Tutorial 4

COMP 5361: Discrete Structures and Formal Languages

Mohammad Reza Davari

Concordia University



Outline

Introduction to Proofs

Proof Methods and Strategy

Practise Questions



Contents of the section

Introduction to Proofs

Proof Methods and Strategy

3 Practise Questions



3 / 48

Definition¹

- Theorem: A theorem is a statement that can be shown to be true and is reserved for a statement that is considered at least somewhat important.
- **Propositions**: Propositions are theorems with less importance.
- Proof: Demonstrates whether a statement (theorem) is true.
- Axioms: Axioms or postulates are statements we assume to be true.
- **Lemma**: Lemma is a less important theorem that is helpful in the proof of other results.
- **Corollary** A corollary is a theorem that can be established directly from a theorem that has been proved.
- **Conjecture** A conjecture is a statement that is being proposed to be a true statement.

Mohammad Reza Davari 4 / 48

Direct Proofs

Strategy

In a direct proof of a conditional statement $p \rightarrow q$:

- Assume that p is true.
- Take advantage of rules of inference.
- Show that q must also be true.



Direct Proofs

Strategy

In a direct proof of a conditional statement $p \rightarrow q$:

- Assume that p is true.
- 2 Take advantage of rules of inference.
- 3 Show that q must also be true.

Example

Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."



Mohammad Reza Davari 5 / 48

Proof by Contraposition

Strategy

Instead of proving $p \to q$, prove its contrapositive, $\neg q \to \neg p$ (since they are equivalent).

- **4** Assume $\neg q$ is true.
- Take advantage of rules of inference.
- **3** Show that $\neg p$ must also be true.



Proof by Contraposition

Strategy

Instead of proving $p \to q$, prove its contrapositive, $\neg q \to \neg p$ (since they are equivalent).

- **1** Assume $\neg q$ is true.
- Take advantage of rules of inference.
- **3** Show that $\neg p$ must also be true.

Example

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



Vacuous Proofs

Caution

While proving $p \to q$ if you realize p is false then you can conclude the statement.



Vacuous Proofs

Caution

While proving $p \rightarrow q$ if you realize p is false then you can conclude the statement.

Example

Show that the proposition P(0) is true, where P(n) is "If n > 1, then $n^2 > n''$ and the domain consists of all integers.



Trivial Proofs

Caution

While proving $p \rightarrow q$ if we can show q is true then you can conclude the statement.



Trivial Proofs

Caution

While proving $p \rightarrow q$ if we can show q is true then you can conclude the statement.

Example

Let P(n) be "If a and b are positive integers with $a \ge b$, then $a^n \ge b^{n}$ " where the domain consists of all non-negative integers. Show that P(0) is true.



Strategy

Suppose we want to prove that a statement p is true.

- **1** Find a contradiction q such that $\neg p \rightarrow q$ is true.
- ② Since q is false and $\neg p \rightarrow q$ is true, then $\neg p$ is false.
- Conclude p is true.

Contradiction g is usually of the form $r \wedge \neg r$ for some proposition r.



Strategy

Suppose we want to prove that a statement p is true.

- **①** Find a contradiction q such that $\neg p \rightarrow q$ is true.
- ② Since q is false and $\neg p \rightarrow q$ is true, then $\neg p$ is false.
- Conclude p is true.

Contradiction q is usually of the form $r \land \neg r$ for some proposition r.

Example

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

Strategy

Suppose we want to prove that a statement p is true.

- **1** Find a contradiction q such that $\neg p \rightarrow q$ is true.
- ② Since q is false and $\neg p \rightarrow q$ is true, then $\neg p$ is false.
- Conclude p is true.

Contradiction q is usually of the form $r \land \neg r$ for some proposition r.

Example

- Show that at least four of any 22 days must fall on the same day of the week.
- ② Prove that $\sqrt{2}$ is irrational.

Strategy

Suppose we want to prove that a statement p is true.

- **①** Find a contradiction q such that $\neg p \rightarrow q$ is true.
- ② Since q is false and $\neg p \rightarrow q$ is true, then $\neg p$ is false.
- Conclude p is true.

Contradiction q is usually of the form $r \land \neg r$ for some proposition r.

Example

- Show that at least four of any 22 days must fall on the same day of the week.
- ② Prove that $\sqrt{2}$ is irrational.
- **③** Prove if 3n + 2 is odd, then n is odd.

Proofs of Equivalence

Strategy

In order to prove a statement of the form $p \leftrightarrow q$ we need to:

- **1** Show $p \rightarrow q$ is true.
- ② Show $q \rightarrow p$ is true.



Proofs of Equivalence

Strategy

In order to prove a statement of the form $p \leftrightarrow q$ we need to:

- **1** Show $p \rightarrow q$ is true.
- ② Show $q \rightarrow p$ is true.

Example

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



Counter Example

Strategy

In order to prove a statement of the form $\forall x P(x)$ is false, you can find a c for which P(c) is false.



Counter Example

Strategy

In order to prove a statement of the form $\forall x P(x)$ is false, you can find a c for which P(c) is false.

Example

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



Mohammad Reza Davari 11 / 48

Watch Out for Mistakes

One important fallacy

Many incorrect arguments are based on a fallacy called **begging the question**. This fallacy occurs when one or more steps of a proof are based on the truth of the statement being proved. In other words, this fallacy arises when a statement is proved using itself, or a statement equivalent to it. That is why this fallacy is also called **circular reasoning**.



Mohammad Reza Davari 12 / 48

Contents of the section

Introduction to Proofs

Proof Methods and Strategy

3 Practise Questions



Exhaustive Proof and Proof by Cases

Idea

It is based on the following tautology:

$$[(p_1 \vee p_2 \vee \cdots \vee p_n) \to q] \leftrightarrow [(p_1 \to q) \wedge (p_2 \to q) \wedge \cdots \wedge (p_n \to q)]$$

It let us proceed with the proof with extra assumptions!



Exhaustive Proof and Proof by Cases

Idea

It is based on the following tautology:

$$[(p_1 \vee p_2 \vee \cdots \vee p_n) \to q] \leftrightarrow [(p_1 \to q) \wedge (p_2 \to q) \wedge \cdots \wedge (p_n \to q)]$$

It let us proceed with the proof with extra assumptions!

Example

• Prove that $(n+1)^3 \ge 3^n$ if n is a positive integer with $n \le 4$.



Mohammad Reza Davari 14 / 48

Exhaustive Proof and Proof by Cases

Idea

It is based on the following tautology:

$$[(p_1 \vee p_2 \vee \cdots \vee p_n) \to q] \leftrightarrow [(p_1 \to q) \wedge (p_2 \to q) \wedge \cdots \wedge (p_n \to q)]$$

It let us proceed with the proof with extra assumptions!

Example

- ① Prove that $(n+1)^3 \ge 3^n$ if n is a positive integer with $n \le 4$.
- 2 Prove that if *n* is an integer, then $n^2 \ge n$



Mohammad Reza Davari

Caution

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.



Caution

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.

Danger

Although this will heavily simply the proofs involving proof by cases, an incorrect use of it will lead to an invalid proof. Be very careful with this statement!



Mohammad Reza Davari 15 / 48

Existence Proofs

Definition

A proof of the form $\exists x P(x)$ is called an existence proof.



Existence Proofs

Definition

A proof of the form $\exists x P(x)$ is called an existence proof.

Strategies

- **Constructive proof**: The proof can be given by finding an element (also called and example or a witness) for which the statement is true.
- Non-constructive proof: You do not look for an example but rather approach the problem using other methods discussed earlier. One common method of giving non-constructive proof is proof by contradiction.



Mohammad Reza Davari 16 / 48

- A 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.



Mohammad Reza Davari 17 / 48

- A 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.
 - $1729 = 10^3 + 9^3 = 12^3 + 1^3$



- A 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.
 - $1729 = 10^3 + 9^3 = 12^3 + 1^3$
- A Nonconstructive Existence Proof:
 - Show that there exist irrational numbers x and y such that x^y is rational.
 - Hint: $\sqrt{2}$



Mohammad Reza Davari

Uniqueness Proofs

Definition

A proof of the form $\exists x (P(x) \land \forall y (y = x \rightarrow \neg P(y)))$ is called a uniqueness proof.



Uniqueness Proofs

Definition

A proof of the form $\exists x (P(x) \land \forall y (y = x \rightarrow \neg P(y)))$ is called a uniqueness proof.

Strategies

To prove a statement of this type we need to show that an element with this property exists and that no other element has this property. The two parts of a uniqueness proof are:

- **Existence**: We show that an element *x* with the desired property exists.
- **Uniqueness**: We show that if $y \neq x$, then y does not have the desired property.

Mohammad Reza Davari

Question

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.



19 / 48

Question

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: We note that $r = \frac{-b}{a}$ is a solution of ar + b = 0 i.e. a real number r exists for which ar + b = 0.



Examples

Question

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**: We note that $r = \frac{-b}{a}$ is a solution of ar + b = 0 i.e. a real number r exists for which ar + b = 0.
- **Uniqueness**: suppose that s is a real number such that as + b = 0. Then we have:

$$ar + b = as + b$$

 $ar = as$
 $r = s$



Contents of the section

Introduction to Proofs

Proof Methods and Strategy

Practise Questions



Question 1

Use rules of inference to show that if $\forall x (P(x) \rightarrow Q(x))$, $\forall x (Q(x) \to R(x))$, and $\exists x (\neg R(x))$ are true, then $\exists x (\neg P(x))$ is true.



$\forall x (P(x) \rightarrow Q(x))$		Given by the problem	(1)
$\forall x (Q(x) \rightarrow R(x))$		Given by the problem	(2)
$\exists x (\neg R(x))$		Given by the problem	(3)
Q(c) o R(c)	for an arbitrary $\it c$	Universal Instantiation: 2	(4)
$\neg(R(c))$	for some c	Existential Instantiation: 3	(5)
$\neg(Q(c))$	for some c	Modus Tollens: 5,4	(6)
P(c) o Q(c)	for an arbitrary $\it c$	Universal Instantiation: 1	(7)
$\neg(P(c))$	for some c	Modus Tollens: 7,6	(8)
$\exists x (\neg P(x))$		Existential Generalization:	8 (9)
$\therefore \exists x (\neg P(x))$		By: 9	(10)

Concordia

Mohammad Reza Davari 22 /

Question 2

Give a direct proof of: "If x is an odd integer and y is an even integer, then x + y is odd."



Direct Proof: Assume x is an odd integer and y is an even integer, we need to show that x + y is odd. By our assumption we have:

$$x = 2k+1$$
 for some $k \in \mathbb{Z}$ (1)

$$y = 2e$$
 for some $e \in \mathbb{Z}$ (2)

$$x + y = 2k + 1 + 2e \tag{3}$$

$$= 2(k+e)+1$$
 (4)

$$\therefore x + y \quad \text{is odd} \tag{5}$$

Note that in Equation 4 k + e is just an integer and can be renamed to some k', hence showing that x + y has the form of an odd integer.



Mohammad Reza Davari 24 / 48

Question 3

Give a proof by contradiction of: "If n is an odd integer, then n^2 is odd."



Mohammad Reza Davari 25 / 48

Proof by Contradiction: Given that n is an odd integer, assume n^2 is not odd i.e. it is even. We have:

$$n = 2k + 1 \text{ for some } k \in \mathbb{Z}$$
 (1)

$$n^2 = 2e \text{ for some} e \in \mathbb{Z}$$
 (2)

Now using Equation 1, we have:

$$n^2 = (2k+1)^2 (3)$$

$$= 4k^2 + 4k + 1 (4)$$

$$= 2(2k^2 + 2k) + 1 (5)$$

Equation 5 shows n^2 is odd which is in contradiction with Equation 2. Hence, our assumption was false, i.e n^2 must be odd.

Mohammad Reza Davari 26 / 48

Question 4

Give an indirect proof of: "If x is an odd integer, then x + 2 is odd."



Proof by Contraposition Assume x + 2 is not odd (it is even) we need to show that x is even. Since x + 2 is even, we can write is as 2k for some $k \in \mathbb{Z}$. Therefore we have:

$$x = 2k - 2 \tag{1}$$

$$= 2(k-1) \tag{2}$$

The second equation shows that x is even, hence we reached our desired conclusion.



Mohammad Reza Davari 28 / 48

Question 5

Use a proof by cases to show that there are no solutions in positive integers to the equation $x^4 + y^4 = 100$.



Mohammad Reza Davari 29 / 48

- **Proof by Cases**: Note that neither x or y can be greater than 3 (since $4^4 = 256 > 100$). Hence, we only need to search for solutions among $\{0,1,2,3\}$.
- Case 1: x = 0, in this case y needs to be as large as possible, y = 3 provides $81 \neq 100$ hence, there is no solution in this case.
- Case 2: x=1, even when y attains the larges possible value, the left side of the equation is still smaller than the right side $(82 \neq 100)$ hence, there is no solution in this case.
- Case 3: x = 2, again with the same reasoning as above cases we can see that the left side of the equation will always be smaller than the right side. Hence, there is no solution in this case.
- Case 4: x = 3 this case has been covered by y = 3 in the previous cases, hence WLOG we can conclude that there is no solution in this case.

Mohammad Reza Davari 30 / 48

Question 6

Prove that given a non-negative integer n, there is a unique non-negative integer m, such that $m^2 \le n < (m+1)^2$.



Since this is a uniqueness proof, we need to show the followings:

- Existence
- Uniqueness

We first show the existence of such m.

Existence: Let m be $\lfloor \sqrt{n} \rfloor$, then:

$$m \le \sqrt{n} \le m + 1 \tag{1}$$

$$\therefore m^2 \le n \le (m+1)^2 \tag{2}$$



Mohammad Reza Davari

Now we attempt to show the uniqueness of the solution.

Uniqueness: Assume $\exists k \neq m$, WLOG we can also assume $m \geq k$, such that:

$$k^2 \le n \le (k+1)^2 \tag{3}$$

$$k \le n \le k+1 \tag{4}$$

Now if we subtract Equations 1 and 4 we would have:

$$m-k\leq 0\tag{5}$$

Since $m \ge k$ then $m - k \ge 0$, considering the Equation 5, we reach to the conclusion:

$$m-k=0$$

$$m = k$$

Hence, the solution is unique.



Mohammad Reza Davari 33 / 48

Question 7

For each of the premise-conclusion pairs below, give a valid step-by-step argument (proof) along with the name of the inference rule used in each step.

① Premise: $\{\neg p \lor q \to r, s \lor \neg q, \neg t, p \to t, \neg p \land r \to \neg s\}$, conclusion: $\neg q$.



Mohammad Reza Davari 34 / 48

Question 7

For each of the premise-conclusion pairs below, give a valid step-by-step argument (proof) along with the name of the inference rule used in each step.

- **②** Premise: $\{\neg p \to r \land \neg s, t \to s, u \to \neg p, \neg w, u \lor w\}$, conclusion: $\neg t \lor w$.



Mohammad Reza Davari 34 / 48

Question 7

For each of the premise-conclusion pairs below, give a valid step-by-step argument (proof) along with the name of the inference rule used in each step.

- **①** Premise: $\{\neg p \lor q \to r, s \lor \neg q, \neg t, p \to t, \neg p \land r \to \neg s\}$, conclusion: $\neg q$.
- ② Premise: $\{\neg p \rightarrow r \land \neg s, t \rightarrow s, u \rightarrow \neg p, \neg w, u \lor w\}$, conclusion: $\neg t \lor w$.
- **③** Premise: $\{p \lor q, q \to r, p \land s \to t, \neg r, \neg q \to u \land s\}$, conclusion: t.



Mohammad Reza Davari 34 / 48

$\neg p \lor q \to r$	Given by the problem	(1)
$s \lor \lnot q$	Given by the problem	(2)
$\neg t$	Given by the problem	(3)
ho o t	Given by the problem	(4)
$\neg p \land r \rightarrow \neg s$	Given by the problem	(5)
$\neg p$	Modus Tollens: 3,4	(6)
$\neg p \vee$	Addition: 6	(7)
r	Modus Ponens: 1,7	(8)
$r \wedge \neg p$	Conjunction: 8,6	(9)
$\neg s$	Modus Ponens: 9,5	(10)
eg q	Disjunctive Syllogism: 10	,2 (11)
∴. ¬ <i>q</i>	By : 11	Concordia

$\neg p o r \wedge \neg s$	Given by the problem	(1)
t o s	Given by the problem	(2)
u o eg p	Given by the problem	(3)
$\neg w$	Given by the problem	(4)
$u \lor w$	Given by the problem	(5)
и	Disjunctive Syllogism: 4	,5 (6)
$\neg p$	Modus Ponens: 3,6	(7)
$r \wedge \neg s$	Modus Ponens: 7,1	(8)
$\neg s$	Simplification: 8	(9)
$\neg t$	Modus Tollens: 9,2	(10)
$\neg t \lor w$	Addition: 10	(11)
$\therefore \neg t \lor w$	By: 11	Concordiza

Mohammad Reza Davari 36 / 48

$p \lor q$	Given by the problem	(1)
q ightarrow r	Given by the problem	(2)
$p \wedge s o t$	Given by the problem	(3)
$\neg r$	Given by the problem	(4)
$\neg q o u \wedge s$	Given by the problem	(5)
$\neg q$	Modus Tollens: 2,4	(6)
р	Disjunctive Syllogism: $6,1$	(7)
$u \wedge s$	Modus Ponens: 5,6	(8)
S	Simplification: 8	(9)
$p \wedge s$	Conjunction: 7,8	(10)
t	Modus Ponens: 10,3	(11)
∴ t	By: 11	Concor(dji2a)

Mohammad Reza Davari 37 / 48

Question 8

Prove that the following four statements are equivalent:

- \bigcirc 1 *n* is even.
- **1** $n^2 + 1$ is even.



It is enough to show:

 1^{st} Statement $\rightarrow 2^{nd}$ Statement

 2^{nd} Statement $\rightarrow 3^{rd}$ Statement

 3^{rd} Statement $\rightarrow 4^{th}$ Statement

 $4^{\it th}$ Statement $ightarrow 1^{\it st}$ Statement

Solution: Question 8 Part (1)

In this part we aim to prove, given that n^2 is odd then 1-n is even. **Proof by Contraposition**: Assume 1-n is odd, we need to prove n^2 is even. Since 1-n is odd we can write it as 2k+1 for some $k\in\mathbb{Z}$. Therefore we have:

$$1-n = 2k+1 \tag{1}$$

$$n = 2(-k) \tag{2}$$

$$n^2 = 4k^2 (3)$$

$$= 2(2k^2) \tag{4}$$

Equation 4 shows that n^2 is a multiple of 2 and hence even.



Mohammad Reza Davari 40 / 48

Solution: Question 8 Part (2)

rename -k to q we then have:

In this part we show the proof for: "If 1 - n is even then n^3 is odd". **Direct Proof**: Assume 1 - n is even, hence it can be written as 2k for some $k \in \mathbb{Z}$. Therefore, n = 2(-k) + 1, i.e. n is odd. For simplicity lets

$$n = 2q + 1 \tag{1}$$

$$n^3 = (2q+1)^3 (2)$$

$$= 8q^3 + 12q^2 + 6q + 1 (3)$$

$$= 2(4q^3 + 6q^2 + 3q) + 1 (4)$$

Equation 4 shows that n^3 is odd, and hence our proof is completed for this part.



Mohammad Reza Davari 41 / 48

Solution: Question 8 Part (3)

In this part we will prove that $n^2 + 1$ is even given that n^3 is odd. We first prove the following lemma which will be helpful to prove the statement.

Lemma: If n^3 is odd then n is odd.

Proof by Contraposition: Assume n is even, we need to show that n^3 is even. Since, n is even, it can be written as 2k for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3 = 2(4k^3)$, which shows n^3 is even.



Mohammad Reza Davari 42 / 48

Solution: Question 8 Part (3)

Now that we have the lemma, we will prove the statement as follows: **Direct Proof:** Since n^3 is odd, then by the lemma we have n is odd. Hence we can write n as 2t + 1 for some $t \in \mathbb{Z}$. We now have:

$$n^2 + 1 = (2t + 1)^2 + 1 (1)$$

$$= 4t^2 + 4t + 2 (2)$$

$$= 2(2t^2 + 2t + 1) (3)$$

Equation 3 shows that $n^2 + 1$ is even and that the proof for this part is completed.



Mohammad Reza Davari 43 / 48

Solution: Question 8 Part (4)

In this part we need to show n^2 is odd given that n^2+1 is even. **Direct Proof**:Assume n^2+1 is even, we need to show that n^2 is odd. Since, n^2+1 is even it can be written as 2k for some $k\in\mathbb{Z}$. Hence, $n^2+1=2k+1$ i.e. it is odd and therefore the proof is completed.

Now that we have show the proof for all 4 parts, we can conclude that the 4 statements given by the problem are all equivalent.



Mohammad Reza Davari 44 / 4

Question 9

Consider the statement concerning integers "If m + n is even, then m - n is even."

• Give a direct proof of the statement.



Question 9

Consider the statement concerning integers "If m + n is even, then m - nis even."

- Give a direct proof of the statement.
- Q Give a proof by contraposition of the statement.



Mohammad Reza Davari

Question 9

Consider the statement concerning integers "If m + n is even, then m - nis even."

- Give a direct proof of the statement.
- Give a proof by contraposition of the statement.
- Prove the statement by contradiction.



Mohammad Reza Davari

Solution: Question 9 Part (1)

Direct Proof: Assume m + n is even, we need to show m - n is even. Since m + n is even we have the following cases:

Case 1: Both m and n are even: Then in this case, m-n would also be even as the subtraction of two even numbers is even.

Case 2: Both m and n are odd: Then in this case, m-n would be even as the subtraction of two odd numbers is even.

We have proved the desired result for all cases, hence the proof is completed.



Mohammad Reza Davari 46 / 48

Solution: Question 9 Part (2)

Proof by Contraposition: Assume m-n is odd, we need to show that m+n is also odd. Since m-n is odd we have that m and n are a pair of odd and even, i.e. one is odd and the other is even. The addition of an odd and even integer is odd, i.e. m+n is odd. Hence, we reached the desired result and this concludes the proof for this case.



Mohammad Reza Davari 47 / 48

Solution: Question 9 Part (3)

Proof by Contradiction: Assume m+n is even and m-n is odd. Sum of an odd and an even integer is odd. Hence if we add m+n and m-n we should have an odd integer. However, m+n+m-n=2m, i.e an even integer. Hence we reached a contradiction in this case, which means our original assumption was false, i.e. m-n must be even.



Mohammad Reza Davari 48 / 48