Chapter 2. Proofs

증명(proof)이란 논리적 법칙을 이용하여 주어진 가정으로부터 결론을 유도해 내는 추론의 한 방법으로서, 어떠한 명제(proposition)나 논증(argument)이 적절하고 타당한 지를 입증하는 작업이다.

연역법(deduction) *vs.* 귀납법(induction)

연역법은 주어진 사실(facts)들과 공리(axioms)들을 기초로 하여 추론(inference) 과정을 거쳐 새로운 사실을 도출하는 것이고, 귀납법은 관찰과 실험을 기반한 가설(hypothesis)을 귀납 추론을 통하여 일반적인 규칙을 입증하는 것이다.

2.1 Mathematical systems

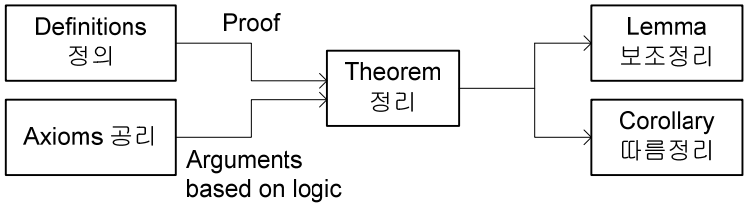

Figure 2-1 Structure of mathematical system

Example 2.1 Euclidean geometry as an axiomatic system: We take followings be true.

(1) Given two distinct points, there is exactly one straight line connecting them.

(2) Given a line and a point not on the line, there is exactly one line parallel to the line through the point.

- Terms *point* and *line* are un-defined terms that are implicitly defined by the axioms that describe their properties.

Example 2.2 Axioms for real number system

(1) $\forall x, y \in R,\ xy = yx$

(2) There is a subset P, such that

(a) If $x, y \in P$, then so are $x + y$ and xy.

(b) If x is a real number, then exactly one of the following statement is true:

$x \in P,\ x = 0,\ -x \in P$

Types of proof

1. Direct proof 직접증명: prove $p \to q$
2. Proof by contradiction 모순에 의한 증명: prove $\sim(p \to q) \equiv p \wedge \sim q$ is always false.
3. Proof by contrapositive 대우에 의한 증명: prove $\sim q \to \sim p$
4. Exhaustive proof 전수 증명
5. Mathematical induction 수학적 귀납법

Direct proof 직접 증명

Given a general form of a theorem,

(2.1) $\forall x_1, x_2, \dots, x_n$, if $p(x_1, x_2, \dots, x_n)$, then $q(x_1, x_2, \dots, x_n)$

A direct proof assumes that $p(x_1, x_2, \dots, x_n)$ is true, and then using $p(x_1, x_2, \dots, x_n)$ together with other axioms, definitions, previously derived theorems, and rules of inference, show directly that $q(x_1, x_2, \dots, x_n)$ is true.

- If $p(x_1, x_2, \dots, x_n)$ is false, the theorem is true by default.

Definitions An integer n is *even*, if there exists an integer k such that $n = 2k$. An integer n is *odd*, if there exists an integer k such that $n = 2k + 1$.

Example 2.3 Prove that, for all integers m and n, if m is odd and n is even, then $m + n$ is odd.

$m = 2k_1 + 1,\ n = 2k_2$

Example 2.4 Prove that, for all sets X, Y and Z, $X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$.

The proposition we need to prove is bi-conditional: or, equivalently we have to show that two sets $X \cap (Y - Z)$ and $(X \cap Y) - (X \cap Z)$ are the same. Thus, we have to show two conditional propositions;

(1) If $x \in X \cap (Y - Z)$, then $x \in (X \cap Y) - (X \cap Z)$, and

(2) If $x \in (X \cap Y) - (X \cap Z)$, then $x \in X \cap (Y - Z)$.

Let $x \in X \cap (Y - Z)$, then $x \in X$, $x \in Y$, and $x \notin Z$. $\Rightarrow$ $x \in X \cap Y$ and $x \notin X \cap Z$. For part (2), we let $x \in (X \cap Y) - (Y \cap Z)$, and show that $x \in X \cap (Y - Z)$.

Example 2.5 If a and b are real numbers, we define $min(a, b)$ to be the minimum of a and b: *i.e.*

(2.2) $$min(a, b) = \begin{cases} a, & a \le b \\ b, & b < a \end{cases}$$

Prove that, for all real numbers d, d_1, d_2 and x, if $d = min(d_1, d_2)$ and $x \le d$, then $x \le d_1$ and $x \le d_2$.

← At first, we claim that, if $d = min(d_1, d_2)$, then $d \le d_1$ and $d \le d_2$.

If $d \le d_1$, $min(d_1, d_2) = d_1$. $\Rightarrow$ $d = d_1 \le d_2$.

Example 2.6 Prove that, for all sets X and Y, $X \cup (Y - X) = X \cup Y$.

$Y - X = Y \cap \overline{X}$ and $X \cup (Y - X) = (X \cup Y) \cap \left(X \cup \overline{X}\right)$

Example 2.7 Prove or disprove that, $\forall n \in N, (2^n - 1)$ is prime (소수).

← The Mersenne primes is a set of prime numbers, $M_n = 2^n - 1$, for some positive integers n. Examples are $\{3,\ 7,\ 31,\ 127,\ 8191, \dots\}$.

← In order to disprove $\forall x\, P(x)$, it suffices to find one member in the domain of discourse that

makes $P(x)$ false. Such a value for x is called a *counter-example* (반례).

- Choose $n = 11$, then $2^{11} - 1 = 2047 = 23 \times 89$.

Example 2.8 (*How to find a counter-example*) Prove or disprove the statement: $(A \cap B) \cup C = A \cap (B \cup C)$.

- Bi-directional proposition: $p \leftrightarrow q$

← First, check if the proposition 'if $x \in (A \cap B) \cup C$, then $x \in A \cap (B \cup C)$' is true.

⇒ If $x \in A \cap B$ or $x \in C$, then $x \in A$ and $x \in B \cup C$.

⇒ $\{(A \cap B) \cup C\} \subseteq \{A \cap (B \cup C)\}$

→ 만약에 반례가 존재한다면, 그 중 하나는, 집합 $(A \cap B) \cup C$의 원소이면서, 집합 $A \cap (B \cup C)$의 원소가 아닌 경우를 찾으면 된다.

→ Venn diagram 을 이용하면 쉽게 반례를 찾을 수 있다. 예를 들어, 하나의 반례는, $x \notin A \cap B$ and $x \in C$의 형태를 띨 것이다.

- Consider $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$, and $C = \{3, 4, 5\}$. Note that $4 \notin A \cap B$ and $4 \in C$, so that $(A \cap B) \cup C = \{2, 3, 4, 5\}$, $A \cap (B \cup C) = \{3\}$ and, we $\{(A \cap B) \cup C\} \nsubseteq \{A \cap (B \cup C)\}$.

2.2 More methods of proof

2.2-1 Proof by contradiction (모순 증명법, 귀류법)

In order to prove $p \rightarrow q$,

(1) Assume that the hypothesis p is true and that the conclusion q is false.

(2) Using p and $\sim q$ as well as other logical tools (such as axioms, definitions, previously derived theorems, and rules of inference), derive a contradiction.

The proof by contradiction is based on the logical equivalence (동치),

(2.3) $\sim(p \rightarrow q) \equiv p \wedge \sim q$

By showing that $p \wedge \sim q$ is false, it proves $\sim(p \rightarrow q)$ is also false. 즉, 명제 $p \wedge \sim q$가 참이라고 가정하고 모순을 유도하면 $p \wedge \sim q$가 거짓, 따라서 $p \rightarrow q$가 참임을 증명하게 된다.

p	q	r	$p \rightarrow q$	$p \wedge \sim q$	$r \wedge \sim r$	$(p \wedge \sim q) \rightarrow (r \wedge \sim r)$
T	T	T	T	F	F	T
T	T	F	T	F	F	T
T	F	T	F	T	F	F
T	F	F	F	T	F	F
F	T	T	T	F	F	T
F	T	F	T	F	F	T
F	F	T	T	F	F	T
F	F	F	T	F	F	T

← 명제 $r \wedge \sim r$는 항상 거짓인 contradiction 명제이다.

← 명제 $p \rightarrow q$와 $(p \wedge \sim q) \rightarrow (r \wedge \sim r)$는 동치이다.

Example 2.9 Prove that, $\forall n \in Z$, if n^2 is even, then n is even.

← It is not easy to prove this statement directly.

← For a proof by contradiction, choose $p = (n^2 \text{ even})$ and $q = (n \text{ even})$. We assume $p = (n^2 \text{ even})$ and $\sim q = (n \text{ odd})$, then prove that $p \wedge \sim q$ is false.

Example 2.10 Prove that, for all real numbers x and y, if $x + y \geq 2$, then either $x \geq 1$ or $y \geq 1$.

← $p: x + y \geq 2$ and $q: x \geq 1$ or $y \geq 1$

$\sim q: \sim\{(x \geq 1) \vee (y \geq 1)\} \equiv (x < 1) \wedge (y < 1) \rightarrow x + y < 2$

Since $p \wedge \sim q$ is a contradiction, $p \rightarrow q$ is true.

Example 2.11 Prove that $\sqrt{2}$ is irrational (무리수).

$\sim q$: $\sqrt{2} = \frac{a}{b}$, a and b coprime:

$\frac{a^2}{b^2} = 2 \Rightarrow a^2$ even and $\exists k \in N$, $a^2 = 2k \Rightarrow b^2 = 2k^2$, even. Thus, a and b are not coprime.

Example 2.12 n이 자연수이고 n이 2가 아닌 소수이면, n은 홀수이다.

- If $n \in P$ and $n \neq 2$, n is odd (P is the set of prime numbers).
- $p \wedge \sim q$: $n \in P$, $n \neq 2$, and n is even.

2.2-2 Proof by contrapositive (대우)

The proof by contrapositive is based on the logical equivalence,

(2.4) $p \rightarrow q \equiv \sim q \rightarrow \sim p$

Example 2.13 Prove that, if $\forall x \in R$, x^2 is irrational, then x is irrational.

- Show that if x is rational, then x^2 is rational.

← Let $x = a/b$, a and b are integers.

2.2-3 Proof by case (exhaustive proof, 전수증명)

This method can be used when the hypothesis naturally divides itself into various cases. Instead of proving the statement

(2.5) $(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$

directly, we prove

(2.6) $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots (p_n \rightarrow q)$

← Suppose that, for any j, p_j is true. Then $p_1 \vee p_2 \vee \ldots \vee p_n$ is also true.

① If q is true, then (2.5) is also true. Likewise, $p_i \rightarrow q$ is true for all i and so is (2.6).

② If q is false, (2.5) is false. Since $p_j \rightarrow q$ is false, so is (2.6).

← What if $p_i \to q$ is false for all i?

Example 2.14 Prove that $2m^2 + 3n^2 = 40$ has no solution in positive integers.

$n \setminus m$	1	2	3	4
1	5	11	21	35
2	14	20	30	44
3	29	35	45	59

2.2-4 Other types of proofs

Example 2.15 (proof of equivalence) Prove that, for every integer n, n is odd, if and only if $n-1$ is even.

To prove that $p_1, p_2, ..., p_n$ are equivalent, the usual method is to prove

(2.7) $(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge ... (p_{n-1} \to p_n) \wedge (p_n \to p_1)$

Example 2.16 (proof of multiple equivalence) Prove that the followings are equivalent:

(a) $A \subseteq B$ (b) $A \cap B = A$ (c) $A \cup B = B$

Example 2.17 (existence proof) Prove that there exists a prime p, such that $2^p - 1$ is composite (*i.e.* not prime).

$2^{11} - 1 = 2047 = 23 \cdot 89$

2.3 Mathematical induction 수학적 귀납법

Principle of mathematical induction

Suppose that we have a propositional function $S(n)$ whose domain of discourse is the set of positive integers. Also, suppose that

(2.8) $S(1)$ is true (Basic step, 기초단계);

(2.9) $\forall n \geq 1$, if $S(n)$ is true (귀납가정, inductive assumption), then $S(n+1)$ is true (Inductive step, 귀납단계).

Then, $S(n)$ is true for every positive integer n.

즉, (1) $S(1)$이 참임을 보이고, (2) $S(n)$이 참이라고 가정한 후, (3) 귀납가정을 기반하여 $S(n+1)$이 참임을 보이는 단계로 구성된다.

Example 2.18 Let

(2.10) $S_n = 1 + 2 + \cdots + n$

Then, $S_n = \frac{1}{2}n(n+1)$

Example 2.19 $\forall n \geq 1,\ n! \geq 2^{n-1}$

$(n+1)! = (n+1)\cdot n! \geq (n+1)\cdot 2^{n-1} \geq 2\cdot 2^{n-1}$

Example 2.20 If $r \neq 1$, then

(2.11) $a + ar + ar^2 + \cdots + ar^n = \frac{a(r^{n+1}-1)}{r-1}$ (geometric sum)

$a + ar + ar^2 + \cdots + ar^{n+1} = a + ar + ar^2 + \cdots + ar^n + ar^n = \frac{a(r^{n+1}-1)}{r-1} + ar^n = \frac{a(r^{n+2}-1)}{r-1}$.

Theorem 4.1 If $|X| = n$, then $|P(X)| = 2^n$, for all $n \geq 0$.

$S(0)$: If $|X| = 0,\ X = \emptyset,\ P(X) = \{\emptyset\}$, and $|P(X)| = 1 = 2^0$

Assume $S(n)$ is true. Suppose $|X| = n+1$ and choose $x \in X$.

- X의 모든 부분집합들은 x를 포함하는 X의 부분집합들의 집합 X_1과 그렇지 않은 집합 X_2로 분류할 수 있다.
- 집합 X_1과 X_2는 집합 $P(X)$의 partition 이며 (즉, $P(X) = X_1 \cup X_2,\ X_1 \cap X_2 = \emptyset$), $|X_1| = |X_2| = 2^n$이고, $|P(X)| = |X_1| + |X_2| = 2\cdot 2^n$이다.
- 예를 들어, $X = \{a,b,c\}$이고 $x = a$이면, $P(X)$는 $X_1(a) = \{\{a\},\{a,b\},\{a,c\},\{a,b,c\}\}$와 $X_2(a) = \{\emptyset,\{b\},\{c\},\{b,c\}\}$로 partition 된다. 그러므로, $|X_1(a)| = |X_2(a)| = 2^2 = 4$이고, $|P(X)| = 4+4 = 2^3$이 된다.

Example 2.21 (Josephus problem) n명으로 구성된 부대가 패배의 위기에 있어 항복 보다는 집단 자살을 선택하기로 하였다. 자결하는 방법으로 다음과 같은 방법을 선택하였다. 먼저 원을 형성하고 시계방향으로 $1,2,\ldots,n$까지 번호를 매기고, 두 번째 사람을 차례로 죽이기로 하였다. $J(n)$을 n 명으로 구성된 집단에서 최후까지 살아남는 사람의 번호를 지칭한다고 할 때,

(1) Compute $J(10)$.

(2) $J(2^i) = 1,\ i \geq 1$, 임을 증명하시오.

(3) For $n \geq 2$, let i be the smallest number such that $2^i \leq n$ (*e.g.*, when $n = 10,\ i = 3$: when $n = 16,\ i = 4$). Also, let $j = n - 2^i$. Show that $J(n) = 2j + 1$.

← At the first round, $\{2,4,\ldots,2j\}$ are killed and there will be $n - j = 2^i$ soldiers alive. $2j+1$에서 시작하여 2^i명이 남아 있으므로, 첫 번째 사람, 즉 $2j+1$번째 군인이 살아 남는다.