CSE2023 Discrete Computational Structures

Lecture 5

1.7 Introduction to proofs

- **Proof**: valid argument that establishes the truth of a mathematical statement, e.g., theorem
- A proof can use hypotheses, axioms, and previously proven theorems
- Formal proofs: can be extremely long and difficult to follow
- Informal proofs: easier to understand and some of the steps may be skipped, or axioms are not explicitly stated

Some terminology

- **Theorem**: a mathematical statement that can be shown to be true
- **Proposition**: less important theorem
- **Axiom** (**postulate**): a statement that is assumed to be true
- **Lemma**: less important theorem that is helpful in the proof of other results
- **Corollary**: a theorem that can be established directly from a theorem that has been proved
- **Conjecture**: a statement proposed to be true, but not proven yet

Direct proofs of p→q

- First assume p is true
- Then show q must be true (using axioms, definitions, and previously proven theorems)
- So the combination of p is true and q is false never occurs
- Thus p→q is true
- Straightforward
- But sometimes tricky and require some insight

Example

- 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
  - Note that an integer is either even or odd
- Show “If n is an odd integer, then n^2 is odd”

Example

- Note the theorem states $\forall n(p(n) \to q(n))$
- By definition of odd integer, n=2k+1, where k is some integer
- $n^2=(2k+1)^2=4k^2+4k+1=2(2k^2+2k)+1$
- By definition of odd integer, we conclude n^2 is an odd integer
- Consequently, we prove that if n is an odd integer, then n^2 is odd

Example

- “If m and n are both perfect squares, then nm is also a perfect square (an integer a is a perfect square if there is an integer b such that $a=b^2$)
- By definition, there are integers s and t such that $m=s^2$, and $n=t^2$
- Thus, $mn=s^2t^2=(st)^2$ (using commutativity and associativity of multiplication)
- We conclude mn is also a perfect square

Proof by contraposition

- **Indirect proof**: sometimes direct proof leads to dead ends
- Based on $p \to q \equiv \neg q \to \neg p$
- Use $\neg q$ as hypothesis and show $\neg p$ must follow

Example

- Show that "if n is an integer and 3n+2 is odd, then n is odd"
- Use $p \to q \equiv \neg q \to \neg p$
- Proof by contraposition:
  - Assume n is even, i.e., n=2k, for some k
  - It follows 3n+2=3(2k)+2=6k+2=2(3k+1)
  - Thus 3n+2 is even

Example

- Prove that if n=ab, where a and b are positive integers, then $\boxed{a \leq \sqrt{n} \text{ or } b \leq \sqrt{n}}$

$$p \to q \equiv \neg q \to \neg p$$

$$\text{Assume } \neg(a \leq \sqrt{n} \vee b \leq \sqrt{n})$$
$$a > \sqrt{n} \wedge b > \sqrt{n}$$
$$ab > \sqrt{n} \cdot \sqrt{n} = n$$
$$ab \neq n$$

Vacuous proof

- Prove p→q is true
- **Vacuous proof**: If we show p is false and then claim a proof of p→q
  - However, often used to establish special case
- Show that p(0) is true when p(n) is "If **n>1**, then **n^2>n**" and the domain consists of all integers
- The fact $0^2>0$ is false is irrelevant to the truth value of the conditional statement

Trivial proof

- **Trivial proof**: a proof of p→q that uses the fact q is true
  - Often important when special cases are proved
- Let p(n) be "If a and b are positive integers with a≥b, then $a^n \geq b^n$ where the domain consists of all integers
- The proposition p(0) is "If a≥b, then $a^0 \geq b^0$". $a^0 \geq b^0$ is true, hence the conditional statement p(0) is true

Example

- Definition: the real number r is rational if there exist integers p and q with q≠0 such that r=p/q
- A real number that is not rational is irrational
- Prove that the sum of two rational numbers is rational (i.e., "For every real number r and every real number s, if r and s are rational numbers, then r+s is rational")
- Direct proof? Proof by contraposition?

Direct proof

- Let r=p/q and s=t/u where p, q, t, u, are integers and q≠0, and u≠0.
- r+s=p/q+t/u=(pu+qt)/qu
- Since q≠0 and u≠0, qu≠0
- Consequently, r+s is the ratio of two integers. Thus r+s is rational

Example

- Prove that if n is an integer and n^2 is odd, then n is odd
- Direct proof? Proof by contraposition?

$\mathrm{p}: n^2$ is odd

$\mathrm{q}: n$ is odd

Direct proof : Let $n^2 = 2k+1$, then $n = \sqrt{2k+1}$

Proof by contradiction : $n = 2k$, it follows that $n^2 = 4k^2 = 2(2k^2)$

Proof by contradiction

- Suppose we want to prove a statement p
- Further assume that we can find a **contradiction** q such that ┐p→q is true
- Since q is false, but ┐p→q is true, we can conclude ┐p is false, which means p is true
- The statement ┐r^r is **contradiction**, we can prove that p is true if we can show that ┐p→(┐r^r), i.e., if p is not true, then there is a contradiction

Example

- Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction
- Let p be the proposition "$\sqrt{2}$ is irrational"
- ┐p: $\sqrt{2}$ is rational, and thus $\sqrt{2}=a/b$ where a and b have no common factors
- Thus $2=a^2/b^2$, $2b^2=a^2$, and thus a^2 is even
- a^2 is even and so a is even (can easily show if n^2 is even, then n is even). Let a=2c for some integer c, $2b^2=a^2=4c^2$, and thus $b^2=2c^2$, and b^2 is even

Example

- Since b^2 is even, b must be even
- ┐p leads to $\sqrt{2}=a/b$ where and b have no common factors, and both a and b are even (and thus a common factor), a contradiction
- That is, the statement "$\sqrt{2}$ is irrational" is true

Proof by contradiction

- Can be used to prove conditional statements
- First assume the negation of the conclusion
- Then use premises and negation of conclusion to arrive a contradiction
- Reason: $p \to q \equiv ((p \wedge \neg q) \to F)$

Proof by contradiction

- Can rewrite a proof by contraposition of a conditional statement $p \to q$ as proof by contradiction
- Proof by contraposition: show if ┐q then ┐p
- Proof by contradiction: assume p and ┐q are both true
- Then use steps of $\neg q \to \neg p$ to show ┐p is true
- This leads to $\neg q \to p \wedge \neg p$, a contradiction

Example

- Proof by contradiction "If 3n+2 is odd, then n is odd"
- Let p be "3n+2 is odd" and q be "n is odd"
- To construct a proof by contradiction, assume both p and ┐q are both true
- Since n is even, let n=2k, then 3n+2=6k+2= 2(3k+1). So 3n+2 is even, i.e. ┐p,
- Both p and ┐p are true, so we have a contradiction

22

Example

- Note that we can also prove by contradiction that $p \rightarrow q$ is true by assuming that p and ┐q are both true, and show that q must be also true
- This implies q and ┐q are both true, a contradiction
- Can turn a direct proof into a proof by contradiction

23

Proof of equivalence

- To prove a theorem that is a biconditional statement $p \leftrightarrow q$, we show $p \rightarrow q$ and $q \rightarrow p$
- The validity is based on the tautology

  $(p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$

24

Example

- Prove the theorem "If n is a positive integer, then n is odd if and only if n^2 is odd"
- To prove "p if and only if q" where p is "n is odd" and q is "n^2 is odd"
- Need to show $p \rightarrow q$ and $q \rightarrow p$

  "If n is odd, then n^2 is odd", and "If n^2 is odd, then n is odd
- We have proved $p \rightarrow q$ and $q \rightarrow p$ in previous examples and thus prove this theorem with iff

25

Equivalent theorems

- $p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n$
- For i and j with $1 \le i \le n$ and $1 \le j \le n$, p_i and p_j are equivalent

  $[p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n] \leftrightarrow [(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \ldots \wedge (p_n \rightarrow p_1)]$
- More efficient than prove $p_i \rightarrow p_j$ for $i \neq j$ with $1 \le i \le n$ and $1 \le j \le n$
- Order is not important as long as we have chain

Example

- Show that these statements about integer n are equivalent
  - P_1: n is even
  - P_2: n-1 is odd
  - P_3: n^2 is even
- Show that by $p_1 \rightarrow p_2$ and $p_2 \rightarrow p_3$ and $p_3 \rightarrow p_1$
- $p_1 \rightarrow p_2$: (direct proof) Suppose n is even, then n=2k for some k. thus n-1=2k-1=2(k-1)+1 is odd

Example

- $p_2 \rightarrow p_3$: (direct proof) Suppose n-1 is odd, then n-1=2k+1 for some k. Hence n=2k+2, and $n^2=(2k+2)^2=4k^2+8k+4=2(2k^2+4k+2)$ is even
- $p_3 \rightarrow p_1$: (proof by contraposition) That is, we prove that if n is not even, then n^2 is not even. This is the same as proving if n is odd, then n^2 is odd (which we have done)

Counterexample

- To show that a statement $\forall x p(x)$ is false, all we need to do is to find a **counterexample**, i.e., an example x for which p(x) is false

Example

- Show that "Every positive integer is the sum of the squares of two integers" is false
- An counterexample is 3 as it cannot be written as the sum of the squares to two integers
- Note that the only perfect squares not exceeding 3 are $0^2=0$ and $1^2=1$
- Furthermore, there is no way to get 3 as the sum of two terms each of which is 0 or 1

Mistakes in proofs

- What is wrong with this proof "1=2"?
  1. a=b (given)
  2. $a^2=ab$ (multiply both sides of 1 by a)
  3. $a^2-b^2 = ab-b^2$ (subtract b^2 from both sides of 2)
  4. (a-b)(a+b)=b(a-b) (factor both sides of 3)
  5. a+b=b (divide both sides of 4 by a-b)
  6. 2b=b (replace a by b in 5 as a=b and simply)
  7. 2=1 (divide both sides of 6 by b)

Solution: Every step is valid except for one, step 5 where we divided both sides by $a-b$. The error is that $a-b$ equals zero; division of both sides of an equation by the same quantity is valid as long as this quantity is not zero. ◀

What is wrong with this proof?

- "Theorem": If n^2 is positive, then n is positive

  "Proof": Suppose n^2 is positive. As the statement "If n is positive, then n^2 is positive" is true, we conclude that n is positive
- p(n): If n is positive, q(n): n^2 is positive. The statement is $\forall n(p(n) \rightarrow q(n))$ and the hypothesis is q(n). From these, we cannot conclude p(n) as no valid rule of inference can be applied
- Counterexample: n=-1

What is wrong with this proof?

- "Theorem": If n^2 is positive, then n is positive

  "Proof": Suppose n^2 is positive. As the

Solution: Let $P(n)$ be "n is positive" and $Q(n)$ be "n^2 is positive." Then our hypothesis is $Q(n)$. The statement "If n is positive, then n^2 is positive" is the statement $\forall n(P(n) \rightarrow Q(n))$. 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. Instead, this is an example of the fallacy of affirming the conclusion. A counterexample is supplied by $n=-1$ for which $n^2=1$ is positive, but n is negative. ◀

is q(n). From these, we cannot conclude p(n) as no valid rule of inference can be applied
- Counterexample: n=-1

Circular reasoning

- Is the following argument correct?

  Suppose that n^2 is even, then $n^2=2k$ for some integer k. Let n=2y for some integer y. This shows that n is even
- Wrong argument as the statement "n=2y for some integer y" is used in the proof
- No argument shows n can be written as 2y
- Circular reasoning as this statement is equivalent to the statement being proved

35

Proofs

- Learn from mistakes
- Even professional mathematicians make mistakes in proofs
- Quite a few incorrect proofs of important results have fooled people for years before subtle errors were found
- Some other important proof techniques
  - Mathematical induction
  - Combinatorial proof

36