Continued....

$$p \to q \equiv \neg p \vee q$$
$$p \to q \equiv \neg q \to \neg p$$
$$p \vee q \equiv \neg p \to q$$
$$p \wedge q \equiv \neg(p \to \neg q)$$
$$\neg(p \to q) \equiv p \wedge \neg q$$
$$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$$
$$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$$
$$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$$
$$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$$

Figure: Logical Equivalences Involving Conditional Statements

$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$$
$$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$$
$$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$$
$$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$$

Figure: Logical Equivalences Involving Biconditional Statements.

Source: “Discrete Mathematics and Its Applications (7th Edition) by Rosen”.

Continued....

Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent by developing a series of logical equivalences.

Solution: We will use one of the equivalences in Table 6 at a time, starting with $\neg(p \vee (\neg p \wedge q))$ and ending with $\neg p \wedge \neg q$. (*Note:* we could also easily establish this equivalence using a truth table.) We have the following equivalences.

$$
\begin{aligned}
\neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) && \text{by the second De Morgan law} \\
&\equiv \neg p \wedge [\neg(\neg p) \vee \neg q] && \text{by the first De Morgan law} \\
&\equiv \neg p \wedge (p \vee \neg q) && \text{by the double negation law} \\
&\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) && \text{by the second distributive law} \\
&\equiv \mathbf{F} \vee (\neg p \wedge \neg q) && \text{because } \neg p \wedge p \equiv \mathbf{F} \\
&\equiv (\neg p \wedge \neg q) \vee \mathbf{F} && \text{by the commutative law for disjunction} \\
&\equiv \neg p \wedge \neg q && \text{by the identity law for } \mathbf{F}
\end{aligned}
$$

Consequently $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent. ◀

Source: “Discrete Mathematics and Its Applications (7th Edition) by Rosen”.

Continued....

Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

Solution: To show that this statement is a tautology, we will use logical equivalences to demonstrate that it is logically equivalent to **T**. (*Note:* This could also be done using a truth table.)

$(p \wedge q) \rightarrow (p \vee q)$	$\equiv \neg(p \wedge q) \vee (p \vee q)$	by Example 3
	$\equiv (\neg p \vee \neg q) \vee (p \vee q)$	by the first De Morgan law
	$\equiv (\neg p \vee p) \vee (\neg q \vee q)$	by the associative and commutative laws for disjunction
	$\equiv \mathbf{T} \vee \mathbf{T}$	by Example 1 and the commutative law for disjunction
	$\equiv \mathbf{T}$	by the domination law

Source: “Discrete Mathematics and Its Applications (7th Edition) by Rosen”.

Methods of Proving Theorems

A theorem in mathematics is a true proposition. Many theorems are implications $H_1 \wedge H_2 \wedge \cdots \wedge H_n \rightarrow C$ is a tautology. Here we can discuss six standard methods for proving theorems:

1. Vacuous proof
2. Trivial proof
3. Direct proof
4. Indirect proof
5. Proof by cases
6. Existence proof

1. Vacuous Proof

- Suppose the hypothesis H of the implication $H \rightarrow C$ is false.
- Then, the implication is true regardless of whether C is true or false.
- Thus, if the hypothesis H can be shown to be false, the theorem $H \rightarrow C$ is true by default.

Example: Since the hypothesis of the statement "*If* $1 = 2$, *then* $3 = 4$" is false, the proposition is vacuously true.

2. Trivial Proof

- Suppose the the conclusion C of the implication $H \rightarrow C$ is true.
- The implication is true irrespective of the truth value of H.
- Consequently, if C can be shown to be true, such a proof is a trivial proof.

Example: Let $P(n)$ be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$," where the domain consists of all non-negative integers. Show that $P(0)$ is true.
Solution: The proposition $P(0)$ is "If $a \geq b$, then $a^0 \geq b^0$". Because $a^0 = b^0 = 1$, the conclusion of the conditional statement: "If $a \geq b$, then $a^0 \geq b^0$" is true. Hence, this conditional statement, which is $P(0)$, is true.

3. Direct Proof

In the direct proof of the theorem $H_1 \wedge H_2 \wedge \cdots \wedge H_n \rightarrow C$, assume the given hypotheses H_i are true. Using the laws of logic or previously known facts, establish the desired conclusion C as the final step of a chain of implications: $H \rightarrow C_1$, $C_1 \rightarrow C_2$, $C_2 \rightarrow C_3, \cdots, C_n \rightarrow C$. Then, by the repeated application of the hypothetical syllogism, it follows that $H \rightarrow C$.

Example: Prove directly that the product of any two odd integers is an odd integer.
Solution: Let x and y be any two odd integers. Then there exist integers m and n such that $x = 2m + 1$ and $y = 2n + 1$. Thus,

$$\begin{aligned} x * y &= (2m + 1) * (2n + 1) \\ &= 4mn + 2m + 2n + 1 \\ &= 2(2mn + m + n) + 1 \\ &= 2k + 1 \end{aligned} \tag{1}$$

where $k = 2mn + m + n$ is an integer. Therefore, xy is an odd integer. This concludes the proof.

4. Indirect Proof

There are two kinds of **indirect proofs** for the theorem $H_1 \wedge H_2 \wedge \cdots H_n \rightarrow C$:

- **proof of the contrapositive**
- **proof by contradiction**

The first method is based on the law of the contrapositive, $H_1 \wedge H_2 \wedge \cdots \wedge H_n \rightarrow C \equiv \neg C \rightarrow (H_1 \wedge H_2 \wedge \cdots H_n)$. In this method, assume the desired conclusion C is false; then using the law of logic, establish that some hypothesis H_i is also false. Once you have done this, the theorem is proved.

Example: Prove indirectly: "If the square of an integer is odd, then the integer is odd".

Proof by Contrapositive

- Let x be any integer such that x^2 is odd. We would like to prove that x must be an odd integer.
- In the indirect method, we assume the conclusion is false, that is, *x is not odd*. In other words, assume that x is an even integer.
- Let $x = 2k$ for some integer k. Then, $x^2 = (2k)^2 = 2(2k^2)$, which is an even integer.
- This makes our hypothesis that x^2 is an odd integer false. Therefore, by the law of the contrapositive, our assumption must be wrong. In other words x must be an odd integer. Thus, if x^2 is an odd integer, then x is also an odd integer.

Proof by Contradiction

- Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg p \rightarrow q$ is true.
- Because q is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that p is true.
- How can we find a contradiction q that might help us prove that p is true in this way?
- Because the statement $r \wedge \neg r$ is a contradiction whenever r is a proposition, we can prove that p is true, if we can show that $\neg p \rightarrow (r \wedge \neg r)$ is true for some proposition r. Proofs of this type are called “proofs by contradiction”.

Continued...

Example: Show that at least four of any 22 days must fall on the same day of the week.
Solution: Let p be the proposition: "At least four of 22 chosen days fall on the same day of the week".
Suppose that $\neg p$ is true. This means that at most three of the 22 days fall on the same day of the week. Because there are seven days of the week, this implies that at most 21 days could have been chosen, as for each of the days of the week, at most three of the chosen days could fall on that day.
This contradicts the premise that we have 22 days under consideration. That is, if r is the statement that 22 days are chosen, then we have shown that $\neg p \rightarrow (r \wedge \neg r)$. Consequently, we know that p is true.
We have proved that at least four of 22 chosen days fall on the same day of the week.

5. Proof by Cases

Suppose we would like to prove a theorem of the form $H_1 \vee H_2 \vee \cdots H_n \rightarrow C$. Since $H_1 \vee H_2 \vee \cdots \vee H_n \rightarrow C \equiv (H_1 \rightarrow C) \vee (H_2 \rightarrow C) \vee (H_n \rightarrow C)$, the statement $H_1 \vee H_2 \vee \cdots \vee H_n \rightarrow C$ is true iff each implication $H_i \rightarrow C$ is true. Consequently, we need only prove that each implication is true.

Example: Prove that if n is an integer, then $n^2 \geq n$.
Solution: We can prove that $n^2 \geq n$ for every integer by considering three cases, when $n = 0$, when $n \geq 1$, and when $n \leq -1$. We split the proof into three cases because it is straightforward to prove the result by considering zero, positive integers, and negative integers separately.

- **Case (i)**: When $n = 0$, because $0^2 = 0$, we see that $0^2 \geq 0$. It follows that $n^2 \geq n$ is true in this case.
- **Case (ii)**: When $n \geq 1$, when we multiply both sides of the inequality $n \geq 1$ by the positive integer n, we obtain $n \cdot n \geq n \cdot 1$. This implies that $n^2 \geq n$ for $n \geq 1$.
- **Case (iii)**: In this case $n \leq -1$. However, $n^2 \geq 0$. It follows that $n^2 \geq n$.

Because the inequality $n^2 \geq n$ holds in all three cases, we can conclude that if n is an integer, then $n^2 \geq n$.

6. Existence Proof

Theorem of the form $(\exists x)P(x)$ also occurs in mathematics. To prove such a theorem, we must establish the existence of an object "a" for which $P(a)$ is true.

Example: Find a positive integer that can be written as the sum of cubes of positive integers in two different ways.
Solution: After considerable computation (such as a computer search) we find that $1729 = 10^3 + 9^3 = 12^3 + 1^3$.
Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done. There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied "No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways."
Note: The Man Who Knew Infinity (2015) (a car used with No. 1729)

Counterexample

We introduced the use of counterexamples to show that certain statements are false. When confronted with a conjecture, you might first try to prove this conjecture, and if your attempts are unsuccessful, you might try to find a counterexample, first by looking at the simplest, smallest examples. If you cannot find a counterexample, you might again try to prove the statement. In any case, looking for counterexamples is an extremely important pursuit, which often provides insights into problems.

Example: Number theorists dream of finding formulas that generate the prime numbers.

Solution: Once such formula was found by Swiss mathematician Leonhard Euler, namely, $E(n) = n^2 - n + 41$. It yields a prime for $n = 1, 2, \cdots, 40$. Suppose we claim that the formula generates a prime for every positive integer n. Since $E(41) = 41^2 - 41 + 41 = 41^2$ is not a prime, 41 is a counterexample; thus, disproving the claim.

Boolean Satisfiability Problem (SAT)

- Let $x_1, x_2, \cdots$ denote the boolean variables (their value is either TRUE (1) or FALSE (0)).
- Let $\bar{x_i}$ denote the negation (or complement) of x_i.
- A *literal* is either a boolean variable or its negation.
- A *formula* in the propositional calculus is an expression that can be constructed using the literals, and the operations **and** ($\wedge$) and **or** ($\vee$). For example, $\phi = (x_1 \vee \bar{x_2}) \wedge x_3$ is a formula or boolean expression.
- ϕ is called "satisfiable" if some assignments of truth values to the boolean variables let the formula ϕ evaluate to 1 (TRUE). Any such assignment is called a "satisfying assignment".
- Here ϕ is satisfiable if $x_1 = 0$, $x_2 = 0$ and $x_3 = 1$.
- Define the following formal problem: $SAT = \{\langle\phi\rangle | \phi \text{ is satisfiable}\}$ is an encoding of all boolean expressions that are satisfiable.

CNF-SAT

- A formula ϕ is in conjunctive normal form (CNF) if and only if it is represented as $\wedge_{i=1}^{k} C_i$, where C_i are the clauses each represented as $\vee l_{ij}$ (l_{ij} are literals, i.e., x_i, $\bar{x}_i$, $\cdots$). For example, $\phi = (x_3 \vee \bar{x}_4) \wedge (x_1 \vee \bar{x}_2)$ is CNF.
- The CNF-satisfiability (CNF-SAT) problem is the satisfiable problem for CNF formulas.
  Formally, $\mathit{CNF\text{-}SAT} = \{\langle\phi\rangle | \phi \text{ is satisfiable}\}$ is an encoding of all CNF boolean expressions that are satisfiable.

DNF-SAT

- A formula ϕ is in disjunctive normal form (DNF) if and only if it is represented as $\vee_{i=1}^{k} C_i$, where C_i are the clauses each represented as $\wedge l_{ij}$ (l_{ij} are literals, i.e., x_i, $\bar{x}_i$, $\cdots$). For example, $\phi = (x_1 \wedge x_2) \vee (x_3 \wedge \bar{x_4})$ is DNF.
- The DNF-satisfiability (DNF-SAT) problem is the satisfiable problem for DNF formulas.
  Formally, $DNF\text{-}SAT = \{\langle\phi\rangle | \phi \text{ is satisfiable}\}$ is an encoding of all DNF boolean expressions that are satisfiable.

3SAT

- The 3-cnf formula is a cnf-formula in which every clause has exactly three (3) literals.
- For example, $\phi = (x_1 \vee \bar{x_2} \vee \bar{x_3}) \wedge (\bar{x_1} \vee \bar{x_1} \vee \bar{x_1}) \wedge (x_2 \vee x_3 \vee \bar{x_4})$ is a 3-cnf formula.
- Consider the following formal problem:
  $3SAT = \{\langle\phi\rangle | \phi \text{ is a satisfiable 3-cnf formula}\}$.

Example: Let $x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 0$. Then,
$x_1 \vee \bar{x_2} \vee \bar{x_3} = 0 \vee 1 \vee 0 = 1$, $\bar{x_1} \vee \bar{x_1} \vee \bar{x_1} = 1 \vee 1 \vee 1 = 1$ and
$x_2 \vee x_3 \vee \bar{x_4} = 0 \vee 1 \vee 1 = 1$. Thus,

$$\begin{aligned} \phi &= (x_1 \vee \bar{x_2} \vee \bar{x_3}) \wedge (\bar{x_1} \vee \bar{x_1} \vee \bar{x_1}) \wedge (x_2 \vee x_3 \vee \bar{x_4}) \\ &= 1 \wedge 1 \wedge 1 \\ &= 1, \textit{true}. \end{aligned}$$

Hence, $(x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 0)$ is a satisfying assignment.