Logic and types of proofs

Theory

- A **proposition** is a statement that is either true of false.

Let p and q be propositions. Then:

- The **negation** of p, denoted by $\neg p$, is the proposition "not p".
- The **conjunction** of p and q, denoted by $p \wedge q$, is the proposition "p and q".
- The **disjunction** of p and q, denoted by $p \vee q$, is the proposition "p or q".
- The **exclusive or** of p and q, denoted by $p \oplus q$, is the proposition "either p or q but not both".
- The **implication** of p and q, denoted by $p \to q$, is the proposition that is false when p is true and q is false and true otherwise.
- The **biconditional** of p and q, denoted by $p \leftrightarrow q$, is the proposition that is true when p and q have the same truth values and is false otherwise.

The truth table

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \to q$	$p \leftrightarrow q$
T	T	F	T	T	F	T	T
T	F	F	F	T	T	F	F
F	T	T	F	T	T	T	F
F	F	T	F	F	F	T	T

- A compound proposition that is always true, no matter what the truth values of the propositions that occur in it, is called a **tautology**.
  Example. $p \vee \neg p$ is a tautology.
- A compound proposition that is always false is called a **contradiction**.
  Example. $p \wedge \neg p$ is a contradiction.
- The propositions p and q are called **logically equivalent** if $p \leftrightarrow q$ is a tautology. The notation $p \Leftrightarrow q$ denotes that p and q are logically equivalent.

Example. Show that $\neg(p \vee q)$ and $(\neg p) \wedge (\neg q)$ are logically equivalent, i.e. "not (p or q) " is the same as "(not p) and (not q)".

Solution. Construct the truth table:

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$(\neg p) \wedge (\neg q)$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

- A statement $P(x)$ that depends on the value of a variable (x in this case) is called a **propositional function**. Once a value has been assigned to the variable x, the statement $P(x)$ becomes a proposition and has a truth value. For example, if $P(x)$ is the statement "$x > 3$", then $P(4)$ is true and $P(2)$ is false.
- $\forall x P(x)$ means "for every x, $P(x)$ is true".
- $\exists x P(x)$ means "there exists x such that $P(x)$ is true".
- $\exists! x P(x)$ means "there exists a unique x such that $P(x)$ is true".

Types of proofs.

Suppose we want to prove an implication "if p then q".

- a **direct** proof just shows how q follows from p.
- a proof **by contradiction** assumes that p and $\neg q$ are true, and derives a contradiction.
- a proof **by contrapositive** shows that $\neg q$ implies $\neg p$.

A proof of a statement of the form "$\exists x P(x)$" can be

- **constructive** - when you construct such an x explicitly, or
- **existential**, or **nonconstructive** - when you show the existence of such an x without actually constructing it.

To prove a statement of the form "$\forall x P(x)$" where the domain of x is a subset of integer numbers, it is often (but not always!) a good idea to use Mathematical Induction.

To prove a statement of the form "$p \leftrightarrow q$", you can either

- prove $p \rightarrow q$ and $q \rightarrow p$ separately, or
- have each step of your proof of the form "if and only if".

To disprove a statement (that is, to show that it is false), it is sufficient to show that there exists at least one **counterexample** (that is, there exists at least one case when the statement does not hold).

Examples

1. Prove that every odd integer is the difference of two perfect squares.

direct proof: An odd integer has the form $2n+1$.
$2n+1 = (n+1)^2 - n^2$.

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

proof by contradiction: Suppose $\sqrt{2}$ is rational. Then there exists an irreducible fraction $\frac{p}{q} = \sqrt{2}$. (Irreducible means that the greatest common divisor of p and q is 1.)
Then
$\frac{p^2}{q^2} = 2$
$p^2 = 2q^2$
Then p^2 is even, so p is even. Let $p = 2m$, then $p = 4m^2$.
We have $4m^2 = 2q^2$
$2m^2 = q^2$
Now q is even. We get a contradiction because we have that on the one hand, p and q have the greatest common divisor 1, but on the other hand p and q are both even.

3. Prove that if a and b are integers and ab is even, then either a or b is even (or both).

proof by contrapositive: Suppose that neither a nor b is even, and we will prove that ab is not even. I.e. we suppose that both a and b are odd, and we will prove that ab is odd.
$ab = (2n+1)(2m+1) = 4nm + 2n + 2m + 1 = 2(2nm + n + m) + 1$ is an odd number.

4. Prove that for every positive integer n there exist n consecutive composite numbers.

constructive proof: We claim that $(n+1)!+2$, $(n+1)!+3$, ... , $(n+1)!+(n+1)$ are all composite. $(n+1)!$ is divisible by 2, by 3, ... , and by $n+1$. Therefore $(n+1)!+2$ is divisible by 2, $(n+1)!+3$ is divisible by 3, ... , $(n+1)!+(n+1)$ is divisible by $n+1$.

5. Prove that $x^3 + x - 1 = 0$ has a real root.

nonconstructive proof: Let $f(x) = x^3 + x - 1$. Then $f(-1) = -3 < 0$ and $f(1) = 1 > 0$. By the Intermediate Value Theorem, there exists c between -1 and 1 such that $f(c) = 0$.

6. Prove or disprove that every odd integer is prime.

counterexample: 9 is odd but not prime. Thus the statement is false.