Recall proof by cases and proof by contradiction

**Direct proof**: $H_1 \land H_2 \land ... \land H_n \Rightarrow C$  
Most natural, and quite common form.

Two types of *indirect proof* use the negation of the Conclusion

**Proof of the contrapositive**: $\neg C \Rightarrow \neg (H_1 \land H_2 \land ... \land H_n )$

**EXAMPLE 1** Let $m, n \in \mathbb{N}$. If $m+n \geq 73$, then $m \geq 37$ or $n \geq 37$. Prove contrapositive.

**EXAMPLE 2** To show a function $f: S \rightarrow T$ is one-to-one, show $s_1 \neq s_2 \Rightarrow f(s_1) \neq f(s_2)$  
Or prove contrapositive.

**Proof by contradiction** $H_1 \land H_2 \land ... \land H_n \land \neg C \Rightarrow$ a contradiction

**EXAMPLE 3** Prove $\sqrt{2}$ is not rational.

**EXAMPLE 4** Cannot show that $\sqrt{4}$ is not rational.

**EXAMPLE 5**. An *artificial proof* that the sum of two odd numbers is an even number.

**EXAMPLE 6**. A *natural* proof of the contrapositive of “If $x^2$ is irrational, then $x$ is irrational.”

**Proof by cases** is natural for $H_1 \lor H_2 \lor ... \lor H_n \Rightarrow C$

**EXAMPLE 7** $|x+y| \leq |x| + |y|$ for $x, y \in \mathbb{R}$ [Six cases, including two trivial cases.]

**EXAMPLE 8** For every $n \in \mathbb{N}$, $n^3 + n$ is even.

$P \Rightarrow Q$ is **vacuously true** or **true by default** if $P$ is false. Often arises in a proof by cases.

**EXAMPLE 9**. (b) $n \geq 4m^2$ implies $n^m < 2^n$. [proved on page 147, on Big-Oh] is **vacuously true** for $n = 0, ..., 4m^2 - 1$. Consider $n = 10$ and $m = 2$, $Q$ is true; but $n = 10$ and $m = 4$, $Q$ is false.

$P \Rightarrow Q$ is **trivially true** if $Q$ is true.

**EXAMPLE 10** If $xy = 0$, then $(x + y)^n = x^n + y^n$ for $n \in \mathbb{P}$. **Trivially true** when $n = 1$

“Existence proof” *styles* are either **constructive** or **nonconstructive**.

A constructive proof either specifies the object or gives an explicit algorithm for determining it.

A nonconstructive proof uses indirect means to establish merely the existence.

**EXAMPLE 11** Proof that there are an infinite number of primes is generally nonconstructive.

**EXAMPLE 12** If the image of an infinite sequence is a finite set $S$, then some $x$ in $S$ is the value of infinitely many terms in the sequence. Etc. [Nonconstructive.]

**EXAMPLE 13** Every positive integer $n$ has the form $2^k m$ for odd integer $m$. [Constructive.]
**MAT251 Examples of proof styles**

**Theorem A:** \((m+n \geq 5) \Rightarrow m \geq 3 \text{ or } n \geq 3 \text{ for } m, n \in \mathbb{N}.

If \(m < 3\) and \(n < 3\) for \(m, n \in \mathbb{N}\) then \(0 \leq m \leq 2\) and \(0 \leq n \leq 2\).

Hence \(0 \leq m+n \leq 4\) by inequality addition; and \(4 < 5\), so \(m+n < 5\).

**Theorem B:** \(\sqrt{5}\) is not a rational number.

If \(\sqrt{5}\) does equal \(p/q\) (where \(p, q\) are integers with no common factors) then \(5 = p^2/q^2\).

Thus \(5q^2 = p^2\). Now by the unique factorization into primes, \(q^2\) has an **even** number of the prime factor 5; and \(p^2\) does also. However \(5q^2 = p^2\) implies that \(p^2\) has an **odd** number of such factors. There **cannot** be an **even** number and an **odd** number of the factor 5 in \(p^2\).

So a rational number cannot equal \(\sqrt{5}\).

**Theorem C:** \(|x + y| \leq |x| + |y|\) for \(x, y \in \mathbb{R}\).

1. If \(x\) and \(y\) are both positive, then \(|x+y| = x+y = |x|+|y|\), so result is true.

2. If \(x\) is negative and \(y\) is positive,
   then \(-|x| = x < 0 < -x = |x|\) \text{ and } \(-|y| = -y < 0 < y = |y|\);
   that is, \(-|x| = x < |x|\) and \(-|y| < y = |y|\). Adding these terms respectively gives:
   \((-|x|)+(-|y|) < x+y < |x|+|y|)\; \text{ that is }\; -(x+y) < x+y < (x+y); \text{ so }|x+y| < (|x|+|y|).

3. If \(x\) and \(y\) are both negative, then \(|x+y| = -(x+y) = (-x)+(-y) = |x|+|y|\), so result is true.

4. If \(x\) is positive and \(y\) is negative, the case is symmetric to case 2, so result is true.

5. If \(x = 0\), then \(|x+y| = |y| = 0 + |y| = |x| + |y|\), so result is true.

6. If \(y = 0\), the case is symmetric to case 5, so result is true.

**Theorem D:** \(n \in \mathbb{N}\) and \(n \geq 4m^2 \Rightarrow n^m < 2^n\) for any positive **constant** \(m\).

The theorem is **vacuously** true for \(n = 0, 1, 2, 3, ..., 4m^2 - 1\).

The **direct** proof for \(n \geq 4m^2\) is given on page 146 in the text.

**Theorem E:** \(\langle (x, y \in \mathbb{R}) \land (xy = 0) \rangle \Rightarrow (x+y)^n = x^n + y^n\) for \(n \geq 1\).

The theorem is **trivially** true for \(n = 1\), whether or not \(xy = 0\).

Another direct proof method [attributed to J. A. Robinson, 1965*] is **proof by resolution**:
If \(p \lor q\) and \(\neg p \lor r\) are both true, then \(q \lor r\) is true. Note that the hypotheses and conclusion are in form of disjoined terms.

**Theorem F:** [(\(p \lor q\)) \land (\(\neg p \lor r\)) \land (\(\neg r \lor s\))] \Rightarrow q \lor s

\((p \lor q)\) and \((\neg p \lor r)\) imply \(q \lor r\). Now this is equivalent to \(r \lor q\).

\((r \lor q)\) and \((\neg r \lor s)\) imply \(q \lor s\). This is the desired conclusion.

A special case of proof by resolution is: If \(p \lor q\) and \(\neg p\) are both true, then \(q\) is true.

---

Methods of proof

Direct proof uses one or more hypotheses to yield a conclusion: $H_1 \land H_2 \land \ldots \land H_n \Rightarrow C$

Simple deduction is the most natural and quite common form.

Theorem. The sum of 3 consecutive natural numbers is a multiple of 3.

Proof by cases is natural for $H_1 \lor H_2 \lor \ldots \lor H_n \Rightarrow C$

Theorem. $|x + y| \leq |x| + |y|$ for $x, y$ in $\mathbb{R}$, can be proved by considering 4 cases.

Proof by induction is natural when a theorem refers to an infinite sequence of statements.

Theorem E: $(x, y \in \mathbb{R}) \land (xy = 0) \Rightarrow (x+y)^n = x^n + y^n$ for $n \geq 1$.

Proof by resolution is a direct proof method: If $p \lor q$ and $\neg p \lor r$ are both true, then $q \lor r$ is true.

Note that the hypotheses and conclusion are disjunctions.

Two types of indirect proof use the negation of the Conclusion, but in different ways.

Proof of the contrapositive: $\neg C \Rightarrow \neg (H_1 \land H_2 \land \ldots \land H_n)$

Theorem. $(m+n \geq 5) \Rightarrow m \geq 3 \text{ or } n \geq 3$ for $m, n \in \mathbb{N}$.

Proof by contradiction $H_1 \land H_2 \land \ldots \land H_n \land \neg C \Rightarrow$ a contradiction

Theorem. $\sqrt{5}$ is not a rational number.

Special arguments of logic:

$P \Rightarrow Q$ is vacuously true or true by default if $P$ is false. [Often arises in a proof by cases.]

Theorem. “If $n > 4$, then $n^2 < 2^n$”, is vacuously true for $n = 3$.

$P \Rightarrow Q$ is trivially true if $Q$ is true.

Theorem E is trivially true when $n = 1$, whether or not $xy = 0$.

“Existence proof” styles are either constructive or nonconstructive.

A constructive proof specifies the object or gives an explicit algorithm for determining it.

Prove that every positive integer $n$ has the form $2^k m$ for odd integer $m$ by algorithm.

A nonconstructive proof uses indirect means to establish merely the existence.

Proof that there are an infinite number of primes is generally nonconstructive.
Exercises 2.4 page 76

1. Prove or disprove the following:
   a) The sum of two even integers is an even integer.
      **Direct:** If \( m = 2k \) and \( n = 2l \), then \( m + n = 2k + 2l = 2(k + l) \), an even integer.
   b) The sum of three odd integers is an odd integer.
      **Direct:** If \( l = 2i + 1 \) and \( m = 2j + 1 \) and \( n = 2k + 1 \), then \( l + m + n = 2i+1+2j+1+2k+1= 2(i+j+k+1)+1. \)
   c) “The sum of two primes is never a prime” is false. Counterexample: 2+3=5.

2. Prove that \( \sqrt{2} \) is irrational. [Proof by contradiction.]
   If \( \sqrt{2} = \frac{p}{q} \), in lowest terms, then \( 3q^2 = p^2 \). This equation shows \( p^2 \) has both an odd and an even number of the prime factor 3. This contradiction means \( \sqrt{2} \) cannot be rational.

3. Prove or disprove the following:
   a) The sum of 3 consecutive integers is divisible by 3.
      **Direct:** We see that \( n + (n + 1) + (n + 2) = 3n + 3 = 3(n + 1). \)
   b) The sum of 4 consecutive integers is not divisible by 4. Counterexample: 1+2+3+4=10 not = 4 \( k \).
   c) The sum of 5 consecutive integers is divisible by 5.
      **Direct:** We see that \( n + (n + 1) + (n + 2) + (n + 3) + (n + 4) = 5n + 10 = 5(n + 2). \)

4. Prove that \( \sqrt[3]{3} \) is irrational. [Proof by contradiction.]
   If \( \sqrt[3]{3} = \frac{p}{q} \), in lowest terms, then \( 2q^3 = p^3 \). This equation shows \( p^3 \) has 2 as a factor both 3\( k \) times and 3\( l+1 \) times. Since 3\( k \) cannot equal 3\( l+1 \), the contradiction means \( \sqrt[3]{3} \) cannot be rational.

5. Prove that \( |x y| = |x||y| \) for real \( x \) and \( y \). [Proof by cases.]
   The cases may be represented by four quadrants and the two axes:
   - Quad 1: If \( x > 0 \) and \( y > 0 \), then \( x y > 0 \), so \( |x y| = x y = |x||y| \).
   - Quad 2: If \( x < 0 \) and \( y > 0 \), then \( x y < 0 \), so \( |x y| = -(x y) = (-x)y = |x||y| \).
   - Quad 3: If \( x < 0 \) and \( y < 0 \), then \( x y > 0 \), so \( |x y| = x y = (-x)(-y) = |x||y| \).
   - Quad 4: If \( x > 0 \) and \( y < 0 \), then \( x y < 0 \), so \( |x y| = -(x y) = x(-y) = |x||y| \).
   - y-axis: If \( x = 0 \), then \( x y = 0 \), so \( |x y| = 0 = |0||y| = |x||y| \).
   - x-axis: If \( y = 0 \), then \( x y = 0 \), so \( |x y| = 0 = |x|0 = |x||y| \).

6. Prove: If \( x \) and \( y \) are real numbers, and \( x y = 0 \), the \( (x + y)^n = x^n + y^n \) for positive integer \( n \). [Proof by cases.] We know that \( x y = 0 \) logically implies \( x = 0 \) or \( y = 0 \).
   - If \( x = 0 \), then \( (x + y)^n = (0 + y)^n = (y)^n = 0 + y^n = x^n + y^n \).
   - If \( y = 0 \), then use the above argument with \( x \) and \( y \) switched.