Introduction to Proofs

Section 1.7

Proofs of Mathematical Statements

A *proof* 증명 is a valid argument 유효한 주장 that establishes the truth of a statement.

Proofs have many practical applications:

- 프로그램이 correct
- OS 가 secure
- AI 추론 프로그램
- 시스템 명세가 일관됨

Forms of Theorems

universal quantifier 전칭 한정자 생략된 형태

예:

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

는 정확히 적으면

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

Proving Conditional Statements: $p \to q$

Trivial Proof: If we know q is true, then

$p \to q$ is true as well.

"If it is raining then 1=1."

Vacuous Proof: If we know p is false then

$p \to q$ is true as well.

"If I am both rich and poor then $2 + 2 = 5$."

Proving Conditional Statements: $p \rightarrow q$ [1]

Direct Proof: p가 참이라고 가정하고 출발해서 … q *가 참이 된다는 것을 보임*

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

Solution: Assume that n is odd. Then $n = 2k + 1$ for an integer k. Squaring both sides of the equation, we get:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1,$$

where $r = 2k^2 + 2k$, an integer.

We have proved that if n is an odd integer, then n^2 is an odd integer.

(marks the end of the proof. Sometimes **QED** is used instead.)

Proving Conditional Statements: $p \rightarrow q$

Proof by Contraposition: Assume $\neg q$ and show $\neg p$ is true also. This is sometimes called an *indirect proof* method. If we give a direct proof of $\neg q \rightarrow \neg p$ then we have a proof of $p \rightarrow$ q.

Example: Prove that if n is an integer and $3n + 2$ is odd 홀수, then n is odd.

Solution*:* Assume n is even. So, $n = 2k$ for some integer k. Thus

$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j$ for $j = 3k + 1$

Therefore $3n + 2$ is even. Since we have shown $\neg q \rightarrow \neg p$, $p \rightarrow q$ must hold as well. If n is an integer and $3n + 2$ is odd (not even) , then n is odd (not even).

Theorems that are Biconditional Statements 쌍조건문

To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

Example: Prove the theorem: "If n is an integer, then n is odd if and only if n^2 is odd."

Solution: We have already shown (previous slides) that both $p \rightarrow q$ and $q \rightarrow p$. Therefore we can conclude $p \leftrightarrow q$.

Sometimes *iff* is used as an abbreviation for "if and only if," as in

"If n is an integer, then n is odd iff n^2 is odd."

Proof Methods and Strategy

Section 1.8

Proof by Cases 1

To prove a conditional statement of the form:

$$\left(p_1 \vee p_2 \vee \ldots \vee p_n\right) \rightarrow q$$

Use the tautology

$$\left[\left(p_1 \vee p_2 \vee \ldots \vee p_n\right) \rightarrow q\right] \leftrightarrow$$
$$\left[\left(p_1 \rightarrow q\right) \wedge \left(p_2 \rightarrow q\right) \wedge \ldots \wedge \left(p_n \rightarrow q\right)\right]$$

Each of the implications $p_i \rightarrow q$ is a *case*.

Proof by Cases 2

Example: Let a @ b = max{a, b} = a if $a \geq b$, otherwise
a @ b = max{a, b} = b.

Show that for all real numbers a, b, c

$$(a @ b) @ c = a @ (b @ c)$$

(This means the operation @ is associative 결합법칙 성립.)

Proof: Let a, b, and c be arbitrary real numbers.

Then 아래 6가지 경우

1. $a \geq b \geq c$
2. $a \geq c \geq b$
3. $b \geq a \geq c$
4. $b \geq c \geq a$
5. $c \geq a \geq b$
6. $c \geq b \geq a$

Continued on next slide →

Proof by Cases[3]

Case 1: $a \geq b \geq c$

$(a @ b) = a$, $a @ c = a$, $b @ c = b$

Hence $(a @ b) @ c = a = a @ (b @ c)$

그러므로, 성립.

6가지 모두 성립함을 보이면 됨

Existence Proofs

Srinivasa Ramanujan

(1887-1920)

Proof of theorems of the form $\exists x P(x)$.

Constructive existence proof:

- Find an explicit value of *c*, for which *P(c)* is true.
- Then $\exists x P(x)$ is true by Existential Generalization (EG).

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

Proof: 1729 is such a number since

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

Godfrey Harold Hardy

(1877-1947)

Counterexamples 반례

Example: “Every positive integer is the sum of the squares of 3 integers.” The integer 7 is a counterexample. So the claim is false.

Uniqueness Proofs

Some theorems asset the existence of a unique element with a particular property. The two parts of a *uniqueness proof* are

- *Existence*: We show that an element x with the property exists.
- *Uniqueness*: We show that if $y \neq x$, then y does not have the property.

Example: Show that if a and b are real numbers and $a \neq 0$, then there is a unique 유일한 real number 실수 r such that $ar + b = 0$.

Solution:

- Existence: The real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$.
- Uniqueness: Suppose that s is a real number such that $as + b = 0$. Then $ar + b = as + b$, where $r = -b/a$. Subtracting b from both sides and dividing by a shows that $r = s$.

Additional Proof Methods

- 수학적 귀납법 Mathematical induction, which is a useful method for proving statements of the form $\forall n\, P(n)$, where the domain consists of all positive integers.