Proofs of Conditional Statements

• Many theorems have the form:
  – *For all* $x$, $H(x) \rightarrow C(x)$

• The cube of every negative real number is negative.
  – For all $x$, $(x^3 < 0) \rightarrow (x < 0)$
  – Domain: set of real numbers.

• If $x^2$ is an odd integer, then $x$ is also an odd integer.
  – For all $x$, $(x^2$ is odd) $\rightarrow$ (x is odd)
  – Domain: set of integers.
Ways to prove conditional statements

• *Prove*: $\forall x \ H(x) \rightarrow C(x)$

• Direct proof
  – Name a generic element $x$ in the domain that satisfies $H(x)$
  – Prove that $C(x)$ is also true

• Implicitly uses universal instantiation.
Ways to prove conditional statements

• **Prove:** \( \forall x \ H(x) \rightarrow C(x) \)
• Proof by contrapositive
  – Name a generic element \( x \) in the domain such that \( C(x) \) is false
  – Prove that \( H(x) \) is also false
  – At the beginning of the proof, state what you are assuming (\( C(x) \) is false) and state what you will prove (\( H(x) \) is false).

• **Proofs by contrapositive work because:**
  – \( \forall x \ H(x) \rightarrow C(x) \) is logically equivalent to
    \[ \forall x \ \neg C(x) \rightarrow \neg H(x) \]
Direct proof example

- **Theorem**: The cube of every even integer is even.
- **Proof**:
  - Let $x$ be an even integer.
  - We will show that $x^3$ is also even.
  - Then $x = 2k$ for some integer $k$.
  - Cube both sides of the equation to get:
    - $x^3 = (2k)^3 = 2^3k^3 = 8k^3 = 2(4k^3)$
  - $4k^3$ is an integer, so $x^3$ can be expressed as 2 times an integer, and therefore $x^3$ is even.
Direct proof example

• Theorem: The product of two rational numbers is rational.
• Proof:
  – Let $x$ and $y$ be rational numbers.
  – We will show that $xy$ is also rational.
  – Then $x = \frac{a}{b}$ and $y = \frac{c}{d}$, where $a, b, c, d$ are integers and $b \neq 0$ and $d \neq 0$.
  – Multiply $x$ and $y$ to get:
    • $xy = \left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \left(\frac{ac}{bd}\right)$
  – $ac$ and $bd$ are both integers. Also $bd \neq 0$ because $b \neq 0$ and $d \neq 0$.
  – Therefore $xy$ is the ratio of two integers with a non-zero denominator which means that $xy$ is rational.
Proof by contrapositive example.

• Theorem: If $n$ is an integer and $3n+7$ is odd then $n$ is even.

• Proof:
  – Let $n$ be an arbitrary integer such that $n$ is odd.
  – We will show that $3n+7$ is even.
  – $n = 2k+1$, for some integer $k$.
  – Plug in the expression $n=2k+1$ into $3n+7$
    • $3n+7 = 3(2k+1)+7 = 6k+3+7 = 6k+10 = 2(3k+5)$
  – Since $k$ is an integer, then $3k+5$ is also an integer. Therefore $3n+7$ can be expressed as 2 times an integer and therefore $3n+7$ is even.
Proof by contrapositive example.

• Theorem: If $x$ is a real number such that $3x$ irrational then $x$ is irrational.

• Before we start:
  – Every real number is rational or irrational.
  – A real number is rational if it can not be expressed as the ratio of two integers.
Proof by contrapositive example.

• Theorem: If $x$ is a real number such that $3x$ irrational then $x$ is irrational.
• Proof
  – Assume that $x$ is a real number and that $x$ is not irrational.
  – Will show that $3x$ is rational and therefore not irrational.
  – Since $x$ is real and not irrational, then it is rational.
  – $x = \frac{a}{b}$, where $b \neq 0$.
  – Therefore $3x = 3 \frac{a}{b} = \frac{3a}{b}$.
  – Since $a$ is an integer $3a$, is also an integer. Furthermore $b \neq 0$. Therefore $3x$ can be expressed as the ratio of two integers with a non-zero denominator which means that $3x$ is rational.
<table>
<thead>
<tr>
<th>Idempotent laws:</th>
<th>( p \lor p \equiv p )</th>
<th>( p \land p \equiv p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associative laws:</td>
<td>(( p \lor q ) \lor r \equiv p \lor ( q \lor r ))</td>
<td>(( p \land q ) \land r \equiv p \land ( q \land r ))</td>
</tr>
<tr>
<td>Commutative laws:</td>
<td>( p \lor q \equiv q \lor p )</td>
<td>( p \land q \equiv q \land p )</td>
</tr>
<tr>
<td>Distributive laws:</td>
<td>( p \lor ( q \land r ) \equiv ( p \lor q ) \land ( p \lor r ) )</td>
<td>( p \land ( q \lor r ) \equiv ( p \land q ) \lor ( p \land r ) )</td>
</tr>
<tr>
<td>Identity laws:</td>
<td>( p \lor F \equiv p )</td>
<td>( p \land F \equiv F )</td>
</tr>
<tr>
<td></td>
<td>( p \lor T \equiv T )</td>
<td>( p \land T \equiv p )</td>
</tr>
<tr>
<td>Involution law:</td>
<td>( \neg \neg p \equiv p )</td>
<td></td>
</tr>
<tr>
<td>Complement laws:</td>
<td>( p \lor \neg p \equiv T )</td>
<td>( p \land \neg p \equiv F )</td>
</tr>
<tr>
<td></td>
<td>( \neg T \equiv F )</td>
<td>( \neg F \equiv T )</td>
</tr>
<tr>
<td>De Morgan's laws:</td>
<td>( \neg ( p \lor q ) \equiv \neg p \land \neg q )</td>
<td>( \neg ( p \land q ) \equiv \neg p \lor \neg q )</td>
</tr>
<tr>
<td>Conditional identities:</td>
<td>( p \rightarrow q \equiv \neg p \lor q )</td>
<td>( p \leftrightarrow q \equiv ( p \rightarrow q ) \land ( q \rightarrow p ) )</td>
</tr>
</tbody>
</table>