1.2 Methods of proof

Reading: Rosen 1.5 – 1.7

A proof is a sequence of statements, where each statement is a given condition or a conclusion obtained from previous statements by some rules of inference.

The following table summarizes the rules of inference to use to create a proof, where statements 1 and 2 are given conditions and statement 3 is the new conclusion obtained by inference.

statement 1	p	$\neg q$	$p \to q$	$p \vee q$	p	$p \wedge q$	p	$p \vee q$
statement 2	$p \to q$	$p \to q$	$q \to r$	$\neg p$			q	$\neg p \vee r$
statement 3	q	$\neg p$	$p \to r$	q	$p \vee q$	p	$p \wedge q$	$q \vee r$

- Direct proof: To prove "if p then q", assume p is true and show that q is true.

  Example: Prove that if m and n are odd numbers, so is mn.

  Proof: Since m and n are odd numbers, then by the definition of odd numbers, m can be written as $m = 2a+1$ for some integer a, and n written as $n = 2b+1$ for some integer b. Then $mn = (2a+1)(2b+1) = 4ab+2a+2b+1 = 2(2ab+a+b)+1$. Since $mn = 2c+1$, where $c = 2ab+a+b$ is an integer, then by the definition of odd numbers, mn is an odd number.

- Proof by contraposition: To prove "if p then q", assume q is false and show p is false. This method is established on top of the equivalence of $p \to q$ and $\neg q \to \neg p$.

  Example: Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

  Proof: Assume the opposite is true, i.e., $a > \sqrt{n}$ and $b > \sqrt{n}$. Then $ab > \sqrt{n} \cdot \sqrt{n} = n$. So $n \neq ab$, which contradicts the given condition $n = ab$.

- Proof by contradiction: To prove "p", assume p is false and show there is r such that r is true and $\neg r$ is true, a contradiction. This method is based on the equivalence of p and $\neg p \to (r \wedge \neg r)$.

  Example: Prove that $\sqrt{2}$ is an irrational number.

  Proof: Assume $\sqrt{2}$ is not irrational, thus is rational. Then by the definition of rational numbers, there are two integers a and b with $gcd(a,b) = 1$ such that $\sqrt{2} = \frac{a}{b}$. Squaring both sides of the equation, we get $2 = \frac{a^2}{b^2}$, thus $2b^2 = a^2$. So a must be an even number, or $a = 2c$ for some integer c. Then the equation $2b^2 = a^2$ becomes $2b^2 = (2c)^2 = 4c^2$, thus $b^2 = 2c^2$. Since b^2 is an even number, b must be an even number. So both a and b are even, thus $gcd(a,b) \neq 1$. A contradiction to $gcd(a,b) = 1$.

  Note: The difference between contraposition and contradiction is subtle. In doing proofs, people usually don't distinguish the two methods, and call both "proof by contradiction".

- Proof by cases: When we are unable to prove a theorem with a single argument that hold for all possible cases, we may need to construct our proof for each of the possible cases, one by one. The rule of inference behind this method lies in the equivalence of $(p_1 \vee p_2 \vee \cdots \vee p_n) \to q$ and $(p_1 \to q) \wedge (p_2 \to q) \wedge \cdots \wedge (p_n \to q)$.

  Example: Show that $|x \cdot y| = |x| \cdot |y|$.

  Proof: We consider the following cases:

  (1) $x \geq 0$ and $y \geq 0$: $|x \cdot y| = x \cdot y = |x| \cdot |y|$.

  (2) $x \geq 0$ and $y < 0$: $|x \cdot y| = -x \cdot y = x \cdot (-y) = |x| \cdot |y|$.

  (3) $x < 0$ and $y \geq 0$: $x \cdot y| = -x \cdot y = (-x) \cdot y = |x| \cdot |y|$.

  (4) $x < 0$ and $y < 0$: $|x \cdot y| = x \cdot y = (-x) \cdot (-y) = |x| \cdot |y|$.

  Example: Show that there are no integer solutions to equation $x^2 + 3y^2 = 8$.

  Proof: Observing the equation, we get $x^2 \leq 8$ and $3y^2 \leq 8$. Since x and y are integers, then $x = 0, \pm 1, \pm 2$ and $y = 0, \pm 1$. This leaves us with only 5×3 possible combinations of x and y to check.

- Existence proof: To prove there exists an object of a certain type, we can simply construct one. This is the constructive existence proof. It is also possible to give a existence proof that is nonconstructive. Sometimes a nonconstructive existence proof uses proof by contradiction.

Example: Prove that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Proof: $1729 = 10^3 + 9^3 = 12^3 + 1^3$.

Example: Prove that there exist irrational numbers x and y such that x^y is rational.

Proof: Consider the irrational number $\sqrt{2}$ and make a number $z = \sqrt{2}^{\sqrt{2}}$. If z is a rational number, then we have found x and y. However, if z is irrational, then let $x = z$ and $y = \sqrt{2}$ so that $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$, a rational!

- Proof by induction: To prove that predicate $P(n)$ is true for all $n \geq 1$, prove that (1) $P(1)$ is true and (2) $\forall k(P(k) \rightarrow P(k+1))$ is true.

  Example: Prove that $1 + 2 + \cdots + n = \frac{1}{2}n(n+1)$ for all $n \geq 1$.

  Proof: Let $P(n)$ be $1 + 2 + \cdots + n = \frac{1}{2}n(n+1)$. We induct on n.

  Basis step: $P(1)$ is obviously true, because $1 = \frac{1}{2} \cdot 1 \cdot (1+1)$.

  Inductive step: Assume $P(k)$ is true, i.e., $1 + 2 + \cdots + k = \frac{1}{2}k(k+1)$. We will show that $P(k+1)$ is also true, i.e., $1 + 2 + \cdots + (k+1) = \frac{1}{2}(k+1)(k+2)$.

$$\begin{aligned} 1 + 2 + \cdots + (k+1) &= (1 + 2 + \cdots + k) + (k+1) \\ &= \frac{1}{2}k(k+1) + (k+1) \\ &= \frac{1}{2}(k+1)(k+2) \end{aligned}$$

  Note: We will revisit the method of induction when we study recursion.