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, ($x^3 < 0$) → ($x < 0$)
      - 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) → (x is odd)
      - Domain: set of integers.

Ways to prove conditional statements

- $Prove\colon \forall x\ H(x) \to C(x)$
- 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 = a/b and y = c/d, where a,b,c,d are integers and b ≠ 0 and d ≠ 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 ≠ 0 because b ≠ 0 and d ≠ 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. Therefire 3n+7 can be expressed as 2 times and 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 ≠ 0.
  - Therefore 3x = $3\frac{a}{b} = \frac{3a}{b}$.
  - Since a is an integer 3a, is also an integer. Furthermore b ≠ 0. Therefore 3x can be expressed as the ratio of two integers with a non-zero denominator which means that 3x is rational.

Idempotent laws:	$p \lor p \equiv p$	$p \land p \equiv p$
Associative laws:	$(p \lor q) \lor r \equiv p \lor (q \lor r)$	$(p \land q) \land r \equiv p \land (q \land r)$
Commutative laws:	$p \lor q \equiv q \lor p$	$p \land q \equiv q \land p$
Distributive laws:	$p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$	$p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$
Identity laws:	$p \lor F \equiv p$ $p \lor T \equiv T$	$p \land F \equiv F$ $p \land T \equiv p$
Involution law:	$\neg\neg p \equiv p$	
Complement laws:	$p \lor \neg p \equiv T$ $\neg T \equiv F$	$p \land \neg p \equiv F$ $\neg F \equiv T$
De Morgan's laws:	$\neg(p \lor q) \equiv \neg p \land \neg q$	$\neg(p \land q) \equiv \neg p \lor \neg q$
Conditional identities:	$p \rightarrow q \equiv \neg p \lor q$	$p \leftrightarrow q \equiv (p \rightarrow q) \land (q \rightarrow p)$