Discrete Structures

Fight for Survival

Dr. Mudassir Shabbir

August 27, 2026

BWOC: By Way of Contradiction

Prove that $(A \lor C \to D) \land \neg B \land (A \lor B) \to D$ is true.

	Statements	Reason
1	$(A \lor C \to D)$	Premise
2	$\neg B$	Premise
3	$A \lor B$	Premise
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \rightarrow D) \wedge \neg B \wedge (A \vee B) \rightarrow D$ is true.

	Statements	Reason
1	$(A \vee C \rightarrow D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	
6		
7		
8		
9		
10		
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6		
7		
8		
9		
10		
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \lor C \to D) \land \neg B \land (A \lor B) \to D$ is true.

	Statements	Reason
1	$(A \lor C \to D)$	Premise
2	$\neg B$	Premise
3	$A \lor B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \lor C)$	1, 4, Modus tollens
6	$\neg A \land \neg C$	
7		
8		
9		
10		
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \rightarrow D) \wedge \neg B \wedge (A \vee B) \rightarrow D$ is true.

	Statements	Reason
1	$(A \vee C \rightarrow D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7		
8		
9		
10		
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7	$\neg A$	
8		
9		
10		
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \rightarrow D) \wedge \neg B \wedge (A \vee B) \rightarrow D$ is true.

	Statements	Reason
1	$(A \vee C \rightarrow D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8		
9		
10		
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8	$\neg A \wedge \neg B$	
9		
10		
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8	$\neg A \wedge \neg B$	2,7
9		
10		
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8	$\neg A \wedge \neg B$	2,7
9	$\neg(A \vee B)$	
10		
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8	$\neg A \wedge \neg B$	2,7
9	$\neg(A \vee B)$	8, DeMorgans Law
10		
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \lor C \to D) \land \neg B \land (A \lor B) \to D$ is true.

	Statements	Reason
1	$(A \lor C \to D)$	Premise
2	$\neg B$	Premise
3	$A \lor B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \lor C)$	1, 4, Modus tollens
6	$\neg A \land \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8	$\neg A \land \neg B$	2,7
9	$\neg(A \lor B)$	8, DeMorgans Law
10	$\cancel{\neg(A \lor C \to D) \lor \neg(\neg B) \lor \neg(A \lor B)}$	
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8	$\neg A \wedge \neg B$	2,7
9	$\neg(A \vee B)$	8, DeMorgans Law
10	$\cancel{\neg(A \vee C \to D) \vee \neg(\neg B) \vee \neg(A \vee B)}$	9, Disjunction
11		
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8	$\neg A \wedge \neg B$	2,7
9	$\neg(A \vee B)$	8, DeMorgans Law
10	$\cancel{\neg(A \vee C \to D) \vee \neg(\neg B) \vee \neg(A \vee B)}$	9, Disjunction
11	$\cancel{\neg((A \vee C \to D) \wedge (\neg B) \wedge (A \vee B))}$	
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8	$\neg A \wedge \neg B$	2,7
9	$\neg(A \vee B)$	8, DeMorgans Law
10	$\cancel{\neg(A \vee C \to D) \vee \neg(\neg B) \vee \neg(A \vee B)}$	9, Disjunction
11	$\cancel{\neg((A \vee C \to D) \wedge (\neg B) \wedge (A \vee B))}$	10, DeMorgans Law
12		
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \lor C \to D) \land \neg B \land (A \lor B) \to D$ is true.

	Statements	Reason
1	$(A \lor C \to D)$	Premise
2	$\neg B$	Premise
3	$A \lor B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \lor C)$	1, 4, Modus tollens
6	$\neg A \land \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8	$\neg A \land \neg B$	2,7
9	$\neg(A \lor B)$	8, DeMorgans Law
10	$\cancel{\neg(A \lor C \to D) \lor \neg(\neg B) \lor \neg(A \lor B)}$	9, Disjunction
11	$\cancel{\neg((A \lor C \to D) \land (\neg B) \land (A \lor B))}$	10, DeMorgans Law
12	$\cancel{(A \lor C \to D) \land (\neg B) \land (A \lor B)}$	
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8	$\neg A \wedge \neg B$	2,7
9	$\neg(A \vee B)$	8, DeMorgans Law
10	$\cancel{\neg(A \vee C \to D) \vee \neg(\neg B) \vee \neg(A \vee B)}$	9, Disjunction
11	$\cancel{\neg((A \vee C \to D) \wedge (\neg B) \wedge (A \vee B))}$	10, DeMorgans Law
12	$\cancel{(A \vee C \to D) \wedge (\neg B) \wedge (A \vee B)}$	1,2,3 (Hypotheses)
13		
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8	$\neg A \wedge \neg B$	2,7
9	$\neg(A \vee B)$	8, DeMorgans Law
10	$\cancel{\neg(A \vee C \to D) \vee \neg(\neg B) \vee \neg(A \vee B)}$	9, Disjunction
11	$\cancel{\neg((A \vee C \to D) \wedge (\neg B) \wedge (A \vee B))}$	10, DeMorgans Law
12	$\cancel{(A \vee C \to D) \wedge (\neg B) \wedge (A \vee B)}$	1,2,3 (Hypotheses)
13	False	
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \to D) \wedge \neg B \wedge (A \vee B) \to D$ is true.

	Statements	Reason
1	$(A \vee C \to D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8	$\neg A \wedge \neg B$	2,7
9	$\neg(A \vee B)$	8, DeMorgans Law
10	$\cancel{\neg(A \vee C \to D) \vee \neg(\neg B) \vee \neg(A \vee B)}$	9, Disjunction
11	$\cancel{\neg((A \vee C \to D) \wedge (\neg B) \wedge (A \vee B))}$	10, DeMorgans Law
12	$\cancel{(A \vee C \to D) \wedge (\neg B) \wedge (A \vee B)}$	1,2,3 (Hypotheses)
13	False	3,9, Contradiction
14		

BWOC: By Way of Contradiction

Prove that $(A \vee C \rightarrow D) \wedge \neg B \wedge (A \vee B) \rightarrow D$ is true.

	Statements	Reason
1	$(A \vee C \rightarrow D)$	Premise
2	$\neg B$	Premise
3	$A \vee B$	Premise
4	$\neg D$	Assumption
5	$\neg(A \vee C)$	1, 4, Modus tollens
6	$\neg A \wedge \neg C$	5, DeMorgan's Law
7	$\neg A$	6, Simplification
8	$\neg A \wedge \neg B$	2,7
9	$\neg(A \vee B)$	8, DeMorgans Law
10	$\cancel{\neg(A \vee C \rightarrow D) \vee \neg(\neg B) \vee \neg(A \vee B)}$	9, Disjunction
11	$\cancel{\neg((A \vee C \rightarrow D) \wedge (\neg B) \wedge (A \vee B))}$	10, DeMorgans Law
12	$\cancel{(A \vee C \rightarrow D) \wedge (\neg B) \wedge (A \vee B)}$	1,2,3 (Hypotheses)
13	False	3,9, Contradiction
14	QED	13

Proofs with Quantifiers

How can we prove statements that involve quantifiers?

Good news is that whatever we have learned so far regarding conditional statement proofs, remains valid here. We just need few additional tools to make it work nicely.

Proofs with Quantifiers

So, the trick lies in figuring out when and how to

1. eliminate a quantifier
2. add a quantifier

An arbitrary element of a domain is an element that shares all of the characteristics of every other element in a domain A particular element of a domain is an element that possesses some characteristic not necessarily shared by all other elements.

Lets see some rules of inference involving quantifiers

Rules of Inference for Quantifiers

- Existential Instantiation (Eliminating a quantifier)
  $\exists x P(x)$ then (c is a particular element) $\wedge P(c)$.
- Existential Generalization (Adding a quantifier)
  (c is an element) $\wedge P(c)$ then $\exists x P(x)$.
- Universal Instantiation (Eliminating a quantifier)
  $\forall x P(x)$ then (c is an element) $\wedge P(c)$.
- Universal Generalization (Adding a quantifier)
  (c is an arbitrary element) $\wedge P(c)$ then $\forall x P(x)$.

Arbitrary element means, it can be any element in the domain. So, we can pick any element and the statement is true for that element.

Proofs with Quantifiers - Example

A student, Luna, in the class knows how to cast a Patronus Charm. Everyone who can cast Patronus joins the Order of the Phoenix. Therefore, someone in the class is a member of the Order.

Proofs with Quantifiers - Example

A student, Luna, in the class knows how to cast a Patronus Charm. Everyone who can cast Patronus joins the Order of the Phoenix. Therefore, someone in the class is a member of the Order.

$C(x)$: x is in the class.
$J(x)$: x knows how to cast a Patronus Charm
$H(x)$: x is a member of the Order of the Phoenix

$$C(Luna) \wedge J(Luna) \wedge \forall x(J(x) \rightarrow H(x)) \rightarrow \exists x(C(x) \wedge H(x))$$

Proofs with Quantifiers - Example

$$C(Luna) \wedge J(Luna) \wedge \forall x(J(x) \to H(x)) \to \exists x(C(x) \wedge H(x))$$

1. $C(Luna)$ Premise
2. $J(Luna)$ Premise
3. $\forall x(J(x) \to H(x))$ Premise
4.
5.
6.
7.
8.

Proofs with Quantifiers - Example

$$C(Luna) \land J(Luna) \land \forall x(J(x) \to H(x)) \to \exists x(C(x) \land H(x))$$

1. $C(Luna)$ Premise
2. $J(Luna)$ Premise
3. $\forall x(J(x) \to H(x))$ Premise
4. $J(Luna) \to H(Luna)$ 3, Universal instantiation
5.
6.
7.
8.

Proofs with Quantifiers - Example

$$C(Luna) \wedge J(Luna) \wedge \forall x(J(x) \rightarrow H(x)) \rightarrow \exists x(C(x) \wedge H(x))$$

1. $C(Luna)$ Premise
2. $J(Luna)$ Premise
3. $\forall x(J(x) \rightarrow H(x))$ Premise
4. $J(Luna) \rightarrow H(Luna)$ 3, Universal instantiation
5. $H(Luna)$ 2,4, Modus ponens
6.
7.
8.

Proofs with Quantifiers - Example

$$C(Luna) \land J(Luna) \land \forall x(J(x) \rightarrow H(x)) \rightarrow \exists x(C(x) \land H(x))$$

1. $C(Luna)$ — Premise
2. $J(Luna)$ — Premise
3. $\forall x(J(x) \rightarrow H(x))$ — Premise
4. $J(Luna) \rightarrow H(Luna)$ — 3, Universal instantiation
5. $H(Luna)$ — 2,4, Modus ponens
6. $C(Luna) \land H(Luna)$ — 1,5, Conjunction
7.
8.

Proofs with Quantifiers - Example

$$C(Luna) \land J(Luna) \land \forall x(J(x) \to H(x)) \to \exists x(C(x) \land H(x))$$

1. $C(Luna)$ — Premise
2. $J(Luna)$ — Premise
3. $\forall x(J(x) \to H(x))$ — Premise
4. $J(Luna) \to H(Luna)$ — 3, Universal instantiation
5. $H(Luna)$ — 2,4, Modus ponens
6. $C(Luna) \land H(Luna)$ — 1,5, Conjunction
7. $\exists x(C(x) \land H(x))$ — 6, Existential generalization
8. QED — 1 - 7

Proofs with Quantifiers - Practice Example

$$\forall x(P(x) \rightarrow (Q(x) \wedge S(x))) \wedge \forall x(P(x) \wedge R(x)) \rightarrow \forall x(R(x) \wedge S(x))$$

Example of a wrong Proof!

Prove the proposition : $\exists x P(x) \land \exists x Q(x) \rightarrow \exists x (P(x) \land Q(x))$

1.	$\exists\ x\ P(x)$	Hypothesis
2.	$\exists x\ Q(x)$	Hypothesis
3.	(c is a particular element) $\land$ P(c)	Existential instantiation, 1
4.	(c is a particular element) $\land$ Q(c)	Existential instantiation, 2
5.	P(c)	Simplification, 3
6.	Q(c)	Simplification, 5
7.	P(c) $\land$ Q(c)	Conjunction, 5, 6
9.	$\exists x$ (P(x) $\land$ Q(x))	Existential generalization, 7
10.	QED	

Example of a wrong Proof!

Prove the proposition : $\exists x P(x) \land \exists x Q(x) \rightarrow \exists x (P(x) \land Q(x))$

1.	$\exists\ x\ P(x)$	Hypothesis
2.	$\exists x\ Q(x)$	Hypothesis
3.	(c is a particular element) $\land$ P(c)	Existential instantiation, 1
4.	(c is a particular element) $\land$ Q(c)	Existential instantiation, 2
5.	P(c)	Simplification, 3
6.	Q(c)	Simplification, 5
7.	P(c) $\land$ Q(c)	Conjunction, 5, 6
9.	$\exists x$ (P(x) $\land$ Q(x))	Existential generalization, 7
10.	QED	

The value of x for which P is true might be different than the value of x for which Q is true. But, we have assumed that it's the same, that is c for both the cases.

Example of a wrong Proof!

Useful Tip:

Be Careful in Using Existential Instantiation

$\exists x\, P(x)$ means that there exists "some" value of x which for which $P(x)$ is true. We cannot just pick the value of our choice and say P is true for that value.

Example of a wrong Proof!

Useful Tip:

Be Careful in Using Universal Generalization
If statement is true for a particular value of variable, then it does not mean that it is necessarily true for all values of variables. In other words, be careful about stereotyping. If you're going to apply "for all" to something, you better be sure it's applicable to "all".

Introduction to General Proofs

A proof is a valid argument that establishes the truth of a mathematical statement.

Proof Terminology

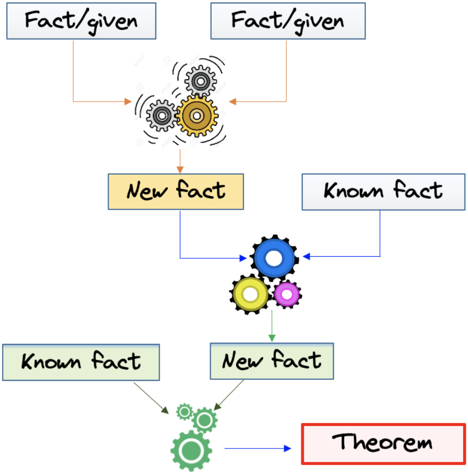
- **Axiom (or postulate):**
  A statement that is assumed to be true
- **Theorem:**
  A statement that has been proven to be true
- **Hypothesis or premises:**
  A hypothesis is a guess (or assumption) without assuming that it is true

Introduction to General Proofs

Important Considerations while Proving

- What do we know?
- What else do we need to know?
- How can we "combine" known facts to get new information.
- Which (mathematical) tools should we apply, and when should we apply them?
- No fixed approach/method
- Its a "creative art" and a skill

Proving a Theorem



Proof Types

- We will see various "approaches" and "techniques" to proving theorems.
- We will try to prove statements involving numbers and more.
- Logic has set up the foundation to move forward.

Proof Types:

- Direct proofs
- Proofs by contrapositive
- Proofs by contradiction
- Proofs by cases or Proofs by exhaustion

Proofs: Some Definitions

Divisibility:

Symbol: $m|n$

Reads: m divides n

Definition: if $m \neq 0$ and $n = k \times m$ for some integer k

Example: $3|6$

Important properties of divisibility:

- If $a|b$ and $b|c$ then $a|c$
- If $d|a$ and $a|b$ then $d|(xa + yb)$ for any integers x, y

Proofs: Some Definitions

Prime number: An integer n is prime if and only if $n > 1$, and for every positive integer m, if $m|n$, then $m = 1$ or $m = n$.

Composite number: An integer n is composite if and only if $n > 1$, and there is an integer $1 < m < n$ such that $m|n$.

Parity The number is odd or even.
Same Parity If two numbers are both even or both odd.
Opposite Parity If one number is odd and the other is even.

Exhaustive Checking Proof

- What: This technique works by checking every possibility in the testing domain.
- When to use:
  - Works well if you only have to perform a small number of tests (e.g., x is an integer such that $3 \leq x \leq 6$).
  - Does not work well with a large domain (e.g., All politicians are liars).
- Difficulty: Easy to use but it will get cumbersome as the domain to test gets larger (kind of like truth tables).

Example: Check whether 289 is prime or composite?

Proof by Cases - Exhaustive proofs

Sometimes we cannot prove a theorem using a single argument that holds for all possible cases. We now introduce a method that can be used to prove a theorem, by considering different cases separately.

$$p \to q = (p_1 \vee p_2 \vee \dots \vee p_n) \to q$$

Some theorems can be proved by examining a relatively small number of examples. Such proofs are called exhaustive proofs, or proofs by exhaustion because these proofs proceed by exhausting all possibilities.

Proof by Cases - Examples

Proof by Cases: $(n+1)^3 \geq 3^n, \forall n \leq 4$

n	$(n+1)^2$	3^n	$(n+1)^3 \geq 3^n$
0	1	1	= (True)
1	8	3	>(True)
2	27	9	>(True)
3	64	27	>(True)
4	125	81	>(True)
5	216	243	>(False)

Proof by Cases - Examples

Proof by cases: If n is an integer then $n^2 >= n$

Proof by Cases - Examples

Proof by cases: If n is an integer then $n^2 >= n$

Proof

We have 3 cases:

I. $n > 0$, n is positive. $n^2 = n.n > n$

II. $n = 0, n^2 = 00 = 0 = n$

III. $n < 0$. n is negative. $n^2 = n.n > 0 > n$ (because n is a negative number.)

Proof by Cases – Examples (Do it by yourself)

There is no solution in integers x and y for equation $x^2 + 3y^2 = 8$

Proof by Cases – Examples (Do it by yourself)

There is no solution in integers x and y for equation $x^2 + 3y^2 = 8$

x	y	$x^2 + 3y^2$	Equal to 8 or not
0	0	0	Less than 8
0	1	3	Less than 8
0	2	12	Exceeds 8
1	0	1	Less than 8
1	1	4	Less than 8
1	2	13	Exceeds 8

Proofs by Contraposition

Prove: For $x \in \mathbb{Z}$, if $7x + 9$ is even, then x is odd.

PROOF by Contraposition:

- x is even $\neg Q$.
- $x = 2k$ Definition of even numbers.
- $7x = 2 \times 7k$
- $7x + 8 = 2 \times 7k + 2 \times 4$ Simplification.
- $7x + 8 = 2 \times (7k + 4)$ Simplification.
- $7x + 8 = 2 \times k'$ Simplification.
- $7x + 9 = 2 \times k' + 1$ Simplification.
- $7x + 9$ is odd Definition of odd numbers.
- $\neg P$
- Q.E.D.

Proofs by Contradiction: $\sqrt{2}$ is irrational.

Suppose $\sqrt{2}$ be a rational number ($\neg Q$). PROOF by Contradiction:

- $\sqrt{2} = p/q, p, q \in \mathbb{Z}$ Def. of rationals.
- $2 \nmid p$ or $2 \nmid q$ otherwise divide both by 2.
- $2 = p^2/q^2,$ Square both sides.
- $p^2 = 2 \times q^2,$ Simplification.
- $2 \mid p$ x^2 is even $\rightarrow x$ is even.
- $p = 2k$ Definition of even numbers.
- $2 = 4k^2/q^2,$ $p = 2k$.
- $q^2 = 2k^2$ $p = 2k$.
- $2 \mid q$ x^2 is even $\rightarrow x$ is even.
- Q.E.D. Contradiction.

Mistakes in Proofs

There are many common errors made in constructing mathematical proofs.

Each step of a mathematical proof needs to be correct and the conclusion needs to follow logically from the steps that precede it.

Many mistakes result from the introduction of steps that do not logically follow from those that precede it.

What is wrong with this famous supposed "proof" that $1 = 2$?

Mistakes in Proofs

What is wrong with this famous supposed "proof" that 1 = 2?

1. Let a and b two variables, such that: $a = b$
2. Multiply both sides by a to get: $a^2 = ab$
3. Subtract b^2 from both sides to get: $a^2 - b^2 = ab - b^2$
4. Factors from both sides: $(a+b)(a-b) = b(a-b)$
5. canceling $(a-b)$ on both sides: $a + b = b$
6. Since $a = b$ (our assumption): $b + b = b$
7. Further solving: $2b = b$
8. Dividing both sides by b: $2 = 1$

Mistakes in Proofs

What is wrong with this famous supposed "proof" that 1 = 2?

1. Let a and b two variables, such that: $a = b$
2. Multiply both sides by a to get: $a^2 = ab$
3. Subtract b^2 from both sides to get: $a^2 - b^2 = ab - b^2$
4. Factors from both sides: $(a+b)(a-b) = b(a-b)$
5. canceling $(a-b)$ on both sides: $a + b = b$
6. Since $a = b$ (our assumption): $b + b = b$
7. Further solving: $2b = b$
8. Dividing both sides by b: $2 = 1$

Mistake: Division of $a - b$ on both sides at step 5.
Reason: $a - b = 0$, we can not divide by zero on both sides

Example of a Simple Elegant Proof

Finally, lets conclude and treat ourselves by looking at one of the simplest, most elegant proofs (presented some 2000 years ago).

Theorem: There are infinitely many primes.

Lets prove it (Also observe the flavor of contradiction, cases)

Infinitely Many Primes!

PROOF by Contradiction:

1. Assume we have the list of all primes: $p_1, p_2, \ldots, p_n$ — By $\neg Q$
2. Consider the number $N = p_1 \times p_2 \times \ldots \times p_n + 1$
3. N is not a prime. — By 1.
4. $\exists p_i, p_i | N$ — Definition of Composite Numbers.
5. $\frac{N}{p_i} = \frac{p_1 \times p_2 \times \ldots \times p_n + 1}{p_i}$ is in $\mathbb{Z}$ — By 4.
6. $= \frac{p_1 \times p_2 \times \ldots p_{i-1} \times p_i \times p_{i+1} \ldots \times p_n + 1}{p_i}$ — Simplification.
7. $p_1 \times p_2 \times \ldots p_{i-1} \times p_{i+1} \ldots \times p_n \frac{1}{p_i} \quad \notin \mathbb{Z}$ — Simplification.
8. Contradiction. — By 5,7.
9. Q.E.D.