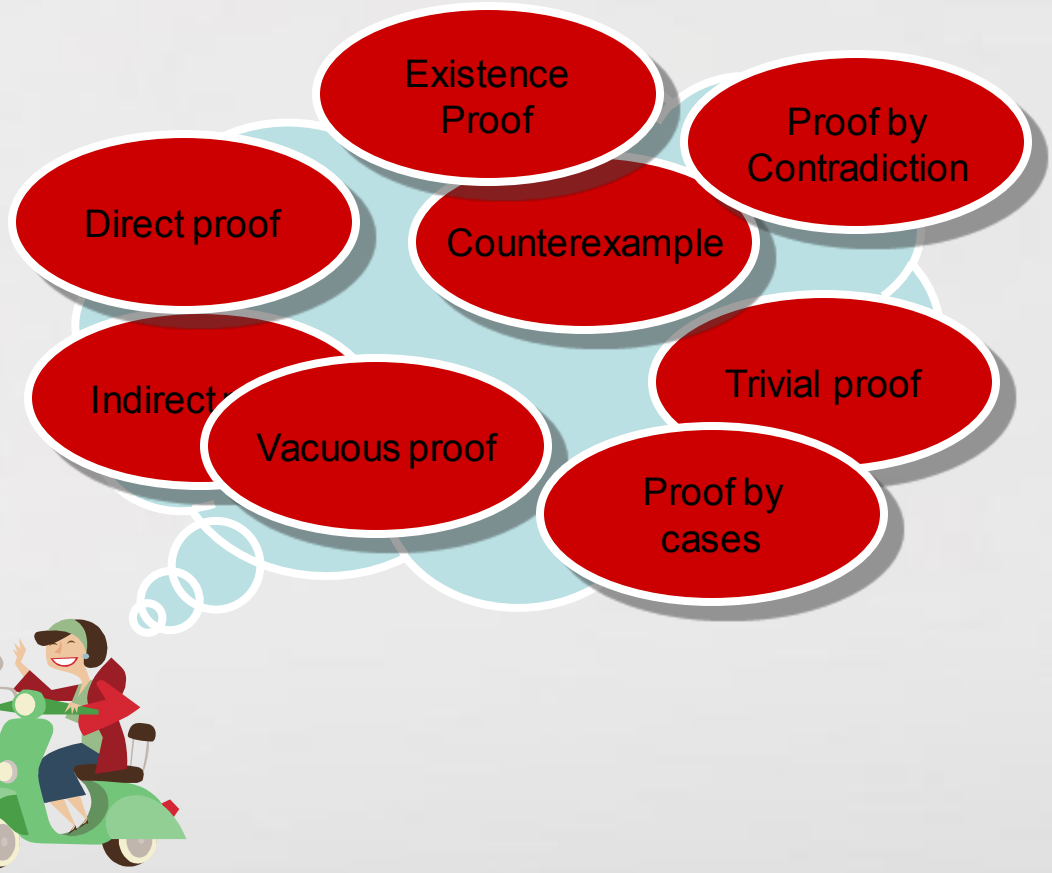
Department of Computer Engineering
Chulalongkorn University

2110200
Discrete Structures

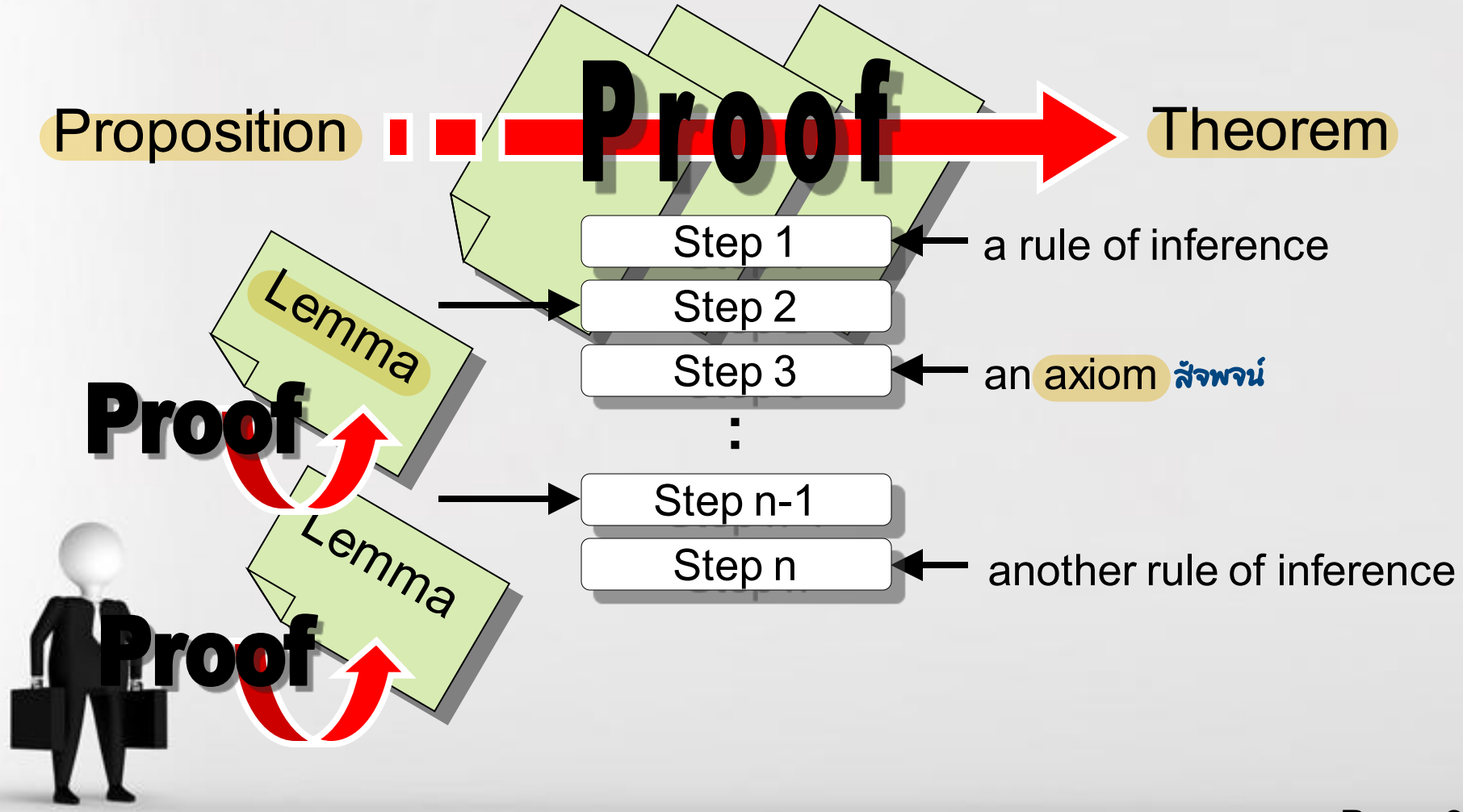
Sections 1.6

Methods of Proving Theorems



Proof Mechanisms

(to be revisited later in the course)



Understanding How theorems are stated

- Many theorems concerns elements in a domain, such as integers or real numbers.

If $x > y$, where x and y are *positive real numbers*, then $x^2 > y^2$

really means

For all positive real numbers, if $x > y$, then $x^2 > y^2$

$\forall x,y \in \mathbb{R}^+ (P(x,y) \rightarrow Q(x,y))$

where $P(x,y) : x < y$

$Q(x,y) : x^2 < y^2$

Proof: Assume $P(x,y)$ ($\equiv T$)

Show $Q(x,y)$ ($\equiv T$)

$\forall x,y \in \mathbb{R}^+$, Let $x<y$

$x \cdot x < x \cdot y$

$x \cdot y < y \cdot y$ } knowledge

$x \cdot x < y \cdot y$

$x^2 < y^2$

$\therefore Q(x,y)$ Q.E.D.

Universal instantiation / Universal generalization

"If n is an even integer, n^2 is an even integer"

$$\forall_{n \in Z_{even}} (P(n) \rightarrow Q(n))$$

$P(n)$: n is an even integer.

$Q(n)$: n^2 is an even integer.

$$\therefore P(c) \rightarrow Q(c)$$ Universal Instantiation

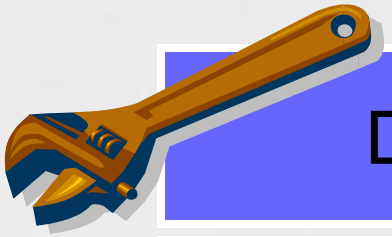
$$P(c) \rightarrow Q(c) \equiv \mathrm{T}$$

When c is any even integer

$$\forall_{n \in Z_{even}} (P(n) \rightarrow Q(n)) \equiv \mathrm{T}$$

Universal Generalization

Proving p→q



- Direct Proof
- Proof by Contraposition
- Vacuous Proof
- Trivial Proof
- Proof by Contradiction

Proving p→q

Direct Proof

Show that if **p** is true, **q** must be true.

Proof by Contraposition

$p \rightarrow q \equiv \neg q \rightarrow \neg p$

Show that if **¬q** is true, **¬p** must be true.

Vacuous Proof

Trivial Proof

Proof by Contradiction

- Example Rosen Ex.1 p.83

  Show that "If n is an odd integer, n^2 is an odd integer"

$\forall n \in Odd$

$\forall n \in \mathbb{Z}\ (P(n) \rightarrow Q(n))$

$P(n)$: n is odd $\equiv \exists k \in \mathbb{Z}\ (n = 2k+1)$

$Q(n)$: n^2 is odd $\equiv \exists m \in \mathbb{Z}\ (n^2 = 2m+1)$

Assume $\exists k \in \mathbb{Z}$ $n = 2k+1$

Show $\exists m \in \mathbb{Z}$ $n^2 = 2m+1$

$n = 2k+1$

$n^2 = (2k+1)^2$

$= 4k^2+4k+1$

$= 2(2k^2+2k)+1$

$n^2 = 2m+1$ where $m = 2k^2+2k$

Q.E.D. $m \in \mathbb{Z}$

DEFINITION 1 The integer n is *even* if there exists an integer k such that $n = 2k$, and n is *odd* if there exists an integer k such that $n = 2k + 1$. (Note that every integer is either even or odd, and no integer is both even and odd.) Two integers have the *same parity* when both are even or both are odd; they have *opposite parity* when one is even and the other is odd.

EXAMPLE 1 Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."

Solution: Note that this theorem states $\forall n\, P((n) \rightarrow Q(n))$, where $P(n)$ is "n is an odd integer" and $Q(n)$ is "n^2 is odd." As we have said, we will follow the usual convention in mathematical proofs by showing that $P(n)$ implies $Q(n)$, and not explicitly using universal instantiation. To begin a direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, namely, we assume that n is odd. By the definition of an odd integer, it follows that $n = 2k + 1$, where k is some integer. We want to show that n^2 is also odd. We can square both sides of the equation $n = 2k + 1$ to obtain a new equation that expresses n^2. When we do this, we find that $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. By the definition of an odd integer, we can conclude that n^2 is an odd integer (it is one more than twice an integer). Consequently, we have proved that if n is an odd integer, then n^2 is an odd integer. ◀

Extra Examples

- Example Rosen Ex.8 p.85

  Show that "If n is an integer and n^2 is odd, then n is odd."

$\forall n \in \mathbb{Z}\,(P(n) \rightarrow Q(n))$

$P(n)$: n^2 is odd $\equiv \exists k \in \mathbb{Z}\ \ n^2 = 2k+1$

$Q(n)$: n is odd $\equiv \exists m \in \mathbb{Z}\ \ n = 2m+1$

Assume $\exists k \in \mathbb{Z}\ \ n^2 = 2k+1$

Show $\exists m \in \mathbb{Z}\ \ n = 2m+1$

* Proof by contraposition *

$\forall n \in \mathbb{Z}\,(\neg Q(n) \rightarrow \neg P(n))$

$\therefore$ Assume $\exists k \in \mathbb{Z}\ \ n = 2k$

Show $\exists m \in \mathbb{Z}\ \ n^2 = 2m$

$n = 2k$

$n^2 = (2k)^2$

$= 2(2k^2)$

$n^2 = 2m$ where $m = 2k^2$

Q.E.D. $k \in \mathbb{Z}$

EXAMPLE 8 Prove that if n is an integer and n^2 is odd, then n is odd.

Solution: We first attempt a direct proof. Suppose that n is an integer and n^2 is odd. Then, there exists an integer k such that $n^2 = 2k + 1$. Can we use this information to show that n is odd? There seems to be no obvious approach to show that n is odd because solving for n produces the equation $n = \pm\sqrt{2k + 1}$, which is not terribly useful.

Because this attempt to use a direct proof did not bear fruit, we next attempt a proof by contraposition. We take as our hypothesis the statement that n is not odd. Because every integer is odd or even, this means that n is even. This implies that there exists an integer k such that $n = 2k$. To prove the theorem, we need to show that this hypothesis implies the conclusion that n^2 is not odd, that is, that n^2 is even. Can we use the equation $n = 2k$ to achieve this? By squaring both sides of this equation, we obtain $n^2 = 4k^2 = 2(2k^2)$, which implies that n^2 is also even because $n^2 = 2t$, where $t = 2k^2$. We have proved that if n is an integer and n^2 is odd, then n is odd. Our attempt to find a proof by contraposition succeeded. ◀

Proofs 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**. Because a proof by contradiction does not prove a result directly, it is another type of indirect proof. We provide three examples of proof by contradiction. The first is an example of an application of the pigeonhole principle, a combinatorial technique that we will cover in depth in Section 6.2.

Example

Rosen ex.4 p.84

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

Proof : $\forall n \in \mathbb{Z}^+ (P(n) \rightarrow Q(n))$

$P(n)$: $\exists a,b \in \mathbb{Z}^+ \quad n = ab$ ← same a,b

$Q(n)$: $\exists a,b \in \mathbb{Z}^+ \quad a \le \sqrt{n}$ or $b \le \sqrt{n}$

Proof : $\forall n \in \mathbb{Z}^+ \exists a,b \in \mathbb{Z}^+ (P(n,a,b) \rightarrow Q(n,a,b))$

$P(n,a,b)$: $n = ab$

$Q(n,a,b)$: $a \le \sqrt{n}$ or $b \le \sqrt{n}$

Proof : By contraposition technique

$\forall n \in \mathbb{Z}^+ \exists a,b \in \mathbb{Z}^+ ((a > \sqrt{n} \wedge b > \sqrt{n}) \rightarrow (n \neq ab))$

$\therefore$ Assume $a > \sqrt{n}$ and $b > \sqrt{n}$

Show $n \neq ab$

$a > \sqrt{n}$

$a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$

$\therefore a \cdot b > n$

$\therefore a \cdot b \neq n$ Q.E.D.

EXAMPLE 4 Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Solution: Because there is no obvious way of showing that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ directly from the equation $n = ab$, where a and b are positive integers, we attempt a proof by contraposition.

The first step in a proof by contraposition is to assume that the conclusion of the conditional statement "If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$" is false. That is, we assume that the statement $(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$ is false. Using the meaning of disjunction together with De Morgan's law, we see that this implies that both $a \leq \sqrt{n}$ and $b \leq \sqrt{n}$ are false. This implies that $a > \sqrt{n}$ and $b > \sqrt{n}$. We can multiply these inequalities together (using the fact that if $0 < s < t$ and $0 < u < v$, then $su < tv$) to obtain $ab > \sqrt{n} \cdot \sqrt{n} = n$. This shows that $ab \neq n$, which contradicts the statement $n = ab$.

Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. Our proof by contraposition succeeded; we have proved that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. ◀

VACUOUS AND TRIVIAL PROOFS We can quickly prove that a conditional statement $p \rightarrow q$ is true when we know that p is false, because $p \rightarrow q$ must be true when p is false. Consequently, if we can show that p is false, then we have a proof, called a **vacuous proof**, of the conditional statement $p \rightarrow q$. Vacuous proofs are often used to establish special cases of theorems that state that a conditional statement is true for all positive integers [i.e., a theorem of the kind $\forall n P(n)$, where $P(n)$ is a propositional function]. Proof techniques for theorems of this kind will be discussed in Section 5.1.

The real number r is rational if there exist integers p and q with $q \neq 0$ such that $r = p/q$

Example

Rosen Ex.7 p.85

Prove that the sum of two rational numbers is rational.

$\forall n, m \in Q \; ((P(n) \wedge P(m)) \rightarrow Q(m,n))$

$P(x): \exists p, q \in Q \; (q \neq 0 \wedge x = p/q)$

$Q(m,n): \exists p, q \in Q \; (q \neq 0 \wedge (n+m) = p/q)$

Assume: $(b \neq 0 \wedge n = a/b) \wedge (d \neq 0 \wedge m = c/d)$

Show: $q \neq 0 \wedge (n+m) = p/q$

$$n = \frac{a}{b}$$

$$n+m = \frac{a}{b} + \frac{c}{d}$$

$$= \frac{ad+bc}{bd}$$

$\therefore n+m = \frac{p}{q}$ where $p = ad+bc$ and $q = bd \neq 0$

Q.E.D.

DEFINITION 2 The real number r is *rational* if there exist integers p and q with $q \neq 0$ such that $r = p/q$. A real number that is not rational is called *irrational*.

EXAMPLE 7 Prove that the sum of two rational numbers is rational. (Note that if we include the implicit quantifiers here, the theorem we want to prove is "For every real number r and every real number s, if r and s are rational numbers, then $r + s$ is rational.)

Extra Examples

Solution: We first attempt a direct proof. To begin, suppose that r and s are rational numbers. From the definition of a rational number, it follows that there are integers p and q, with $q \neq 0$, such that $r = p/q$, and integers t and u, with $u \neq 0$, such that $s = t/u$. Can we use this information to show that $r + s$ is rational? The obvious next step is to add $r = p/q$ and $s = t/u$, to obtain

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu}.$$

Because $q \neq 0$ and $u \neq 0$, it follows that $qu \neq 0$. Consequently, we have expressed $r + s$ as the ratio of two integers, $pu + qt$ and qu, where $qu \neq 0$. This means that $r + s$ is rational. We have proved that the sum of two rational numbers is rational; our attempt to find a direct proof succeeded. ◀

Proving p→q

- Direct Proof
- Proof by Contraposition
- Vacuous Proof
- Trivial Proof
- Proof by Contradiction

Show that **p** is false.
So, **p→q** is always true.

Show that **q** is true.
So, **p→q** is always true.

Used in *Math Induction*

Proving p→q

- Example Rosen Ex.5 P.84

  P(*n*) = "If *n* > 1, then $n^2 > n$" (*n*: false)

  Show that P(*0*) is true. Vacuous Proof

- Example Rosen Ex.6 P.85

  P(*n*) = "If *a* and *b* are positive integers with $a \geq b$, then $a^n \geq b^n$" (a^n: true) Trivial Proof

  Show that P(*0*) is true.

EXAMPLE 5 Show that the proposition $P(0)$ is true, where $P(n)$ is "If $n > 1$, then $n^2 > n$" and the domain consists of all integers.

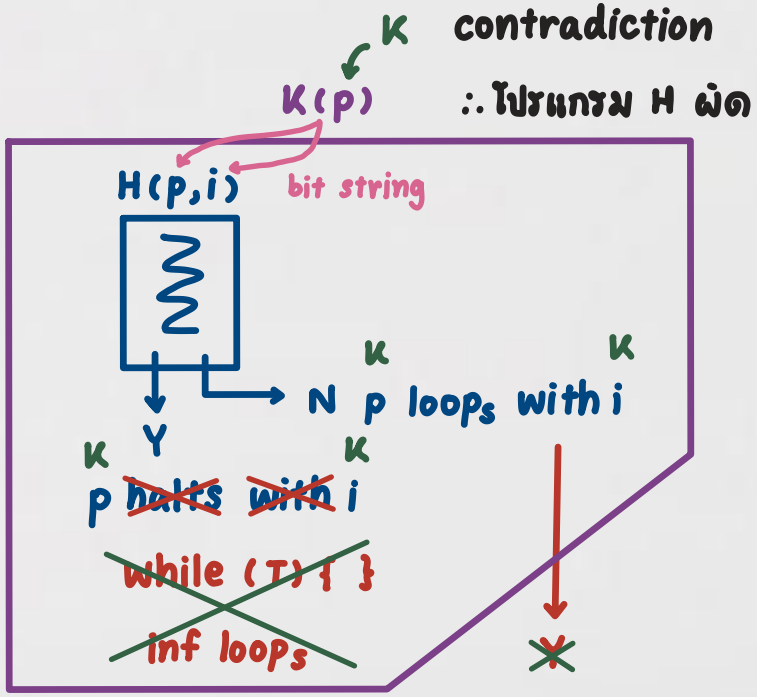
Solution: Note that $P(0)$ is "If $0 > 1$, then $0^2 > 0$." We can show $P(0)$ using a vacuous proof. Indeed, the hypothesis $0 > 1$ is false. This tells us that $P(0)$ is automatically true. ◀

Remark: The fact that the conclusion of this conditional statement, $0^2 > 0$, is false is irrelevant to the truth value of the conditional statement, because a conditional statement with a false hypothesis is guaranteed to be true.

EXAMPLE 6 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 nonnegative 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. This is an example of a trivial proof. Note that the hypothesis, which is the statement "$a \geq b$," was not needed in this proof. ◀

Halting problem



Sections 1.6

Proof By Contradiction

and
other proof techniques

Show $p \equiv T$

Assume $\neg p \equiv T \rightarrow X$

$\neg p \equiv$

$\equiv$

$\equiv F$ (ex. $p \wedge \neg p \equiv F$)

$\neg p \rightarrow F \equiv T$

$\therefore \neg p \equiv F$

$\therefore p \equiv T$

Proof by Contradiction

การบอกว่า ¬S เป็นเท็จเสมอ
ก็คือการบอกว่า S เป็นจริงเสมอ

- Proof by Contradiction
  - Suppose we want to prove a statement ***s***
  - Start by assuming ¬ ***s*** is true.
  - Show that ¬ ***s*** implies a contradiction. (¬ ***s*** → ***F***)
  - Then, ¬ ***s*** must be false (or ***s*** must be true).

Proof by Contradiction

- Example:

  Show that at least 10 of any 64 days chosen must fall on the same day of the week.

Proof : Let d_i = n days fall day i $(1 \le i \le 7)$

$\sum_{\text{all } i} d_i = 64$

Show $\exists d_i (d_i \ge 10)$

By contradiction technique

Assume $\neg(\exists d_i (d_i \ge 10))$

$\equiv \forall d_i (d_i \le 9)$

$\therefore \sum_{\text{all}} d_i \le 7 \times 9 = 63$

$\therefore \sum_{\text{all}} d_i \le 63$

$\therefore$ contradiction

$(\sum_{\text{all}} d_i = 64 \wedge \sum_{\text{all}} d_i \le 63)$

Proof p→q by Contradiction

- Proof by Contradiction
  - Start by assuming $\neg (p \rightarrow q)$ is true.
  - That means $p \wedge \neg q$ is true.

    (since $\neg (p \rightarrow q) \equiv \neg (\neg p \vee q) \equiv p \wedge \neg q$)
  - Show that $p \wedge \neg q$ is a contradiction
  - Then, $\neg (p \rightarrow q)$ must be false

    (or $(p \rightarrow q)$ must be true).

Proving p→q

- Example:

  Prove that "If n is an integer and n^3+5 is odd, then n is even". Using a proof by contradiction.

$\forall n \in \mathbb{Z}\,(\exists m \in \mathbb{Z}\,(n^3+5 = 2m+1) \rightarrow \exists p \in \mathbb{Z}\,(n=2p))$

Prove by contradiction technique,

Assume $\exists m \in \mathbb{Z}\,(n^3+5 = 2m+1)$ odd

and $\forall p \in \mathbb{Z}\,(n \neq 2p)$

$\therefore \exists q \in \mathbb{Z}\ n = 2q+1$

$n^3 = 8q^3 + 12q^2 + 6q + 1$

$n^3+5 = 8q^3+12q^2+6q+6$

$= 2(4q^3+6q^2+3q+3)$

even $\therefore n^3+5 = 2m$ when $m = 4q^3+6q^2+3q+3$

$\equiv F$

Q.E.D.

Exercises

1. Prove or disprove that the product of irrational and rational numbers is irrational.
2. Prove that if n is an integer and $3n + 2$ is even, then n is even.
3. Show that if a is an integer and b is a positive integer, then $0 \leq a \bmod b \leq b - 1$.

① $\forall n,m \in Q\ ((P(n) \wedge P(m) \rightarrow Q(n,m))$

$P(n) = \exists a,b \in Q\ (n = a/b \wedge b \neq 0)$

$P(m) = X$ irrational

$Q(n,m) = Y$

Prove by contradiction technique,

Assume $(\exists a,b \in Q\ (n = a/b \wedge b \neq 0) \wedge X)$

and $\exists c,d \in Q\ (nm = c/d \wedge d \neq 0)$

$$\frac{a}{b} \times X = \frac{c}{d}$$

$X = \frac{cb}{ad}$ rational

$\equiv F$ Q.E.D

② $\forall n \in \mathbb{Z}\ (3n+2 = \text{even} \rightarrow n = \text{even})$ $\quad p \rightarrow q$

$3n + 2 = 2m \quad ; \exists m \in \mathbb{Z}$

$n = \frac{2m-2}{3}$ ×

Prove by contradiction technique $\quad p \wedge \neg q$

$n = 2m+1 \quad ; \exists m \in \mathbb{Z}$

$3n = 6m+3$

$3n+2 = 6m+5$

$= 2(3m+2)+1$

odd $\therefore 3n+2 = 2k+1$ when $k = 3m+2$

$\equiv F$ $\quad k \in \mathbb{Z}$

Q.E.D.

③ $\forall a \leq \mathbb{Z}\ \forall b \in \mathbb{Z}^+ (0 \leq a \bmod b \leq b-1)$

Def $a \bmod b = a - b\left\lfloor \frac{a}{b} \right\rfloor$

Th: $\lfloor x \rfloor = m$ iff $x-1 < m \leq x$; $m \in \mathbb{Z}$

$$\frac{a}{b} - 1 < \left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b}$$

$$a - b < b\left\lfloor \frac{a}{b} \right\rfloor \leq a$$

$$-a \leq -b\left\lfloor \frac{a}{b} \right\rfloor < b - a$$

$$0 \leq a - b\left\lfloor \frac{a}{b} \right\rfloor < b$$

$$0 \leq a - b\left\lfloor \frac{a}{b} \right\rfloor \leq b-1$$

backward reasoning (ทดๆ)

$$0 \leq a - b\left\lfloor \frac{a}{b} \right\rfloor \leq b-1 \quad \text{ต้องแสดง}$$

$$-a \leq -b\left\lfloor \frac{a}{b} \right\rfloor \leq -a+b-1 < -a+b$$

$$a-b < a-b+1 \leq b\left\lfloor \frac{a}{b} \right\rfloor \leq a$$

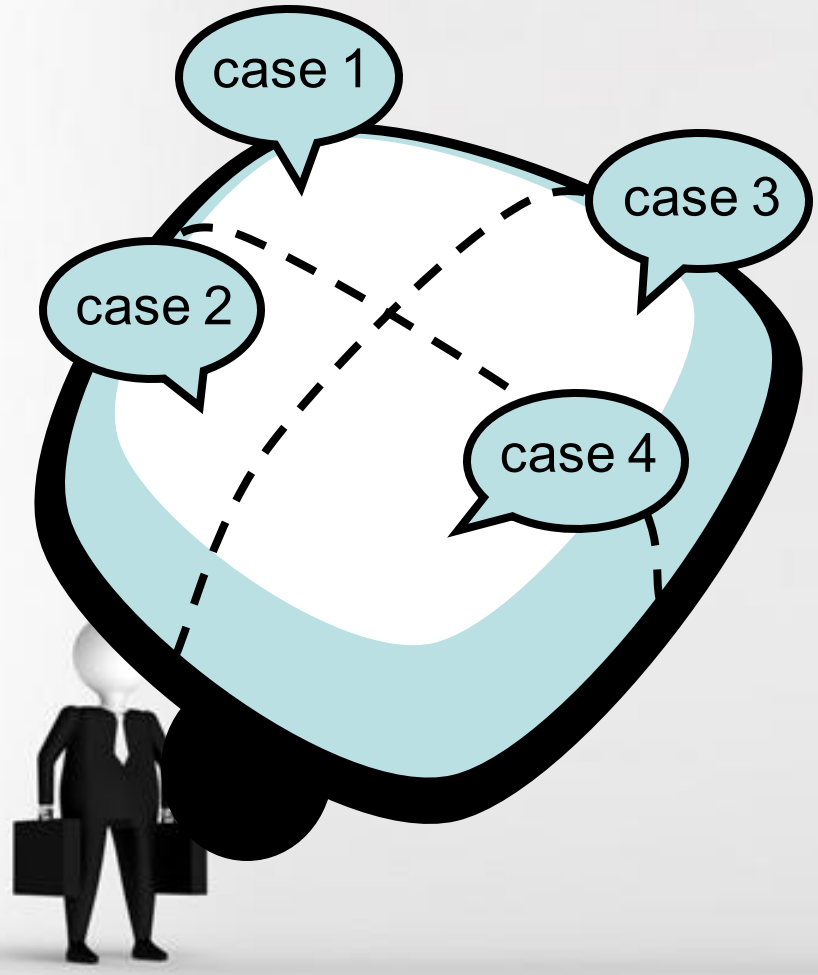
$$\frac{a}{b} - 1 < \frac{a}{b} - 1 + \frac{1}{b} \leq \left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b}$$

$$\frac{a}{b} - 1 < \left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b}$$

$$x - 1 < \lfloor x \rfloor \leq x$$

Proof by Cases

$$A = CASE1 \cup CASE2 \cup CASE3 \cup CASE4$$



- $\forall_{n \in CASE1}(P(n) \rightarrow Q(n))$
- $\forall_{n \in CASE2}(P(n) \rightarrow Q(n))$
- $\forall_{n \in CASE3}(P(n) \rightarrow Q(n))$
- $\forall_{n \in CASE4}(P(n) \rightarrow Q(n))$

- $\forall_{n \in A}(P(n) \rightarrow Q(n))$

Proof by Cases

- Example:

  Show that $|xy| = |x||y|$, where x and y are real numbers.

$\forall x, y \in \mathbb{R}$

$|xy| = |x||y|$

note

$$|x| = \begin{cases} -x \; ; \; x < 0 \\ x \; ; \; x \geq 0 \end{cases}$$

Proof: Prove by cases

1) $x \geq 0 \wedge y \geq 0$

2) $x \geq 0 \wedge y < 0$

3) $x < 0 \wedge y \geq 0$

4) $x < 0 \wedge y < 0$

Proof of $p \leftrightarrow q$

- Since $(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$, then *prove both $p \rightarrow q$ and $q \rightarrow p$*
- Equivalent propositions ($p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n$) are proven by *proving $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$, …, $p_n \rightarrow p_1$*

Equivalent Propositions

- Example Rosen Ex.13 p.88

  Show that these statements are equivalent:

  p_1: *n* is an even integer.

  p_2: *n -1* is an odd integer.

  p_3: n^2 is an even integer.

$p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$, $p_3 \rightarrow p_1$

EXAMPLE 13 Show that these statements about the integer n are equivalent:

p_1: n is even.
p_2: $n - 1$ is odd.
p_3: n^2 is even.

Solution: We will show that these three statements are equivalent by showing that the conditional statements $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$, and $p_3 \rightarrow p_1$ are true.

We use a direct proof to show that $p_1 \rightarrow p_2$. Suppose that n is even. Then $n = 2k$ for some integer k. Consequently, $n - 1 = 2k - 1 = 2(k - 1) + 1$. This means that $n - 1$ is odd because it is of the form $2m + 1$, where m is the integer $k - 1$.

We also use a direct proof to show that $p_2 \rightarrow p_3$. Now suppose $n - 1$ is odd. Then $n - 1 = 2k + 1$ for some integer k. Hence, $n = 2k + 2$ so that $n^2 = (2k + 2)^2 = 4k^2 + 8k + 4 = 2(2k^2 + 4k + 2)$. This means that n^2 is twice the integer $2k^2 + 4k + 2$, and hence is even.

To prove $p_3 \rightarrow p_1$, we use a proof by contraposition. That is, we prove that if n is not even, then n^2 is not even. This is the same as proving that if n is odd, then n^2 is odd, which we have already done in Example 1. This completes the proof. ◀

Proof of Proposition Involving Quantifiers

- Existence proofs: A proof of $\exists x P(x)$
- *Constructive existence proof:*
  - Find an element c such that $P(c)$ is true.
- *Non-constructive existence proof:* ยาก
  - Do not find an element c such that $P(c)$ is true, but use some other ways.

Existence Proofs

- Example : Non-constructive

  Show that $\exists x \exists y$ (x^y is rational.) where x and y are irrational.

Proof: $\exists x \exists y$ (x^y = rational) ; x, y = irrational

consider $\sqrt{2}^{\sqrt{2}}$

case 1) $\sqrt{2}^{\sqrt{2}}$ = rational

$x = \sqrt{2} \wedge y = \sqrt{2}$

case 2) $\sqrt{2}^{\sqrt{2}}$ = irrational

$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ = rational

$x = \sqrt{2}^{\sqrt{2}} \wedge y = \sqrt{2}$

Proof of Proposition Involving Quantifiers

- Uniqueness proofs: showing that there is a unique element x such that P(x).

  1) *Existence*:

     Show that $\exists x P(x)$

  2) *Uniqueness*:

     Show that if $y \neq x$, P(y) is false.

is the same as proving:

contradiction

$$\exists x(P(x) \wedge \forall y(y \neq x \rightarrow \neg P(y)))$$

Uniqueness Proofs

- Example:

  Show every integer has a unique additive inverse. (If p is an integer, there exists a unique integer q such that p+q = 0.)

Proof : $\forall p \in \mathbb{Z}\ \exists q \in \mathbb{Z}\ (p+q=0)$

we have to show that

1) $\forall p \in \mathbb{Z}\ \exists q \in \mathbb{Z}\ \ p+q=0$

Let $q = -p \quad \therefore p+q = p+(-p) = 0$

2) $\exists q_1, q_2 \in \mathbb{Z}\ (q_1 \neq q_2) \wedge (p+q_1=0) \wedge (p+q_2=0)$

By contradiction

$p+q_1 = 0 = p+q_2$

$q_1 = q_2$ contradict with $q_1 \neq q_2$

Q.E.D.

Counterexamples

- Show that $\forall x P(x)$ is false.

$\forall n \in \mathbb{Z}\ \exists a,b,c \in \mathbb{Z}\ (n = a^2+b^2+c^2) \equiv F$

$\exists n \in \mathbb{Z}\ \forall a,b,c \in \mathbb{Z}\ (n \neq a^2+b^2+c^2)$

Let $n = 7$ $\quad a,b,c = \{-2,-1,0,1,2\}$

- Example: Rosen Ex.38

  "Every positive integer is the sum of the squares of three integers" ?

38. We must find a number that cannot be written as the sum of the squares of three integers. We claim that 7 is such a number (in fact, it is the smallest such number). The only squares that can be used to contribute to the sum are 0, 1, and 4. We cannot use two 4's, because their sum exceeds 7. Therefore we can use at most one 4, which means that we must get 3 using just 0's and 1's. Clearly three 1's are required for this, bringing the total number of squares used to four. Thus 7 cannot be written as the sum of three squares.

Example

Show that there are n consecutive composite positive integers for every positive integers n.

Prove that : $\forall n \; \exists x$ (x+i is composite for i = 1 2 3 … n)

Proof: Let x = (n+1)! +1. Consider the integers

x+1, x+2, x+3, …, x+n.

Note that i+1 divides x+i = (n+1)! + (i+1) for i = 1 2 3 … n.

Hence, n consecutive composite integers have been given.

$\forall n \in \mathbb{Z}^+ \; \exists c_1, c_2, \ldots c_n \in \mathbb{Z}$

c_i = Composite

$c_{i+1} = c_i + 1 \quad ; \; 1 \le i \le n-1$

$\exists c \in \mathbb{Z} \quad c$ = composite

$c+i$ = composite $\; ; \; 1 \le i \le n-1$

$c, c+1, \ldots, c+n-1, c+n$

$c = (n+1)! + 1$ $\begin{matrix} +1 \\ +2 \\ +3 \\ \\ +n \end{matrix}$

$n = 2$ 8,9

$n = 3$ 14,15,16

QED

Example

Show that there is a prime greater than n for every positive integer n.

Prove that : $\forall n \, \exists x$ (x is prime and x > n).

Proof: Consider the integer n!+1.

There is at least one prime divides n!+1.

Note that $n!+1 \equiv 1 \pmod{k}$ for k = 1 2 3 … n.

Hence, any prime factor of n!+1 must be greater than n.

QED

Example

Prove the following: there exists an integer x such that

If x is divisible by 3 then $5x^2$ is divisible by 6.

Proof: Let x = 6.

6 is divisible by 3 and $5 \times 6^2 = 180$.

180 is divisible by 6.

QED

Example

Prove that "If n is not divisible by 3, then n^2 mod 3 = 1".

Proof:

Suppose that n is not divisible by 3.

Case 1 : n mod 3 = 1.

So n = 3k+1. Since $n^2 = 3(3k^2+2k)+1$.

Hence n^2 mod 3 = 1.

Case 2 : n mod3 = 2.

So n = 3k+2. Since $n^2 = 3(3k^2+4k+1)+1$

Hence n^2 mod 3 = 1. QED.