The Foundations: Logic and Proofs

Chapter 1, Part III: Proofs

UWO – January 26, 2021

The Foundations: Logic and Proofs

Chapter 1, Part III: Proofs

UWO – January 26, 2021

Plan for Part III

Plan for Part III

Proofs of mathematical statements

1. A *proof* is a valid argument that establishes the truth of a statement.
2. In mathematics, computer science and other disciplines, informal proofs are commonly used. Those proofs are generally short, easier to understand and to explain to people. They rely on the following typical "simplifications":
   a. more than one rule of inference are often used in one step,
   b. steps may be skipped,
   c. the rules of inference used are not explicitly stated.
3. These simplifications easily lead to errors.
4. Moreover, automating proofs on computers require to fully understand proof mechanisms.
5. Indeed, automated proofs have many practical applications:
   a. verification that computer programs are correct,
   b. establishing that operating systems are secure,
   c. enabling software to make inferences in artificial intelligence,
   d. showing that system specifications are consistent, etc.

Definitions

1. A *theorem* is a statement that can be shown to be true using:
   a. definitions,
   b. other theorems,
   c. *axioms* (statements which are given as true),
   d. rules of inference.
2. A *lemma* is a ‘helping theorem’ or a result which is needed to prove a theorem.
3. A *corollary* is a result which follows directly from a theorem.
4. Less important theorems are sometimes called *propositions*.
5. A *conjecture* is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.

Forms of theorems

1. Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, or some of the discrete structures that we will study in this class.
2. Often the universal quantifier (needed for a precise statement of a theorem) is omitted by standard mathematical convention.
   a. For example, the statement:

      "If $x > y$ holds, where x and y are positive real numbers, then $x^2 > y^2$ holds as well"

   b. really means:

      "For all positive real numbers x and y, if $x > y$ holds, then $x^2 > y^2$ holds as well."

Proving theorems

1. Many theorems have the form:
$$\forall x \ \ (P(x) \rightarrow Q(x))$$
2. To prove them, we show that where c is an arbitrary element of the domain:
$$P(c) \rightarrow Q(c)$$
3. By universal generalization (UG) (an inference rule, opposite of universal instantiation UI) the truth of the original formula follows.
4. So, we must prove something of the form:
$$p \rightarrow q$$

Plan for Part III

Proving conditional statements: $p \to q$

1. *Trivial Proof*: If we know q is true, then $p \to q$ is true as well.

   "If it is raining then $1{=}1$."

2. *Vacuous Proof*: If we know p is false then $p \to q$ is true as well.

   "If I live on Saturn then $2 + 2 = 5$."

3. Even though these examples seem silly, both trivial and vacuous proofs are often used in mathematical induction, as we will see in Chapter 5.

Even and odd integers

Definition

The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k, such that $n = 2k + 1$.

1. Note that every integer is either even or odd and no integer is both even and odd.

2. We will need this basic fact about the integers in some of the example proofs to follow.

Proving conditional statements: $p \to q$: direct proof

Assume that p is true. Use rules of inference, axioms, and logical equivalences to show that q must also be true.

1. Give a direct proof of "If n is an odd integer, then n^2 is odd."
2. **Solution**:
   a. Assume that n is odd. Then $n = 2k + 1$ for an integer k.
   b. Squaring both sides of the equation, we get:

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \\ &= 2r + 1 \end{aligned}$$

   c. where $r = 2k^2 + 2k$ is an integer. $\blacksquare$
   d. We have proved that if n is an odd integer, then so is n^2.

The symbol $\blacksquare$ marks the end of the proof and is referred to as a 'tombstone.' Sometimes **QED** (abbreviation for the Latin sentence "quod erat demonstrandum", meaning "what was to be demonstrated") or $\lhd$ is used instead.

Proving conditional statements: $p \to q$: indirect proof

Proof by Contraposition (a.k.a. *indirect proof*): Assume $\neg q$ and show $\neg p$ is true also. If we give a direct proof of $\neg q \to \neg p$ then we have a proof of $p \to$ q.

1. Prove that if n is an integer and $3n + 2$ is odd, then n is odd as well.
2. **Solution**:
   a. Assume n is even.
   b. By definition of even numbers, we have $n = 2k$ for some integer k.
   c. Thus, we have $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j$ for $j = 3k + 1$.
   d. Therefore, we have proved that $3n + 2$ is even.
   e. Since we have shown $\neg q \to \neg p$, then $p \to q$ must hold as well.
   f. If n is an integer and $3n + 2$ is odd (not even), then n is odd (not even). ■

Proving conditional statements: $p \to q$: indirect proof

1. Prove that for all integer n, if n^2 is odd, then n is odd.
2. Solution: use proof by contraposition.
   a. Assume n is even (i.e., not odd).
   b. Therefore, there exists an integer k such that $n = 2k$.
   c. Hence, $n^2 = 4k^2 = 2\ (2k^2)$,
   d. thus n^2 is even (i.e., not odd).
   e. We have shown that if n is an even integer, then n^2 is even. Therefore by contraposition, if n^2 is odd, then n is odd. ∎

Proof by contradiction

1. To prove p, assume $\neg p$ and derive some proposition contradicting the assumptions, say q. That is, so that $\neg p \wedge q \equiv \mathbf{F}$.
2. Explanation:
   a. The proposition $\neg p \wedge q \equiv \mathbf{F}$ directly proves $\neg p \rightarrow \mathbf{F}$.
   b. Thus, its contrapositive $\mathbf{T} \rightarrow p$ also holds.
   c. Therefore, applying *modus ponens* (inference rule: if A is true and implication A $\rightarrow$ B is true then B must be true), we deduce that p is true.

Example: Prove that at least 4 of any 22 days from the calendar must fall on the same day (Mo, Tu, We, Th, Fr, Sa, Su) of the week. **Solution**:

1. Assume that no more than 3 days (out of 22) fall on the same day of the week.
2. There are 7 different days of the week.
3. Since each of them was selected at most 3 times, then we picked at most 7 x 3 (21) days.
4. This contradicts an assumption that 22 days are selected. ■

Proof by contradiction

1. Use a proof by contradiction to show that $\sqrt{2}$ is irrational.
2. **Solution:**
   a. Suppose $\sqrt{2}$ is rational. Then there exist two integers a and b with $\sqrt{2} = \frac{a}{b}$, where $b \neq 0$ and a and b have no common factors (see Chapter 4). Then, we have:

$$2 = \frac{a^2}{b^2}$$
$$2b^2 = a^2$$

   b. Therefore a^2 must be even. If a^2 is even then a must be even (earlier exercise) and we have $a = 2c$ for some integer c. Thus:

$$2b^2 = 4c^2$$
$$b^2 = 2c^2$$

   c. Therefore b^2 is even, then b must be even as well.
   d. But then 2 must divide both a and b,
   e. contradicting the fact that a and b have no common factors.
   f. Thus, we have proved by contradiction that $\sqrt{2}$ is irrational . ■

Proof by contradiction

1. **Example**: Prove that there is no largest prime number.
2. **Solution**:
   a. Assume that there is a largest prime number. Call it p_n.
   b. Hence, we can list all the primes 2,3,.., p_n
   c. Now we consider the following number r:
   $$r = p_1 \times p_2 \times \cdots \times p_n + 1$$
   d. None of the prime numbers on the list divides r.
   e. Therefore, by a theorem in Chapter 4, either r is prime or there is a smaller prime that divides r (but it is not on the list).
   f. This contradicts the assumption that p_n is the largest prime.
   g. Therefore, there is no largest prime. $\blacksquare$

Plan for Part III

Theorems that are biconditional statements

To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

1. **Explanation**: We use this tautology:
$$(p \rightarrow q) \wedge (q \rightarrow p) \equiv p \leftrightarrow q.$$
2. **Example**: Prove the theorem: "For all integer n: n is odd if and only if n^2 is odd."
3. **Solution:**
   a. We have already shown that both $p \rightarrow q$ and $q \rightarrow p$ are true.
   b. Therefore, we have: $p \leftrightarrow q$.

Sometimes **iff** is used as an abbreviation for "**if an only if** ," as in "If n is an integer, then n is odd iif n^2 is odd."

Plan for Part III

What is wrong with this?

"Proof" that $1 = 2$

Step	**Reason**
1. $a = b$	There exist such integera, b
2. $a^2 = a \times b$	Multiply both sides of (1) by a
3. $a^2 - b^2 = a \times b - b^2$	subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Algebra on (3)
5. $a + b = b$	Divide both sides by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$
7. $2 = 1$	Divide both sides of (6) by b

Solution: Step 5. $a - b = 0$ by the premise and division by 0 is undefined.

Looking ahead

1. If direct methods of proof do not work:
   a. We may need a clever use of a proof by contraposition,
   b. or a proof by contradiction.
2. In the next section, we will see strategies that can be used when straightforward approaches do not work.
3. In later chapters, we will see techniques that are specific to certain types of statements:
   a. in Chapter 5, we will see mathematical induction and related techniques,
   b. in Chapter 6, we will see combinatorial proofs.

Plan for Part III

1. Basic Proof Methods

1.1 Mathematical Statements and their proofs

1.2 Proving Conditional Statements

1.3 Theorems that are Biconditional Statements

1.4 Errors in proofs

2. Proof Strategies

2.1 Proof by case inspection

2.2 Without Loss of Generality

2.3 Existence Proofs

2.4 Counterexamples

2.5 Uniqueness Proofs

2.6 Proof Strategies for implications

2.7 Backward Reasoning

2.8 Universally Quantified Assertions

2.9 Open Problems

2.10 Additional proof methods

Plan for Part III

Proof by case inspection

1. To prove a conditional statement of the form:
$$(p_1 \vee p_2 \vee \cdots \vee p_n) \to q$$
2. One can use the following logical equivalence:
$$[(p_1 \vee p_2 \vee \cdots \vee p_n) \to q] \equiv [(p_1 \to q) \wedge (p_2 \to q) \wedge \cdots \wedge (p_n \to q)]$$
3. Therefore, one can prove each of the implications (**cases**) of $p_i \to q$ separately.

Proof by case inspection: example

1. Define $a \,@\, b \equiv max a, b$. That is:

$$a \,@\, b = \begin{cases} a & \text{if} \quad a \geq b \\ b & \text{if} \quad a < b \end{cases}$$

2. Show that for all real numbers a, b, c we have

$$(\mathrm{a}\ @\mathrm{b})\ @\ \mathrm{c} = \mathrm{a}\ @\ (\mathrm{b}\ @\ \mathrm{c})$$

3. (This means the max operation @ is associative.)
4. **Proof**: Let a, b, and c be arbitrary real numbers. Then one of the following 6 cases must hold:

$$\begin{cases} p_1: & a \geq b \geq c \\ p_2: & a \geq c \geq b \\ p_3: & b \geq a \geq c \\ p_4: & b \geq c \geq a \\ p_5: & c \geq a \geq b \\ p_6: & c \geq b \geq a \end{cases}$$

Proof by case inspection

Prove by cases:

$$(p_1 \vee p_2 \vee p_3 \vee p_4 \vee p_5 \vee p_6) \rightarrow \texttt{(a @b) @ c = a @ (b @ c)}$$

1. **Case 1:**
   a. $a \geq b \geq c$
   b. $(a@b) = a$, $a@c = a$, $b@c = b$
   c. Hence $(a@b)@c = a = a@(b@c)$
   d. Therefore the equality holds for the first case.
2. A complete proof requires that the equality be shown to hold for all 6 cases. But the proofs of the remaining cases are similar. Try them. ■

Plan for Part III

Without loss of generality

Example: Show that, for all integers x and y, if both $x \cdot y$ *and* $x + y$ are even, then both x and y are even as well.

Proof: Use a proof by contraposition.

1. Suppose x and y are not both even.
2. Then, at least one of them is odd.
3. Without loss of generality, assume that x is odd.
4. Then $x = 2m + 1$ for some integer m.
   a. **Case 1:** y is even. Then $y = 2n$ for some integer n, so $x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd.
   b. **Case 2:** y is odd. Then $y = 2n + 1$ for some integer n, so $x \cdot y = (2m + 1)(2n + 1) = 2(2m \cdot n + m + n) + 1$ is odd.
5. Therefore, for any integer y, the integers $x \cdot y$ *and* $x + y$ are not both even. ■
6. We only covered the case where x is odd and the case where y is odd is similar.
7. The phrase *without loss of generality* (WLOG) indicates this.

Plan for Part III

Existence proofs

1. Proof of theorems of the form: $\exists x \; P(x)$.
2. **Constructive** existence proof:
   a. Find an explicit value of c, for which $P(c)$ is true.
   b. Then $\exists x \; P(x)$ is true by *existential generalization* (EG).
3. **Example**: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways:
4. **Proof**: 1729 is such a number since
   $1729 = 10^3 + 9^3 = 12^3 + 1^3$ ■

Godfrey Harold Hardy (1877-1947)

Srinivasa Ramanujan (1887-1920)

Existence proofs

1. **Nonconstructive** existence proof: some techniques allow to prove existence $\exists x P(x)$ without finding a specific element c where P(c) is true.
2. **Example**: Show that there exist irrational numbers x and y such that x^y is rational.
3. **Proof:**
   a. We know that $\sqrt{2}$ is irrational.
   b. Consider the number $\sqrt{2}^{\sqrt{2}}$.
   c. If it is rational, we are done (for $x = y = \sqrt{2)}.$
   d. Assume not, i.e. $\sqrt{2}^{\sqrt{2}}$ is irrational.
      Then choose $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so that

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2.$$

$\blacksquare$

Note, at the end of this proof we know that x^y is rational either for x=y= $\sqrt{2}$ or for $x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$ (exclusive or) but we do not know for which specific pair.

Plan for Part III

Counterexamples

1. Recall $\neg\forall x P(x) \equiv \exists x \neg P(x)$.
2. To establish that $\forall x P(x)$ is false (that is, $\neg\forall x P(x)$ is true) find a c such that $\neg P(c)$ is true (that is $P(c)$ is false).
3. Such a c is called a **counterexample** to the assertion

$$\forall x P(x)$$

Example: "Every positive integer is the sum of the squares of 3 integers." The integer 7 is a counterexample. So the claim is false.

Plan for Part III

Uniqueness proofs

1. Some theorems assert the existence of a **unique** element satisfying a particular property (predicate) P, denoted as follows
$$\exists! x \; P(x).$$
2. The two parts of a *uniqueness proof* are:
   a. *Existence*: we show that an element x satisfying $P(x)$ exists.
   b. *Uniqueness*: we show that if two elements y and x satisfy $P(x)$ and $P(y)$, then we must have $x = y$.
3. **Example**: Show that for all real numbers a and b, with $a \neq 0$, there is a unique real number r such that we have $ar + b = 0$.
4. **Solution**:
   a. *Existence*: The real number $r = -\frac{b}{a}$ is a solution of $ar + b = 0$ because $a(-\frac{b}{a}) + b = -b + b = 0$.
   b. *Uniqueness*: Suppose that there is also a real number s such that $as + b = 0$. Then $ar + b = as + b$, where $r = -\frac{b}{a}$. Subtracting b from both sides and dividing by a shows that $r = s$. ∎

Plan for Part III

Proof strategies for proving $p \to q$

1. Choose a method.
   a. First try a direct method of proof.
   b. If this does not work, try an indirect method (e.g., try to prove the contrapositive).
2. For whichever method you are trying, choose a strategy.
   a. First try *forward reasoning*.
      1. Start with the axioms and known theorems and construct a sequence of steps $r_i \to r_{i+1}$ starting with $r_1 = p$ and ending with $r_n = q$ (for direct proof), or
      2. starting with $r_1 = \neg q$ and ending with $r_n = \neg p$ (for indirect proof).
   b. *Explanation*: $(A \to B) \wedge (B \to C) \to (A \to C)$ is a tautology
   c. If this doesn't work, try *backward reasoning*.
      1. When trying to prove $p \to q$, find a sequence $r_{i-1} \to r_i$ starting with $r_n = q$ and ending with $r_1 = p$ (for direct proof), or
      2. starting with $r_n = \neg p$ and ending with $r_1 = \neg q$ (for indirect proof).

Plan for Part III

Backward reasoning example

1. Suppose that two people play a game taking turns removing, 1, 2, or 3 stones at a time from a pile that begins with 15 stones. The person who removes the last stone wins the game.
2. To show this theorem, we shall prove that the first player can win the game, no matter what the second player does.
3. **Proof**: Let n be the last step of the game.
   a. **Step n:** Player 1 can win if the pile contains 1,2, or 3 stones.
   b. **Step n-1**: Player 2 will have to leave such a pile if the pile that he/she is faced with has 4 stones.
   c. **Step n-2**: Player 1 can leave 4 stones when there are 5,6, or 7 stones left at the beginning of his/her turn.
   d. **Step n-3**: Player 2 must leave such a pile, if there are 8 stones.
   e. **Step n-4**: Player 1 has to have a pile with 9,10, or 11 stones to ensure that there are 8 left.
   f. **Step n-5**: Player 2 needs to be faced with 12 stones to be forced to leave 9,10, or 11.
   g. **Step n-6**: Player 1 can leave 12 stones by removing 3 stones.
4. Now reasoning forward, the first player can ensure a win by removing 3 stones and leaving 12.

Plan for Part III

Universally quantified assertions

1. To prove theorems of the form $\forall x \quad P(x)$,
   1. assume x is an arbitrary member of the domain and show that $P(x)$ must be true.
   2. Using UG (universal generalization) it follows that $\forall x P(x)$.
2. **Example**: An integer x is even if and only if x^2 is even.
3. **Solution**:
   1. The quantified assertion is:
   $$\forall x \quad (x \text{ is even} \leftrightarrow x^2 \text{ is even}).$$
   2. We assume x is arbitrary.
   3. Recall that $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$
   4. So, we have two cases to consider. These are considered in turn.

Continued on the next slide

Universally quantified assertions

1. **Case 1.** We show that if x is even then x^2 *is* even using a direct proof (the *only if* part or *necessity*).
   a. If x is even then $x = 2k$ for some integer k.
   b. Hence $x^2 = 4k^2 = 2(2k^2)$ which is even since it is an integer divisible by 2.
   c. This completes the proof of case 1.

Case 2 on the next slide.

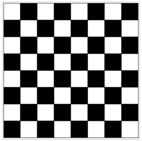
Universally quantified assertions

1. **Case 2.** We show that if x^2 is even then x must be even (the *if* part or *sufficiency*). We use a proof by contraposition.
   a. Assume x is not even and then show that x^2 is not even.
   b. If x is not even then it must be odd. So, $x = 2k + 1$ for some k. Then $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2\text{k}) + 1$
   c. which is odd and hence not even.
   d. This completes the proof of case 2.
2. Since x was arbitrary, the result follows by UG.
3. Therefore we have shown that x is even if and only if x^2 is even. ■

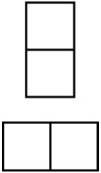
Proof and disproof: Tilings

Example 1: Can we tile the standard checker-board using dominos?

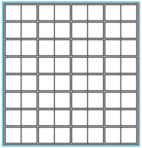
Solution: Yes! One example provides a constructive existence proof.



Standard Checkerboard



Two Dominoes



One Possible Solution

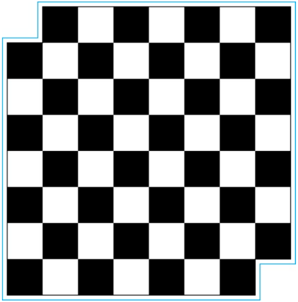
Example 2: Can we tile a checker-board obtained by removing one of the four corner squares of a standard checker-board?

Solution:

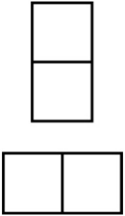
a. Our checker-board has $64 - 1 = 63$ squares.
b. Since each domino has two squares, a board with a tiling must have an even number of squares.
c. The number 63 is not even.
d. We have a contradiction. ∎

Tilings

Example 3: Can we tile a board obtained by removing both the upper left and the lower right squares of a standard checker-board?



Nonstandard Checker-board



Two Dominoes

Continued on next slide

Tilings

Solution:

a. There are 62 squares in this board.
b. To tile it we need 31 dominos.
c. *Key fact*: Each domino covers one black and one white square.
d. Therefore the tiling covers 31 black squares and 31 white squares.
e. Our board has either 30 black squares and 32 white squares or 32 black squares and 30 white squares.
f. Contradiction! ■

Plan for Part III

The role of open problems

1. Unsolved problems have motivated much work in mathematics. Fermat's Last Theorem was conjectured more than 300 years ago. It has only recently been finally solved.

   Fermat's Last Theorem: The equation $x^n + y^n = z^n$ has no solutions in integers x, y, and z, with $xyz \neq 0$ whenever n is an integer with $n > 2$.

   A proof was found by Andrew Wiles in the 1990s.

An open problem

1. **The 3x + 1 Conjecture**: Let T be the transformation that sends an even integer x to $\frac{x}{2}$ and an odd integer x to $3x + 1$. For all positive integers x, when we repeatedly apply the transformation T, we will eventually reach the integer 1.

   For example, starting with $x = 13$:

   $T(13) = 3{\cdot}13 + 1 = 40$, $T(40) = 40/2 = 20$, $T(20) = 20/2 = 10$,

   $T(10) = 10/2 = 5$, $T(5) = 3{\cdot}5 + 1 = 16$,$T(16) = 16/2 = 8$,

   $T(8) = 8/2 = 4$, $T(4) = 4/2 = 2$, $T(2) = 2/2 = 1$

   The conjecture has been verified using computers up to $5 \times 6 \times 10^{13}$.

Plan for Part III

Additional proof methods

1. Later we will see many other proof methods:
   a. Mathematical induction, which is a useful method for proving statements of the form $\forall n\ P(n)$, where the domain consists of all positive integers.
   b. Structural induction, which can be used to prove such results about recursively defined sets.
   c. Cantor diagonalization is used to prove results about the size of infinite sets.
   d. Combinatorial proofs use counting arguments.