**
  - because the existence of an element $x$ for which $\neg P(x)$ holds proves that $\exists x \ \neg P(x)$
  - which is the negation of $\forall x \ P(x)$
Counter Examples: Example

• Example: Disprove $n^2+n+1$ is a prime number for all $n \geq 1$
• A simple counterexample is $n=4$.
• In fact: for $n=4$, we have

\[
 n^2+n+1 = 4^2+4+1 \\
 = 16+4+1 \\
 = 21 = 3 \times 7 , \text{ which is clearly not prime } \quad \text{QED}
\]