Study Title <2> PROOFS Date

※ 2.1 Mathematical Systems, Direct Proofs, and Counterexample

- Mathematical system

  - consist of axioms, definitions, undefined terms.
    - axioms → Assumed to be true.
    - definitions ↳ used to create new concepts. (existing ones)
    - undefined terms ↳ Implicitly defined by the axioms.

  - theorem: proposition that has been proved to be true.

    - lemmas: special kinds of theorem ①
      → usually not too interesting in its own right but useful in proving another theorem.

    - Corollary: special kinds of theorem ②
      → follows easily from another theorem.

  - Proof: An argument that establishes the truth of a theorem.
    → then. Logic is a tool for the analysis of proofs

- Direct Proof

  - Def: assumes that assumption is true, and then shows directly that conclusion is true.

  - only consider the case hypothesis is true
    → because of vacuously true

  - In constructing a proof, we may find that we need some auxiliary results.
    → Subproof: proofs of auxiliary results

- Disproving a universally Quantified Statement.

  - Counterexample: value for x in the domain of discourse that makes false

- Some Common Errors

  1. The same notation for two possibly distinct quantities.
  2. Showing that the propositional function is true for specific values in the domain of discourse is not a proof
     → propositional function is true for all value in the domain of discourse.
  3. cannot assume what you are supposed to prove.
     → begging the question or circular reasoning

Study Title ____________ Date ______

※ 2.2 More Methods of Proof

• Proof by Contradiction

∘ def: establishes $p \to q$ by assumming that p is true, q is false and then, derives contradiction
↓
proposition of the form $r \wedge \neg r$ (r may be any propos)

∘ Point 1. this proof assumes that conclusion is negated.
2. Justified by noticing $p \to q$ and $(p \wedge \neg q) \to (r \wedge \neg r)$ are equivalence.

• Proof by Contrapositive

∘ def: using that $p \to q$ and $\neg q \to \neg p$ are equivalent

· Proof by Cases (exhausitve proof)

∘ def: proof by using when the original hypothesis naturally divides itself into various cases.
↓
to prove $p \to q$ ⇒ $p_1 \vee p_2 \vee \cdots \vee p_n$ is equal to p

∘ we prove $(p_1 \to q) \wedge (p_2 \to q) \wedge \cdots \wedge (p_n \to q)$ … ⓐ
equals to $(p_1 \vee p_2 \vee \cdots \vee p_n) \to q$

∘ Process
1. Suppose that q is true.
▫ If q is true, then all Implications in ⓐ are true. regardless of the truth value of the hyphothesis.

2. Suppose that q is false.

▫ If q is false, and all p_i are false, then ⓐ are true.
↓

▫ 〃 . and for some j, p_j is true, $p_1 \vee p_2 \vee \cdots \vee p_n$ is true. so $(p_1 \vee p_2 \vee \cdots \vee p_n) \to q$ is false.
Since $p_j \to q$ is false, ⓐ is false.

• Proofs of Equivalence

∘ def: prove by using the equivalence

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

∘ It can use the proof by cases
↓
$(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \cdots \wedge (p_{n-1} \to p_n) \wedge (p_n \to p_1)$

• Extensive Proof

∘ Def: A proof of $\exists x P(x)$

Study Title ______________________ Date __________

※ 2.4 Mathematical Induction

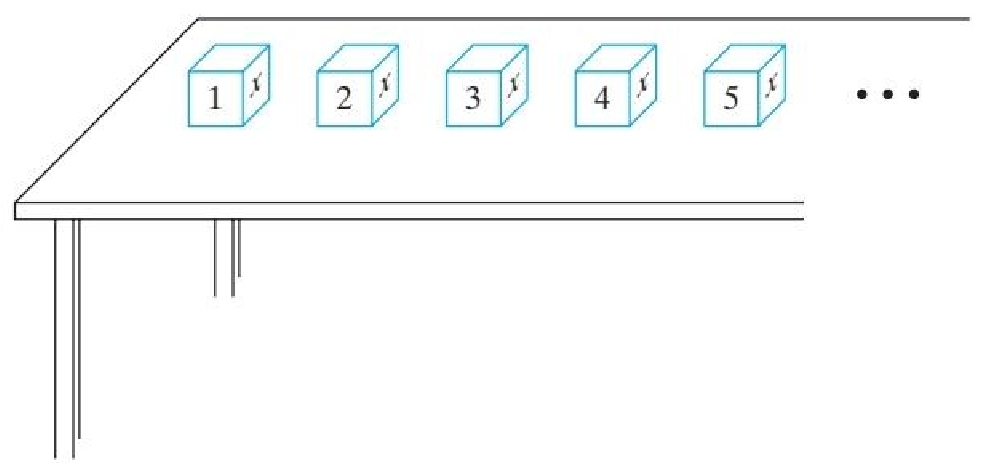

Figure 2.4.1 Numbered blocks on a table.

· Suppose that a sequence of blocks numbered 1, 2, …, sits on an long table and some blocks are marked "x"

① The first block is marked

② For all n, if block n is marked, then block n+1 is also marked.

→ Thus block 2, 3, … is also marked

· This preceding example illustrate the Principle of Mathematical Induction.

↳ How to prove the proposition that all natural number satisfy the given proposition.

→ using the axioms, $1 \in X$, $n \in X \rightarrow n+1 \in X$

· $S_n = 1+2+\cdots+n = \frac{n(n+1)}{2}$

$S_{n+1} = ?$

$$\rightarrow S_{n+1} = 1+2+\cdots+n+n+1$$

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

$$= \frac{n^2+n+2n+2}{2} = \frac{(n+1)(n+2)}{2}$$

· Proof using induction consisted of two steps.

① verify that the statement corresponding to $n=1$ is true // Basic Step

② n is true, and then proves that statement n+1 is also true. // Inductive Step

※ 2.5 Strong Form of Induction and the Well-Ordering Property

• Strong Form of Induction

∘ Def: Suppose that we have a propositional function $S(n)$ whose domain of discourse is the set of integer greater than or equal to n_0.

1. $S(n_0)$ is true
2. for all $n > n_0$, if $S(k)$ is true for all k, $(n_0 \le k < n)$, then $S(n)$ is true.

→ $P(1)$ is true, then for all integer k, $P(1), P(2), \ldots, P(k)$ is true, then $P(k+1)$ is true.

∘ When?

▫ Strong form: you have to know the result before the k_{th}

▫ Normal form: when the k+1 can be proved only with the k expression.

• Well-Ordering Property

∘ def: every nonempty set of non-negative integer has a least element.

→ It is equivalent to the axioms of Induction.

∘ Quotient - Remainder Theorem

▫ If d and n are integer ($d>0$), there exist integer q and r satisfying $n = dq + r$ (q: quotient, r: remainder)

ex) $n=74$, $d=13$

$$\begin{array}{r} 5 \cdots q \\ d \cdots 13\overline{)74} \\ \underline{65} \\ 9 \cdots r \end{array}$$

$n = dq + r$

$74 = 13 \cdot 5 + 9$