제2장 Proofs

2.1 Mathematical Systems, Direct Proofs, and Counterexamples

2.2 More Methods of Proofs

2.3 Resolutions Proofs

2.4 Mathematical Induction

2.5 Strong Form of Induction and the Well -Ordering Property

2.1 Mathematical Systems, Direct Proofs, and Counterexamples

- A mathematical system consists of **axiom**공리, **definition**정의, and **undefined term**미정의 용어.
  - Axioms are assumed to be true.
    - Given two distinct points, there is exactly one line that contains them.
    - Given a line and a point not on the line, there is exactly one line through the point which is parallel to the line.
  - Definitions are used to create new concepts in terms of existing ones.
    - Two triangles are congruent if their vertices can be paired so that the corresponding sides are equal and so are the corresponding angles.
    - Two angles are supplementary if the sum of their measures is 180 degrees.

2.1 Mathematical systems, Direct Proofs, and Counterexamples

- A mathematical system consists of **axiom**공리, **definition**정의, and **undefined term**미정의 용어.
  - Some terms are not explicitly defined but rather are implicitly defined by the axioms.
  - Point, Line
- A **theorem**정리 is a proposition that has been proved to be true.
- A **lemma**보조정리 is a theorem that is usually not too interesting in its own right but is useful in proving another theorem.
- A **corollary**따름정리 is a theorem that follows easily from another theorem.
  - If a triangle is an isosceles triangle, the angles are equal
- An argument that establishes the truth of a theorem is called a **proof**증명.

2.1 Mathematical systems, Direct Proofs, and Counterexamples (직접 증명 direct proof)

- Theorems are often of the form:

  For all $x_1, x_2, \ldots, x_n$, if $p(x_1, x_2, \ldots, x_n)$, then $q(x_1, x_2, \ldots, x_n)$.

- This universally quantified statement is true provided that

  $$\text{if } p(x_1, x_2, \ldots, x_n), \text{ then } q(x_1, x_2, \ldots, x_n) \qquad (1.1)$$

  is true for all $x_1, x_2, \ldots, x_n$ in the domain of discourse.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

- To prove (1.1),
  we assume that $x_1, x_2, \ldots, x_n$ are arbitrary members of the domain of discourse.
  If $p(x_1, x_2, \ldots, x_n)$ is false, (1.1) is true.

  A **direct proof** assumes that $p(x_1, x_2, \ldots, x_n)$ is true and then shows directly that $q(x_1, x_2, \ldots, x_n)$ is true.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

2.1 Mathematical systems, Direct Proofs, and Counterexamples (직접 증명 direct proof)

- Definition 2.1.7 An integer n is even짝수 if there exists an integer k such that $n = 2k$. An integer n is odd홀수 if there exists an integer k such that $n = 2k + 1$.
- 예제 2.1.10
  For all integers m and n, if m is odd and n is even, then $m + n$ is odd.
- Proof) Let m and n be arbitrary integers, and suppose that m is odd and n is even. We must prove that $m + n$ is odd.

  By definition, since m is odd, there exists an integer k_1 such that $m = 2k_1 + 1$. Also, by definition, since n is even, there exists an integer k_2 such that $n = 2k_2$.

  Now $m + n = (2k_1 + 1) + (2k_2) = 2(k_1 + k_2) + 1$. Thus, there exists an integer k (namely $k = k_1 + k_2$) such that
  $m + n = 2k + 1$. Therefore, $m + n$ is odd.

2.1 Mathematical systems, Direct Proofs, and Counterexamples (직접 증명direct proof)

예제 2.1.11 Prove that for all sets X, Y, and Z, $X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$

- Poof) We must show that for all x,
  if $x \in X \cap (Y - Z)$, then $x \in (X \cap Y) - (X \cap Z)$ (1.3)
  if $x \in (X \cap Y) - (X \cap Z)$, then $x \in X \cap (Y - Z)$ (1.4)
- Let any $x \in X \cap (Y - Z)$. Then $x \in X$ and $x \in Y - Z$.
  Since $x \in Y - Z$, $x \in Y$ and $x \notin Z$. Since $x \in X$ and $x \in Y$, $x \in X \cap Y$.
  Since $x \notin Z$, $x \notin X \cap Z$. Since $x \in X \cap Y$ and $x \notin X \cap Z$,
  then $x \in (X \cap Y) - (X \cap Z)$. We have proved equation (1.3).
- Let any $x \in (X \cap Y) - (X \cap Z)$. Then $x \in X \cap Y$, $x \notin X \cap Z$
  Since $x \in X \cap Y$, $x \in X$ and $x \in Y$. Since $x \in X$ and $x \notin X \cap Z$, $x \notin Z$
  Since $x \in Y$ and $x \notin Z$, $x \in Y - Z$
  Since $x \in X$ and $x \in Y - Z$, $x \in X \cap (Y - Z)$. proved equation (1.4).

2.1 Mathematical systems, Direct Proofs, and Counterexamples (Disproving a Universally Quantified Statement 전칭 한정된 문장의 반증)

- To disprove $\forall x P(x)$ we simply need to find one member x in the domain of discourse that makes $P(x)$ false. Such a value for x is called a counterexample반례.
- 예제 2.1.14 Prove that the statement $\forall n \in \boldsymbol{Z}^{+}$ $(2^{n} + 1$ is prime) is false.
  A counterexample is $n = 3$ since $2^{3} + 1 = 9$, which is not prime소수.

2.1 Mathematical systems, Direct Proofs, and Counterexamples (Some Common Errors.)

- For all integer m and n, if m and n are even integers then mn is a square (i.e., $mn = a^2$ for some integer a)
- Faulty proof) Since m and n are even, $m = 2k$ and $n = 2k$. Now $mn = (2k)(2k) = (2k)^2$. If we let a = $2k$, then $mn = a^2$ ($m = 2k_1$ and $n = 2k_2$ for some integers k_1 and k_2. The integers k_1 and k_1 need not be equal.)

- Circular reasoning순환 추론: For all integers m and n, if m and $m + n$ are even, then n is even:
  Erroneous proof) Let $m = 2k_1$ and $n = 2k_2$.
  Then $m + n = 2k_1 + 2k_2$. Therefore,
  $$n = (m + n) - m = (2k_1 + 2k_2) - 2k_1 = 2(k_1 + k_2 - k_1)$$
  Thus n is even.
  (We cannot write $n = 2k_2$, which is supposed to prove!).

2.2 More Methods of Proofs (proof by contradiction)

- A contradiction모순 is a proposition of the form $r \wedge \neg r$.
- To prove $p \to q$ is true,
  assume p is true and q is false, and derive a contradiction.
  Since the derivation shows that $(p \wedge \neg q) \to (r \wedge \neg r)$ is true,
  $(p \wedge \neg q) \to (r \wedge \neg r) \equiv p \to q$ justifies the proof method.
- 예제 2.2.1 A proof by contradiction.
  For every $n \in \boldsymbol{Z}$, if n^2 is even, then n is even.
- We assume the hypothesis n^2 is even and that the conclusion is false, n is odd.
  Since n is odd, there exists an integer k such that $n = 2k + 1$.
  $$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$
  Thus n^2 is odd, which contradicts the hypothesis n^2 is even.
  The proof by contradiction is complete.

2.2 More Methods of Proofs (proof by contradiction)

- 예제 2.2.2 For all real numbers x and y,
  if $x + y \geq 2$, then either $x \geq 1$ or $y \geq 1$.

- Proof) Let x and y be arbitrary real numbers.
  Suppose that the conclusion is false, i.e,
  $\neg(x \geq 1 \vee y \geq 1)$ is true.

  By De Morgan's laws of logic,

  $\neg(x \geq 1 \vee y \geq 1) \equiv \neg(x \geq 1) \wedge \neg(y \geq 1) \equiv (x < 1) \wedge (y < 1)$
  In words, we are assuming that $x < 1$ and $y < 1$.
  Adding these inequalities to obtain $x + y < 1 + 1 = 2$.

  At this point, we have derived a contradiction:
  $x + y \geq 2$ and $x + y < 2$.
  Thus we conclude that for all real numbers x and y,
  if $x + y \geq 2$, then either $x \geq 1$ or $y \geq 1$.

2.2 More Methods of Proofs (proof by contradiction)

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

- Assume $\neg p$ and derive a contradiction.
  Since the derivation shows that
  $\neg p \to (r \wedge \neg r)$ is true, so $\neg p$ is false, i.e., p is true.
- 예제 2.2.3 Prove that $\sqrt{2}$ is irrational무리수.
  Proof) Assume that $\sqrt{2}$ is rational. Then there exist integers p and q such that $\sqrt{2} = p/q$. p/q is in lowest term so that p and q are not both even.
  Squaring $\sqrt{2} = p/q$ then multiplying by q^2 gives $2q^2 = p^2$.
  So p^2 is even.
  By 예제 2.2.1., p is even, Thus $p = 2k$ for some integer k.
  $2q^2 = (2k)^2 = 4k^2$. Canceling 2 gives $q^2 = 2k^2$. Therefore q^2 is even. q is even.
  Thus p and q are both even, which contradicts our assumption that p and q are not both even. Therefore, $\sqrt{2}$ is irrational.

2.2 More Methods of Proofs (proof by contrapositive)

- $p \to q \equiv \neg q \to \neg p$
- 예제 2.2.5 Proof by Contrapositive.
  For all $x \in \boldsymbol{R}$, if x^2 is irrational무리수, then x is irrational.
- Proof) We begin by letting x be an arbitrary real number.
  We prove the contrapositive of the given statement:
    if x is not irrational, then x^2 is not irrational or, equivalently,
    if x is rational유리수, then x^2 is rational.
  So suppose that x is rational.
  Then $x = p/q$ for some integers p and q.
  Now $x^2 = p^2/q^2$.
  Since x^2 is the quotient of integers, x^2 is rational.
  The proof is complete.

2.2 More Methods of Proofs (proof by cases)

- Proof by cases is used when the original hypothesis naturally divides itself into various cases. e.g.,
  - "x is a real number" can be divided into cases:

  (a) x is a nonnegative real number

  (b) x is a negative real number.

- Suppose that the task is to prove $p \rightarrow q$ and that p is equivalent to $p_1 \vee p_2 \vee \cdots \vee p_n$ ($p_1, \ldots, p_n$ are the cases).
- Instead of proving

$$(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$$

  we prove

$$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q). \quad (2.2)$$

- As we will show, proof by cases is justified because the two statements are equivalent.

2.2 More Methods of Proofs (proof by cases)

- $(p_1 \vee p_2 \vee \cdots \vee p_n) \to q$ ①
  $(p_1 \to q) \wedge (p_2 \to q) \wedge \cdots \wedge (p_n \to q)$ ②

- Suppose that q is true.
  Then all the implications in ① and ② are true.
  Thus ① and ② are true.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

- Suppose that q is false.
  If all the p_i are false, then all the implications in ① and ② are true, so ① and ② are true.
  If for some j, p_j is true, then $p_1 \vee \cdots \vee p_n$ is true, so ① is false.
  Since $p_j \to q$ is false, ② is false. Thus ① and ② are false.

- Therefore, ① and ② are equivalent.

2.2 More Methods of Proofs (proof by cases)

- Exhaustive proof(전수증명) Sometimes the number of cases to prove is finite, so we can check them all one by one.

- 예제 2.2.6 Prove that $2m^2 + 3n^2 = 40$ has no solution in positive integers. (i.e., $2m^2 + 3n^2 = 40$ is false for all positive integers m and n.)

- Proof) If $2m^2 + 3n^2 = 40$,
  we must have $2m^2 \leq 40$. Thus $m^2 \leq 20$ and $m \leq 4$.
  Similarly, we must have $3n^2 \leq 40$. Thus $n^2 \leq 40/3$ and $n \leq 3$.
  Thus it suffices to check the cas .

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

  Since $2m^2 + 3n^2 \neq 40$ for $m = 1, 2, 3, 4$ and $n = 1, 2, 3$, and $2m^2 + 3n^2 > 40$ for $m > 4$ or $n > 3$, we conclude that $2m^2 + 3n^2 = 40$ has no solution in positive integers.

2.2 More Methods of Proofs (proof by cases)

- 예제 2.2.7 Prove that for every real number x, $x \leq |x|$.
- Discussion Since x is a real number, either $x \geq 0$ *or* $x < 0$. We use this *or* statement to divide the proof into cases. We divide the proof into cases because the definition of absolute value is itself divided into cases $x \geq 0$ and $x < 0$.
  Case 1 is $x \geq 0$ and case 2 is $x < 0$.
- Proof) If $x \geq 0$, by definition $|x| = x$. Thus $|x| \geq x$.
  If $x < 0$, by definition $|x| = -x$.
  Since $|x| = -x > 0$ and $x < 0$, $|x| \geq x$.
  In either case, $|x| \geq x$; so the proof is complete.

2.2 More Methods of Proofs (Proofs of Equivalence)

- To prove
  p if and only if q
  prove
  if p then q and if q then p
- This is justified by $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
- 예제 2.2.9 Prove that for all integer n, n is odd iff $n - 1$ is even.
- Proof) We first prove that if n is odd then $n - 1$ is even.
  If n is odd, then $n = 2k + 1$ for some integer k.
  Now $n - 1 = (2k + 1) - 1 = 2k$. Therefore, $n - 1$ is even.
  Next we prove that if $n - 1$ is even then n is odd.
  If $n - 1$ is even, then $n - 1 = 2k$ for some integer k.
  Now $n = 2k + 1$. Therefore, n is odd.
  The proof is complete.

2.2 More Methods of Proofs (Existence Proofs)

- A proof of $\exists x\, P(x)$.
- An existence proof of $\exists x\, P(x)$ that exhibits an element a of the domain of discourse that makes $P(a)$ true is called a **constructive proof**건설적인 증명.
- 예제 2.2.12 Let a and b be real numbers with $a < b$. Prove that there exists a real number x satisfying $a < x < b$.
- Proof) It suffices to find one real number x satisfying $a < x < b$. The real number

$$x = \frac{a+b}{2}$$

surely satisfies $a < x < b$.

2.3 Resolution Proofs분해증명

- Resolution proof was Proposed by J. A. Robinson (1965)
  - Hypothesis and conclusion are written as clauses
  - clause : a compound statement with terms separated by "or ($\vee$)", and each term is a single variable or the negation ($\neg$) of a single variable

    Ex) $p \vee q \vee (\neg r)$ is a clause, $(p \wedge q) \vee r \vee (\neg s)$ is not a clause
  - depends on a single rule:

    If $p \vee q$ and $\sim p \vee r$ are both true, then $q \vee r$ is true
- 예제 2.3.1 $a \vee b \vee \neg c \vee d$ is a clause
- 예제 2.3.2 $xy \vee w \vee \neg c$ is not a clause as xy consists of two variables
- 예제 2.3.3 $p \rightarrow q$ is not a clause since terms are separated by $\rightarrow$

2.3 Resolution Proofs분해증명

- 예제 2.3.4 Prove the following using resolution

  1. $a \vee b$
  2. $\neg a \vee c$
  3. $\neg c \vee d$

  $\therefore b \vee d$

  - Sol) From 1 and 2, we drive 4. $b \vee c$

    From 3 and 4, we drive $b \vee d$

- Special cases

  If $p \vee q$ and $\neg p$ are both true, then q is true

  If $\neg p \vee r$ and p are both true, then r is true

2.3 Resolution Proofs분해증명

- 예제 2.3.5 Prove the following using resolution

  1. a
  2. $\neg a \vee c$
  3. $\neg c \vee d$

  $\therefore d$

  - Sol) From 1 and 2, we drive 4. c

    From 3 and 4, we drive d

- Hypothesis must be expressed by equivalent expressions

  $\neg (a \vee b) \equiv \neg a \neg b,$ $\quad \neg (ab) \equiv \neg a \vee \neg b$

  $a \vee bc \equiv (a \vee b)\ (a \vee c)$

2.3 Resolution Proofs분해증명

- 예제 2.3.6 Prove the following using resolution

  1. $a \lor \neg bc$
  2. $\neg (a \lor d)$

  $\therefore \neg b$

Sol) 1.1 $a \lor \neg b$

2.1 $a \lor c$ 　　1.1 and 2.1 are derived from 1

3.1 $\neg a$

4.1 $\neg d$ 　　3.1 and 4.1 are derived from 2

$\therefore \neg b$

2.4 수학적 귀납법Mathematical Induction

- **Principle of Mathematical Induction**수학적 귀납법의 원리

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

  $$S(1) \text{ is true;} \tag{4.7}$$

  $$\text{for all } n \geq 1, \text{ if } S(n) \text{ is true, then } S(n+1) \text{ is true.} \tag{4.8}$$

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

- (4.7) **Basis Step**기본단계, (4.8) **Inductive Step**귀납단계

- Hereafter, "induction" will mean "mathematical induction."

- To verify that the statements

  $$S(n_0),\quad S(n_0+1),...$$

  are true, the Basis Step become $S(n_0)$ is true.

  the Inductive Step become

  for all $n \geq n_0$, if $S(n)$ is true, then $S(n+1)$ is true.

2.4 수학적 귀납법 Mathematical Induction

- 예제 2.4.3 Use induction to show that $n! \geq 2^{n-1}$ for all $n \geq 1$. (4.9)

- Basis Step ($n = 1$): We must show that (4.9) is true if $n = 1$.
  $1! = 1,\ 2^{1-1} = 1. \therefore 1! \geq 2^{1-1}$

- Inductive Step: We assume that $n! \geq 2^{n-1}$ is true.
  We must prove that
  $$(n+1)! \geq 2^n \qquad (4.11)$$
  is true.
  $$\begin{aligned}(n+1)! &= (n+1)(n!) \\ &\geq (n+1)2^{n-1} && \text{by the assumption} \\ &\geq 2 \cdot 2^{n-1} && \text{since } n+1 \geq 2 \\ &= 2^n.\end{aligned}$$
  Therefore, (4.11) is true.

- Since the Basis Step and the Inductive Step have been verified, the Principle of Mathematical Induction tells us that (4.9) is true for every positive integer n.

2.4 수학적 귀납법Mathematical Induction

- 예제 2.4.4 Use induction to show that if $r \neq 1$,

$$a + ar^1 + ar^2 + \cdots + ar^n = \frac{a(r^{n+1} - 1)}{r - 1} \qquad (4.12)$$

for all $n \geq 0$.

- Basis Step ($n = 0$): For $n = 0$, (4.12) becomes $a = a(r^1 - 1) / (r - 1)$, which is true.

- Inductive Step: Assume that statement (4.12) is true for n.

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

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

- Since the Basis Step and the Inductive Step have been verified, the Principle of Mathematical Induction tells us that (4.12) is true for all $n \geq 0$.

2.4 수학적 귀납법Mathematical Induction

- 예제 2.4.5 Show that $5^n - 1$ is divisible by 4 for all $n \geq 1$.
- Basis Step ($n = 1$)
  If $n = 1$, $5^n - 1 = 5^1 - 1 = 4$, which is divisible by 4.
- Inductive Step
  We assume that $5^n - 1$ is divisible by 4.
  We must then show that $5^{n+1} - 1$ is divisible by 4.
  Since $5^n - 1$ is divisible by 4, $5^n - 1 = 4k$ for some integer k.
  So $5^n = 4k + 1$.
  $$5^{n+1} - 1 = 5 \cdot 5^n - 1 = 5 \cdot (4k + 1) - 1 = 4(5k + 1),$$
  Thus $5^{n+1} - 1$ is divisible by 4
- Since the Basis Step and the Inductive Step have been verified, the Principle of Mathematical Induction tells us that $5^n - 1$ is divisible by 4 for all $n \geq 1$.

2.4 수학적 귀납법Mathematical Induction

- 정리 2.4.6 Let X be a set. If $|X| = n$, then

  for all $n \geq 0$ $|\mathcal{P}(X)| = 2^n$ (4.13)

$\{a\}$	$\{\}$
$\{a, b\}$	$\{b\}$
$\{a, c\}$	$\{c\}$
$\{a, b, c\}$	$\{b, c\}$

- Proof

  1) Basis Step ($n = 0$)
  If $n = 0$, X is the empty set. $\mathcal{P}(X) = \{\emptyset\}$. Thus, $|\mathcal{P}(X)| = 1 = 2^0 = 2^n$. Thus, (4.13) is true for $n = 0$.

  2) Inductive Step: Assume that (4.13) holds for n.
  Let X be a set with $n + 1$ elements. Choose $x \in X$.

  Lemma: Since each subset S of X that contains x can be paired uniquely with $S - \{x\}$, exactly half of the subsets of X contain x, and exactly half of the subsets of X do not contain x.

  If $Y = X - \{x\}$, Y has n elements. By the inductive assumption, $|\mathcal{P}(Y)| = 2^n$. But the subsets of Y are precisely the subsets of X that do not contain x. By the previous Lemma, we conclude that $|\mathcal{P}(Y)| = |\mathcal{P}(X)|/2$.
  Therefore, $|\mathcal{P}(X)| = 2|\mathcal{P}(Y)| = 2 \cdot 2^n = 2^{n+1}$.

2.4 수학적 귀납법Mathematical Induction

- A **loop invariant(루프 불변)** is a statement about program variables that
  is true just before a loop begins executing
  and is also true after each iteration of the loop.
- A loop invariant is true after the loop finishes, at which point the invariant tells us something about the state of the variables.
- ```
  while (condition)
      // loop body
  ```
- We can use mathematical induction to prove that an invariant has the desired behavior.
- The Basis Step proves that the invariant is true before the condition that controls looping is tested for the first time.
- The Inductive Step assumes that the invariant is true and then proves that if the condition that controls looping is true, the invariant is true after the loop body executes.
  ```

2.4 수학적 귀납법Mathematical Induction

- 예제 2.4.8 Use a loop invariant to prove that when the pseudocode terminates, `fact` is equal to `n!`.

```
i = 1
fact = 1
while (i < n) {
    i = i + 1
    fact = fact * i
}
```

- Sol) We prove that `fact = i!` is an invariant for the while loop.
- Just before the while loop begins executing, `i = 1` and `fact = 1`, so `fact = 1!`. We have proved the Basis Step.
- Assume that `fact = i!`. If `i < n` is true, `i` becomes `i + 1` and `fact` becomes `fact * (i + 1) = i! * (i + 1) = (i + 1)!`. We have proved the Inductive Step. Therefore, `fact = i!` is an invariant for the while loop.
- The while loop terminates when `i = n`. Because `fact = i!` is an invariant, at this point, `fact = n!`.

2.5 강한 형식의 귀납법 및 정렬 순서 속성

- Strong Form of Mathematical Induction
  Suppose that we have a propositional function $S(n)$ whose domain of discourse is the set of integers greater than or equal to n_0. Suppose that
  Basic Step : $S(n_0)$ is true
  Induction Step : for all $n > n_0$, if $S(k)$ is true for all $k, n_0 \leq k < n$, then $S(n)$ is true.
  Then $S(n)$ is true for every integer $n \geq n_0$.

- The two forms of mathematical induction are logically equivalent.

2.5 강한 형식의 귀납법 및 정렬 순서 속성

- 예제 2.5.1 Show that postage우편 요금 of 4 cents or more can be achieved by using only 2-cent and 5-cent stamps우표.
- Basis Steps ($n = 4,\ n = 5$)
  We can make 4-cents postage by using two 2-cent stamps.
  We can make 5-cents postage by using one 5-cent stamp.
  The Basis Steps are verified.

$$\boxed{n - 2 \geq 4}$$

- Inductive Step
  We assume that $n \geq 6$ and that postage of k cents or more can be achieved by using only 2-cent and 5-cent stamps for $4 \leq k < n$. By the inductive assumption, we can make postage of $n - 2$ cents. We add a 2-cent stamp to make n cents postage.
  The Inductive Step is complete.

2.5 강한 형식의 귀납법 및 정렬 순서 속성

- 예제 2.5.2 If the sequence $c_1, c_2, \ldots$ is defined by the equations
  $c_1 = 0, \quad c_n = c_{\lfloor n/2 \rfloor} + n$ for all $n > 1$.
  then $c_n < 2n$, for all $n \geq 1$.

$$c_2 = c_{\lfloor 2/2 \rfloor} + 2 = c_1 + 2 = 2$$
$$c_5 = c_{\lfloor 5/2 \rfloor} + 5 = c_2 + 5 = 7$$

- Basis Step $(n = 1)$
  Since $c_1 = 0 < 2 = 2 \cdot 1$, the Basis Step is verified.

- Inductive Step
  We assume that $c_k < 2k$, for all k, $1 \leq k < n$,
  and prove that $c_n < 2n$, for all $n > 1$.
  Since $1 < n$, $2 \leq n$. Thus $1 \leq n/2 < n$. Thus $1 \leq \lfloor n/2 \rfloor < n$.
  By the inductive assumption

$$c_{\lfloor n/2 \rfloor} = c_{\mathrm{k}} < 2k = 2\lfloor n/2 \rfloor$$

Now

$$c_n = c_{\lfloor n/2 \rfloor} + n < 2\lfloor n/2 \rfloor + n \leq 2(n/2) + n = 2n.$$

The Inductive Step is complete.

2.5 강한 형식의 귀납법 및 정렬 순서 속성

- The **Well-Ordering Property** for nonnegative integers:
  Every nonempty set of nonnegative integers has a least element.

- This property is equivalent to the two forms of induction.

- 정리 2.5.6 **Quotient-Remainder Theorem** 몫-나머지 정리
  If d and n are integers, $d > 0$, there exist integers q (quotient) and r (remainder) satisfying $n = dq + r, \quad 0 \leq r < d$.
  Furthermore, q and r are unique.

- Proof) Let $X = \{n - dk \mid n - dk \geq 0, k \in \boldsymbol{Z}\}$.
  We show that X is nonempty using proof by cases.
  If $n \geq 0$, then $n - d \cdot 0 = n \geq 0$ so n is in X.
  Suppose that $n < 0$. Since d is a positive integer, $1 - d \leq 0$.
  Thus $n - dn = n(1 - d) \geq 0$. In this case, $n - dn$ is in X.
  Therefore X is nonempty.

2.5 강한 형식의 귀납법 및 정렬 순서 속성

- Since X is a nonempty set of nonnegative integers, by the Well-Ordering Property, X has a smallest element r. We let q denote the specific value of k for which $r = n - dq$. Then $n = dq + r$. Since r is in X, $r \geq 0$. We use proof by contradiction to show that $r < d$. Suppose that $r \geq d$. Then $n - d(q+1) = n - dq - d = r - d$.

  Since $r - d \geq 0$, $r - d \in X$ and $r - d < r$. But r is the smallest integer in X. This contradiction shows that $r < d$.
- We have shown that if d and n are integers, $d > 0$, there exist integers q and r satisfying $n = dq + r$ $\quad 0 \leq r < d$.

2.5 강한 형식의 귀납법 및 정렬 순서 속성

- We turn now to the uniqueness of q and r. Suppose that

$$n = dq_1 + r_1 \qquad 0 \le r_1 < d$$

and

$$n = dq_2 + r_2 \qquad 0 \le r_2 < d$$

We must show that $q_1 = q_2$ and $r_1 = r_2$.
Subtracting the previous equations, we obtain

$$0 = (dq_1 + r_1) - (dq_2 + r_2) = d(q_1 - q_2) - (r_2 - r_1)$$

which can be rewritten $d(q_1 - q_2) = r_2 - r_1$.

The preceding equation shows that d divides $r_2 - r_1$.

Because $0 \le r_1 < d$ and $0 \le r_2 < d$, $-d < r_2 - r_1 < d$.

But the only integer between $-d$ and d divisible by d is 0.
Therefore, $r_1 = r_2$. Thus, $d(q_1 - q_2) = 0$; hence, $q_1 = q_2$.

The proof is complete.