CSE2023 Discrete Computational Structures

Lecture 7

Common mistakes in exhaustive proof and proof by cases

- Draw incorrect conclusions from insufficient number of examples
- Need to cover every possible case in order to prove a theorem
- Proving a theorem is analogous to showing a program always produces the desired output
- No matter how many input values are tested, unless all input values are tested, we cannot conclude that the program always produces correct output

Example

- Is it true that every positive integer is the sum of 18 4^{th} powers of integers?
- The 4^{th} powers of integers: 0, 1, 16, 81, …
- Select 18 terms from these numbers and add up to n, then n is the sum of 18 4^{th} powers
- Can show that integers up to 78 can be written as the sum as such
- However, if we decided this is enough (or stop earlier), then we come to wrong conclusion as 79 cannot be written this way

Example

- What is wrong with this “proof”

  “Theorem”: If x is a real number, then x^2 is a positive real number

  “Proof”: Let p_1 be “x is positive” and p_2 be “x is negative”, and q be “x^2 is positive”.

  First show $p_1 \rightarrow q$, and then $p_2 \rightarrow q$. As we cover all possible cases of x, we complete this proof

Example

- We missed the case x=0
- When x=0, the supposed theorem is false
- If p is "x is a real number", then we need to prove results with p_1, p_2, p_3 (where p_3 is the case that x=0)

$$((p_1 \vee p_2 \vee p_3) \rightarrow q) \leftrightarrow ((p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge (p_3 \rightarrow q))$$

8

Existence proof

- A proof of a proposition of the form $\exists x p(x)$
- Constructive proof: find one element a such that p(a) is true
- Non-constructive proof: prove that $\exists x p(x)$ is true in some other way, usually using proof by contradiction

9

Constructive existence proof

- Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways
- By intuition or computation, we find that $1729=10^3+9^3=12^3+1^3$
- We prove this theorem as we show one positive integer can be written as the sum of cubes in two different ways

10

Non-constructive existence proof

- Show that there exist irrational numbers x and y such that x^y is rational
- We previously show that $\sqrt{2}$ is irrational
- Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, we have two irrational number x and y with x^y is rational (x=$\sqrt{2}$, y=$\sqrt{2}$)
- On the other hand if $\sqrt{2}^{\sqrt{2}}$ is not rational, then we let $x=\sqrt{2}^{\sqrt{2}}, y=\sqrt{2}$, and thus $x^y=(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}=\sqrt{2}^{\sqrt{2}\sqrt{2}}=\sqrt{2}^2=2$
- We have not found irrational numbers x and y such that x^y is rational
- Rather we show 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!

11

Uniqueness proof

- Some theorems assert the existence of a unique element with a particular property
- Need to show
  - Existence: show that an element x with the desired property exists
  - Uniqueness: show that if y≠x, then y does not have the desired property
- Equivalently, show that if x and y both have the desired property, then x=y
- Showing that there is a unique element x such that p(x) is the same as proving the statement

$$\exists x(p(x) \wedge \forall y((y \neq x) \rightarrow \neg p(y)))$$

12

Example

- Show that if a and b are real numbers and a≠0, then there is a unique number r such that ar+b=0
- Note that the real number r=-b/a is a solution of ar+b=0. Consequently a real number r exists for which ar+b=0
- Second, suppose that s is a real number such that as+b=0. Then ar+b=as+b. Since a≠0, s must be equal to r. This means if s≠r, as+b≠0

13

Proof strategy

- Can be challenging
- First analyze what the hypotheses and conclusion mean
- For conditional statements, usually start with direct proof, then indirect proof, and then proof by contradiction

14

Forward/backward reasoning

- Direct proof:
  - start with premises, together with axioms and known theorems,
  - we can construct a proof using a sequence of steps that lead to conclusion
- A type of forward reasoning
- Backward reasoning: to prove q, we find a stement p that we can prove that p→q

15

Example

- For two distinct positive real numbers x, y, their arithmetic mean is (x+y)/2, and their geometric mean is $\sqrt{xy}$. Show that the arithmetic mean is always larger than geometric mean
- To show $(x+y)/2>\sqrt{xy}$, we can work backward by finding equivalent statements

$$(x+y)/2>\sqrt{xy}$$
$$(x+y)^2/4>xy$$
$$x^2+2xy+y^2>4xy$$
$$(x-y)^2>0$$

16

Example

- For two distinct real positive real numbers, x and y, $(x-y)^2>0$
- Thus, $x^2-2xy+y^2>0$, $x^2+2xy+y^2>4xy$, $(x+y)^2>4xy$. So, $(x+y)/2>\sqrt{xy}$
- We conclude that if x and y are distinct positive real numbers, then their arithmetic mean is greater than their geometric mean

17

Example

- 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.
- Show that the first player can win the game no matter what the second play does

18

Example

- At the last step, the first player can win if this player is left with a pile with 1, 2, or 3 stones
- The second player will be forced to leave 1, 2 or 3 stones if this player has to remove stones from a pile containing 4 stones
- The first player can leave 4 stones when there are 5, 6, or 7 stones left, which happens when the second player has to remove stones from a pile with 8 stones

19

Example

- That means, there are 9, 10 or 11 stones when the first player makes this move
- Similarly, the first player should leave 12 stones when this player makes the first move
- We can reverse this argument to show that the first player can always makes this move to win (successively leave 12, 8, and 4 stones for 2nd player)

Adapting existing proof

- Take advantage of existing proofs
- Borrow some ideas used in the existing proofs
- We proved $\sqrt{2}$ is irrational. We now conjecture that $\sqrt{3}$ is irrational. Can we adapt previous proof to show this?
- Mimic the steps in previous proof
- Suppose $\sqrt{3} = c/d$, then $3 = c^2/d^2, 3d^2 = c^2$
- Can we use this to show that 3 must be a factor of both c and d?

Example

- We will use some results from number theory (discussed in Chapter 3)
- As 3 is factor of c^2, it must be a factor of c Thus, 9 is a factor of c^2, which means 9 is a factor of $3d^2$
- Which implies 3 is a factor d^2, and 3 is factor of d
- This means 3 is factor of c and d, a contradiction

Looking for counterexamples

- When confronted with a conjecture, try to prove it first
- If the attempt is not successful, try to find a counterexample
- Process of finding counterexamples often provides insights into problems

Example

- We showed the statement "Every positive integer is the sum of two squares of integers" is false by finding a counterexample
- Is the statement "Every positive integer is the sum of the squares of three integers" true?
- Look for an counterexample: $1=0^2+0^2+1^2$, $2=0^2+1^2+1^2$, $3=1^2+1^2+1^2$, $4=0^2+0^2+2^2$, $5=0^2+1^2+2^2$, $6=1^2+1^2+2^2$, but cannot do so for 7

24

Example

- The next question is to ask whether every positive integer is the sum of the squares of 4 positive integers
- Some experiments provide evidence that the answer is yes, e.g., $7=1^2+1^2+1^2+2^2$, $25=4^2+2^2+2^2+1^2$, and $87=9^2+2^2+1^2+1^2$
- It turns the conjecture "Every positive integer is the sum of squares of four integers" is true

25

Proof strategy in action

- Formulate conjectures based on many types of possible evidence
- Examination of special cases can lead to a conjecture
- If possible, prove the conjecture
- If cannot find a proof, find a counterexample
- A few conjectures remain unproved
- Fermat's last theorem (a conjecture since 1637 until Andrew Wiles proved it in 1995)

$$\text{no three positive integers satisfy } a^n+b^n=c^n,\ n \text{ is any integer} > 2$$

26