

BBM 205 Discrete Mathematics
Hacettepe University
<http://web.cs.hacettepe.edu.tr/~bbm205>

Lecture 2: Proof Techniques

Lecturer: Lale Özkahya

Resources:

Kenneth Rosen, “Discrete Mathematics and App.”
cs.colostate.edu/cs122/Spring15/home_resources.php
<http://www.cs.nthu.edu.tw/wkhon/math16.html>

Proof Terminology

Theorem: statement that can be shown to be true

Proof: a valid argument that establishes the truth of a theorem

Axioms: statements we assume to be true

Lemma: a less important theorem that is helpful in the proof of other results

Corollary: theorem that can be established directly from a theorem that has been proved

Conjecture: statement that is being *proposed* to be a true statement

Learning objectives

- Direct proofs
- Proof by contrapositive
- Proof by contradiction
- Proof by cases

Technique #1: Direct Proof

- Direct Proof:
 - First step is a premise
 - Subsequent steps use rules of inference or other premises
 - Last step proves the conclusion

Methods of Proving

- A **direct proof** of a conditional statement

$$p \rightarrow q$$

first **assumes that p is true**, and uses axioms, definitions, previously proved theorems, with rules of inference, **to show that q is also true**

- The above targets to show that the case where p is true and q is false never occurs
 - Thus, $p \rightarrow q$ is always true

Direct Proof (Example 1)

- Show that

if n is an odd integer, then n^2 is odd.

- Proof :

Assume that n is an odd integer. This implies that there is some integer k such that

$$n = 2k + 1.$$

Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Thus, n^2 is odd.

Direct Proof (Example 2)

- Show that

if m and n are both square numbers,
then mn is also a square number.

- Proof :

Assume that m and n are both squares. This implies that there are integers u and v such that

$$m = u^2 \quad \text{and} \quad n = v^2.$$

Then $mn = u^2 v^2 = (uv)^2$. Thus, mn is a square.

Class Exercise

- Prove: If n is an even integer, then n^2 is even.
 - If n is even, then $n = 2k$ for some integer k .
 - $n^2 = (2k)^2 = 4k^2$
 - Therefore, $n = 2(2k^2)$, which is even.

Can you do the formal version?

	Step	Reason
1.	n is even	Premise
2.	$\exists k \in \mathbf{Z} \ n = 2k$	Def of even integer in (1)
3.	$n^2 = (2k)^2$	Squaring (2)
4.	$= 4k^2$	Algebra on (3)
5.	$= 2(2k^2)$	Algebra on (4)
6.	$\therefore n^2$ is even	Def even int, from (5)

Technique #2:

Proof by Contrapositive

- A direct proof, but starting with the contrapositive equivalence:
 - $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- If you are asked to prove $p \rightarrow q$
- you instead prove $\neg q \rightarrow \neg p$
- Why? Sometimes, it may be easier to directly prove $\neg q \rightarrow \neg p$ than $p \rightarrow q$

Methods of Proving

- The **proof by contraposition** method makes use of the equivalence

$$p \rightarrow q \equiv \neg q \rightarrow \neg p$$

- To show that the conditional statement $p \rightarrow q$ is true, we first **assume $\neg q$ is true**, and use axioms, definitions, proved theorems, with rules of inference, **to show $\neg p$ is also true**

Proof by Contraposition (Example 1)

- Show that

if $3n + 2$ is an odd integer, then n is odd.

- Proof :

Assume that n is even. This implies that

$$n = 2k \text{ for some integer } k.$$

Then, $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$,
so that $3n + 2$ is even. Since the negation of
conclusion implies the negation of hypothesis,
the original conditional statement is true

Proof by Contraposition (Example 2)

- Show that

if $n = a b$, where a and b are positive,
then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

- Proof :

Assume that both a and b are larger than \sqrt{n} .
Thus, $a b > n$ so that $n \neq a b$. Since the
negation of conclusion implies the negation of
hypothesis, the original conditional statement
is true

Proof by contrapositive

Prove: If n^2 is an even integer, then n is even.

$$(n^2 \text{ even}) \rightarrow (n \text{ even})$$

By the contrapositive: This is the same as showing that

- $\neg(n \text{ even}) \rightarrow \neg(n^2 \text{ even})$
- If n is odd, then n^2 is odd.
- We already proved this on slides 4 and 5.

Since we have proved the contrapositive:

$$\neg(n \text{ even}) \rightarrow \neg(n^2 \text{ even})$$

We have also proved the original hypothesis:

$$(n^2 \text{ even}) \rightarrow (n \text{ even})$$

Technique #3:

Proof by contradiction

Prove: If p then q .

Proof strategy:

- Assume the negation of q .
- In other words, assume that $p \wedge \neg q$ is true.
- Then arrive at a contradiction $p \wedge \neg p$ (or something that contradicts a known fact).
- Since this cannot happen, our assumption must be wrong.
- Thus, $\neg q$ is false. q is true.

Proof by contradiction example

Prove: *If $(3n+2)$ is odd, then n is odd.*

Proof:

- Given: $(3n+2)$ is odd.
- Assume that n is not odd, that is n is even.
- If n is even, there is some integer k such that $n=2k$.
- $(3n+2) = (3(2k)+2)=6k+2 = 2(3k+1)$, which is 2 times a number.
- Thus $3n+2$ turned out to be even, but we know it's odd.
- This is a contradiction. Our assumption was wrong.
- Thus, n must be odd.

Proof by Contradiction Example

Prove that the $\sqrt{2}$ is irrational.

Assume that “ $\sqrt{2}$ is irrational” is false, that is, $\sqrt{2}$ is rational.

Hence, $\sqrt{2} = \frac{a}{b}$ and a and b have no common factors. The fraction is in its lowest terms.

So $a^2 = 2b^2$ which means a must be even,

Hence, $a = 2c$

Therefore, $b^2 = 2c^2$ then b must be even, which means a and b must have common factors.

Contradiction.

Technique #4: Proof by cases

- Given a problem of the form:
 - $(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q$
 - where p_1, p_2, \dots, p_n are the cases
- This is equivalent to the following:
 - $[(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)]$
- So prove all the clauses are true.

Proof by cases (example)

- Prove: If n is an integer, then $n^2 \geq n$
 - $(n = 0 \vee n \geq 1 \vee n \leq -1) \rightarrow n^2 \geq n$
- Show for all the three cases, i.e.,
 - $(n = 0 \rightarrow n^2 \geq n) \wedge (n \geq 1 \rightarrow n^2 \geq n)$
 $\wedge (n \leq -1 \rightarrow n^2 \geq n)$
- Case 1: Show that $n = 0 \rightarrow n^2 \geq n$
 - When $n=0$, $n^2= 0$.
 - $0=0$ 😊

Proof by cases (example contd)

- Case 2: Show that $n \geq 1 \rightarrow n^2 \geq n$
 - Multiply both sides of the inequality $n \geq 1$ by n
 - We get $n^2 \geq n$

Proof by cases (example contd)

- Case 3: Show that $n \leq -1 \rightarrow n^2 \geq n$
 - Given $n \leq -1$,
 - We know that n^2 cannot be negative, i.e., $n^2 > 0$
 - We know that $0 > -1$
 - Thus, $n^2 > -1$. We also know that $-1 \geq n$ (given)
 - Therefore, $n^2 \geq n$

Proof by Cases Example

Theorem: Given two real numbers x and y ,

$$\text{abs}(x*y) = \text{abs}(x)*\text{abs}(y)$$

Exhaustively determine the premises

Case p1: $x \geq 0, y \geq 0$, so $x*y \geq 0$ so $\text{abs}(x*y) = x*y$ and $\text{abs}(x) = x$ and $\text{abs}(y) = y$ so $\text{abs}(x)*\text{abs}(y) = x*y$

Case p2: $x < 0, y \geq 0$

Case p3: $x \geq 0, y < 0$

Case p4: $x < 0, y < 0$

Methods of Proving

- When **proving bi-conditional statement**, we may make use of the equivalence

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

- In general, when proving several propositions are equivalent, we can use the equivalence

$$\begin{aligned} p_1 \leftrightarrow p_2 \leftrightarrow \dots \leftrightarrow p_k \\ \equiv (p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \dots \wedge (p_k \rightarrow p_1) \end{aligned}$$

Proofs of Equivalence (Example)

- Show that the following statements about the integer n are equivalent :

$p :=$ “ n is even”

$q :=$ “ $n - 1$ is odd”

$r :=$ “ n^2 is even”

- To do so, we can show the three propositions

$$p \rightarrow q, \quad q \rightarrow r, \quad r \rightarrow p$$

are all true. Can you do so ?

Methods of Proving

- A proof of the proposition of the form $\exists x P(x)$ is called an **existence** proof
- Sometimes, we can find an element s , called a **witness**, such that $P(s)$ is true

This type of existence proof is **constructive**

- Sometimes, we may have **non-constructive** existence proof, where we do not find the witness

Existence Proof (Examples)

- Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.
- Proof: $1729 = 1^3 + 12^3 = 9^3 + 10^3$
- Show that there are irrational numbers r and s such that r^s is rational.
- Hint: Consider $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$

Common Mistakes in Proofs

- Show that $1 = 2$.
- **Proof:** Let a be a positive integer, and $b = a$.

Step

1. $a = b$

2. $a^2 = a b$

3. $a^2 - b^2 = a b - b^2$

4. $(a - b)(a + b) = b(a - b)$

5. $a + b = b$

6. $2b = b$

7. $2 = 1$

Reason

Given

Multiply by a in (1)

Subtract by b^2 in (2)

Factor in (3)

Divide by $(a - b)$ in (4)

By (1) and (5)

Divide by b in (6)

Common Mistakes in Proofs

- Show that
if n^2 is an even integer, then n is even.

- **Proof :**

Suppose that n^2 is even.

Then $n^2 = 2k$ for some integer k .

Let $n = 2m$ for some integer m .

Thus, n is even.

Common Mistakes in Proofs

- Show that
if x is real number, then x^2 is positive.
- **Proof**: There are two cases.

Case 1: x is positive

Case 2: x is negative

In Case 1, x^2 is positive.

In Case 2, x^2 is also positive

Thus, we obtain the same conclusion in all cases, so that the original statement is true.

Proof Strategies

- Adapting Existing Proof
- Show that $\sqrt{3}$ is irrational.
- Instead of searching for a proof from nowhere, we may recall some similar theorem, and see if we can slightly modify (adapt) its proof to obtain what we want

Proof Strategies

- Sometimes, it may be difficult to prove a statement q directly
- Instead, we may find a statement p with the property that $p \rightarrow q$, and then prove p
Note: If this can be done, by Modus Ponens, q is true
- This strategy is called **backward reasoning**

Backward Reasoning (Example)

- Show that for distinct positive real numbers x and y ,

$$0.5 (x + y) > (xy)^{0.5}$$

- Proof: By backward reasoning strategy, we find that

1. $0.25 (x + y)^2 > xy \rightarrow 0.5 (x + y) > (xy)^{0.5}$

2. $(x + y)^2 > 4xy \rightarrow 0.25 (x + y)^2 > xy$

3. $x^2 + 2xy + y^2 > 4xy \rightarrow (x + y)^2 > 4xy$

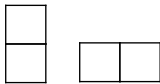
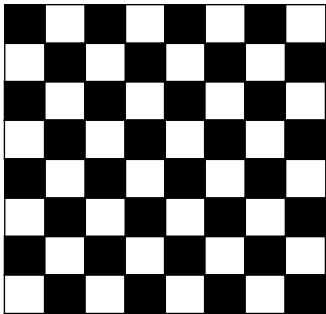
4. $x^2 - 2xy + y^2 > 0 \rightarrow x^2 + 2xy + y^2 > 4xy$

5. $(x - y)^2 > 0 \rightarrow x^2 - 2xy + y^2 > 0$

6. $(x - y)^2 > 0$ is true, since x and y are distinct.

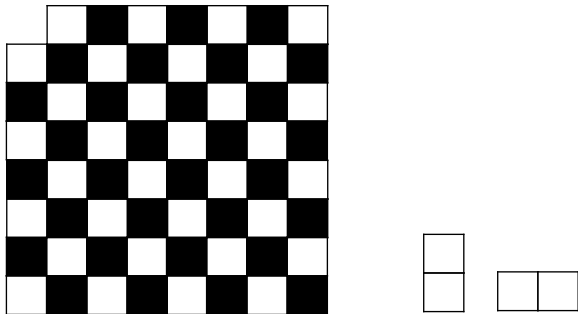
Thus, the original statement is true.

Interesting Examples



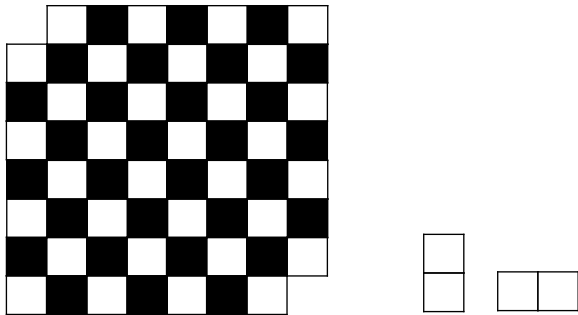
Can a checkerboard be tiled by 1×2 dominoes?

Interesting Examples



What if the top left corner is removed ?

Interesting Examples



What if the lower right corner is also removed ?