

2 Proofs

2.1. Mathematical Systems, Direct Proofs, and Counter Examples

Some Terminologies

Axiom: Assumption to be true (often **unproven**) *undefined terms*
defining the **structures** about which we are reasoning.

Theorem: A statement that has been **proven** to be true. $p \rightarrow q$

Rules of inference: Patterns of logically valid deductions
from **hypotheses** to **conclusion**.

Lemma: A minor theorem used as a stepping stone
to prove a major theorem

Corollary: A minor theorem proven
as an **easy consequence** of a major theorem

Conjecture: A statement whose **truth** has **not** been **proven**.
(A conjecture may be widely believed to be true, regardless)

Theory: The set of **all axioms and theorems** that

can be proven from a **given set of axioms**

Direct Proof

$\forall x \in D: P(x) \Rightarrow Q(x)$ *predicate logic*

$P(c) \rightarrow Q(c)$ *universal generalization(\Downarrow) instantiation(\Uparrow)*

$p \rightarrow q$ *propositional logic*

Def. 2.1.7 $\forall n \in \mathbf{Z}: E(n) \equiv (\Leftrightarrow) \exists k \in \mathbf{Z}: n=2k$

$\forall n \in \mathbf{Z}: O(n) \equiv (\Leftrightarrow) \exists k \in \mathbf{Z}: n=2k+1.$

Exa. 2.1.10 $\forall n, m \in \mathbf{Z}: (O(n) \wedge E(m) \Rightarrow E(n+m))$

proof $\exists i, j \in \mathbf{Z}: n = 2i + 1 \wedge m = 2j$ **Def. 2.1.7**(\Rightarrow)

$n + m = 2(i+j) + 1 = 2k + 1$ *calculus, $k = i+j$*

$(\exists k \in \mathbf{Z}: n+m = 2k+1) \Rightarrow n+m \in O(n)$ **Def. 2.1.7**(\Leftarrow)

$\forall n, m \in \mathbf{Z}: (O(n) \wedge E(m) \Rightarrow E(n+m))$ *universal instantiation*

Proofs of Set equalities

Let A and B be sets. Then $A = B$.

proof

$$1)(\Rightarrow) \quad A \subseteq B \quad \forall x \in A \Rightarrow x \in B.$$

$$2)(\Leftarrow) \quad B \subseteq A \quad \forall x \in B \Rightarrow x \in A.$$

Exa. 2.1.12 Let (If in this text) X , Y , and Z be sets. Then

$$X \cap (Y - Z) = (X \cap Y) - (X \cap Z).$$

proof 1)(\Rightarrow) $x \in X \cap (Y - Z)$ universal instantiation of **hypothesis**

$$x \in X \wedge (x \in Y \wedge x \notin Z) \quad \text{def. of } \cap \text{ and } -$$

$$(x \in X \wedge x \in Y) \wedge (x \notin Z) \quad \text{itempotent(???)}$$

$$(x \in X \wedge x \in Y) \wedge (x \notin X \wedge x \notin Z) \quad \text{???)}$$

$$(x \in X \cap Y) \wedge (x \notin X \cap Z) \quad \text{def of } \cap \text{ alg. rules}$$

$$x \in (X \cap Y) - (X \cap Z) \quad \text{def. of } -$$

2)(\Leftarrow) left for exercise

$$\begin{aligned}
 \text{proof2 } X \cap (Y - Z) &= X \cap (Y \cap \bar{Z}) && \text{def. of } - \\
 &= (X \cap Y) \cap (X \cap \bar{Z}) && \text{dis. law} \\
 &= X \cap Y \cap \bar{Z} && \text{disjunctive normal form} \\
 X \cap (Y \cap \bar{Z}) &= X \cap Y \cap \bar{Z} && \text{disj. n. f.} \\
 &\text{Q.E.D.}
 \end{aligned}$$

proof3 Venn diagram and disjunctive (normal) form

Exa. 2.1.13 Let X and Y be sets. Then

$$X \cup (Y - X) = X \cup Y.$$

$$\begin{aligned}
 \text{proof3 } X \cup (Y - X) &= X \cup (Y \cap \bar{X}) && \text{def. of } - \\
 &= (X \cup Y) \cap (X \cup \bar{X}) = (X \cup Y) \cap U && \text{dist. and comp} \\
 &= X \cup Y = (X \cap U) \cup (Y \cap U) && \text{idemp. and ident.} \\
 &= (X \cap (Y \cup \bar{Y})) \cup (Y \cap (X \cup \bar{X})) && \text{complement} \\
 &= (X \cap Y) \cup (X \cap \bar{Y}) \cup (X \cap Y) \cup (\bar{X} \cap Y) && \text{distribution} \\
 &= (X \cap Y) \cup (\bar{X} \cap Y) \cup (X \cap \bar{Y}) && \text{idemp. and d.n.f} \\
 X \cup Y &= (X \cap Y) \cup (\bar{X} \cap Y) \cup (X \cap \bar{Y}) && \text{d.n.f}
 \end{aligned}$$

Disproving a univerrally quantified statement

$$\forall x \in D: P(x)$$

To **disprove** the above statement, find atmost one **counterexample**.

Exa. 2.1.15 Let $A, B, abd C$ be sets. Prove the statement

$$(A \cap B) \cup C = A \cap (B \cup C)$$

or give a **counterexample**.

proof insight Venn diagram

$$\overline{A} \cdot B \cdot C, \overline{A} \cdot \overline{B} \cdot C \not\subseteq (A \cap B) \cup C \text{ but } \subseteq A \cap (B \cup C)$$

$$U = \{1, 2, 3, 4, 5, 6, 7, 8\}, A = \{1, 4, 5, 7\}, B = \{2, 4, 6, 7\}, C = \{3, 5, 6, 7\}$$

$$A \cdot B \cdot C = \{7\} \quad A \cdot \overline{B} \cdot C = \{5\} \quad A \cdot B \cdot \overline{C} = \{4\} \quad A \cdot \overline{B} \cdot \overline{C} = \{1\}$$

$$\overline{A} \cdot B \cdot C = \{6\} \quad \overline{A} \cdot \overline{B} \cdot C = \{3\} \quad \overline{A} \cdot B \cdot \overline{C} = \{2\} \quad \overline{A} \cdot \overline{B} \cdot \overline{C} = \{8\}$$

$\{A \cdot B \cdot C, A \cdot \overline{B} \cdot C, A \cdot B \cdot \overline{C}, A \cdot \overline{B} \cdot \overline{C}, \overline{A} \cdot B \cdot C, \overline{A} \cdot \overline{B} \cdot C, \overline{A} \cdot B \cdot \overline{C}, \overline{A} \cdot \overline{B} \cdot \overline{C}\}$ is a partion of U .

$$\overline{A} \cdot B \cdot C = \{6\}, \overline{A} \cdot \overline{B} \cdot C = \{3\} \quad \text{counterexamples}$$

2.2 More Methods of Proofs

Proofs by Contradiction

$$p \Rightarrow q \equiv (p \wedge \neg q) \Rightarrow (r \wedge \neg r) \equiv (p \wedge \neg q) \Rightarrow \mathbf{F}$$

proof Truth table in the text

$$p \Rightarrow q = \neg p \vee q$$

$$(p \wedge \neg q) \Rightarrow (r \wedge \neg r) = \neg(p \wedge \neg q) \vee \mathbf{F} = \neg p \vee q \quad \text{def. of } \Rightarrow \text{ \& comp.}$$

$$(p \wedge \neg q) \Rightarrow \mathbf{F} = \neg(p \wedge \neg q) \vee \mathbf{T} = \neg p \vee q. \quad \text{def. of } \Rightarrow \text{ \& De Morgan's.}$$

Exa 2.2.1 $\forall n \in \mathbf{Z}: E(n^2) \Rightarrow E(n)$.

proof $n^2 = 2k, \exists k' . \exists. n = 2k'$. *difficult*

proof by contradiction, negation of the conclusion

$$E(n^2) \Rightarrow O(n). \quad \forall k \in \mathbf{Z}, n = 2k+1$$

$$n^2 = 4k^2 + 4k + 1 = 2(k^2 + k) + 1 \quad O(n^2).$$

$$(E(n^2) \wedge \neg E(n)) \Rightarrow \mathbf{F} \equiv E(n^2) \Rightarrow E(n).$$

Proof by Contrapositive

$$p \Rightarrow q \equiv \neg q \Rightarrow \neg p$$

$$p \Rightarrow q \equiv \neg q \Rightarrow \neg p$$

Exa. 2.2.4 “ $\forall x \in \mathbf{R}: x^2$ is irrational $\Rightarrow x$ is irrational.

proof Assume x is rational, $x = p/q$ where $p, q \in \mathbf{Z}$.

$x^2 = p^2/q^2$. x^2 is rational. Q.E.D.

Proof by Cases(exhaustive proof)

$$(p_1 \vee p_2 \vee \dots \vee p_n) \Rightarrow q \equiv (p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \dots \wedge (p_n \Rightarrow q).$$

Exa. 2.2.5 $\forall m, n \in \mathbf{Z}^+, 2m^2 + 3n^2 = 40$ has no solution(is **F**).

proof $2m^2 \leq 40, 3n^2 \leq 40.$ $m^2 \leq 20, n^2 \leq 14.$

$m = 1, 2, 3, 4.$ $n = 1, 2, 3.$ $4 \times 3 = 12$ cases.

See table in p.80.

Proof of Equivalence

p if and only if q.

$$p \Leftrightarrow q. (p \equiv q, p = q)$$

$$p \Rightarrow q \wedge q \Rightarrow p.$$

Exa 2.2.9 Let A , B , and C be sets. Following statements are **equivalent**.

(a) $A \subseteq B$

(b) $A \cap B = A$

(c) $A \cup B = B$.

proof [(a) \Rightarrow (b)] Assume $A \subseteq B$ and prove $A \cap B = A$.

$\forall x \in A \cap B, x \in A$ by the definition of \cap

$\forall x \in A, x \in B$ (since $A \subseteq B$), $\therefore \forall x \in A \cap B$.

[(b) \Rightarrow (c)], [(c) \Rightarrow (a)].

Existence proof

$$\exists x P(x)$$

Exa 2.2.11 \exists a prime p \exists . $2^p - 1$ is **not prime** (composite)

proof By tryial and error, we foind $2^p - 1$ is **prime** for $p = 2, 3, 5, 7$.

for $p = 11, 2^{11} - 1 = 2048 - 1 = 2047 = 23 \cdot 89$.

Mersenne(1588-1648) prime(p 84)

2006, 44th Mersenne prime $2^{3258,2657} - 1 \cong 980,8358$ dec. digits
(GIMPS) Great Internet Mersenne Prime Search

Exa 2.2.12 Let $A = \sum_{j \in J} s_j / n$ where $J = \{1, 2, \dots, n\}$.

Then $\exists i \in J . \exists. s_i \geq A$.

proof by contradiction

Assume $\neg \exists i: (s_i \geq A) = \forall i \in J: (s_i < A)$.

Since $|A| = n$, $\sum_{j \in J} s_j < n \cdot A$. $\therefore \sum_{j \in J} s_j / n < A$

contradiction with hypothesis

constructive proof

2.2.5, 2.2.9, 2.2.11

nonconstructive proof

2.2.4, 2.2.12

Vacuous proof

If $p = \mathbf{F}$, $p \Rightarrow q$ is a tautology.

Trivial proof

If $q = \mathbf{T}$, $p \Rightarrow q$ is a tautology.

Mistakes in Proof

Example 16 divide by zero

Example 17 $(p \Rightarrow q)$ does not implies $(q \Rightarrow p)$

Example 18 $(p \Rightarrow q)$ does not implies $(\neg p \Rightarrow \neg q)$

Fallacies in Implication

$((p \rightarrow q) \wedge q) \Rightarrow p$ *fallacy of affirming the conclusion*

*Implication says **nothing** even though the conclusin is true!*

$((p \rightarrow q) \wedge \neg p) \Rightarrow \neg q$ *fallacy of denying the hypothesis*

*Implication says **nothing** when the hypotheses are false!*

Example 9

$p =$ “At least four of any 22 days must fall on the same day of the week”

$\neg p =$ “At most three of 22 days ...”

$r =$ “22 days are chosen”

$\neg p \rightarrow (r \wedge \neg r)$, p is a tautology.

Example 10 Prove that $\sqrt{2}$ is irrational.

$p =$ “ $\sqrt{2}$ is irrational”

$\neg p =$ “ $\sqrt{2}$ is rational”

$\sqrt{2} = a/b$, a and b are integers.

$$2 = a^2/b^2$$

$$2b^2 = a^2.$$

a^2 is even, a is also even. $a = 2c$.

$$a^2 = 4c^2 = 2b^2.$$

$$b^2 = 2c^2.$$

b^2 is even. b is even.

$\sqrt{2} = a/b$, a and b are **even** integers

2.3 Resolution Proofs

$$(p \vee q) \wedge (\neg p \vee r) \Rightarrow q \vee r.$$

useful rules for reducing size of propositions

resolvent $q \vee r$

$$\text{Let } q = r \text{ then } (p \vee q) \wedge (\neg p \vee r) \Rightarrow q.$$

$$\text{Let } r = \mathbf{F} \text{ then } (p \vee q) \wedge (\neg p \vee \mathbf{F}) \Rightarrow q.$$

Prolog resolution rules for qualified statements

Automatic theorem proving in propositional logic

hypotheses and conclusion must be expressed in clauses

clause: disjunction (\vee ; or) of variables or the negation of these variables

$$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r) \quad \text{Two clauses(statement) } p \vee q \text{ and } p \vee r.$$

$$\neg(p \vee q) = \neg p \wedge \neg q \quad \text{Two clauses(statement) } \neg p \text{ and } \neg q.$$

Exa 2.3.6 1. $a \vee b$

2. $\underline{\neg b \vee c}$

$\therefore a \vee c$

3. $\underline{\neg c \vee d}$

$\therefore a \vee d$

Exa 2.3.6 1. $a \vee \neg bc$

2. $\underline{\neg(a \vee d)}$

$\therefore \neg b$

proof 1.1 $a \vee \neg b$

1.2 $a \vee c$

2.1 $\neg a$

2.2 $\underline{\neg d}$

$\therefore \neg b$

2.4 Mathematical Induction

The First Principle of Mathematical Induction

$S(1)$	<i>basis</i>
$\forall n \geq 1: S(n) \Rightarrow S(n+1)$	<i>induction</i>
$\therefore \forall n \geq 1: S(n).$	

proof

$S(1).$

$S(1) \Rightarrow S(2).$

$S(2) \Rightarrow S(3).$

...

$S(n) \Rightarrow S(n+1).$

...

Q.E.D.

domino effect

$S(n)$ ***induction hypothesis(IH)***

Generalization of basis**basis** $S(n_0)$ **recursion** $\underline{\forall n \geq n_0: S(n) \Rightarrow S(n+1)}$ $\therefore \forall n \geq n_0: S(n).$ **Exa. 2.4.4 Geometric sum** (기하급수). Let $r \neq 1$. Then $\forall n \geq 0$:

$$\sum_{j \in \{0, 1, \dots, n\}} ar^j = a + ar + ar^2 + \dots + ar^n = a(r^{n+1} - 1)/(r-1).$$

basis ($n=0$) $a = a(r^1 - 1)/(r-1) = a.$ **induction** ($\forall n \geq 0$) Assume $\sum_{j \in N_n} ar^j = a(r^{n+1} - 1)/(r-1).$ (IH) Then

$$\begin{aligned} \sum_{j \in N_{n+1}} ar^j &= a(r^{n+1} - 1)/(r-1) + ar^{n+1} \\ &= a(\mathbf{r^{n+1}} - 1)/(r-1) + ar^{n+1}(\mathbf{r-1})/(r-1) = a(r^{n+2} - 1)/(r-1). \end{aligned}$$

 $\therefore \forall n \geq n_0: \sum_{j \in N_n} ar^j = a(r^{n+1} - 1)/(r-1).$

Exa. 2.4.4' Proof is easy but how to **define** the above theorem? $\stackrel{?}{\equiv}$

$$0 \quad \sum_{j \in N_0} ar^j = ar^0 = a(1) \quad \stackrel{?}{=} a(r^1 - 1)/(r-1)$$

$$1 \quad \sum_{j \in N_1} ar^j = a + ar = a(1+r) \quad \stackrel{?}{=} a(r^2 - 1)/(r-1)$$

$$\dots \quad \stackrel{?}{=} \dots$$

$$n \quad \sum_{j \in N_n} ar^j = a(1 + r + \dots + r^n) \quad \stackrel{?}{=} a(r^{n+1} - 1)/(r-1)$$

$$n+1 \quad \sum_{j \in N_{n+1}} ar^j = a(1 + r + \dots + r^n + r^{n+1}) \quad \stackrel{?}{=} a(r^{n+2} - 1)/(r-1)$$

Exa. 2.4.4' How about **Arithmetic Sum**(산술급수)

$$0 \quad \sum_{j \in N_0} arj = ar0 = 0 \quad \stackrel{?}{=} ar \cdot 0 \cdot 1/2$$

$$1 \quad \sum_{j \in N_1} arj = ar(0 + 1) = \quad \stackrel{?}{=} ar \cdot 1 \cdot 2/2$$

$$\dots \quad \stackrel{?}{=} \dots$$

$$n \quad \sum_{j \in N_n} arj = ar(0 + 1 + \dots + n) \quad \stackrel{?}{=} ar \cdot n(n+1)/2$$

$$n+1 \quad \sum_{j \in N_{n+1}} arj = ar(0 + 1 + \dots + n + n + 1) \quad \stackrel{?}{=} ar \cdot (n+1)(n+2)/2$$

Thm 2.4.6 Let $|X| = n$. Then $|2^X| = 2^n$, $\forall n \geq 0$.

proof Induction on $|A|$

basis $|X| = n = 0$. $X = \emptyset$. $2^\emptyset = \{\emptyset\}$. $|2^\emptyset| = 2^{|\emptyset|} = 2^0 = 1$.

induction Assume $|X| = n$ and $|2^X| = 2^n$. **induction hypothesis**

Consider $Y \supset X$ and $|Y| = n+1$.

$\therefore \exists y \in Y$ but $y \notin X$.

$2^Y = 2^X \cup (\{x \in 2^X\} \cup \{y\}) \wedge 2^X \cap (\{x \in 2^X\} \cup \{y\}) = \emptyset$.

$\therefore |2^X| = |\{x \in 2^X\} \cup \{y\}| = 2^n$, $\therefore |2^Y| = 2^{n+1}$.

Q. E. D.

Loop invariance

<i>before the loop</i>	<i>initialize</i>
<i>just after loop body</i>	<i>update(standard</i>
<i>exit the loop</i>	<i>final condition = (loop inv. \wedge loop exit cond)</i>

$(fact, i) := (1, 1); \mathbf{do} \ i < n \rightarrow i := i + 1; fact := fact * i \ \mathbf{od}$ *in the text*

$(fact, i) := (1, 1); \mathbf{do} \ i \leq n \rightarrow fact := fact * i; i := i + 1 \ \mathbf{od}$ *my program*

loop invariance condition \wedge *exiting condition* = *final condition*

$(fact = i!) \wedge (i = n) \equiv fact = n!$ *mult. (n-1) times*

$(fact = (i-1)!) \wedge (i = n+1) \equiv fact = n!$ *mult. n times*

for statement in C

for (init; test; update) loopbody

init; **while** test **do** loopbody; update **od**

Recursive(Inductive) Definition

Def. 2.4.0 *Peano Lemma for the definition of natural numbers*
basis $0 \in \aleph_0$.

recursion ($\forall n > 0$): $n \in \aleph_0 \Rightarrow \sigma(n)(=n+1) \in \aleph_0$.

Def. 2.4.0.1 $+$: $\aleph_0 \times \aleph_0 \rightarrow \aleph_0$. (*infix notation*)

basis $\forall n \in \aleph_0: n + 0 =_B n$

recursion $\forall n \in \aleph_0, \forall m \in \aleph_1: n + \sigma(m) =_R \sigma(n + m)$

$$5+2=5+\sigma(1) =_R \sigma(5+1)=\sigma(5+\sigma(0)) =_R \sigma(\sigma(5+0))=_B \sigma(\sigma(5))=\sigma^2(5)=7.$$

Def. 2.4.0.2 \cdot : $\aleph_0 \times \aleph_0 \rightarrow \aleph_0$. (*infix notation*)

basis $\forall n \in \aleph_0: n \cdot 0 =_B 0$

recursion $\forall n \in \aleph_0, \forall m \in \aleph_1: n \cdot (m+1) =_R n + n \cdot m$

$$5 \cdot 2 = 5 \cdot \sigma(1) =_R 5 + 5 \cdot 1 = 5 + 5 \cdot \sigma(0) =_R 5 + 5 + 5 \cdot 0 =_B 5 + 5 = 10.$$

Def. 2.4.1 $\forall k, n \in \mathbb{N}_1: k^n$ where $\mathbf{N}_1 = \{1, 2, \dots\}$

basis $\forall k, (n = 1) \in \mathbb{N}_1: k^1 =_B k,$

recursion ($\forall n > 1$) $\in \mathbb{N}_2: k^{n+1} =_R k \cdot k^n$ (or $k^n \cdot k$).

$$5^3 =_R 5 \cdot 5^2 =_R 5 \cdot 5 \cdot 5^1 =_B 5 \cdot 5 \cdot 5 = 125$$

Def. 2.4.1' $\forall k, n \in \mathbb{N}_0: k^n$ where $\mathbf{N}_0 = \{0, 1, \dots\}$

basis $\forall k, (n = 0) \in \mathbb{N}_0: k^0 =_B 1,$

recursion ($\forall n > 0$) $\in \mathbb{N}_1: k^{n+1} =_R k \cdot k^n$ (or $k^n \cdot k$).

$$5^3 =_R 5 \cdot 5^2 =_R 5 \cdot 5 \cdot 5^1 =_R 5 \cdot 5 \cdot 5 \cdot 5^0 =_B 5 \cdot 5 \cdot 5 \cdot 1 = 5 \cdot 5 \cdot 5 = 125$$

2.5 Strong Form of Induction and Well-Ordering Property

The Strong Form of Mathematical Induction (Strong Induction)

$S(n_0)$ *basis*

$\forall n > n_0: n_0 \leq \forall k < n: S(k) \Rightarrow S(n)$ *induction*

$\therefore \forall n \geq n_0: S(n).$

Why strong?

$(\forall n > n_0: n_0 \leq \forall k < n: P(k))$ is **stronger** than $\forall n \geq n_0: P(n).$

Generalized Strong Induction

Let $K \geq 1.$

$\forall n: n_0 \leq n \leq n_0 + K - 1, S(n)$ *K-bases*

$\forall n: n > n_0, S(n) \Rightarrow S(n+K)$ *K-step inductions*

$\therefore \forall n \geq n_0: S(n).$

Well-ordering property

Every nonempty set of nonnegative integers has a least element.

$$\forall S: \emptyset \subset S \subseteq \mathbf{N}, \exists m \in S .\exists. \forall n \in S, m \leq n.$$

m: least element

proof Assume $S = \{n \in \mathbf{N} \mid \neg P(n)\} \supset \emptyset$ and $m \in S$, is the **least element**.

*m ≠ 0, since P(0) by **basis**.*

m - 1 ∈ N, but m - 1 ∉ S.

*P(m - 1) → P(m) is **contradicted by induction**.*

Thm 2.5.6 *If d, n ∈ Z, d > 0. Then*

$$\exists^1 q(\text{quotient}), r(\text{remainder}) \in \mathbf{Z}, .\exists. n = dq + r, 0 \leq r < d.$$

proof Let $X = \{n-dq \mid n-dq \geq 0, q \in \mathbf{Z}\}$

X ≠ ∅, since you can make negative integer q with large absolute value.

*∴ ∃ the **least element** r = n-dq₀ ∈ X.*