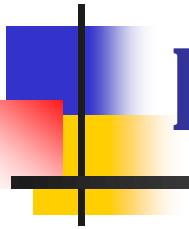
Discrete Mathematics and Its Applications



Methods of Proof

Wenjing Li

wjli@bupt.edu.cn

School of Computer Science

Beijing University of Posts & Telecommunications

Outline

- Form of theorems
- Proof Methods for Implications
- Proof Methods for Existence
- Proof Methods for Unique Existence
- Proof Methods for Nonexistence
- Proof Methods for Universally Quantified Assertions
- Some Fallacies

Methods of Proof

- **Definition:**
  - A ***theorem*(定理)** is a *valid* (正确) logical assertion which can be proved using
    - other theorems
    - ***axioms*** **(公理)** (statements which are given to be true) and
    - ***rules of inference*** (推理规则) (logical rules which allow the deduction of conclusions from premises).
  - A ***lemma*** **(引理)** is a 'pre-theorem' or a result which is needed to prove a theorem.
  - A ***corollary*** **(推论)** is a 'post-theorem' or a result which follows directly from a theorem.
  - A ***conjecture*** (猜想) is a statement that is being proposed to be a true statement.

Form of theorems

- **Implication**
  - $P \rightarrow Q$
- **Existence or nonexistence**
  - $\exists x P(x)$, $\sim\exists x P(x)$
- **Uniqueness**
  - $\exists ! x P(x)$
- **Universally Quantified Assertions**
  - $\forall x P(x)$, $\sim\forall x P(x)$

Proof Methods for Implications

- We wish to establish the truth of the 'theorem'

$$P \rightarrow Q.$$

- P may be a conjunction of other hypotheses

$$P_1 \wedge P_2 \wedge \ldots \wedge P_k$$

- $P \rightarrow Q$ is a *conjecture* (推测) until a proof is produced.

Proof Methods for Implications

For proving implications $p \rightarrow q$, we have:

- ***Direct*** proof: Assume p is true, and prove q.
- ***Indirect*** proof: Assume $\neg q$, and prove $\neg p$.
- ***Trivial*** proof: Prove q by itself.
- ***Vacuous*** proof: Prove $\neg p$ by itself.
- Proof by ***contradiction***: Assume $\neg p$, Prove $\neg p \rightarrow (q \wedge \neg q)$.
- Proof by ***cases:*** $(a \vee b) \rightarrow q$, *prove* $(a \rightarrow q) \wedge (b \rightarrow q)$.
- ***Exhaustive*** Proof: Exhaust all instances.

Direct proof

- **Method: Assume *p* is true, and prove *q*.**
  - assumes the hypotheses are true
  - uses the rules of inference, axioms and any logical equivalences to establish the truth of the conclusion.

- **Example:**
  - Theorem: *If 6x + 9y = 101, then x or y is not an integer.*
- **Proof:** (*Direct*)
  - Assume 6x + 9y = 101 is true.
  - Then from the rules of algebra 3(2x + 3y) = 101.
  - But 101/3 is not an integer so it must be the case that one of 2x or 3y is not an integer (maybe both).
  - Therefore, one of x or y must not be an integer.

非形式化证明

- Q.E.D.

Indirect proof

- **Method:**
- **A direct proof of the contrapositive（逆反式）**
  - assumes the conclusion of $P \rightarrow Q$ is false ($\sim Q$ is true)
  - uses the rules of inference, axioms and any logical equivalences to establish the premise P is false.
  - Note, in order to show that a conjunction of hypotheses is false is suffices to show just one of the hypotheses is false.

$$P_1 \wedge P_2 \wedge \ldots \wedge P_k \rightarrow Q$$
$$\Leftrightarrow \neg Q \rightarrow \neg(P_1 \wedge P_2 \wedge \ldots \wedge P_k)$$
$$\Leftrightarrow \neg Q \rightarrow (\neg P_1 \vee \neg P_2 \vee \ldots \neg \vee P_k)$$

Indirect proof

- **Example:**
  - A *perfect number* is one which is the sum of all its divisors except itself.
  - For example, 6 is perfect since 1 + 2 + 3 = 6. So is 28， 496.
- **Theorem:**
  - *A perfect number is not a prime.*
- **Proof**: (*Indirect*).
  - We assume the number *p* is a prime and show it is not perfect.
  - But the only divisors of a prime are 1 and itself.
  - Hence the sum of the divisors less than *p* is 1 which is not equal to *p*.
  - Hence *p* cannot be perfect.
  - Q.E.D.

Trivial proof (平凡证明)

- **Method: If we know *Q* is true then $P \rightarrow Q$ is true.**

  If it's raining today then the void set is a subset of every set.

  - The assertion is *trivially* true independent of the truth of *P*.

- **Example:**
  - **Theorem:** (For integers *n*) If *n* is the sum of two prime numbers, then either *n* is odd or *n* is even.
  - **Proof:** *Any* integer *n* is either odd or even. So the conclusion of the implication is true regardless of the truth of the antecedent. Thus the implication is true trivially.

Vacuous proof (空证明)

- **Method:**
- If we know one of the hypotheses in P is false then $P \rightarrow Q$ is *vacuously true*.

  If I am both rich and poor then hurricane Fran was a mild breeze.
- This is of the form $(P \wedge \sim P) \rightarrow Q$
  - and the hypotheses form a contradiction.
  - Hence Q follows from the hypotheses vacuously.
- **Example:**
  - **Theorem:** (For all n) If n is both odd and even, then $n^2 = n + n$.
  - **Proof:** The statement "n is both odd and even" is necessarily false, since no number can be both odd and even. So, the theorem is vacuously true.

Proof by contradiction(矛盾)

- **Method:**
- To prove that a statement P is true
  - assumes the statement P is false
  - derives a contradiction, usually of the form $Q \wedge \sim Q$ which establishes $\sim P \rightarrow (Q \wedge \sim Q)$
  - from which it follows that P must be true.

Contrast: The contrapositive proof:

To proof $P \rightarrow Q$, construct and proof $\sim Q \rightarrow \sim P$.

Proof by contradiction(矛盾)

- **Example**
- **Theorem:** *There is no largest prime number*.
  - We assume the conclusion 'there is no largest prime number' is false.
  - There is a largest prime number. Call it p.
  - Hence, the set of all primes lie between 1 and p.
  - Form the product of these primes:

    $r = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot p$.
  - Let $n = r+1$, n is a prime or n has a prime factor $q > p$. (Why?).
  - Thus, there is a prime which is larger than p.

    This contradicts the assumption that there is a largest prime.

Q.E.D.

Proof by Cases

- Break the premise of $P \rightarrow Q$ into an equivalent disjunction of the form

  $P_1 \vee P_2 \vee ... \vee P_n$

- Then use the logical equivalence

  $(P_1 \vee P_2 \vee ... \vee P_n) \rightarrow Q \Leftrightarrow (P_1 \rightarrow Q) \wedge (P_2 \rightarrow Q) \wedge ... \wedge (P_n \rightarrow Q)$

  Each of the implications $P_i \rightarrow Q$ is a *case*.

- You must
  - Convince the reader that the cases are inclusive, i.e., they exhaust all possibilities
  - establish all implications

Proof by Cases

- **Example:**
- Let $\otimes$ be the operation 'max' on the set of integers:

  if $a \geq b$ then $a \otimes b = \max\{a, b\} = a = b \otimes a$.
- **Theorem:**
  - *The operation $\otimes$ is associative.*
  - For all a, b, c

    $$(a \otimes b) \otimes c = a \otimes (b \otimes c).$$

Proof by Cases

- **Solution:**
  - Let a, b, c be arbitrary integers.
  - Then one of the following 6 cases must hold (are exhaustive):
    1. $a \geq b \geq c$
    2. $a \geq c \geq b$
    3. $b \geq a \geq c$
    4. $b \geq c \geq a$
    5. $c \geq a \geq b$
    6. $c \geq b \geq a$
  - Case 1: $a \otimes b = a$, $a \otimes c = a$, and $b \otimes c = b$.
  - Hence $(a \otimes b) \otimes c = a = a \otimes (b \otimes c)$.
  - Therefore the equality holds for the first case. …

Proof by Cases

- **Example:**
  - **Theorem:** $\forall n \in \mathbf{Z}\ \neg(2|n \vee 3|n) \rightarrow 24|(n^2-1)$
  - **Proof:**
    - Since $2 \cdot 3=6$, the value of $n \bmod 6$ is sufficient to tell us whether $2|n$ or $3|n$.
    - If $(n \bmod 6) \in \{0,3\}$ then $3|n$; if it is in $\{0,2,4\}$ then $2|n$. Thus $(n \bmod 6) \in \{1,5\}$.
      - **Case #1:** If $n \bmod 6 = 1$, then $(\exists k)\ n=6k+1$. $n^2=36k^2+12k+1$, so $n^2-1=36k^2+12k = 12(3k+1)k$. Note $2|(3k+1)k$ since either k or $3k+1$ is even. Thus $24|(n^2-1)$.
      - **Case #2:** If $n \bmod 6 = 5$, then $n=6k+5$. $n^2-1 = (n-1)\cdot(n+1) = (6k+4)\cdot(6k+6) = 12\cdot(3k+2)\cdot(k+1)$. Either $k+1$ or $3k+2$ is even. Thus, $24|(n^2-1)$.

Common errors

- **Example 9：** What is wrong with this "proof?"
  - **Theorem:** If x is a real number, then x^2 is a positive real number.
  - **Proof：**
    - Let p1 be "x is positive," let p2 be "x is negative," and let q be "x^2 is positive."
    - To show that p1 → q is true, note that when x is positive, x^2 is positive because it is the product of two positive numbers, x and x.
    - To show that p2 → q, note that when x is negative, x^2 is positive because it is the product of two negative numbers, x and x.
    - This completes the proof.
- **Note:** The problem with this "proof" is that we missed the case of x = 0. When x = 0, $x^2 = 0$ is not positive, so the supposed theorem is false.
- If p is "x is a real number," then we can prove results where p is the hypothesis with three cases, p1, p2, and p3, where p1 is "x is positive," p2 is "x is negative," and p3 is "x = 0" because of the equivalence p ↔ p1 ∨ p2 ∨ p3.

Exhaustive Proof

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

Exhaustive Proof

- **Solution: a proof by exhaustion.**
  - Look at all perfect powers not exceeding 100 and checking whether the next largest integer is also a perfect power.
  - The squares of positive integers: 1, 4, 9, 16, 25, 36, 49, 64, 81, and 100.
  - The cubes of positive integers: 1, 8, 27, and 64.
  - The fourth powers of positive integers: 1, 16, and 81.
  - The fifth powers of positive integers : 1 and 32.
  - The sixth powers of positive integers: 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.

Proof by Examples?

- **Remember:** A universal statement can never be proven by using examples, unless the universe can be validly reduced to only finitely many examples, and your proof covers all of them!
- **Theorem:**
  - $\neg\exists x,y\in\mathbf{Z}: x^2+3y^2 = 8$.
- **Proof:**
  - If $|x|\geq 3$ or $|y|\geq 2$ then $x^2+3y^2 > 8$.
  - This leaves $x^2\in\{0,1,4\}$ and $3y^2\in\{0,3\}$.
  - The largest pair sum to $4+3 = 7 < 8$.

Without Loss of generality

- **Example 7**
  - Show that if x and y are integers and both xy and $x + y$ are even, then both x and y are even.
  - proof by contraposition, the notion of without loss of generality, and proof by cases.
    - 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, to show that xy is odd or $x + y$ is odd.

Without Loss of generality

- **Solution**
  - *Case 1*: y is even.
    - $y = 2n$ for some integer n
    - $x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd.
  - *Case 2*: y is odd.
    - $y = 2n + 1$ for some integer n
    - $x \cdot y = (2m + 1)(2n + 1) = 2(2m \cdot n + m + n) + 1$ is odd.
  - We only cover the case where x is odd because the case where y is odd is similar. The use phrase *without loss of generality* (WLOG) indicates this.

Proof Methods for Existence

- We wish to establish the truth of

  $$\exists x P(x).$$

- ***Constructive*** existence proof:
  - Establish $P(c)$ is true for some c in the universe.
  - Then $\exists x P(x)$ is true by ***Existential Generalization (EG).***
- ***Nonconstructive*** existence proof:
  - Assume no c exists which makes P(c) true and then derive a contradiction.

Constructive Existence Proof

- **Theorem:**
  - *There exists an integer solution to the equation*
    - $x^2 + y^2 = z^2$.
- **Proof:**
  - Choose $x = 3$, $y = 4$, $z = 5$.

- **Example 10:** Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways:
- **Proof:**

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

Constructive Existence Proof

- **Theorem:** For any integer $n>0$, there exists a sequence of n consecutive composite integers.
  - Same statement in predicate logic:
    $\forall n>0\ \exists x\ \forall i\ (1\le i\le n)\rightarrow(x+i \text{ is composite})$

- **Proof:**
  - Given $n>0$, let $x = (n + 1)! + 1$.
  - Let $1\le i \le n$, and consider $x+i$.
  - Note $x+i = (n+1)! + (i+1)$.
  - Note $(i+1)|(i+1)$.
  - Also $(i+1)|(n+1)!$, since $2 \le i+1 \le n+1$.
  - So, $(i+1)|(x+i)$.
  - $\therefore$ $x+i$ is composite. $\therefore$ $\forall n\ \exists x\ \forall 1\le i\le n : x+i$ is composite.

Q.E.D.

Nonconstructive existence proof

- **Method:** Assume no c exists which makes $P(c)$ true and then derive a contradiction.
- **Theorem:** There are infinitely many prime numbers.
  - Any finite set of numbers must contain a maximal element, so we can prove the theorem if we can just show that there is no *largest* prime number.
  - *I.e.*, proof that for any prime number, there is a larger number that is *also* prime.
  - More generally: For *any* number, ∃ a larger prime.
  - Formally: Show $\forall n\ \exists p > n : p$ **is prime**.

Nonconstructive existence proof

- **Proof：using *proof by cases***
  - $\forall n>0$, prove there is a prime $p>n$.
  - Consider $x = n!+1$. Since $x>1$, we know that (x is prime)$\vee$(x is composite).
  - **Case 1:** Suppose x is prime. Obviously $x>n$, so let $p=x$ and we're done.
  - **Case 2:** Suppose x is a composite and has a prime factor p. But if $p\leq n$, then $p \bmod x = 1$, So $p>n$, and we're done.

Nonconstructive Existence Proof

- **Example 11:**

  Show that there exist irrational numbers x and y such that x^y is rational.

- **Proof:**
  - We know that $\sqrt{2}$ irrational.
  - Consider the number $\sqrt{2}^{\sqrt{2}}$.
    - If it is rational, $x = \sqrt{2}$ and $y = \sqrt{2}$
    - If it is irrational, $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$,

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

Refer to Example 11/p90

Nonconstructive Existence Proof

- **Example 12：** 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/or 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?

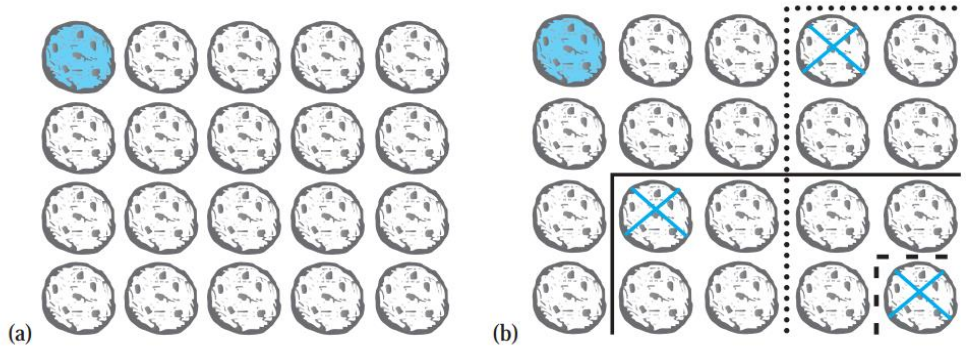


FIGURE 1 (a) Chomp (Top Left Cookie Poisoned). (b) Three Possible Moves.

Nonconstructive Existence Proof

- **Solution:**
  - We will give a nonconstructive existence proof of a winning strategy for the first player.(That is, we will show that the first player always has a winning strategy without explicitly describing the moves this player must follow)
  - 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

Proof Methods for Uniqueness

- **Method:** $\exists x(P(x) \wedge \forall y(y \neq x \rightarrow \neg P(y)))$

  $\exists x(P(x) \wedge \forall y(P(y) \rightarrow y = x))$

- **Example13:** Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.
- **Solution:**
  - **Existence:**
    The real number $r = -b/a$ is a solution of $ar + b = 0$
    because $a(-b/a) + b = -b + b = 0$.
  - **Uniqueness:**
    Suppose that s is a real number such that $as + b = 0$.
    Then $ar + b = as + b$, where $r = -b/a$.
    Subtracting b from both sides and dividing by a shows that
    $r = s$.

Proof Methods for Nonexistence

- **Nonexistence Proof: $\sim\exists x P(x)$**
  - We wish to establish the truth of $\sim\exists x P(x)$ (which is equivalent to $\forall x \sim P(x)$).
  - Use a proof by contradiction by assuming there is a c which makes $P(c)$ true.

- **Example:**
- **Theorem: there is not a largest prime**
- **Proof:**
  - Assume there is a largest prime p.

Universally Quantified Assertions

- **Method:**
  - We wish to establish the truth of $\forall x P(x)$.
  - We assume that x is an arbitrary member of the universe and show P(x) must be true.
  - Using UG it follows that $\forall x P(x)$.

- **Example:**
- **Theorem:** *For the universe of integers, x is even iff x^2 is even.*
- **Proof:**
  - The quantified assertion is $\forall x[x \text{ is even} \leftrightarrow x^2 \text{ is even}]$
  - Assume *x* is arbitrary.
  - Recall that $P \leftrightarrow Q$ is equivalent to $(P \rightarrow Q) \wedge (Q \rightarrow P)$.

Universally Quantified Assertions

- ***only if part*** **($P \rightarrow Q$).** Show if x is even then x^2 is even using a direct proof.
  - If x is even then $x = 2k$ for some integer k.
  - Hence, $x^2 = 4k^2 = 2(2k^2)$ which is even since it is an integer which is divisible by 2.
  - This completes the proof of case 1.
- ***if part*** **($Q \rightarrow P$).** Show if x^2 is even then x is even using an indirect proof .
  - Assume x is not even and show x^2 is not even.
  - If x is not even then it must be odd. So, $x = 2k + 1$ for some k.
  - Then $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd.
  - This completes the proof of the second case.

- Therefore we have shown x is even iff x^2 is even.
- Since x was arbitrary, the result follows by UG.

Q.E.D.

Universally Quantified Assertions

- **Proof by Counter example (反例)**
- **Universally Quantified Proof: ~∀*xP*(*x*)**
  - Recall that ~∀*xP*(*x*) ⇔ ∃*x*~*P*(*x*) .
  - To establish that ~∀*xP*(*x*) is true (or ∀*xP*(*x*) is false), construct a *c* such that ~*P(c)* is true or *P(c)* is false.
  - In this case *c* is called a ***counterexample*** to the assertion ∀*xP*(*x*)
- **Example:**
  - show "Every positive integer is the sum of the squares of two integers" is false. **~∀*xP*(*x*)**
  - ***counterexample*** **：3**

Fallacies (谬论) - incorrect inferences

- **The Fallacy of Affirming the Consequent**
  - *If the butler did it he has blood on his hands.*
  - *The butler had blood on his hands.*
  - *Therefore, the butler did it.*

- **This argument has the form**
  - $P \rightarrow Q$
  - Q
  - $\therefore P$

  or

$$[(P \rightarrow Q) \wedge Q] \rightarrow P$$

Fallacies (谬论) - incorrect inferences

- **The Fallacy of Denying the Antecedent**
  - *If the butler is nervous, he did it.*
  - *The butler is really mellow.*
  - *Therefore, the butler didn't do it.*

- **This argument has the form**
  - $P \rightarrow Q$
  - $\sim P$
  - $\therefore \sim Q$

  or

$$[(P \rightarrow Q) \wedge \sim P] \rightarrow \sim Q$$

What is wrong with this?

- **Example 16:**
- **Proof: 1=2** （***where a and b are two equal positive integers***）

Step	Reason
1. $a = b$	Premise
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

- **What's Wrong?**
  - Step 5. *a - b = 0* by the premise and division by 0 is undefined.

What is wrong with this?

- **Example 17:**
- **Theorem:** If n^2 is positive, then n is positive.
- **Attempted Proof:**
  - Let *P(n)* be "n is positive" and *Q(n)* be "n^2 is positive."
  - Hypothesis is *Q(n)* and the statement "If n is positive, then n^2 is positive" is the statement: $\forall n(P(n) \rightarrow Q(n))$.
  - Because $\forall n(P(n) \rightarrow Q(n))$ is true, and *Q(n)* is true, we can conclude that n is positive.
- **What's Wrong?**
  - From the hypothesis *Q(n)* and the statement $\forall n(P(n) \rightarrow Q(n))$ we cannot conclude P(n), because we are not using a valid rule of inference.
  - A counterexample : $n = -1$ for which $n^2 = 1$ is positive, but n is negative.

What is wrong with this?

- **Example 18:**
- **Theorem:** If n is not positive, then n^2 is not positive. (This is the contrapositive of the "theorem" in Example 17.)
- **Attempted Proof:**
  - Let $P(n)$ be "n is positive" and $Q(n)$ be "n^2 is positive."
  - Hypothesis is $\neg P(n)$, and the statement "If n is positive, then n^2 is positive" is the statement $\forall n(P(n) \rightarrow Q(n))$.
  - Because $\forall n(P(n) \rightarrow Q(n))$ is true, and $\neg P(n)$ is true, we can conclude that n^2 is not positive.
- **What's Wrong?**
  - From the hypothesis $\neg P(n)$ and the statement $\forall n(P(n) \rightarrow Q(n))$ we cannot conclude $\neg Q(n)$,because we are not using a valid rule of inference.
  - A counterexample : $n = -1$ for which $n^2 = 1$ is positive.

Fallacies :Circular Reasoning

- **Method:**
  - The fallacy of (explicitly or implicitly) assuming the very statement you are trying to prove in the course of its proof.
- **Example 19:**
  - Prove that an integer n is even, if n^2 is even.
  - **Attempted proof:**
    - Assume n^2 is even. Then $n^2=2k$ for some integer k.
    - Dividing both sides by n gives $n = (2k)/n = 2(k/n)$.
    - So there is an integer $j = k/n$ such that $n=2j$. Therefore n is even."
  - **Circular reasoning is used in this proof. Where?**

*Begs the question: How do you show that $j=k/n=n/2$ is an integer, without **first** assuming that n is even?*

Fallacies :Circular Reasoning

- **A correct proof:**
  - We know that *n* must be either odd or even.
  - If n were odd, then n^2 would be odd, since an odd number times an odd number is always an odd number.
  - Since n^2 is even, it is not.
  - Thus, by modus tollens, *n* is not odd either.
  - Thus, by disjunctive syllogism, *n* must be even.

This proof is correct, but not quite complete,
since we used several lemmas without proving them.
Can you identify what they are?

A More Verbose Version

Uses some number theory we haven't defined yet.

- Suppose n^2 is even (premise)
- $\therefore 2|n^2 \ \therefore \ n^2 \bmod 2 = 0$. Of course $n \bmod 2$ is either 0 or 1.
- If it's 1, then $n \equiv 1 \pmod 2$, so $n^2 \equiv 1 \pmod 2$, using the theorem that if $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then $ac \equiv bd \pmod m$, with $a=c=n$ and $b=d=1$.
- Now $n^2 \equiv 1 \pmod 2$ implies that $n^2 \bmod 2 = 1$. By the hypothetical syllogism rule, ($n \bmod 2 = 1$) implies ($n^2 \bmod 2 = 1$).
- Since we know $n^2 \bmod 2 = 0 \neq 1$, by *modus tollens* we know that $n \bmod 2 \neq 1$.
- So by disjunctive syllogism we have $n \bmod 2 = 0 \ \therefore 2|n \ \therefore \ n$ is even.

Dear students

- *Learning how to construct proofs is probably one of the most **difficult** things you will face in life.*
- *Few of us are gifted enough to do it with ease. One only learns how to do it by **practicing.***

Proof strategy Overview

- **we already saw:**
  - Several types of proofs of implications $p \rightarrow q$:
    - Direct, Indirect, Vacuous, Trivial, Proof by cases…
  - Types of existence proofs:
    - Constructive vs. Nonconstructive.
  - Some methods of proving general statements p:
    - proof by contradiction.
- **In this section, we will show examples of:**
  - Forward vs. backward reasoning.
  - Adapting existing proofs.
  - Turning conjectures into proofs.

Forward Reasoning

- **Have premises *p*, and want to prove *q*.**
  - Find a s_1 such that $p \rightarrow s_1$
    - Then, modus ponens gives you s_1.
  - Then, find an s_2 (such that) $s_1 \rightarrow s_2$.
    - Then, modus ponens gives you s_2.
  - And hope to eventually get to an s_n , $s_n \rightarrow q$.

- **The problem with this method is…**
  - It can be tough to see the path looking from *p*.

Backward Reasoning

- **It can often be easier to see the *very same path* if you just start looking from the conclusion *q* instead…**
  - That is, *first* find an s_n such that $s_n \rightarrow q$.
  - *Then*, find an s_{n-1} , $s_{n-1} \rightarrow s_n$, and so on…
  - Working back to an s_1 , $p \rightarrow s_1$.
- Note we *still* are using ***modus ponens*** to propagate truth *forwards* down the chain from p to s_{-n} to … to s_{-1} to q!
  - We are *finding* the chain *backwards*, but *applying* it *forwards*.
  - This is not quite the same thing as an indirect proof…
    - In that, we would use *modus tollens* and $\neg q$ to prove $\neg s_{-1}$, *etc.*
  - However, it is similar.

Backward Reasoning

- **Example 14:**
- **Theorem:**

  $\forall a>0, b>0, a\neq b: (a+b)/2 > (ab)^{1/2}$.

- **Proof:**
  - Notice it is not obvious how to go from the premises $a>0$, $b>0$, $a\neq b$ directly forward to the conclusion $(a+b)/2 > (ab)^{1/2}$.
  - So, let's work ***backwards*** from the conclusion, $(a+b)/2 > (ab)^{1/2}$

Backward Reasoning

- **Thinking:**
  - $(a+b)/2 > (ab)^{1/2} \Leftrightarrow$ (squaring both sides)
    - This preserves the "$>$" since both sides are positive.
  - $(a+b)^2/4 > ab \Leftrightarrow$ (multiplying through by 4)
  - $(a+b)^2 > 4ab \Leftrightarrow$ (squaring $a+b$)
  - $a^2+2ab+b^2 > 4ab \Leftrightarrow$ (subtracting out $4ab$)
  - $a^2-2ab+b^2 > 0 \Leftrightarrow$ (factoring left side)
  - $(a-b)^2 > 0$
  - Now, since $a \neq b$, $(a-b) \neq 0$, thus $(a-b)^2 > 0$, and we can work our way back along the chain of steps…

Backward Reasoning

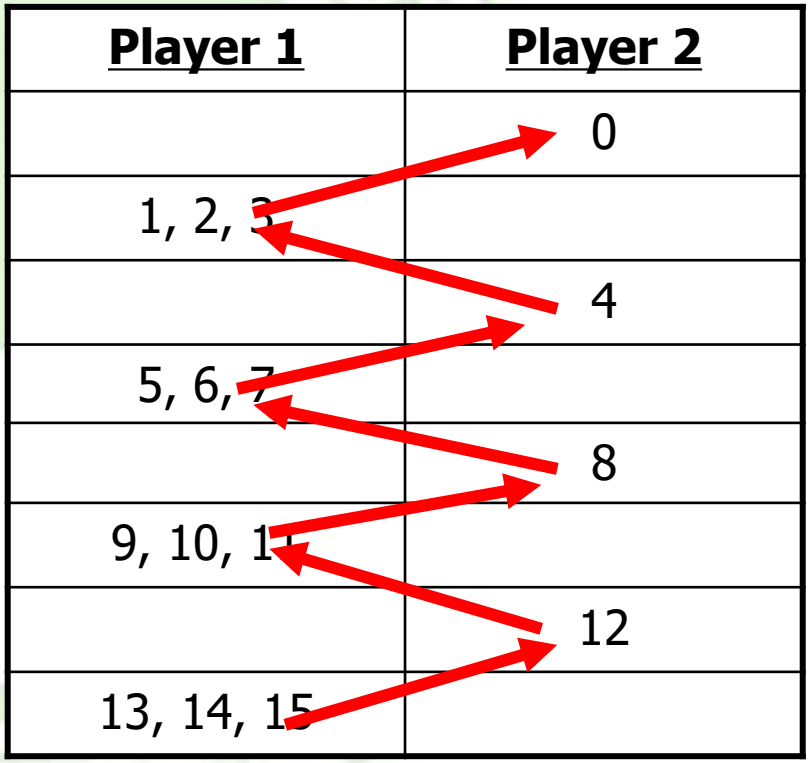
- **Theorem:** $\forall a>0, b>0, a\neq b: (a+b)/2 > (ab)^{1/2}$.
- **Proof.**
  - If Since $a\neq b$, $(a-b)\neq 0$. Thus, $(a-b)^2>0$, *i.e.*, $a^2-2ab+b^2 > 0$. Adding $4ab$ to both sides, $a^2+2ab+b^2 > 4ab$. Factoring the left side, we have $(a+b)^2 > 4ab$, so $(a+b)^2/4 > ab$. Since ab is positive, we can take the square root of both sides and get $(a+b)/2 > (ab)^{1/2}$.
  - This is just a simple proof proceeding directly from premises to conclusion, but if you don't realize how it was obtained, it looks "magical."
  - A common student reaction: "But how did you *know* to pick $4ab$ out of thin air, to add to both sides?"
  - Answer: ***By working backwards from the conclusion!***

Backward Reasoning--Stone Game Example

- **Example 15：Game rules:**
  - There are 15 stones in a pile.
  - Two players take turns removing either 1, 2, or 3 stones.
  - Whoever takes the last stone wins.
- **Theorem:** There is a strategy for the first player that guarantees him a win.
- **How do we prove this**? Constructive proof…
  - Looks complicated… How do we pick out the winning strategy from among all possible strategies?
  - Work backwards from the endgame!

Backward Reasoning--Stone Game Example

- **Working Backwards in the Game**
  - Player 1 wins if it is player 2's turn and there are no stones…
  - P1 can arrange this if it is his turn, and there are 1, 2, or 3 stones…
  - This will be true as long as player 2 had 4 stones on his turn…
  - And so on…

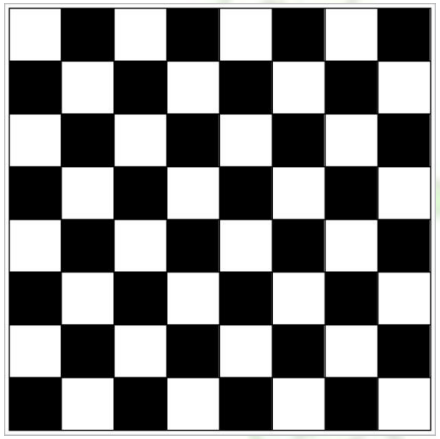


Backward Reasoning--Stone Game Example

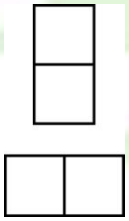
- **Forwardized version**
- **Theorem.** Whoever moves first can always force a win.
- **Proof.**
  - Player 1 can remove 3 stones, leaving 12.
  - After player 2 moves, there will then be either 11, 10, or 9 stones left. In any of these cases, player 1 can then reduce the number of stones to 8.
  - Then, player 2 will reduce the number to 7, 6, or 5. Then, player 1 can reduce the number to 4.
  - Then, player 2 must reduce them to 3, 2, or 1. Player 1 then removes the remaining stones and wins.

Proof and Disproof: Tilings

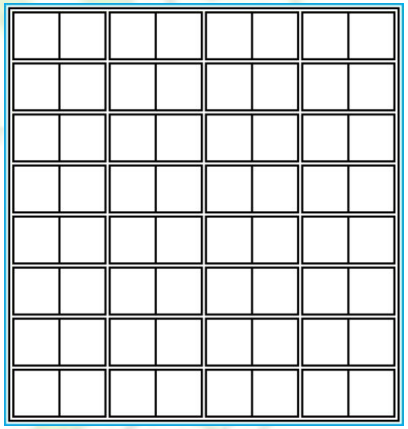
- **Example 1:** Can we tile the standard checkerboard using dominos?
- **Solution:** Yes! One example provides a constructive existence proof.



The Standard Checkerboard



Two Dominoes



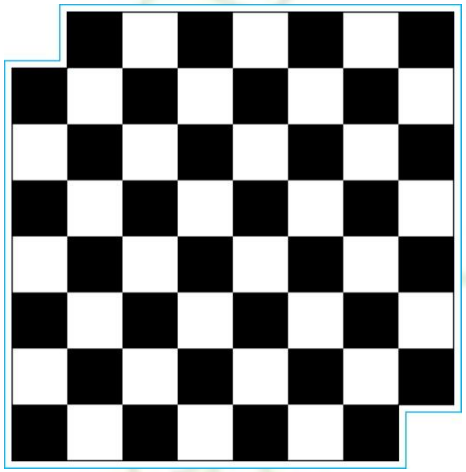
One Possible Solution

Proof and Disproof: Tilings

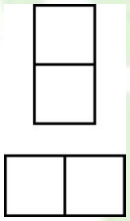
- **Example 2:** Can we tile a checkerboard obtained by removing one of the four corner squares of a standard checkerboard?
- **Solution:**
  - Our checkerboard has $64 - 1 = 63$ squares.
  - Since each domino has two squares, a board with a tiling must have an even number of squares.
  - The number 63 is not even.
  - We have a contradiction.

Proof and Disproof: Tilings

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



Nonstandard Checkerboard



Dominoes

Proof and Disproof: Tilings

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

Even Great Mathematicians Can Propose False Conjectures!

- Euler conjectured that for $n>2$, the sum of $n-1$ n^{th} powers of positive integers is not an n^{th} power.
  - Remained true for all cases checked for 200 years, but no proof was found.
- Finally, in 1966, someone noticed that
  $$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$
  - More counter-examples have also been found for n=4 (1988), n=7 (1999) and n=8 (2000).

Fermat's "Last Theorem"

- **Theorem:**
- $x^n+y^n=z^n$ has no solutions in integers $xyz \neq 0$ with integer $n>2$.
  - In the 1600s, Fermat famously claimed in a marginal note that he had a "wondrous proof" of the theorem.
    - But unfortunately, if he had one, he never published it!
  - The theorem remained a publicly unproven conjecture for the next ~400 years!
  - Finally, a proof that requires hundreds of pages of advanced mathematics was found by Wiles at Princeton in 1990.
    - It took him 10 years of work to find it!
- **Challenge:**
  - Find a *short*, *simple* proof of Fermat's last theorem, and you will become instantly famous!

Some Open Conjectures

- **Conjecture:** (The Hailstone Problem)
  - If $h(x) = x/2$ when x is even, and $3x+1$ when x is odd, then $\forall x \in \mathbf{N}$ $\exists n \in \mathbf{N}$ $h^n(x) = 1$ (where the superscript denotes composition of h with itself n times).
- **For example:**
  - starting with x = 13,
  - h(13) = 3·13 + 1 = 40, h(40) = 40/2 = 20, h(20) = 20/2 = 10,
  - h(10) = 10/2 = 5, h(5) = 3·5 + 1 = 16,h(16) = 16/2 = 8,
  - h(8) = 8/2 = 4, h(4) = 4/2 = 2, h(2) = 2/2 = 1

The conjecture has been verified using computers up to $5.6 \cdot 10^{13}$.

Prove any of these, and you can probably have a lifetime career sitting around doing pure mathematics…

Additional Proof Methods

- **Later we will see many other proof methods:**
  - 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.
  - Structural induction, which can be used to prove such results about recursively defined sets.
  - Cantor diagonalization is used to prove results about the size of infinite sets.
  - Combinatorial proofs use counting arguments.

Homework

- **§ 1.7**
  - 8(Perfect square), 20, 30
- **§ 1.8**
  - 14, 16, 32, 40