Discrete Structures

Joy Chandra Mukherjee

August 29, 2023

Chapter 1

Proof Techniques

A **proof** is a valid argument that establishes the truth of a mathematical statement. In this chapter, we move from **formal proofs** of theorems toward more **informal proofs**. The arguments we used to show that statements involving propositions and quantified statements are true were formal proofs, where all steps were supplied, and the rules for each step in the argument were given. However, formal proofs of useful theorems can be extremely long and hard to follow. In practice, the proofs of theorems designed for human understanding are almost always informal proofs, where more than one rule of inference may be used in each step, where steps may be skipped, where the axioms being assumed and the rules of inference used are not explicitly stated.

1.1 Some Terminology

Formally, a **theorem** is a statement that can be shown to be true. In mathematical writing, the term theorem is usually reserved for a statement that is considered to be important. Less important theorems sometimes are called **propositions**. A theorem may be the universal quantification of a conditional statement with one or more premises and a conclusion. However, it may be some other type of logical statement. For example, "For all positive real numbers x and y, if $x > y$, then $x^2 > y^2$".

To prove a theorem of the form $\forall x(P(x) \rightarrow Q(x))$, our goal is to show that $P(c) \rightarrow Q(c)$ is true, where c is an arbitrary element of the domain, and then apply universal generalization. In this proof, we need to show that a conditional statement is true. Recall that $p \rightarrow q$ is true except the case p is true but q is false. Note that to prove the statement $p \rightarrow q$, we need only show that q is true if p is true.

We demonstrate that a theorem is true with a proof. A **proof** is a valid argument that establishes the truth of a theorem. The statements used in a proof can include **axioms** (or **postulates**), which are statements we assume to be true, the premises, if any, of the theorem, and previously proven theorems. Axioms may be stated using primitive terms that do not require definition, but all other terms used in theorems and their proofs must be defined. Rules of inference, together with definitions of terms, are used to draw conclusions from other assertions, tying together the steps of a proof. In practice, the final step of a proof is usually just the conclusion of the theorem.

A less important theorem that is helpful in the proof of other results is called a **lemma** (plural **lemmas** or **lemmata**). Complicated proofs are usually easier to understand when they are proved using a series of lemmas, where each lemma is proved individually. A **corollary** is a theorem that can be established directly from a theorem that has been proved. A **conjecture** is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert. When a proof of a conjecture is found, the conjecture becomes a theorem. Many times conjectures are shown to be false, so they are not theorems.

1.2 Direct Proofs

A **direct proof** of a conditional statement $p \rightarrow q$ is constructed by showing that if p is true, then q must also be true, so that the combination p true and q false never occurs. In a direct proof, we assume that p is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that q must also be true.

Definition 1 *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. Two integers have the* **same parity***, when both are even or both are odd; they have* **opposite parity***, when one is even and the other is odd. An integer a is a perfect square, if there is an integer b such that* $a = b^2$.

Definition 2 (Rational number) *The real number r is rational if there exist integers p and q with* $q \neq 0$ *such that* $r = p/q$*, where p and q have no common factors. A real number that is not rational is called irrational.*

Example 3 *Prove that "If n is an odd integer, then* n^2 *is odd".*

Example 4 *Prove that "If m and n are both perfect squares, then nm is also a perfect square".*

Example 5 *Prove that for every real number r and every real number s, if r and s are rational numbers, then r + s is rational.*

1.3 Proofs by Contraposition

Proofs by contraposition make use of the fact that the conditional statement $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$. In a proof by contraposition of $p \rightarrow q$, we take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\neg p$ must follow. Typically, the proof by contraposition is used, when we cannot easily find a direct proof.

Example 6 *Prove that if n is an integer and 3n + 2 is odd, then n is odd.*

Example 7 *Prove that if* $n = ab$*, where a and b are positive integers, then* $a \leq \sqrt{n}$ *or* $b \leq \sqrt{n}$.

Example 8 *Prove that if n is an integer and* n^2 *is odd, then n is odd.*

Definition 9 (Vacuous proof) *If we can show that p is false, then we have a proof, called a vacuous proof, of the conditional statement $p \to q$. The fact that the truth value of the conclusion q of a conditional statement, $p \to q$, is irrelevant to the truth value of the conditional statement $p \to q$, because a conditional statement with a false hypothesis p is guaranteed to be true.*

Definition 10 (Trivial proof) *If we can show that q is true, then we have a proof, called a trivial proof, of the conditional statement $p \to q$. The fact that the truth value of the hypothesis p of a conditional statement, $p \to q$, is irrelevant to the truth value of the conditional statement $p \to q$, because a conditional statement with a true conclusion q is guaranteed to be true.*

1.4 Proofs by Contradiction

Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg p \to q$ is true. Because q is false, but $\neg p \to q$ is true, we can conclude that $\neg p$ is false, which means that p is true. How can we find a contradiction q that might help us prove that p is true in this way?

Because the statement $r \wedge \neg r$ is a contradiction, whenever r is a proposition, we can prove that p is true if we can show that $\neg p \to (r \wedge \neg r)$ is true for some proposition r. Proofs of this type are called **proofs by contradiction**.

Example 11 *Show that at least four of any 22 days must fall on the same day of the week.*

Example 12 *Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.*

Solution: *Solution: Let p be the proposition "$\sqrt{2}$ is irrational". To start a proof by contradiction, we suppose that $\neg p$ is true. Note that $\neg p$ is the statement, which says that "$\sqrt{2}$ is rational". We will show that assuming that $\neg p$ is true leads to a contradiction.*

If $\sqrt{2}$ is rational, there exist integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors (so that the fraction a/b is in lowest

terms). Here, we are using the fact that every rational number can be written in lowest terms. Because $\sqrt{2} = a/b$*, it follows that* $2 = a^2/b^2$*, or* $2b^2 = a^2$*.*

By the definition of an even integer it follows that a^2 *is even. We next use the fact that if* a^2 *is even,* a *must also be even. Furthermore, because* a *is even, by the definition of an even integer,* $a = 2c$ *for some integer* c*. Thus,* $2b^2 = 4c^2$*, or* $b^2 = 2c^2$*.*

By the definition of even, this means that b^2 *is even. Again using the fact that if the square of an integer is even, then the integer itself must be even, we conclude that* b *must be even as well.*

We have now shown that the assumption of $\neg p$ *leads to the equation* $\sqrt{2} = a/b$*, where* a *and* b *have no common factors, but both* a *and* b *are even, that is, 2 divides both* a *and* b*. Note that the statement that* $\sqrt{2} = a/b$*, where* a *and* b *have no common factors, means, in particular, that 2 does not divide both* a *and* b*. Because our assumption of* $\neg p$ *leads to the contradiction that 2 divides both* a *and* b*, and 2 does not divide both* a *and* b*,* $\neg p$ *must be false. That is, the statement* p*, "*$\sqrt{2}$ *is irrational" is true.*

Note that we can rewrite a proof by contraposition of a conditional statement as a proof by contradiction. In a proof of $p \rightarrow q$ by contraposition, we assume that $\neg q$ is true. We then show that $\neg p$ must also be true. To rewrite a proof by contraposition of $p \rightarrow q$ as a proof by contradiction, we suppose that both p and $\neg q$ are true. Then, we use the steps from the proof of $\neg q \rightarrow \neg p$ to show that $\neg p$ is true. This leads to the contradiction $p \wedge \neg p$, completing the proof.

Note that we can rewrite a direct proof of a conditional statement as a proof by contradiction. In a direct proof of $p \rightarrow q$, we assume that p is true. We then show that q must also be true. To rewrite a direct proof of $p \rightarrow q$ as a proof by contradiction, we suppose that both p and $\neg q$ are true. Then, we use the steps from the proof of $p \rightarrow q$ to show that q is true. This leads to the contradiction $q \wedge \neg q$, completing the proof.

1.5 Proofs by Equivalence

To prove a theorem that is a biconditional statement of the form $p \longleftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true. The validity of this approach is based on the tautology $(p \longleftrightarrow q) \equiv (p \rightarrow q) \wedge (q \rightarrow p)$.

Example 13 *Prove the theorem "If n is an integer, then n is odd if and only if n^2 is odd".*

To show that a statement of the form $\forall x P(x)$ is false, we need only find a **counterexample**, that is, an example x for which $P(x)$ is false.

Example 14 *Show that the statement "Every positive integer is the sum of the squares of two integers" is false.*

Solution: *The number 3 cannot be written as the sum of the squares of two integers*

Example 15 *Show that the statement "Every positive integer is the sum of the squares of three integers" is false.*

Solution: *The number 7 cannot be written as the sum of the squares of two integers*

1.6 Proofs by Exhaustion

Some theorems can be proved by examining a relatively small number of examples. Such proofs are called **exhaustive proofs**, or **proofs by exhaustion**, because these proofs proceed by exhausting all possibilities.

Example 16 *Prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.*

Solution: *We use a proof by exhaustion. We only need verify the inequality $(n+1)^3 \geq 3^n$ when $n = 1$, 2, 3, and 4. For $n = 1$, we have $(n+1)^3 = 2^3 =$*

8 and $3^n = 3^1 = 3$. *For* $n = 2$, *we have* $(n+1)^3 = 3^3 = 27$ *and* $3^n = 3^2 = 9$. *For* $n = 3$, *we have* $(n+1)^3 = 4^3 = 64$ *and* $3^n = 3^3 = 27$. *For* $n = 4$, *we have* $(n+1)^3 = 5^3 = 125$ *and* $3^n = 3^4 = 81$.

In each of these four cases, we see that $(n+1)^3 \geq 3^n$. *We have used the method of exhaustion to prove that* $(n+1)^3 \geq 3^n$ *if* n *is a positive integer with* $n \leq 4$.

Example 17 *Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9. (An integer n is a perfect power if it equals* m^a, *where* m *is an integer and* a *is an integer greater than 1.)*

Solution: *We use a proof by exhaustion. The squares of positive integers not exceeding 100 are 1, 4, 9, 16, 25, 36, 49, 64, 81, and 100. The cubes of positive integers not exceeding 100 are 1, 8, 27, and 64. The fourth powers of positive integers not exceeding 100 are 1, 16, and 81. The fifth powers of positive integers not exceeding 100 are 1 and 32. The sixth powers of positive integers not exceeding 100 are 1 and 64. There are no powers of positive integers higher than the sixth power not exceeding 100, other than 1. Looking at this list of perfect powers not exceeding 100, we see that n = 8 is the only perfect power n for which n + 1 is also a perfect power. That is,* $2^3 = 8$ *and* $3^2 = 9$ *are the only two consecutive perfect powers not exceeding 100.*

1.7 Proofs by Cases

To prove a conditional statement of the form $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$, the tautology $[(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q] \longleftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$ can be used as a rule of inference. Such an argument is called a **proof by cases**.

Example 18 *Prove that if* n *is an integer, then* $n^2 \geq n$.

Solution: *We can prove that* $n^2 \geq n$ *for every integer by considering three cases, when* $n = 0$, *when* $n \geq 1$, *and when* $n \leq$ -1.

Example 19 *Recall that* $|a|$, *the absolute value of* a, *equals* a *when* $a \geq 0$

and equals $-a$ when $a < 0$.Use a proof by cases to show that $|xy| = |x||y|$, where x and y are real numbers.

Solution: *We can prove that $|xy| = |x||y|$ by considering four cases, (i) x and y are both non-negative, (ii) x is non-negative and y is negative, (iii) x is negative and y is non-negative, and (iv) x and y are both negative.*

Example 20 *Formulate a conjecture about the final decimal digit of the square of an integer and prove your result.*

Solution: *The final decimal digit of an integer is between 0 and 9. Since $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16$, $5^2 = 25$, $6^2 = 36$, $7^2 = 49$, $8^2 = 64$, $9^2 = 81$, the final decimal digit of the square of an integer is x, where $x \in \{0, 1, 4, 5, 6, 9\}$.*

Example 21 *Show that there are no solutions in integers x and y of $x^2 + 3y^2 = 8$.*

Solution: *We can quickly reduce a proof to checking just a few simple cases because $x^2 > 8$ when $|x| \geq 3$, i.e., x equals -2, -1, 0, 1, or 2. Again, $3y^2 > 8$ when $|y| \geq 2$, i.e., x equals -1, 0, or 1. We can finish using an exhaustive proof. To dispense with the remaining cases, we note that possible values for x^2 are 0, 1, and 4, and possible values for $3y^2$ are 0 and 3, and the largest sum of possible values for x^2 and $3y^2$ is 7. Consequently, it is impossible for $x^2 + 3y^2 = 8$ to hold when x and y are integers.*

In general, when the phrase "**without loss of generality**" is used in a proof (often abbreviated as **WLOG**), we assert that by proving one case of a theorem, no additional argument is required to prove other specified cases. That is, other cases follow by making straightforward changes to the argument, or by filling in some straightforward initial step.

Example 22 *Show that if x and y are integers and both xy and $x + y$ are even, then both x and y are even.*

Solution: *We will use proof by contraposition, the notion of without loss of generality, and proof by cases. First, suppose that x and y are not both even.*

That is, assume that x is odd or that y is odd (or both). Without loss of generality, we assume that x is odd, so that x = 2m + 1 for some integer m.

To complete the proof, we need to show that xy is odd or x + y is odd. Consider two cases: (i) y is even, and (ii) y is odd. In (i), y = 2n for some integer n, so that x + y = (2m + 1) + 2n = 2(m + n) + 1 is odd. In (ii), y = 2n + 1 for some integer n, so that xy = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1 is odd. This completes the proof by contraposition.

Example 23 *Is it true that every positive integer is the sum of 18 fourth powers of integers?*

Solution: *To determine whether a positive integer n can be written as the sum of 18 fourth powers of integers, we might begin by examining whether n is the sum of 18 fourth powers of integers for the smallest positive integers. Because the fourth powers of integers are 0, 1, 16, 81, ..., if we can select 18 terms from these numbers that add up to n, then n is the sum of 18 fourth powers. We can show that all positive integers up to 78 can be written as the sum of 18 fourth powers. However, the integer 79 is not the sum of 18 fourth powers of integers.*

1.8 Proofs by Existence

Many theorems are assertions that objects of a particular type exist. A theorem of this type is a proposition of the form $\exists x P(x)$, where P is a predicate. A proof of a proposition of the form $\exists x P(x)$ is called an existence proof. There are several ways to prove a theorem of this type.

Sometimes an existence proof of $\exists x P(x)$ can be given by finding an element a, called a witness, such that P(a) is true. This type of existence proof is called constructive.

It is also possible to give an existence proof that is nonconstructive by proving that we do not find an element a such that P(a) is true, which we refer to as a proof by contradiction.

Example 24 (A Constructive Proof by Existence) *Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.*

Solution: $1729 = 10^3 + 9^3 = 12^3 + 1^3$ *is "the smallest number expressible as the sum of cubes in two different ways", as replied by an Indian prodigy, Srinivasa Ramanujan in the hospital, when the English mathematician Godfrey Harold Hardy remarked that "1729, the number of the cab he took, was rather dull".*

Example 25 (A Nonconstructive Proof by Existence) *Show that there exist irrational numbers x and y such that x^y is rational.*

Solution: *We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. Two cases may be possible.*

Case 1: $\sqrt{2}^{\sqrt{2}}$ *is rational. We are done.*

Case 2: $\sqrt{2}^{\sqrt{2}}$ *is irrational. Then* $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$ *is rational. We are done.*

This proof is an example of a nonconstructive existence proof, because we have not found irrational numbers x and y such that x^y is rational. Rather, we have shown that either the pair x = $\sqrt{2}$, y = $\sqrt{2}$ or the pair x = $\sqrt{2}^{\sqrt{2}}$, y = $\sqrt{2}$ have the desired property, but we do not know which of these two pairs works.

Example 26 Chomp *is a game played by two players. In this game, cookies are laid out on a rectangular grid. The cookie in the top left position is poisoned. The two players take turns making moves; at each move, a player is required to eat a remaining cookie, together with all cookies to the right and below it. The loser is the player who has no choice but to eat the poisoned cookie. We ask whether one of the two players has a winning strategy. That is, can one of the players always make moves that are guaranteed to lead to a win?*

Solution: *For any rectangular starting position, other than 1 × 1, the first player can always win. We will give a nonconstructive existence proof of a*

winning strategy for the first player without explicitly describing the moves the player. First, note that the game ends and cannot finish in a draw because with each move at least one cookie is eaten, so after no more than $m \times n$ moves the game ends, where the initial grid is $m \times n$. Now, suppose that the first player begins the game by eating just the cookie in the bottom right corner. There are two possibilities, this is the first move of a winning strategy for the first player, or the second player can make a move that is the first move of a winning strategy for the second player. In this second case, instead of eating just the cookie in the bottom right corner, the first player could have made the same move that the second player made as the first move of a winning strategy and then continued to follow that winning strategy. This would guarantee a win for the first player.

1.9 Proof by Forward Reasoning

Example 27 *Given two positive real numbers x and y, prove that their arithmetic mean is $(x + y)/2$ is greater than their geometric mean is $\sqrt{xy}$.*

Solution: *Suppose that x and y are distinct positive real numbers. Then $(x - y)^2 > 0$ because the square of a nonzero real number is positive. This implies that $x^2 - 2xy + y^2 > 0$. Adding $4xy$ to both sides, we obtain $x^2 + 2xy + y^2 > 4xy$. This means that $(x + y)^2 > 4xy$. Dividing both sides of this equation by 4, we see that $(x + y)2/4 > xy$. Finally, taking square roots of both sides yields $(x + y)/2 > \sqrt{xy}$.*

1.10 Proof by Backward Reasoning

Example 28 *Suppose that two people play a game taking turns removing one, two, or three stones at a time from a pile that begins with 15 stones. The person who removes the last stone wins the game. Show that the first player can win the game no matter what the second player does.*

Solution: *To prove that the first player can always win the game, we work backward. At the last step, the first player can win if this player is left with a*

pile containing one, two, or three stones. The second player will be forced to leave one, two, or three stones if this player has to remove stones from a pile containing four stones. Consequently, one way for the first person to win is to leave four stones for the second player on the next-to-last move. The first person can leave four stones when there are five, six, or seven stones left at the beginning of this player's move, which happens when the second player has to remove stones from a pile with eight stones. Consequently, to force the second player to leave five, six, or seven stones, the first player should leave eight stones for the second player at the second-to-last move for the first player. This means that there are nine, ten, or eleven stones when the first player makes this move. Similarly, the first player should leave twelve stones when this player makes the first move. We can reverse this argument to show that the first player can always make moves so that the player wins the game, no matter what the second player does. These moves successively leave twelve, eight, and four stones for the second player. The first player picks three stones in the first move.

1.11 Tilings of Checkerboards

There are two famous books in the topic: (i) *Polyominoes: A Guide to Puzzles and Problems in Tiling* by G. E. Martin and (ii) *Polyominoes* by S.W. Golomb.

Definition 29 (Checkerboard) *A* **checkerboard** *is a rectangle divided into squares of the same size by horizontal and vertical lines. The game of checkers is played on a board with 8 rows and 8 columns; this board is called the* **standard checkerboard**. *In this section we use the term board to refer to a checkerboard of any rectangular size as well as parts of checkerboards obtained by removing one or more squares.*

Definition 30 (Domino) *A domino is a rectangular piece that is one square by two squares. We say that a board is tiled by dominoes when all its squares are covered with no overlapping dominoes and no dominoes overhanging the board.*

Example 31 *Can we tile the standard checkerboard using dominoes?*

Solution: *For a constructive existence proof, we need to find just one such tiling. We can tile it by placing 32 dominoes horizontally, where we cover one row by 4 dominoes. We can tile it by placing 32 dominoes vertically, where we cover one column by 4 dominoes. We can place some tiles vertically and some horizontally.*

Example 32 *Can we tile a board obtained by removing one of the four corner squares of a standard checkerboard?*

Solution: *A standard checkerboard has 64 squares. Removing a square produces a board with 63 squares. Now suppose that we could tile a board obtained from the standard checkerboard by removing a corner square. The board has an even number of squares because each domino covers two squares and no two dominoes overlap and no dominoes overhang the board. Consequently, we can prove by contradiction that a standard checkerboard with one square removed cannot be tiled using dominoes because such a board has an odd number of squares.*

Example 33 *Can we tile the board obtained by deleting the upper left and lower right corner squares of a standard checkerboard?*

Solution: *Suppose we can use dominoes to tile a standard checkerboard with opposite corners removed. Note that the standard checkerboard with opposite corners removed contains 64 - 2 = 62 squares. The tiling would use 62/2 = 31 dominoes. Note that each domino in this tiling covers one white and one black square. Consequently, the tiling covers 31 white squares and 31 black squares. However, when we remove two opposite corner squares, either 32 of the remaining squares are white and 30 are black, or else 30 are white and 32 are black. This contradicts the assumption that we can use dominoes to cover a standard checkerboard with opposite corners removed.*

Definition 34 (Polyomino) *A polyomino is an identically shaped piece constructed from congruent squares that are connected along their edges. The term polyomino is coined in 1953 by the mathematician Solomon Golomb in his book Polyominoes. Two polyominoes with the same number of squares are*

considered to be the same if we can rotate and/or flip one of the polyominoes to get the other one.

Definition 35 (Triomino) *There are two types of triominoes, which are polyominoes made up of three squares connected by their sides. One type of triomino, the straight triomino, has three horizontally connected squares; the other type, right triominoes, resembles the letter L in shape, flipped and/or rotated, if necessary.*

Example 36 *Can you use straight triominoes to tile a standard checkerboard?*

Solution: *The standard checkerboard contains 64 squares. Each triomino covers three squares. Consequently, if triominoes tile a board, the number of squares of the board must be a multiple of 3. Because 64 is not a multiple of 3, triominoes cannot be used to cover an 8 × 8 checkerboard.*

Example 37 *Can we use straight triominoes to tile a standard checkerboard with one of its four corners removed?*

Solution: *An 8 × 8 checkerboard with one corner removed contains 64 - 1 = 63 squares. Any tiling by straight triominoes of one of these four boards uses 63/3 = 21 triominoes. Because we are using straight triominoes, we color the squares using three colors blue, black and white. If a tiling is possible for an 8 × 8 checkerboard, then there are 21 blue squares, 21 black squares, and 22 white squares in this coloring.*

Next, we make the crucial observation that when a straight triomino covers three squares of the checkerboard, it covers one blue square, one black square, and one white square. Next, note that each of the three colors appears in a corner square. Thus, without loss of generality, we may assume that we have rotated the coloring so that the missing square is colored blue. Therefore, the remaining board contains 20 blue squares, 21 black squares, and 22 white squares. This is a contradiction. Therefore, we cannot tile this board using straight triominoes.