CS170: Discrete Methods in Computer Science
Summer 2023
Basics of Mathematical Proofs

Instructor: Shaddin Dughmi[1]

[1] These slides adapt some content from similar slides by Aaron Cote.

Outline

1. Intro
2. Common Forms/Styles of Proof
3. Some Tricks and Shortcuts
4. Misc Mathematical Lingo and Notation

Mathematical Proofs

- In the previous two lectures, we looked at formal proofs in propositional logic
    - Very detailed and easy to verify (whether by human or computer)
    - Tedious to write, read, and understand
- This is not how working mathematicians or computer scientists write proofs

Mathematical Proofs

- In the previous two lectures, we looked at formal proofs in propositional logic
  - Very detailed and easy to verify (whether by human or computer)
  - Tedious to write, read, and understand
- This is not how working mathematicians or computer scientists write proofs
- A common mathematical proof is written in a form of natural language that is more brief, pleasant to read, and easier to understand, but ridden of imprecision and ambiguity by the use of some mathematical terminology and notation
- These proofs take larger steps than a formal proof in logic, but are still rigorous (precise, detailed)
  - The level of detail depends on mathematical maturity and technical/domain background of your intended audience

Mathematical Proofs

- In the previous two lectures, we looked at formal proofs in propositional logic
  - Very detailed and easy to verify (whether by human or computer)
  - Tedious to write, read, and understand
- This is not how working mathematicians or computer scientists write proofs
- A common mathematical proof is written in a form of natural language that is more brief, pleasant to read, and easier to understand, but ridden of imprecision and ambiguity by the use of some mathematical terminology and notation
- These proofs take larger steps than a formal proof in logic, but are still rigorous (precise, detailed)
  - The level of detail depends on mathematical maturity and technical/domain background of your intended audience
- Intended reader should be able to:
  - Convince themselves of any step after momentary reflection
  - Be able to turn your proof into a formal one given ample time, paper, energy, and patience

Mathematical Proofs

- In the previous two lectures, we looked at formal proofs in propositional logic
  - Very detailed and easy to verify (whether by human or computer)
  - Tedious to write, read, and understand
- This is not how working mathematicians or computer scientists write proofs
- A common mathematical proof is written in a form of natural language that is more brief, pleasant to read, and easier to understand, but ridden of imprecision and ambiguity by the use of some mathematical terminology and notation
- These proofs take larger steps than a formal proof in logic, but are still rigorous (precise, detailed)
  - The level of detail depends on mathematical maturity and technical/domain background of your intended audience
- Intended reader should be able to:
  - Convince themselves of any step after momentary reflection
  - Be able to turn your proof into a formal one given ample time, paper, energy, and patience
- Your intended audience in this class: Fellow 170 students!

Logical Foundations of Proofs

- You can think of a common mathematical proof as a human-friendly abbreviation of a formal logical proof
- In other words, it should in principle be able to converted to logic, but which logic?

Logical Foundations of Proofs

- You can think of a common mathematical proof as a human-friendly abbreviation of a formal logical proof
- In other words, it should in principle be able to converted to logic, but which logic?
- The statements and proofs we write will involve variables and quantification (for all, there exists)
    - e.g. Show that for all integers n, if n is odd then n^2 is odd
- Propositional logic cannot capture these, so we need something more general

Logical Foundations of Proofs

- You can think of a common mathematical proof as a human-friendly abbreviation of a formal logical proof
- In other words, it should in principle be able to converted to logic, but which logic?
- The statements and proofs we write will involve variables and quantification (for all, there exists)
  - e.g. Show that for all integers n, if n is odd then n^2 is odd
- Propositional logic cannot capture these, so we need something more general

First Order Logic

Propositional logic with variables and quantifiers

Logical Foundations of Proofs

- You can think of a common mathematical proof as a human-friendly abbreviation of a formal logical proof
- In other words, it should in principle be able to converted to logic, but which logic?
- The statements and proofs we write will involve variables and quantification (for all, there exists)
  - e.g. Show that for all integers n, if n is odd then n^2 is odd
- Propositional logic cannot capture these, so we need something more general

First Order Logic

Propositional logic with variables and quantifiers

Logical Foundation of Modern Mathematics

First order logic, plus some axioms about how sets behave. This is often called set theory or ZFC.

Logical Foundations of Proofs

- You can think of a common mathematical proof as a human-friendly abbreviation of a formal logical proof
- In other words, it should in principle be able to converted to logic, but which logic?
- The statements and proofs we write will involve variables and quantification (for all, there exists)
  - e.g. Show that for all integers n, if n is odd then n^2 is odd
- Propositional logic cannot capture these, so we need something more general

First Order Logic

Propositional logic with variables and quantifiers

Logical Foundation of Modern Mathematics

First order logic, plus some axioms about how sets behave. This is often called set theory or ZFC.

Don't worry about these for now, will come back to them later.

Some Useful Logical Terminology and Notation

- A predicate is a template for propositions involving variables
  - It doesn't have a truth value until the variables are specified or quantified (see below)
  - E.g. "n is odd" is a predicate. "7 is odd" is a proposition. "There exists n such that n is odd" is a proposition.

Some Useful Logical Terminology and Notation

- A predicate is a template for propositions involving variables
  - It doesn't have a truth value until the variables are specified or quantified (see below)
  - E.g. "n is odd" is a predicate. "7 is odd" is a proposition. "There exists n such that n is odd" is a proposition.
- Quantifiers "for all" (denoted $\forall$) and "there exists" (denote $\exists$) turn predicates into propositions. For example:
  - $\forall$ integers n, if n is odd then n^2 is odd.
  - $\exists$ irrational numbers x, y such that x^y is rational.
  - $\forall n \, \exists p \;\; p > n$ and p is prime. (nesting, omission of types)

Some Useful Logical Terminology and Notation

- A predicate is a template for propositions involving variables
  - It doesn't have a truth value until the variables are specified or quantified (see below)
  - E.g. "n is odd" is a predicate. "7 is odd" is a proposition. "There exists n such that n is odd" is a proposition.
- Quantifiers "for all" (denoted $\forall$) and "there exists" (denote $\exists$) turn predicates into propositions. For example:
  - $\forall$ integers n, if n is odd then n^2 is odd.
  - $\exists$ irrational numbers x, y such that x^y is rational.
  - $\forall n\ \exists p\ \ p > n$ and p is prime. (nesting, omission of types)
- Moving a negation inside a quantifier flips the quantifier. E.g. the following are equivalent:
  - $\neg\forall n\ \exists p\ \ p > n$ and p is prime.
  - $\exists n \neg\exists p\ \ p > n$ and p is prime.
  - $\exists n \forall p\ \neg\ (p > n$ and p is prime).
  - $\exists n \forall p\ \ p \leq n$ or p is not prime.

Some Useful Logical Terminology and Notation

- Given an implication statement $p \Rightarrow q$, we define its
  - Converse: $q \Rightarrow p$
  - Inverse: $\neg p \Rightarrow \neg q$
  - Contrapositive: $\neg q \Rightarrow \neg p$.
- Notice that an implication is equivalent to its contrapositive, and the converse is equivalent to the inverse.
- An equivalence $p \iff q$ is the conjunction of $p \Rightarrow q$ and its converse $q \Rightarrow p$.
  - Often phrased as: p if and only if q.

Outline

1. Intro
2. Common Forms/Styles of Proof
3. Some Tricks and Shortcuts
4. Misc Mathematical Lingo and Notation

Forms of Proofs, at a High Level

- There is almost limitless creativity in how you construct proofs
- However, there are some forms that are quite common, and it is instructive to learn and practice them
- These forms are not mutually exclusive: often they are combined, or multiple different ones can work
- The list I give you is not exhaustive, and researchers often discover new and creative ways of structuring proofs

Direct Proof

- This is the most basic and common kind of proof
- Start with assumptions, and then derive statements one by one until you arrive at your desired conclusion.

Direct Proof

- This is the most basic and common kind of proof
- Start with assumptions, and then derive statements one by one until you arrive at your desired conclusion.

Prove: If an integer n is odd, then n^2 is odd.

- n is odd
- $n = 2k + 1$ for some integer k
- $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
- Let $m = 2k^2 + 2k$.
- m is an integer, and $n^2 = 2m + 1$
- Therefore, n^2 is odd.

Proof by Contraposition

To prove p implies q, sometimes it is easier to prove the contrapositive: $\neg q$ implies $\neg p$

- Recall: they are equivalent

Proof by Contraposition

To prove p implies q, sometimes it is easier to prove the contrapositive: $\neg q$ implies $\neg p$

- Recall: they are equivalent

Theorem

If n^2 is odd, then n is odd

Proof by Contraposition

To prove p implies q, sometimes it is easier to prove the contrapositive: $\neg q$ implies $\neg p$

- Recall: they are equivalent

Theorem

If n^2 is odd, then n is odd

Let's try a direct proof

- Suppose n^2 is odd
- $n^2 = 2k + 1$ for some integer k
- $n = \sqrt{n^2} = \sqrt{2k+1}$
- ???

Proof by Contraposition

To prove p implies q, sometimes it is easier to prove the contrapositive: $\neg q$ implies $\neg p$

- Recall: they are equivalent

Theorem

If n^2 is odd, then n is odd

Proof by Contraposition

- Suppose n is even
- $n = 2k$ for some integer k
- $n^2 = 4k^2 = 2(2k^2)$.
- $2k^2$ is an integer, therefore n^2 is even.

Equivalence

If your claim is an equivalence (if and only if), then commonly you have to prove both directions

Prove: An integer n is odd if and only if n^2 is odd

- Forwards direction: if n is odd then n^2 is odd
  - See two slides ago
- Backwards direction: If n^2 is odd then n is odd
  - See last slide

Proof by Contradiction

- This is a generalization of proof by contraposition
- Can be used to prove statements that aren't an if-then.
- At a high level: To prove p, assume $\neg p$ and derive a contradiction
  - I.e., conclude that q and $\neg q$, for some statement q
- Since what you concluded can't be true, your starting assumption $\neg p$ must have been false. I.e., p must be true.

Proof by Contradiction

Theorem

There are arbitrarily large primes.

Proof by Contradiction

Theorem

There are arbitrarily large primes.

- Assume for a contradiction that there is a biggest prime p
- $p!$ is divisible by all primes less than or equal to p
- $p! + 1$ is not divisible by any prime less than or equal to p (remainder is 1)
- By fundamental theorem of arithmetic, $p! + 1$ has a prime factorization
- Each prime in that factorization must be $> p$.
- There if a prime $> p$, contradiction.

Proof by Contradiction

Claim

$\sqrt{2}$ is irrational.

Proof by Contradiction

Claim

$\sqrt{2}$ is irrational.

- Suppose for a contradiction that $\sqrt{2}$ is rational.
- There are a, b with $\frac{a}{b} = \sqrt{2}$.
- Take such a and b with no common divisors (i.e. cancel out the common prime divisors).
- $a^2 = 2b^2$.
- a^2 is even, therefore a is even (recall slide 8) and can be written as $a = 2k$ for an integer k.
- $b^2 = \frac{a^2}{2} = \frac{4k^2}{2} = 2k^2$
- b^2 is even, therefore b is even (recall slide 8)
- Both a and b are even, but we chose a and b with no common divisors, a contradiction!

Case Analysis

Sometimes, you need to break up your proof into cases, and prove your conclusion in each case. The cases should cover all possibilities.

Proposition

In a group of 6 people, there must be 3 who all know each other or there must be 3 who don't know each other.

Proof

- Let a be one of the people, chosen arbitrarily
- There are 3 people that a knows, or 3 people that a does not know.
- Case 1: There are three people that a knows
  - If those people all don't know each other, then we are done
  - Otherwise, at least two of them b and c know each other, so a, b, c all know each other and we are done.
- Case 2: There are three people that a does not know
  - If those people all know each other, then we are done
  - Otherwise, at least two of them b and c don't know each other, so a, b, c all don't know each other, and we are done.

Existence Proofs

Often, you want to prove that some mathematical object, satisfying some desired properties, exists.

Prove: There exists an odd number that is a perfect square

9 is odd since $9 = 2 * 4 + 1$, and it is a perfect square since $9 = 3^2$.

This proof is constructive, since our proof explicitly provides the object (or, more generally, describes an algorithm for constructing it). Often, such proofs require no or minimal justification that your object has the desired property.

Existence Proofs

Often, you want to prove that some mathematical object, satisfying some desired properties, exists.

Prove: There exists an odd number that is a perfect square

9 is odd since $9 = 2 * 4 + 1$, and it is a perfect square since $9 = 3^2$.

This proof is constructive, since our proof explicitly provides the object (or, more generally, describes an algorithm for constructing it). Often, such proofs require no or minimal justification that your object has the desired property.

Prove: There exists irrational x, y such that x^y is rational

We proved this in Lecture 1 . . .

That proof was nonconstructive, since it did not provide x and y explicitly.

Our proof of the Pigeonhole principle in Lecture 1 was also nonconstructive.

Outline

1. Intro
2. Common Forms/Styles of Proof
3. Some Tricks and Shortcuts
4. Misc Mathematical Lingo and Notation

Visual Proofs

- You are allowed to use visual aids in your proof
  - E.g. recall our visually-aided proof on the board that in any group of 6 people, there must be at least 3 that know each other or don't know each other.
- When you do this, you must ensure that your figures do not make spurious assumptions
  - For example, if you want to prove a fact about general triangles, you shouldn't draw an isosceles triangle and use that property implicitly
- In other words, your proof has to still be general, and not tied to the particulars of the figure you choose to draw.
- Usually a good idea to accompany the visual aid with a natural language proof to avoid loss of generality.

Without Loss of Generality

- Often in your proofs, you have a mathematical object (or set of mathematical objects) that can be easily converted to having a certain useful property
- Example: In our proof that $\sqrt{2}$ is irrational, we were able to enforce that a and b have no common divisors by dividing those out.
- In those cases, we can write "we assume without loss of generality that . . . "
- In the above example, we say "We assume without loss of generality that a and b have no common divisors".

Symmetry

- Often in your proofs, there are two cases that are essentially identical by some sort of symmetry
- Example: In our proof that a group of 6 people must have 3 that know each other or don't know each other, the two cases are identical by interchanging the roles of knowing each other (which we drew as a blue edge on the board) and not knowing each other (which we drew as a red edge).
- In those situations, it is a kindness to your reader to point out this symmetry, and omit part of your proof.
- In our example, you can say "The argument for case 2 is symmetrical by interchanging the role of knowing and not knowing (or interchanging blue and red)", and omit the proof of Case 2.

Outline

1. Intro
2. Common Forms/Styles of Proof
3. Some Tricks and Shortcuts
4. Misc Mathematical Lingo and Notation

Mathematical Statements

There are many labels that mathematicians use for statements

- Theorem: A mathematical statement which has been proven, is interesting in its own right, and is thought of as important, useful, difficult, or deeply insightful. This is the highest stature an established mathematical fact can have.

Mathematical Statements

There are many labels that mathematicians use for statements

- Theorem: A mathematical statement which has been proven, is interesting in its own right, and is thought of as important, useful, difficult, or deeply insightful. This is the highest stature an established mathematical fact can have.
- Other proven mathematical statements go by different names
  - Lemma: A mathematical statement that is primarily useful as a tool for proving other statements (mainly theorems).
  - Corollary: A mathematical statement that is a relatively simple consequence of a more general or deeper Theorem.
  - Proposition, Claim, Fact: These are statements that stand alone, but are thought of as too “easy” to qualify as theorems. Sometimes they are too easy to warrant a written proof, and are left as an exercise for the reader.

Mathematical Statements

There are many labels that mathematicians use for statements

- Conjecture: A mathematical statement which has not been proven, but is believed to be true (by the person asserting the conjecture, or a broader subset of the research community). Often, these are also believed to be important, or a barrier to further progress in a field. Posing a conjecture is an invitation for others to help you prove it.

QED

- It is customary to end a mathematical proof with one of the following:
  - The abbreviation Q.E.D.: This stands for “quod erat demonstrandum”, which is Latin for “which was to be demonstrated”.
  - The Q.E.D. symbol: A square, which can be solid ■ or hollow □
- Symbolizes the end of a proof, indicating that the argument is complete.
- In typeset modern mathematics, the symbol is most common.