1.8 Introduction to Proofs

Credit

Ming-Hsuan Yang

Husni Al-Muhtaseb

1.8 Introduction to proofs

- **Proof**: valid argument that establishes the truth of a mathematical statement, e.g., theorem
- A proof can use hypotheses, axioms, and previously proven theorems
- **Formal proofs**: can be extremely long and difficult to follow
- **Informal proofs**: easier to understand and some of the steps may be skipped, or axioms are not explicitly stated

Some terminology

- **Theorem** نظرية: a mathematical statement that can be shown to be true (fact or result)
- **Proposition** فرضية: less important theorem
- **Axiom** بديهية (**postulate** مسلمة): a statement that is assumed to be true
- **Lemma**: less important theorem that is helpful in the proof of other results
- **Corollary** لازمة: a theorem that can be established directly from a theorem that has been proved
- **Conjecture** حدس: a statement proposed to be true, but not proven yet

Proof Techniques (Methods)

- Four primary proof methods:
  - Direct Proof
  - Indirect Proof
    - Proof by Contradiction

      (Another type of Indirect Proof)
  - Proof by Induction
- We will cover Proof by Induction later

Direct Proof

- Used to prove: "$p \rightarrow q$" Or $\forall x\,(P(x) \rightarrow Q(x))$
- To prove such statements
  - Assume that p (or P(c) for arbitrary c) is true
  - Use all possible facts, lemmas, theorems, and rules of inference and try to show that q (or Q(c)) is true.
  - A direct proof often uses the form:

$$p \rightarrow p_1,$$
$$p_1 \rightarrow p_2,$$
$$p_2 \rightarrow \ldots,$$
$$p_{n\text{-}1} \rightarrow p_n,$$
$$p_n \rightarrow q$$

  - Because $\rightarrow$ *is transitive*, we conclude that $p \rightarrow q$

Definition

- Integer n is even if there exists an integer k such that $n = 2k$ Ex: $82 = 2 \times 41$ Ex: $120 = 2 \times 60$ 120 is even

82 is even

- Integer n is odd if there exists an integer k such that $n = 2k + 1$ Ex: $131 = 2 \times 65 + 1$ Ex: $17 = 2 \times 8 + 1$ 17 is Odd

131 is Odd

- Integer n is a perfect square if there exists an integer k such that $n = k^2$ Ex: $144 = 12^2$ Ex: $25 = 5^2$ 144 is perfect square

25 is perfect square

- Note that an integer is either even or odd Zero is even

Let Z be the set of integers: (negative, zero, positive)

- $n \in Z$ is even $\leftrightarrow \exists k \in Z$ such that $n = 2k$
- $n \in Z$ is odd $\leftrightarrow \exists k \in Z$ such that $n = 2k + 1$
- $n \in Z$ is a perfect square $\leftrightarrow n = k^2$ for some $k \in Z$.

Note: $n \in Z \rightarrow n$ is either even or n is odd

Zero is neither positive nor negative

Direct Proof – Example

Prove that if $n \in Z$ is odd, then n^2 is odd, i.e.,
$\forall n \in Z\ \ (n \text{ is odd} \rightarrow n^2 \text{ is odd})$.

Proof (direct):

Assume that $n \in Z$ is odd, then by definition

$$\exists k \in Z \text{ such that } n = 2k + 1$$

Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$

$$= 2(\underline{2k^2 + 2k}) + 1 = 2m + 1 \text{ for some integer } m$$

$$m = (\underline{2k^2 + 2k})$$

Thus, n^2 is odd.

Direct Proof – Example

Prove that if $n, m \in \mathbb{Z}$ are perfect squares, then nm is a perfect square.

The integer n is a perfect square if there exists an integer k such that $n = k^2$ Ex: $144 = 12^2$ $25 = 5^2$

Proof (direct):

Let n, m be perfect squares.

Then $n = k^2$ and $m = j^2$ for some $k, j \in \mathbb{Z}$.

Then $nm = k^2 j^2$

$= k\,k\,j\,j = k\,j\,k\,j$

(using commutativity and associativity of multiplication)

$= (k\,j)^2$

$= r^2$ for some integer r $\quad r = (k\,j)$

Thus, nm is a perfect square.

Definitions: Rational vs. Irrational Numbers

A real number r *is rational* iff there are two integers n and m such that $r = n / m$ where $m \neq 0$.

Examples: 7 = 7/1, 1/2, 0.333333… = 1/3

7, ½, 0.333… are rational numbers

A real number r *is irrational* iff it is not rational.

Examples:

π (Pi) = 3.14159265358979323846264338327 95…

Note: 22/7 is an approximation for π

22/7 = 3.1428571428571…

The number e (Euler's Number)

2.71828182845904523536028747135 27…

Pi (π) is irrational

22/7 rational

We use Q to denote the set of rational numbers.

Direct Proof – Example

Prove that the sum of two rational numbers is a rational number.

Proof (direct):

Let $x, y \in Q$.

Q denotes the set of rational numbers.

Then $x = n_1 / m_1$, $y = n_2 / m_2$, where n_1, m_1, n_2, m_2, are integers and $m_1 \neq 0$ and $m_2 \neq 0$

Then $(x + y) = n_1 / m_1 + n_2 / m_2 = (n_1m_2 + n_2m_1) / (m_1m_2) = k / j$ for some integers k, j *and* $j \neq 0$

$k = (n_1m_2 + n_2m_1)$ and $j = (m_1m_2)$

Consequently, $(x + y) \in Q$

Indirect Proof (Proof by contraposition)

- An indirect proof of $p \rightarrow q$ uses the contrapositive
- Because $p \rightarrow q \equiv \neg q \rightarrow \neg p$, we can prove $p \rightarrow q$ by proving $\neg q \rightarrow \neg p$
- Thus an indirect proof of $p \rightarrow q$ starts by assuming $\neg q$ and continues to show $\neg p$; i.e., the proof uses the form:

$$\neg q \rightarrow r_1,$$
$$r_1 \rightarrow r_2,$$
$$r_2 \rightarrow \ldots,$$
$$r_{n\text{-}1} \rightarrow r_n,$$
$$r_n \rightarrow \neg p$$

Indirect Proof – Example

Prove that for an integer n, if $\underbrace{3n + 2 \text{ is odd}}_{p}$, then $\underbrace{n \text{ is odd}}_{q}$. $p \to q$

Proof (by contraposition): $\neg q \to \neg p$

We need to show that if $\underbrace{n \text{ is not odd}}_{\neg q}$ then $\underbrace{3n + 2 \text{ is not odd}}_{\neg p}$

We need to show that if $\underline{n \text{ is even}}$ then $\underline{3n + 2 \text{ is even}}$

Thus, we assume that n is even

Then $n = 2k$ for some integer k

Thus, $3n + 2 = 6k + 2 = 2\,(3k + 1) = 2m$ for some integer m $m = (3k + 1)$

Thus, $3n + 2$ is even. Hence if n is even then $3n + 2$ is even. The contrapositive of this statement is
if $3n + 2$ is odd, then n is odd. This completes the proof.

When to use an indirect proof

- Sometimes a direct proof leads to a dead end.

Theorem: Prove that if $n \in$ Z and n^2 is even, p

q then n is even. (*We will use this theorem in a latter proof*)

Try a direct proof: $p \to q$

(start with p) $n^2 = 2k$, and so

$n = \sqrt{2k}$, and then ....???

Try an indirect proof (using contrapositive): $\neg q \to \neg p$

$(\neg q)$ n is odd $\to n = 2k + 1 \to n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$
$= 2(2k^2 + 2k) + 1 = 2m + 1$ for some integer m

$\to$ n^2 is odd $(\neg p)$

Example p

- Prove that if $n = ab$, where a and b are positive integers, then $p \to q$

q $a \le \sqrt{n}$ or $b \le \sqrt{n}$.

- What is the contrapositive??

$\neg q \to \neg p$

Prove that if $a > \sqrt{n}$ and $b > \sqrt{n}$, where a and b are positive integers, then $n \ne ab$.

Prove by contraposition $(p \to q \equiv \neg q \to \neg p)$

Assume $\neg(a \le \sqrt{n} \vee b \le \sqrt{n})$

$\equiv (a > \sqrt{n} \wedge b > \sqrt{n})$

$ab > \sqrt{n}.\sqrt{n} = n$ $\quad ab > n$

$ab \ne n$, that is $\neg(n = ab)$

- We have shown that if $a > \sqrt{n}$ and $b > \sqrt{n}$, where a and b are positive integers, then $n \ne ab$. Which is the contrapositive of "if $n = ab$, where a and b are positive integers, then $a \le \sqrt{n}$ or $b \le \sqrt{n}$."

Proof by Contradiction (another type of indirect proof)

- Can be used to prove statements of the form: p *or* $p \to q$
- To prove p by contradiction, we show that the negation of p (i.e., $\neg p$) leads to some kind of a contradiction (false proposition) like $(r \wedge \neg r)$
- To prove $p \to q$ by contradiction, we assume the negation of $p \to q$ and try to get a contradiction.
  - $\neg(p \to q) \equiv \neg(\neg p \vee q) \equiv (p \wedge \neg q)$
  - (i.e., we assume $p \wedge \neg q$) and try to get a contradiction, i.e., $(p \wedge \neg q) \to \mathrm{F}$ or $(p \wedge \neg q) \to \neg p$ [or $(p \wedge \neg q) \to q$]

Proof by Contradiction – Ex: Prove that $\sqrt{2}$ is irrational.

- Assume $\sqrt{2}$ is not irrational, i.e., $\sqrt{2}$ is rational. i.e., $\sqrt{2} = n/m$ for some integers n and $m \neq 0$ where n and m have no common factors.
- If $\sqrt{2} = n/m$ then $2 = n^2/m^2$, i.e., $2m^2 = n^2$ (1)
- (1) states that n^2 is even $\rightarrow$ n is even (by previous theorem) **(*P*)**
- Because n is even (assume $n = 2k$), we can rewrite (1) as

  $2m^2 = n^2$ $\qquad$ $2m^2 = (2k)^2$ $\qquad$ $2m^2 = 4k^2$
- Thus (by dividing both sides by 2),

  $m^2 = 2k^2$ (2)
- (2) state that m^2 is even $\rightarrow$ m is even (by previous theorem) **(*Q*)**
- We have just shown (*P* and *Q*) that both n and m are even, i.e., they have a common factor. This is a contradiction with our starting assumption.

Example

- Proof by contradiction "If $3n + 2$ is odd, then n is odd"
- Let p be "$3n + 2$ is odd" and q be "n is odd"
- So we want to prove that $p \to q$ *or* $(\neg p \vee q)$ is true.
- To construct a proof by contradiction, assume both p and $\neg q$ (n is even) are both true, i, e.
$$\neg(\neg p \vee q)$$
- Since n is even, let $n = 2k$, then $3n + 2 = 6k + 2 = 2(3k + 1)$. So $3n + 2$ is even, i.e. $\neg p$,
- Both p and $\neg p$ are true, so we have a contradiction

Proof by Contradiction – Example

Prove that if 16 bicycles are painted *red*, *white* and *green* then at least 6 bicycles will have the same color.

Proof (by contradiction):

- Assume not, i.e., for each color there is < 6 (i.e., ≤ 5) bicycles.
- Then (compute the number of bicycles from the view point of colors) the number of bicycles is $(3 \times (\leq 5)) \leq 15$ bicycles,
  which contradicts the premise that there are 16 bicycles.

Theorem

- n is even *if and only if* n^k is even for any integer $k > 1$.
- n is odd *if and only if* n^k is odd for any integer $k > 1$.
- ***Reminder***
  - "*p if and only if q*" is often written as $p \leftrightarrow q$ (that is, $p \rightarrow q$ and $q \rightarrow p$)
  - To prove "*p if and only if q*", we must prove "if p then q" and "if q then p".

Example

- Prove the theorem "If n is a positive integer,
p then n is odd if and only if n^2 is odd" q $p \leftrightarrow q$
- To prove "p if and only if q" ($p \leftrightarrow q$) where p is "n is odd" and q is "n^2 is odd"
- Need to show $p \rightarrow q$ and $q \rightarrow p$

  "If n is odd, then n^2 is odd", and "If n^2 is odd, then n is odd"
- We have proved $p \rightarrow q$ and $q \rightarrow p$ in previous examples and thus prove this theorem with iff ($\leftrightarrow$)

Proof of equivalence

- To prove a theorem that is a biconditional statement $p \leftrightarrow q$, we show $p \rightarrow q$ and $q \rightarrow p$
- The validity is based on the tautology

$$(p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \land (q \rightarrow p))$$

Proving Equivalence of Three Propositions

- To prove that $P \leftrightarrow Q \leftrightarrow R$, it suffices (and is more efficient) to prove:

$$(P \rightarrow Q) \wedge (Q \rightarrow R) \wedge (R \rightarrow P)$$

- In general,

$$[p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n] \leftrightarrow [(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \ldots \wedge (p_n \rightarrow p_1)]$$

- ***Example***: Prove that the following are equivalent
  - P: n is even
  - Q: n - 1 is odd
  - R: n^2 is even

Prove that the following are equivalent:

P: n is even, **Q**: $n - 1$ is odd, **R**: n^2 is even

- (P) n is even $\rightarrow n = 2k$
  $\rightarrow n - 1 = 2k - 1 = 2(k - 1) + 1 = 2m + 1$
  $\rightarrow n - 1$ is odd (Q)
- (Q) $n - 1$ is odd $\rightarrow n - 1 = 2k + 1 \rightarrow n = 2k + 1 + 1 = 2k + 2$
  $\rightarrow n = 2(k + 1) \rightarrow n^2 = 4\,(k + 1)^2 = 2\,(2\,(k + 1)^2) = 2m$
  $\rightarrow n^2$ is even (R)
- (R) n^2 is even $\rightarrow n$ is even (P) by a previous theorem

Equivalent theorems

- $p_1 \leftrightarrow p_2 \leftrightarrow \dots \leftrightarrow p_n$
- For i and j with $1 \le i \le n$ and $1 \le j \le n$, p_i and p_j are equivalent

  $[p_1 \leftrightarrow p_2 \leftrightarrow \dots \leftrightarrow p_n] \leftrightarrow$
  $[(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \dots \wedge (p_n \rightarrow p_1)]$
- More efficient than prove $p_i \rightarrow p_j$ for $i \neq j$ with $1 \le i \le n$ and $1 \le j \le n$
- Order is not important as long as we have chain

Prove False by a Counterexample

- Prove that every positive integer is the sum of the squares of two integers.
- The statement to be proven is false.
  - The following is a counterexample:

For number 3, 3 = 2 + 1 or 3 = 3 + 0.
None of these cases is a sum of two squares.

Vacuous & Trivial Proofs

Consider $p \rightarrow q$

- *Vacuous proof*: if p is false then $p \rightarrow q$ is always true.
- *Trivial proof*: if q is true then $p \rightarrow q$ is always true.
- *Examples*:
  - If $0 > 1$, then $n^2 > n$ for any integer n.
    - (vacuous proof)

  - For integers a, b if $a > b$, then $a^2 \geq 0$
    - (trivial proof)

Vacuous Proofs

- The implication $p \rightarrow q$ is always true if the premise p is false
- A vacuous proof is a proof that relies on the fact that no element in the universe of discourse satisfies the premise (thus the statement exists in vacuum (empty domain)).
- *Examples*:
  - If x is a prime number divisible by 16, then x^2 is negative
  - No prime number is divisible by 16, thus this statement is true

Trivial Proofs

- The implication $p \rightarrow q$ is always true if the conclusion q is true
- A trivial proof is where the conclusion is shown to be (always) true independent of the premise p
- *Examples*:
  - "if you score A+ then 2 > 1"
  - "If Math is easy then the Earth is round"

Trivial Proofs

Prove If $x > 0$ then $(x + 1)^2 - 2x \geq x^2$

Proof:

It is easy to see:

$$
\begin{aligned}
(x + 1)^2 - 2x \\
&= (x^2 + 2x + 1) - 2x \\
&= x^2 + 1 \\
&\geq x^2
\end{aligned}
$$

- Note that the conclusion holds <u>without</u> using the hypothesis.

Mistakes in proofs

- What is wrong with this proof

Proof for "if $a = b$ *then* $1 = 2$"?

1. $a = b$ (given)
2. $a^2 = ab$ (multiply both sides of 1 by a)
3. $a^2 - b^2 = ab - b^2$ (subtract b^2 from both sides of 2)
4. $(a - b)(a + b) = b(a - b)$ (factor both sides of 3)
5. $a + b = b$ (divide both sides of 4 by $(a - b)$)
6. $2b = b$ (replace a by b in 5 as $a = b$ and simply)
7. $2 = 1$ (divide both sides of 6 by b)

$(a - b)$ equals zero. Dividing by zero is invalid.

What is wrong with this proof?

- "Theorem": If n^2 is positive, then n is positive **not valid**

  "Proof": Suppose n^2 is positive. As the statement "If n is positive, then n^2 is positive" is true, we conclude that n is positive
- $P(n)$: If n is positive, $Q(n)$: n^2 is positive. The statement is $\forall n(P(n) \rightarrow Q(n))$
- The hypothesis is $Q(n)$. From these, we cannot conclude $P(n)$ as no valid rule of inference can be applied
- Counterexample: $n = -1$

What is wrong with this proof?

- "Theorem": If n is not positive, then n^2 is not positiv not valid
  "Proof": Suppose that n is not positive. Because the conditional statement "If n is positive, then n^2 is positive" is true, we can conclude that n^2 is not positive.
- $P(n)$: If n is positive, $Q(n)$: n^2 is positive. The statement is $\forall n(P(n) \rightarrow Q(n))$
- From our hypothesis $(\neg P(n))$ and $\forall n(P(n) \rightarrow Q(n))$ we cannot conclude $\neg Q(n)$ as no valid rule of inference can be used
- Counterexample: $n = -1$

Circular reasoning (**begging the question**)

- Is the following argument correct to show that
  If n^2 is even, then n is even
  Suppose that n^2 is even, then $n^2 = 2k$ for some integer k. Let $n = 2y$ for some integer y. This shows that n is even
- Wrong argument as the statement "$n = 2y$ for some integer y" is used in the proof
- No argument shows n can be written as $2y$
- Circular reasoning as this statement is equivalent to the statement being proved

Proofs

- Learn from mistakes
- Even professional mathematicians make mistakes in proofs
- Quite a few incorrect proofs of important results have fooled people for years before subtle errors were found
- Some other important proof techniques
  - Mathematical induction
  - Combinatorial proof