Notes Summary: Method of Proofs

Guoxuan Ma*

July 25, 2022

1 A brief Introduction

A (mathematical) result is a true statement. Depending on its signi cance and relevance to the conclusion, a result may be formulated as a lemma, proposition, theorem, corollary, etc. The proof of a result is the process of verifying its truthfulness. Below is a brief review of some common proof techniques.

- A result of form $P \to Q$ is trivial if Q is a tautology; it is vacuous if P is a contradiction.
- A direct proof of a result of form $P \to Q$ is to find a finite intermediate steps (statements) $P_1, P_2, ..., P_n$ such that $P \to P_1, P_1 \to P_2, ..., P_n \to Q$ are all tautologies.
- A proof by contrapositive of a result of form $P \to Q$ is a direct proof of its contrapositive $\neg Q \to \neg P$.
- A proof by cases of a result of form $(\forall x \in D)\ P(x)$ is to find a finite partition $\{D_1, D_2, ..., D_n\}$ of D such that $(\forall x \in D_1)P(X)$, $(\forall x \in D_2)P(X)$,..., $(\forall x \in D_n)P(X)$ are tautologies.
- A proof by contradiction of a result P is to nd a contradiction C such that $\sim P \to C$ is a tautology.
- A proof by mathematical induction of a result of form $(\forall n \in \mathbb{N})P(n)$ is by proving (i) $P(1)$; and (ii) $(\forall n \in \mathbb{N})(P(n) \to P(n+1))$.

4 main Methods of Proof:

- deduction
- contraposition
- induction
- contradiction

1.1 Proof by Deduction

A list of statements, the last of which is the statement to be proven. Each statement in the list is either

- an axiom: a fundamental assumption about mathematics, or part of definition of the object under study; or
- a previously established theorem; or
- follows from previous statements in the list by a valid rule of inference

Example 1. Prove that the function $f(x) = x^2$ is continuous at $x = 5$. Recall from one-variable calculus that $f(x) = x^2$ is continuous at $x = 5$ means $\forall \epsilon > 0,\ \exists \delta > 0\ |x - 5| < \delta \quad \Rightarrow |f(x) - f(5)| < \epsilon$. "For every $\epsilon > 0$ there exists a $\delta > 0$ such that whenever x is within δ of 5, $f(x)$ is within ϵ of $f(5)$." The proof must systematically verify that this definition is satisfied.

*Disclaimer: This notes borrows mainly from the online material, i.e., ECON 204 Robert M. Anderson, https://eml.berkeley.edu/~anderson/Econ204/204index.html

Proof. Suppose we're given $\epsilon > 0$. Let

$$\delta = \min\left\{1, \frac{\epsilon}{11}\right\} > 0$$

Where did that come from ?...
Suppose $|x-5| < \delta$. Since $\delta \leq 1$, $4 < x < 6$, so $9 < x+5 < 11$, so $|x+5| < 11$. Then

$$\begin{aligned} |f(x) - f(5)| &= |x^2 - 25| \\ &= |(x-5)(x+5)| \\ &= |x-5||x+5| \\ &< \delta * 11 \\ &\leq \frac{\epsilon}{11} \cdot 11 \\ &= \epsilon \end{aligned}$$

Thus, we have shown that for every $\epsilon > 0$, there exists $\delta > 0$ such that $|x-5| \leq \delta \;\Rightarrow |f(x) - f(5)| < \epsilon$, so $f(x) = x^2$ is continuous at $x = 5$. □

Remark 1. To prove $A \Rightarrow Z$, deduction goes like $A \Rightarrow B \Rightarrow ... \Rightarrow Y \Rightarrow Z$.

1.2 Proof by Contraposition

- $\neg p$ means "P is false."
- $p \wedge Q$ means "P is true and Q is true."
- $p \vee Q$ means "P is true or Q is true (or possibly both)."
- $\neg p \wedge Q$. means $(\neg p) \wedge Q$; $\neg p \vee Q$ means $(\neg p) \vee Q$..
- $P \Rightarrow Q$ means "whenever P is satisfied, Q is also satisfied."
- Formally, $P \Rightarrow Q$ is equivalent to $\neg p \vee Q$.
- The contrapositive of the statement P $\Rightarrow$ Q is the statement

$$\neg Q \Rightarrow \neg P$$

Theorem 1. *$P \Rightarrow Q$ is true if and only if $\neg Q \Rightarrow \neg P$ is true.*

Proof. Suppose $P \Rightarrow Q$ is true. Then either P is false, or Q is true (or possibly both). Therefore, either $\neg P$ is true, or $\neg Q$ is false (or possibly both), so $\neg(\neg Q) \;\vee (\neg P)$ is true, $\neg Q \Rightarrow \neg P$ is true. Conversely, suppose $\neg Q \Rightarrow \neg P$ is true. Then either $\neg Q$ is false, or $\neg P$ is true (or possibly both), so either Q is true, or P is false (or possibly both), so $\neg P \vee Q$ is true, so $P \Rightarrow Q$ is true. See the book for an example of the use of proof by contraposition □

1.3 Proof by Induction

A typical structure of proof is For $n = 0$ (or other initial value), show that the statement is true. This is the base step. For $n = k$; suppose that the statement is true. This is the inductive hypothesis. For $n = k+1$; use what we get from the inductive hypothesis to show that the statement holds for the case of $n = k+1$ Conclude that the statement is true for all n.

Theorem 2. *For every $n \in N_0 = \{0, 1, , 2, 3, ...\}$*

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

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

Proof. Base step $n = 0$: $L.S. = \sum_{k=1}^{0} k = 0$. $R.S. = \frac{0.1}{2} = 0$. So the theorem is true for $n = 0$.
Induction step: Suppose

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}, \text{ for some } n$$

We must show that

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

where

$$\begin{aligned} L.S. &= \sum_{k=1}^{n+1} k \\ &= \sum_{k=1}^{n} k + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \text{ by the induction hypothesis} \\ & (n+1)(\frac{n}{2}+1) \\ & \frac{(n+1)(n+2)}{2} \end{aligned}$$

where

$$\begin{aligned} R.S. &= \frac{(n+1)((n+1)+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \\ &= L.S. \end{aligned}$$

so by mathematical induction, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ for all $n \in \boldsymbol{N}_0$. □

1.4 Proof by Contradiction

Theorem 3. *Theorem 3 There is no rational number q such that q2 = 2.*

Proof: Suppose $q^2 = 2, q \in \boldsymbol{Q}$. We can write $q = m/n$ for some $m, n \in \boldsymbol{Z}$. Moreover, we can assume that m and n have no common factor; if they did, we could divide it out. (Aside: this is actually a subtle point. We are using the fact that the expression of a natural number as a product of primes is unique.)

$$2 = q^2 = \frac{m^2}{n^2}$$

Therefore, $m^2 = 2n^2$, so m^2 is even.
We claim that m is even. If not (Aside: This is a proof by contradiction within a proof by contradiction!) m is odd, so $m = 2p + 1$ for some $p \in \boldsymbol{Z}$. Then

$$\begin{aligned} m^2 &= (2p+1)^2 \\ &= 4p^2 + 4p + 1 \\ &= 2(2p^2 + 2p) + 1 \end{aligned}$$

which is odd, contradiction. Therefore, m is even, so $m = 2r$ for some $r \in \boldsymbol{Z}$.

$$\begin{aligned} 4r^2 &= (2r)^2 \\ &= m^2 \\ &= 2n^2 \\ n^2 &= 2r^2 \end{aligned}$$

so n^2 is even, which implies (by the argument given above) that n is even. Therefore, $n = 2s$ for some $s \in \boldsymbol{Z}$, so m and n have a common factor, namely 2, contradiction. Therefore, there is no rational number q such that $q^2 = 2$.