Lecture 2: Strategies for Proofs

1 Introduction

Thales of Miletus of sixth century BC is credited with introducing the concepts of logical proof for abstract propositions. Euclid popularized the axiomatic system of proofs in his book The elements, written over 2000 years ago. In this book, he proves a number of geometric theorems based on axioms.

We must ask why do we need proofs. There are four mains reasons for this endeavor. First, intuition is fallible (sometimes we see what we want to see). Therefore, proofs are necessary to infallibly ascertain facts. Second, we need proofs to explain why things are true. Not all proofs are instructive, however non-intuitive proofs are still better than no proofs. Third, writing proofs provide us a thorough understanding of the problem at hand. Last but not the least, proofs are useful to communicate ideas in language of mathematics.

2 Proofs

Definition 2.1 (Mathematical Proof). A convincing argument that starts from the premises and logically deduces the desired conclusion.

We usually prove theorems, propositions, lemmas, corollaries, and exercises. Theorems are important results, propositions are less important results. Lemmas are small independent statements that can be used to prove other results. Corollaries follow easily from other results, and exercise is something left for reader to verify.

To prove theorems, we need existing theorems and definitions. Axioms are starting points for this chain.

Definition 2.2 (Axioms). Facts about mathematical objects assumed without proof are called **axioms**.

Definition 2.3 (Axiomatic System). Body of knowledge that can be derived from a set of axioms is called **axiomatic system**.

Sets are fundamental objects and considered basis for all arguments. Each branch of mathematics has specific st of axioms for associated objects. For example, algebra has axiomatically defined objects such as groups, rings, fields, etc.

Example 2.4. Show that "sum of even numbers are even." Precise statement for the above problem is " if n and m are even integers, then $n + m$ is an even integer."
Proving this statement precise definition of terms, such as integers where even and odd are defined. We also need understanding of standard properties such as closure under addition, subtraction, and multiplication, and distributive law of these properties over integers.

Definition 2.5. Let n be an integer. We say that n is **even** if there is some integer k such that $n = 2k$. We say that n is **odd** if there is some integer j such that $n = 2j + 1$.

Theorem 2.6. *Let n and m be integers.*

i If n and m are both even, then $n + m$ is even.

ii If n and m are both odd, then $n + m$ is even.

iii If n is even and m is odd, then $n + m$ is odd.

Proof. We will prove part i. Suppose n and m are both even, then there exist integers k and l such that $n = 2k$ and $m = 2l$. Therefore, $n + m = 2(k + l)$ by distributive law of multiplication over additions on integers. Further, $(k+l)$ is also an integer by closure property of integer addition. Hence, $n + m$ is even. Parts ii and iii can be shown similarly. □

Following are features of good proof.

- A proof should rely completely on the definitions.
- A proof should be written in grammatically correct language.
- A proof uses rules of inference implicitly.

2.1 Types of Proofs

There are three types of proofs for $P \to Q$.

Direct Proofs. Assume that P is true and produce a series of steps, each one following from the previous ones, eventually leading to Q.

There are few steps in formulating a direct proof. First, we must specify the assumptions, and then specify what we are trying to prove. Second, we assume premise and see where it leads. Then we look at the conclusion, and see what's needed to prove this conclusion. However, in the final proof, we start with the premise, and produce a series of steps till conclusion is reached.

Proof by contrapositive. Since we know that $P \to Q \Leftrightarrow \neg Q \to \neg P$. We can provide a direct proof for $\neg Q \to \neg P$ instead. Assume Q is false, and produce a series of arguments to conclude P is false.

Proof by contradiction. We also know that $\neg(P \to Q) \Leftrightarrow P \wedge \neg Q$. Assume $P \wedge \neg Q$ is true, then derive a logical contradiction. This implies that $P \wedge \neg Q$ is false. Hence $P \to Q$ is true by double negation equivalence.

Definition 2.7 (Rational number). Let x be a real number. We say x is a **rational number** if there exist integers m and n such that $m \neq 0$ and $x = \frac{n}{m}$ and there are no common factors between n and m other than 1 or -1. If x is not a rational number, we say it is **irrational number**.

Theorem 2.8. *Prove that $\sqrt{2}$ is an irrational number.*

Proof. We will prove this by contradiction. We assume $x = \sqrt{2}$ is a rational number. Then $x^2 = 2$. Since x is rational, there are integers n and m such that $x = \frac{n}{m}$, and n and m have no common factors other than 1 and -1.

Since $x^2 = 2$, we get $n^2 = 2m^2$. Therefore, n^2 is even, hence n must be even. By definition of even integers, there exists an integer k such that $n = 2k$. Thus, we have $2k^2 = m^2$, and m must also be even. We thus have a contradiction, since m and n have 2 as common factor. Hence, $x = \sqrt{2}$ is not rational. □

2.2 Cases

There are times when premise P and conclusion Q of a conditional $P \to Q$ are compound statements. In such a scenario, we need to consider cases. We look at four simple scenarios. Let A and B be statements.

i Premise P consists of statements A and B, then conditional $(A \wedge B) \to Q$ needs to be shown. We can show a direct proof by assuming both statements A and B true, and showing conclusion Q to be true.

ii Conclusion consists of statements A and B, then we need to show conditional $P \to (A \wedge B)$. However, we know conditional $P \to (A \wedge B)$ is equivalent to statement $(P \to A) \wedge (P \to B)$. Therefore, we can provide a direct proof by assuming premise P and showing both statements A and B to be true.

iii Premise P consists of statements A or B, such that we need to show conditional $(A \vee B) \to Q$. Since conditional $(A \vee B) \to Q$ is equivalent to statement $(A \to Q) \wedge (B \to Q)$, we need to prove both conditionals $(A \to Q)$ and $(B \to Q)$.

iv Conclusion Q is A or B, that is we need to show conditional $P \to (A \vee B)$ to be true. Since $P \to (A \vee B)$ is equivalent to $(\neg A \wedge \neg B) \to \neg P)$, we can assume both statements A and B to be false, to show premise P false. We also know that conditional $P \to (A \vee B)$ is equivalent to statement $(P \wedge \neg A) \to B$. Therefore, we can assume premise P true and statement A false, to show conclusion Q.

2.3 If and Only If

It is easy to see that $P \leftrightarrow Q \Leftrightarrow (P \to Q) \wedge (Q \to P)$. Therefore to show biconditional is a tautology, we need to show both conditionals $(P \to Q)$ and $(Q \to P)$ are tautologies as well.

2.4 The Following Are Equivalent

Often we would need to show a number of statements are equivalent. Usually written TFAE stands for "The Following Are Equivalent." If there are n statements, then we need to show pair-wise equivalence, leading to $n(n-1)$ implications. However, we can reduce this number significantly by showing n implications of form statement i implies statement $i+1$ for first $n-1$ statements and showing statement n implies statement 1. We can logically deduce all pair-wise equivalences from this. We will see one example below.

Theorem 2.9. *Let M be an upper triangular matrix of size 2×2 with integer entries. Specifically,*

$$M = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}.$$

The following are equivalent.

1. $\det M = 1$.

2. $a = d = \pm 1$.

3. $\operatorname{tr} M = \pm 2$ *and* $a = d$.

Proof. We will show (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1).

(1) $\Rightarrow$ (2): Assume that $\det M = 1$. This means that $ad = 1$. Since, $a, d \in \mathbb{Z}$, either $a = d = 1$ or $a = d = -1$.

(2) $\Rightarrow$ (3): Assume that $a = d = \pm 1$. First suppose that $a = d = 1$, then $\operatorname{tr} M = a + d = 2$. Second, suppose that $a = d = 1$, then $\operatorname{tr} M = a + d = -2$. Hence, $\operatorname{tr} M = \pm 2$ and $a = d$.

(3) $\Rightarrow$ (1): Assume that $\operatorname{tr} M = \pm 2$ and $a = d$. Then, $(a + d)^2 = 4ad = 4$. That is, $\det M = ad = 1$.

□

3 Quantifiers in Theorems

Quantifiers are used to describe variables in statements.

Definition 3.1 (Universal Quantifiers). The universal quantifier is a symbol which expresses that the statement is true "for all" or "any" element x in a given set U. For example, a statement such as " $(\forall x \text{ in } U)P(x)$" $\Longleftrightarrow$ "if x is in U then $P(x)$ is true."

Direct proof. To prove a statement with universal quantifiers to be true, prove that the statement is true for any arbitrary x in U. Since choice of x was arbitrary, this will be true for any x in U.

Proof by contradiction. Let y be in U and suppose that $P(y)$ is false. Then using logical arguments arrive at a contradiction.

Proof by contrapositive. We assume $P(x)$ to be false, and then show that x is not in U.

Example 3.2. Expression $f(n) = n^2 + n + 41$ is prime for all n in $\{0, \ldots, 39\}$. However, $f(40) = 1681 = 41^2$ and hence not prime. Therefore, $f(n)$ is not prime for all n.

Definition 3.3 (Existential Quantifiers). The existential quantifier $\exists$ is a symbol which represents that there exists some element x in a given set U, for which statement $P(x)$ is true. For example, a statement such as " $(\exists x \text{ in } U)P(x)$" $\Longleftrightarrow$ "there exists x in U such that $P(x)$ is true.

Direct proof. To prove a statement with existential quantifier to be true, we need to find some element z_0 in set U such that statement $P(z_0)$ holds.

4 Tips for Writing Mathematics

1. A written proof should stand on its own, without any need for clarification. State everything explicitly and clearly. Don't assume that reader is a mind reader.

2. Write precisely and clearly. There is no room for ambiguity in mathematics. Make sure what you write is what you mean. Revise several times, and read as a third person. Make theorems, lemmas, propositions, to be self-contained with all the hypotheses.

3. Prove what is appropriate. Assume reader to be at same level of knowledge, except the proof.

4. Be careful with saying things are "obvious". Obviously, clearly, similarly are covers for uncertainty and laziness. An obvious statement is that someone with equal mathematical knowledge should figure out in very little time with very little effort. A trivial statement is the one for which a simple proof can be found after some (possibly a long time) thought.

5. Use full sentences and correct grammar. For example, $x = z^2$ could be written as "the variable x equals to the square of variable z". Use therefore, hence, it follows liberally to help guide the logical flow.

6. Use "=" sign properly. Use = when needed and only there. Don't use any backward step in the proof.

7. Define all symbols and terms you make up. Declare all variables before use, as in programming. Avoid exotic alphabets and complicated notations.

8. Break up a long proof into steps. Isolate preliminary part as lemmas of precise statements. Outline proof strategy prior to details for long proofs.

9. Distinguish formal vs informal writing.

10. Miscellaneous Tips

    (a) No mathematical symbols right after punctuation symbols.

    (b) Don't use logical symbols such as $\vee, \wedge, \exists, \forall, \implies$ for words in proof.

    (c) Use equal sign only in equations.

    (d) Use consistent notation.

    (e) Display long formulas (or short important ones) on their own lines. Still use punctuation when using equations.

(f) Avoid colons.

(g) Capitalize names such as Theorem 2.3, Lemma 1.7.