COMPSCI/SFWRENG 2FA3
Discrete Mathematics with Applications II
Winter 2020

1 Mathematical Proof

William M. Farmer

Department of Computing and Software
McMaster University

January 8, 2020

Admin — January 8

- Tutorials start next week.
  - Bring your laptop with you to the tutorial if you need help installing LaTeX.
- Regular lecture on Friday.
- M&Ms start next week after the lecture on Friday.
- Thank you for your bio sheets.
- Office hours: To see me please send me a note with times.
- Are there any questions?

Mathematical Proofs (iClicker)

In mathematics, a proof is

A. Similar to a scientific experiment.
B. A preponderance of evidence for the truth of a statement.
C. A plausible argument that a statement is true.
D. An evaluation of a boolean-valued expression.
E. None of the above.

Mathematical Proof

- In mathematics, a proof is a deductive argument intended to show that a conclusion follows from a set of premises.
- A theorem is a statement (i.e., that a conclusion follows from a set of premises) for which there is a proof.
- A conjecture is a statement for which there is reason to believe that it is true but there is not yet a proof.
- Proof is the preeminent technique of mathematics.
- As a means to establish truth, proof is unique to mathematics!

Reading Mathematical Proofs (iClicker)

How comfortable are you with reading proofs?

A. It scares me to death!
B. It is like reading a foreign language I don't know.
C. I can do it, but I don't enjoy it.
D. It is hard to do, but it gives me a deeper understanding of computing.
E. Reading proofs is as natural as breathing.

Writing Mathematical Proofs (iClicker)

How comfortable are you with writing proofs?

A. It scares me to death!
B. It is like reading a foreign language I don't know.
C. I can do it, but I don't enjoy it.
D. It is hard to do, but it gives me a deeper understanding of computing.
E. Writing proofs is as natural as breathing.

Purposes of Mathematical Proof

1. Communicating mathematical ideas.
2. Certifying that mathematical results are correct.
3. Organizing mathematical knowledge.
4. Discovering new mathematical facts.
5. Learning mathematics.
6. Showing the universality of mathematical results.
7. Establishing coherency with a body of mathematical knowledge.
8. Creating mathematical beauty.

Styles of Mathematical Proof

- There are many styles of proof such as:
  - A description of a deduction.
  - A prescription of how to produce a deduction.
  - A deduction presented in a two-column format.
  - A computation.
  - A construction.
  - A geometric proof.
  - A visual proof.
  - A classic (nonconstructive) proof.
  - A constructive proof.
- Two important — and competing — styles are:
  1. The traditional proof style.
  2. The formal proof style.

Traditional Proof Style

- A traditional proof is an argument for some intended audience expressed in a stylized form of natural language.
- The terminology and notation may be ambiguous, assumptions may be unstated, and the argument may contain gaps.
- Reader is expected to be able to resolve the ambiguities, identify the unstated assumptions, and fill in the gaps.
- Writer has great freedom to express traditional proofs in whatever manner that is deemed to be most effective.
  - The main focus is on making key ideas understandable.
  - Low-level details are usually performed by computation or left to be verified by the reader.
- The traditional proof style is primarily good for communication but also for organization, discovery, and beauty.

Formal Proof Style

- A formal proof is a derivation in a proof system for a formal logic.
- A formal proof can be presented in two ways:
  - As a description of the actual derivation.
  - As a prescription for creating the derivation.
- Software systems can be used to interactively develop and mechanically check formal proofs.
- Writer is highly constrained by the logic, the proof system, and the fact that every detail must be verified.
- As a result, the meaning of the theorem and the key ideas of proof may not be readily apparent to the reader.
- There is a very high assurance that the theorem is correct!
- The formal proof style is primarily good for certification but also for organization and discovery.

Traditional vs. Formal Proofs (iClicker)

Which style of proof do you prefer?

A. Traditional.

B. Formal.

Writing Traditional Proofs (iClicker)

To learn how to write traditional proofs, you should

A. Read proofs given in mathematics articles and textbooks.

B. Write proofs of facts you already know.

C. Translate formal proofs into traditional proofs.

D. Do exercises that ask for a proof.

Proving a Conjunction (iClicker)

Which is not a valid way to prove $A \wedge B$?

A. Prove A and B separately.

B. Prove A and B together.

C. Prove A and then prove B assuming A.

D. $\boxed{\text{Prove } A \text{ assuming } B \text{ and prove } B \text{ assuming } A.}$

Methods of Proof for Propositional Formulas

- How does one usually prove an implication $A \Rightarrow B$?

  Assume A and then prove B using A.

- How does one usually prove a negation $\neg A$.
  - Assume A and then derive a contradiction.
- How does one usually prove a conjunction $A \wedge B$?

  Prove A and then prove B assuming A.

- How does one usually prove a disjunction $A \vee B$?

  Assume $\neg A$ and then prove B,
  or assume $\neg B$ and then prove A.

- How does one usually prove a biconditional $A \Leftrightarrow B$?

  Prove $A \Rightarrow B$ and $B \Rightarrow A$.

Methods of Proof for Quantified Formulas

- How does one usually prove a universal statement $\forall x \in S \,.\, A$?
  1. Assume $x \in S$ and then prove A.
  2. Assume $\exists x \in S \,.\, \neg A$ and then derive a contradiction.
  3. If $S = \{a_1, \ldots, a_n\}$, then prove $A[x \mapsto a_1], \ldots, A[x \mapsto a_n]$.
  4. If there is an inductive principle for S, then prove $\forall x \in S \,.\, A$ by induction.
- How does one usually prove an existential statement $\exists x \in S \,.\, A$?
  1. For some $a \in S$, prove $A[x \mapsto a]$.
  2. Assume $\forall x \in S \,.\, \neg A$ and then derive a contradiction.

Kinds of Theorems

- A theorem is a statement for which there is a proof.
- The following terms are used to classify theorems:
  1. An axiom is a theorem whose truth is assumed.
  2. A proposition is a theorem that is immediately or easily proved.
  3. A lemma is a theorem, usually of a technical nature, that is used to prove other more fundamental theorems.
  4. A theorem is a theorem of fundamental importance.
  5. A corollary is a theorem, usually of fundamental importance, that follows immediately from other theorems.

Proof Terminology [1/2]

- The phrase "if and only if (iff)" means logical equivalence.
- The word "obvious" means almost no thinking is needed.
- The word "clearly" or phrase "can be easily shown" signals to the reader that the result can be verified with little effort.
- The phrases "trivial case" and "trivial argument" refer, respectively, to a case and an argument with extremely simple structure.
- The phrase "straightforward argument" means an argument, that may be long, in which each step of the argument is obvious.
- A proof is "similar" to another proof if it employs the same structure or techniques.

Proof Terminology [2/2]

- A "brute force verification" is one in which every possible case is individually verified.
- A "symmetric argument" is an argument that is obtained from another argument by a structure-preserving transformation.
- A notion is "well-defined" if its definition is fully and precisely given.
- The phrase "the following are equivalent (TFAE)" refers to a list of logically equivalent statements.
- The phrase "without loss of generality (WLOG)" is used to signal to the reader that it suffices to consider a special case instead of the general case.
- "QED (quod erat demonstrandum)", $\square$, or $\blacksquare$ signifies that the proof is complete.