1.2&2.1 Proof

Logical arguments

Most theorems (or results) are stated as implications.

Trivial and Vacuous Proofs[1]

Let $P(x)$ and $Q(x)$ be open sentences over a domain D. Consider the quantified statement $\forall x \in D, P(x) \Rightarrow Q(x)$, i.e.

For $x \in D$, if $P(x)$ then $Q(x)$. (#)

or *Let $x \in D$. If $P(x)$, then $Q(x)$.*

`The truth table for implication` $P(x) \Rightarrow Q(x)$ `for an arbitrary (but fixed) element` $x \in D$:

$P(x)$	$Q(x)$	$P(x) \Rightarrow Q(x)$
T	T	T
T	F	F
F	T	T
F	F	T

Trivial Proof If it can be shown that $Q(x)$ is true for all $x \in D$ (regardless the truth value of $P(x)$), then (#) is true (according the truth table for implications).

Vacuous Proof If it can be shown that $P(x)$ is false for all $x \in D$ (regardless of the truth value of $Q(x)$), then (#) is true (according the truth table for implications).

EXAMPLE 1. *Let $x \in \mathbb{R}$. If $x^6 - 3x^4 + x + 3 < 0$, then $x^4 + 1 > 0$.*

EXAMPLE 2. *Let $a, b \in \mathbb{R}$. If $a^2 + 2ab + b^2 + 1 \leq 0$, then $a^7 + b^7 \geq 7$.*

[1]These kind of proofs are rarely encountered in mathematics, however, we consider them as important reminders of implications.

Integers and some of their basic properties and definitions

Let $a, b, c \in \mathbb{Z}$:

property	w.r.t.addition	w.r.t. multiplication
Closure	$a + b \in \mathbb{Z}$	$a \cdot b \in \mathbb{Z}$
Associative	$(a + b) + c = a + (b + c)$	$(ab)c = a(bc)$
Commutative	$a + b = b + a$	$ab = ba$
Distributive	$a(b + c) = ab + ac$	
Identity	$a + 0 = a$	$a \cdot 1 = a$ Note: $0 \neq 1$ and $a \cdot 0 = 0$.
Inverse	There exists a unique integer $-a = (-1) \cdot a$ such that $a + (-a) = 0$	
Subtraction	$b - a := b + (-a)$	
No divisors of 0		If $ab = 0$ then $a = 0$ or $b = 0$.
Cancellation	If $a + c = b + c$, then $a = b$.	If $ab = ac$ and $a \neq 0$, then $b = c$.

Order properties:

1. If $a < b$ and $b < c$ then $a < c$. (**transitivity**)
2. Exactly one of $a < b$ or $a = b$ or $a > b$ holds. (**trichotomy**)
3. If $a < b$, then $a + c < b + c$.
4. If $c > 0$, then $a < b$ iff $ac < bc$.
5. If $c < 0$, then $a < b$ iff $ac > bc$.

Mathematical definitions are always <u>biconditional</u> statements.

DEFINITION A. *An integer n is defined to be* **even** *if $n = 2k$ for some integer k. An integer n is defined to be* **odd** *if $n = 2k + 1$ for some integer k.*

DEFINITION B. *The integers m and n are said to be* **of the same parity** *if m and n are both even, or both odd. The integers m and n are said to be* **of opposite parity** *if one of them is even and the other is odd.*

DEFINITION C. Let a and b be integers. We say that b **divides** a, written $b|a$, if there is an integer c such that $bc = a$. We say that b and c are **factors** of a, or that a is **divisible** by b and c.

FACT *Every integer is either even, or odd.*

DEFINITION D. A real number x is **rational** if $x = \frac{m}{n}$ for some integer numbers m and n. Also, x is **irrational** if it is not rational, that is

DIRECT PROOFS

Let $P(x)$ and $Q(x)$ be open sentences over a domain D.

To prove (directly) a statement of the form "For all $x \in D$, $P(x)$ is true":

- Assume x is an arbitrary (but now fixed) element $x \in D$.
- Demonstrate that $P(x)$ is true.

EXAMPLE 3. *Let $n \in \mathbb{Z}$. Prove that if n is even, then $5n^5 + n + 6$ is even.*

To prove (directly) a statement of the form "For all $x \in D$, $P(x) \Rightarrow Q(x)$":

- Assume that $P(x)$ is true for an arbitrary (but now fixed) element $x \in D$.
- Draw out consequences of $P(x)$.
- Use these consequences to show that $Q(x)$ must be true as well for this element x.

REMARK 4. Note that if $P(x)$ is false for some $x \in D$, then $P(x) \Rightarrow Q(x)$ is ________ for this element x. This is why we need only be concerned with showing that $P(x) \Rightarrow Q(x)$ is true for all $x \in D$ for which $P(x)$ is true.

EXAMPLE 5. The following is an attempted proof of a result. What is the result and is the attempted proof correct?

Proof. Let a be an even integer and b be an odd integer. Then $a = 2n$ and $b = 2n + 1$ for some integer n. Therefore,

$$3a - 5b = 3(2n) - 5(2n + 1) = 6n - 10n - 5 = -4n - 5 = 2(-2n - 2) - 1.$$

Since $-2n - 2$ is an integer, $3a - 5b$ is odd. □

THEOREM 6. 1. *The sum and product of every two even integers is even.*

2. *The sum of every two odd integers is even.*
3. *The product of every two odd integers is odd.*

HINT: First express the statements in the form *"For all ..., if ... then..."* using symbols to represent variables.

THEOREM 7. *The sum and product of every two rational numbers is rational.*

EXAMPLE 8. *Let* $a, b, c, d \in \mathbb{Z}$ *with* $a \neq 0$ *and* $b \neq 0$*. Prove the following:*

(a) *If* $a|b$ *and* $b|c$*, then* $a|c$*.*

(b) *If* $a|c$ *and* $b|d$*, then* $ab|cd$*.*

PROOF BY CASES

may be useful while attempting to give a proof of a statement concerning an element x in some set D. Namely, if x possesses one of two or more properties, then it may be convenient to divide a case into other cases, called *subcases.*

Result	Possible cases
$\forall n \in \mathbb{Z}, R(n)$	Case 1. $n \in \mathbb{E}$; Case 2. ________________
$\forall x \in \mathbb{R}, Q(x)$	Case 1. $x < 0$; Case 2. ________________ Case 3. $x > 0$
$\forall n \in \mathbb{Z}^+, P(n)$	Case 1. ________________; Case 2. $n \geq 2$.
$\forall x, y \in \mathbb{R} \ni xy \neq 0, P(x, y)$	Case 1. $xy < 0$; Case 2. ________________

EXAMPLE 9. *Prove that if* n *is an integer, then* $n^2 + 3n + 4$ *is an even integer.*

Disproving Statements

Case 1. Counterexamples

Let $S(x)$ be an open sentence over a domain D. If the quantified statement ($\forall x \in D, S(x)$.) is *false*, then its negation is true, i.e.

Such an element x is called a **counterexample** of the false statement $\forall x \in D, S(x)$.

EXAMPLE 10. ***Disprove** the statement:* *"If $n \in \mathbb{O}$, then $3|n^2+2$."*

Solution.

EXAMPLE 11. *Negate the statement: "For all $x \in D, P(x) \Rightarrow Q(x)$."*

The value assigned to the variable x that makes $P(x)$ true and $Q(x)$ false is a **counterexample** of the statement "For all $x \in D, P(x) \Rightarrow Q(x)$."

EXAMPLE 12. *S: If n is an integer and n^2 is a multiple of 4 then n is a multiple of 4.*
Question: Is the following "proof" valid?
Let $n = 6$. Then $n^2 = 6^2 = 36$ and 36 is a multiple of 4, but 6 is not a multiple of 4. Therefore, the statement S is FALSE.□

EXAMPLE 13. Disprove the following statement:
If a real-valued function is continuous at some point, then this function is differentiable there.

Case 2: Existence Statements

Consider the quantified statement $\exists x \in D \ni S(x)$. If this statement is *false*, then its negation is true, i.e.

EXAMPLE 14. *Disprove the statement:* "There exist an even integer n such that $3n + 5$ is even."

2.2 Indirect proofs: Proofs by contradiction and contrapositive

Contrapositive

Recall that the statement $\neg Q \Rightarrow \neg P$ is called the **contrapositive** of the statement $P \Rightarrow Q$. Moreover,

$$P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P.$$

In other words, in order to prove $P \Rightarrow Q$, we may choose instead to prove $\neg Q \Rightarrow \neg P$.

EXAMPLE 15. *What is the contrapositive of the statement* $\forall x \in D, P(x) \Rightarrow Q(x)$ *?*

PROOF BY CONTRAPOSITIVE

Let $P(x)$ and $Q(x)$ be open sentences over a domain D. A proof by contrapositive of an implication is a direct proof of its contrapositive; that is **to prove that for all** $x \in D$**,** $P(x) \Rightarrow Q(x)$

- Assume that $\neg Q(x)$ is true for an arbitrary (but now fixed) element $x \in D$.
- Draw out consequences of $\neg Q(x)$.
- Use these consequences to show that $\neg P(x)$ must be true as well for this element x.
- It follows that $P(x) \Rightarrow Q(x)$ for all $x \in D$.

REMARK 16. If you use a contrapositive method, you must declare it in the beginning and then state **what is sufficient to prove.**

EXAMPLE 17. *Let x be an integer. If $5x - 7$ is even, then x is odd.*

EXAMPLE 18. *Let $x, y \in \mathbb{Z}$. If $7 \nmid xy$, then $7 \nmid x$ and $7 \nmid y$.*

Proving biconditional statements

Prove that $\forall x \in D, P(x) \Leftrightarrow Q(x)$.

Proof. Let $x \in D$.

Assume $P(x)$. Then show $Q(x)$.

Conversely, assume $Q(x)$. Then show $P(x)$.$\square$

EXAMPLE 19. *Let $x, y \in \mathbb{Z}$. Prove that x and y are of opposite parity if and only if $x + y$ is odd.*

THEOREM 20. *Let n be an integer. Then n is even if and only if n^2 is even.*

Proof.

REMARK 21. $(P \Leftrightarrow Q) \equiv (\neg P \Leftrightarrow \neg Q)$

COROLLARY 22. *Let n be an integer. Then n is odd iff n^2 is odd.*

COROLLARY 23. *For every integer n, both n and n^2 are of the same parity.*

EXAMPLE 24. *Let $x \in \mathbb{Z}$. Prove that if $2|(x^2 - 1)$ then $4|(x^2 - 1)$.*

PROOF BY CONTRADICTION

To prove a statement S is true by contradiction:

- Assume that $\neg S$ is true.
- Deduce a contradiction.
- Then conclude that S is true.

REMARK 25. If you use a proof by contradiction to prove that S, you should alert the reader about that by saying (or writing) one of the following

- Suppose that the statement S is false.
- Assume, to the contrary, that the statement S is false.
- By contradiction, assume, that the statement S is false.

EXAMPLE 26. *Prove that there is no smallest positive real number.*

2.3 One important theorem

Recall that a real number x is **rational** if $x = \frac{m}{n}$ for some integer numbers m and n. Note that if necessary, we may assume (without loss of generality) that the integers m and n have no common positive factors other than 1. (In other words, we may assume that every fraction can be *reduced to least terms*.)

THEOREM 27. *The number $\sqrt{2}$ is irrational.*

PROOF BY CONTRADICTION (continued)

THEOREM 28. *Let S and C be statement forms. Then $\neg S \Rightarrow (C \wedge \neg C)$ is logically equivalent to S.*

Proof.

COROLLARY 29. *Let P, Q and C be statement forms. Then*

$$(P \Rightarrow Q) \equiv ((P \wedge \neg Q) \Rightarrow (C \wedge \neg C))$$

Proof.

To prove a statement $P \Rightarrow Q$ by contradiction:

- Assume that P is true.
- To derive a contradiction, assume that $\neg Q$ is true.
- Prove a false statement C, using negation $\neg(P \Rightarrow Q) \equiv (P \wedge \neg Q)$.
- Prove $\neg C$. It follows that Q is true. (The statement $C \wedge \neg C$ must be false, i.e. a contradiction.)

REMARK 30. If you use a proof by contradiction to prove that $P \Rightarrow Q$, your proof might begin with one of the following.

- Assume, to the contrary, that the statement P is true and the statement Q is false.
- By contradiction, assume, that the statement P is true and $\neg Q$ is true.

REMARK 31. If you use a proof by contradiction to prove the quantified statement

$$\forall x \in D, P(x) \Rightarrow Q(x),$$

then the proof begins by assuming the existence of a counterexample of this statement. Therefore, the proof might begin with one of the following.

- Assume, to the contrary, that there exists some element $x \in D$ for which $P(x)$ is true and $Q(x)$ is false.
- By contradiction, assume, that there exists an element $x \in D$ such that $P(x)$ is true, but $\neg Q(x)$ is true.

PROPOSITION 32. *If m and n are integers, then $m^2 \neq 4n + 2$.*

COROLLARY 33. *The equation $m^2 - 4n = 2$ has no integer solutions.*

COROLLARY 34. *If the square of an integer is divided by 4, the remainder cannot be equal 2.*

COROLLARY 35. *The square of an integer cannot be of the form $4n + 2$, $n \in \mathbb{Z}$.*

Proof of the Proposition 32.

A Review of Three Proof Techniques

How to prove that $\forall x \in D, P(x) \Rightarrow Q(x)$.

Technique	direct proof	proof by contrapositive	proof by contradiction
Assume			
Goal			

EXAMPLE 36. *Prove the following statement by a direct proof, by a proof by contrapositive and by a proof by contradiction:*

"If n is an even integer, then $5n + 9$ is odd."

Direct Proof.

Proof by Contrapositive.

Proof by Contradiction.

Existence Proofs

An existence theorem can be expressed as a quantified statement
$\exists x \in D \ni S(x)$:

There exists $x \in D$ such that $S(x)$ is true.

A proof of an existence theorem is called an existence proof.

EXAMPLE 37. *There exists real numbers a and b such that $\sqrt{a^2+b^2} = a+b$.*

Proof.

THEOREM 38. (**Intermediate Value Theorem of Calculus**) *If f is a real-valued function that is continuous on the closed interval $[a, b]$ and m is a number between $f(a)$ and $f(b)$, then there exists a number $c \in (a, b)$ such that $f(c) = m$.*

EXAMPLE 39. *Prove that following equation has a real number solution (a root) between $x = 2/3$ and $x = 1$:*

$$x^3 + x^2 - 1 = 0.$$

Uniqueness Proof

An element belonging to some prescribed set D and possessing a certain property P is **unique** if it is the only element of D having property P. A typical way to prove uniqueness is a proof by contradiction: *Assume that x and y are distinct elements of D and show that $x = y$.*

EXAMPLE 40. *Prove that following equation has a unique real number solution (a root) between $x = 2/3$ and $x = 1$:*

$$x^3 + x^2 - 1 = 0.$$

1 3.1 Principle of Mathematical Induction

"Domino Effect"

Step 1. The first domino falls.

Step 2. When any domino falls, the next domino falls.

Conclusion. All dominoes will fall!

THEOREM 41. *(*`Principle of Mathematical Induction (PMI)`*) Let $P(n)$ be a statement about the positive integer n so that n is a free variable in $P(n)$.* ***Suppose the following:***

(PMI 1) *The statement $P(1)$ is true.*

(PMI 2) *For all positive integers k, if $P(k)$ is true, then $P(k+1)$ is true.*

Then*, for all positive integers n, $P(n)$ is true.*

Strategy

The proof by induction consists of the following steps:

Base Case: Verify that $P(1)$ is true.

Inductive hypothesis: Assume that k is a positive integer for which $P(k)$ is true .

Inductive Step: With the assumption made, prove that $P(k+1)$ is true.

Conclusion: $P(n)$ is true for every positive integer n.

EXAMPLE 42. *Prove by induction the formula for the sum of the first n positive integers*

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}. \tag{1}$$

EXAMPLE 43. *Prove that* $3|(8^n - 5^n)$ *for every positive integer* n.

EXAMPLE 44. *Find the sum of all odd numbers from* 1 *to* $2n+1$ *(*$n \in \mathbb{Z}^+$*).*

Paradox: All horses are of the same color.
Question: What's wrong in the following "proof" of G. Pólya?

Basic Step. If there is only one horse, there is only one color.

Inductive step. Assume as induction hypothesis that within any set of k horses, there is only one color. Now look at any set of $k+1$ horses. Number them: $1, 2, 3, ..., k, k+1$. Consider the sets $\{1, 2, 3, ..., k\}$ and $\{2, 3, 4, ..., k+1\}$. Each is a set of only k horses, therefore within each there is only one color. But the two sets overlap, so there must be only one color among all $k+1$ horses.