CS 105: Department Introductory Course on Discrete Structures

Instructor : S. Akshay

Aug 01, 2024

Lecture 03 – Theorems, types of proofs

Logistics and recap

Course material, references are being posted at

- `http://www.cse.iitb.ac.in/~akshayss/teaching.html`

Logistics and recap

Course material, references are being posted at

- http://www.cse.iitb.ac.in/~akshayss/teaching.html
- Join Piazza if haven't already done so:
  - https://piazza.com/iit_bombay/fall2024/cs105

Logistics and recap

Course material, references are being posted at

- http://www.cse.iitb.ac.in/~akshayss/teaching.html
- Join Piazza if haven't already done so:
  - https://piazza.com/iit_bombay/fall2024/cs105

Recap of two lectures

- What are discrete structures?
- Course outline
- Chapter 1: Proofs and structures
  - Propositions: statements that can be assigned a truth value
  - Predicates: propositions with variables
  - Quantifiers

A bit more about quantifiers

Negating Quantifiers

- What is the negation of “All students have MA105”?

A bit more about quantifiers

Negating Quantifiers

- What is the negation of “All students have MA105”?
  There exists a student who does not have MA105.

A bit more about quantifiers

Negating Quantifiers

- What is the negation of "All students have MA105"?
  There exists a student who does not have MA105.
- $\neg \forall x P(x) \equiv \exists x \neg P(x)$ [1]

[1] $\equiv$ stands for "is logically equivalent to".

A bit more about quantifiers

Negating Quantifiers

- What is the negation of "All students have MA105"?

  There exists a student who does not have MA105.
- $\neg\forall x P(x) \equiv \exists x \neg P(x)$ [1]
  - $\neg\forall x P(x)$ is true iff $\forall x P(x)$ is false
  - $\forall x P(x)$ is false iff there is some x s.t. $\neg P(x)$ is true.
  - i.e., $\exists x \neg P(x)$.

[1] $\equiv$ stands for "is logically equivalent to".

A bit more about quantifiers

Negating Quantifiers

- What is the negation of "All students have MA105"?

  There exists a student who does not have MA105.
- $\neg\forall x P(x) \equiv \exists x \neg P(x)$ [1]
  - $\neg\forall x P(x)$ is true iff $\forall x P(x)$ is false
  - $\forall x P(x)$ is false iff there is some x s.t. $\neg P(x)$ is true.
  - i.e., $\exists x \neg P(x)$.
- $\neg\exists x P(x) \equiv \forall x \neg P(x)$

[1] $\equiv$ stands for "is logically equivalent to".

A bit more about quantifiers

Negating Quantifiers

- What is the negation of "All students have MA105"?

  There exists a student who does not have MA105.
- $\neg \forall x P(x) \equiv \exists x \neg P(x)$ [1]
  - $\neg \forall x P(x)$ is true iff $\forall x P(x)$ is false
  - $\forall x P(x)$ is false iff there is some x s.t. $\neg P(x)$ is true.
  - i.e., $\exists x \neg P(x)$.
- $\neg \exists x P(x) \equiv \forall x \neg P(x)$

Exercises

1. What is the negation of $\forall x (x^2 > x)$?
2. Show that $\neg \forall x (P(x) \rightarrow Q(x)) \equiv \exists x (P(x) \wedge \neg Q(x))$.

[1] $\equiv$ stands for "is logically equivalent to".

A bit more about quantifiers

Negating Quantifiers

- What is the negation of “All students have MA105”?

  There exists a student who does not have MA105.
- $\neg\forall x P(x) \equiv \exists x \neg P(x)$ [1]
  - $\neg\forall x P(x)$ is true iff $\forall x P(x)$ is false
  - $\forall x P(x)$ is false iff there is some x s.t. $\neg P(x)$ is true.
  - i.e., $\exists x \neg P(x)$.
- $\neg\exists x P(x) \equiv \forall x \neg P(x)$

Exercises

1. What is the negation of $\forall x (x^2 > x)$? $\exists x (x^2 \leq x)$
2. Show that $\neg\forall x (P(x) \to Q(x)) \equiv \exists x (P(x) \wedge \neg Q(x))$.

[1] $\equiv$ stands for “is logically equivalent to”.

A bit more about quantifiers

Negating Quantifiers

- What is the negation of "All students have MA105"?

  There exists a student who does not have MA105.
- $\neg\forall x P(x) \equiv \exists x \neg P(x)$ [1]
  - $\neg\forall x P(x)$ is true iff $\forall x P(x)$ is false
  - $\forall x P(x)$ is false iff there is some x s.t. $\neg P(x)$ is true.
  - i.e., $\exists x \neg P(x)$.
- $\neg\exists x P(x) \equiv \forall x \neg P(x)$

Exercises

1. What is the negation of $\forall x(x^2 > x)$? $\exists x(x^2 \leq x)$
2. Show that $\neg\forall x(P(x) \rightarrow Q(x)) \equiv \exists x(P(x) \wedge \neg Q(x))$.
3. Use predicates and quantifiers to say "Every email larger than 10MB will be compressed."

[1] $\equiv$ stands for "is logically equivalent to".

A bit more about quantifiers

Negating Quantifiers

- What is the negation of "All students have MA105"?

  There exists a student who does not have MA105.
- $\neg \forall x P(x) \equiv \exists x \neg P(x)$ [1]
  - $\neg \forall x P(x)$ is true iff $\forall x P(x)$ is false
  - $\forall x P(x)$ is false iff there is some x s.t. $\neg P(x)$ is true.
  - i.e., $\exists x \neg P(x)$.
- $\neg \exists x P(x) \equiv \forall x \neg P(x)$

Exercises

1. What is the negation of $\forall x (x^2 > x)$? $\exists x (x^2 \leq x)$
2. Show that $\neg \forall x (P(x) \rightarrow Q(x)) \equiv \exists x (P(x) \wedge \neg Q(x))$.
3. Use predicates and quantifiers to say "Every email larger than 10MB will be compressed."$\forall M (S(M, 10) \rightarrow C(M))$

---

[1] $\equiv$ stands for "is logically equivalent to".

Theorems and proofs

A theorem is a proposition which can be shown true

Classwork: Prove the following theorems.

1. $\neg(p \wedge q)$ is logically equivalent to $\neg p \vee \neg q$
2. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.
3. If 6 is prime, then $6^2 = 30$.
4. For all $x \in \mathbb{Z}$, x is an even iff $x + x^2 - x^3$ is even.

Theorems and proofs

A theorem is a proposition which can be shown true

Classwork: Prove the following theorems.

1. $\neg(p \wedge q)$ is logically equivalent to $\neg p \vee \neg q$
2. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.
3. If 6 is prime, then $6^2 = 30$.
4. For all $x \in \mathbb{Z}$, x is an even iff $x + x^2 - x^3$ is even.

5. There are infinitely many prime numbers.
6. There exist irrational numbers x, y such that x^y is rational.
7. For all $n \in \mathbb{N}$, $n! \leq n^n$.
8. There does not exist a program which will always determine whether an arbitrary (input-free) program will halt.

Theorems and proofs

Contrapositive and converse

- The contrapositive of "if A then B" is "if $\neg B$ then $\neg A$".

Theorems and proofs

Contraposite and converse

- The contrapositive of "if A then B" is "if $\neg B$ then $\neg A$".
- A statement is logically equivalent to its contrapositive, i.e., it suffices to show one to imply the other.

Theorems and proofs

Contraposive and converse

- The contrapositive of "if A then B" is "if $\neg B$ then $\neg A$".
- A statement is logically equivalent to its contrapositive, i.e., it suffices to show one to imply the other.
- i.e., $p \to q$ is logically equivalent to $\neg q \to \neg p$ (check this!)

Theorems and proofs

Contrapositive and converse

- The contrapositive of "if A then B" is "if $\neg B$ then $\neg A$".
- A statement is logically equivalent to its contrapositive, i.e., it suffices to show one to imply the other.
- i.e., $p \to q$ is logically equivalent to $\neg q \to \neg p$ (check this!)
- The converse of "if A then B" is "if B then A".

Theorems and proofs

Contrapositive and converse

- The contrapositive of "if A then B" is "if $\neg B$ then $\neg A$".
- A statement is logically equivalent to its contrapositive, i.e., it suffices to show one to imply the other.
- i.e., $p \to q$ is logically equivalent to $\neg q \to \neg p$ (check this!)
- The converse of "if A then B" is "if B then A".
- Common mistake: Contrapositive not the same as converse!

Theorems and proofs

Contrapositive and converse

- The contrapositive of "if A then B" is "if $\neg B$ then $\neg A$".
- A statement is logically equivalent to its contrapositive, i.e., it suffices to show one to imply the other.
- i.e., $p \to q$ is logically equivalent to $\neg q \to \neg p$ (check this!)
- The converse of "if A then B" is "if B then A".
- Common mistake: Contrapositive not the same as converse!

To show "A iff B", you must show two things:

1. A implies B and
2. its converse, B implies A

Theorems and proofs

Contrapositive and converse

- The contrapositive of "if A then B" is "if $\neg B$ then $\neg A$".
- A statement is logically equivalent to its contrapositive, i.e., it suffices to show one to imply the other.
- i.e., $p \rightarrow q$ is logically equivalent to $\neg q \rightarrow \neg p$ (check this!)
- The converse of "if A then B" is "if B then A".
- Common mistake: Contrapositive not the same as converse!

To show "A iff B", you must show two things:

1. A implies B and
2. its converse, B implies A OR $\neg A$ implies $\neg B$.

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Two directions.

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Two directions.

- Forward direction ($\Longrightarrow$)

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Two directions.

- Forward direction ($\implies$)
  1. Let $x \in \mathbb{Z}$ and x even.

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Two directions.

- Forward direction ($\implies$)
  1. Let $x \in \mathbb{Z}$ and x even.
  2. i.e., $x = 2k$ for some $k \in \mathbb{Z}$.

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Two directions.

- Forward direction ($\implies$)
  1. Let $x \in \mathbb{Z}$ and x even.
  2. i.e., $x = 2k$ for some $k \in \mathbb{Z}$.
  3. Then $x + x^2 - x^3 = 2k + 4k^2 - 8k^3 = 2(k + 2k^2 - 4k^3)$ which is even.

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Two directions.

- Forward direction ($\implies$)
  1. Let $x \in \mathbb{Z}$ and x even.
  2. i.e., $x = 2k$ for some $k \in \mathbb{Z}$.
  3. Then $x + x^2 - x^3 = 2k + 4k^2 - 8k^3 = 2(k + 2k^2 - 4k^3)$ which is even.
- Reverse direction ($\impliedby$)

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Two directions.

- Forward direction ($\implies$)
  1. Let $x \in \mathbb{Z}$ and x even.
  2. i.e., $x = 2k$ for some $k \in \mathbb{Z}$.
  3. Then $x + x^2 - x^3 = 2k + 4k^2 - 8k^3 = 2(k + 2k^2 - 4k^3)$ which is even.
- Reverse direction ($\impliedby$)
  1. We will show contrapositive!

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Two directions.

- Forward direction ($\implies$)
  1. Let $x \in \mathbb{Z}$ and x even.
  2. i.e., $x = 2k$ for some $k \in \mathbb{Z}$.
  3. Then $x + x^2 - x^3 = 2k + 4k^2 - 8k^3 = 2(k + 2k^2 - 4k^3)$ which is even.
- Reverse direction ($\impliedby$)
  1. We will show contrapositive! i.e., x is not even $\implies$ $x + x^2 - x^3$ is not even, i.e., x is odd $\implies$ $x + x^2 - x^3$ is odd.

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Two directions.

- Forward direction ($\implies$)
  1. Let $x \in \mathbb{Z}$ and x even.
  2. i.e., $x = 2k$ for some $k \in \mathbb{Z}$.
  3. Then $x + x^2 - x^3 = 2k + 4k^2 - 8k^3 = 2(k + 2k^2 - 4k^3)$ which is even.
- Reverse direction ($\impliedby$)
  1. We will show contrapositive! i.e., x is not even $\implies$ $x + x^2 - x^3$ is not even, i.e., x is odd $\implies$ $x + x^2 - x^3$ is odd.
  2. Let $x \in \mathbb{Z}$ be odd, i.e., $x = 2k + 1$ for some $k \in \mathbb{Z}$.

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Two directions.

- Forward direction ($\implies$)
  1. Let $x \in \mathbb{Z}$ and x even.
  2. i.e., $x = 2k$ for some $k \in \mathbb{Z}$.
  3. Then $x + x^2 - x^3 = 2k + 4k^2 - 8k^3 = 2(k + 2k^2 - 4k^3)$ which is even.
- Reverse direction ($\impliedby$)
  1. We will show contrapositive! i.e., x is not even $\implies$ $x + x^2 - x^3$ is not even, i.e., x is odd $\implies$ $x + x^2 - x^3$ is odd.
  2. Let $x \in \mathbb{Z}$ be odd, i.e., $x = 2k + 1$ for some $k \in \mathbb{Z}$.
  3. Then $x + x^2 - x^3$ is odd! (check this!).

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Two directions.

- Forward direction ($\implies$)
  1. Let $x \in \mathbb{Z}$ and x even.
  2. i.e., $x = 2k$ for some $k \in \mathbb{Z}$.
  3. Then $x + x^2 - x^3 = 2k + 4k^2 - 8k^3 = 2(k + 2k^2 - 4k^3)$ which is even.
- Reverse direction ($\impliedby$)
  1. We will show contrapositive! i.e., x is not even $\implies$ $x + x^2 - x^3$ is not even, i.e., x is odd $\implies$ $x + x^2 - x^3$ is odd.
  2. Let $x \in \mathbb{Z}$ be odd, i.e., $x = 2k + 1$ for some $k \in \mathbb{Z}$.
  3. Then $x + x^2 - x^3$ is odd! (check this!). Hence proved.

Proof of Theorem 4

Theorem 4.: For all $x \in \mathbb{Z}$, x is even iff $x + x^2 - x^3$ is even.

Two directions.

- Forward direction ($\implies$)
  1. Let $x \in \mathbb{Z}$ and x even.
  2. i.e., $x = 2k$ for some $k \in \mathbb{Z}$.
  3. Then $x + x^2 - x^3 = 2k + 4k^2 - 8k^3 = 2(k + 2k^2 - 4k^3)$ which is even.
- Reverse direction ($\impliedby$)
  1. We will show contrapositive! i.e., x is not even $\implies$ $x + x^2 - x^3$ is not even, i.e., x is odd $\implies$ $x + x^2 - x^3$ is odd.
  2. Let $x \in \mathbb{Z}$ be odd, i.e., $x = 2k + 1$ for some $k \in \mathbb{Z}$.
  3. Then $x + x^2 - x^3$ is odd! (check this!). Hence proved.

$\square$

Proof by contradiction

Theorem 5.: There are infinitely many primes.

Proof by contradiction:

Proof by contradiction

Theorem 5.: There are infinitely many primes.

Proof by contradiction:

1. Suppose there are only finitely many primes, say $p_1 < p_2 < \ldots < p_r$.

Proof by contradiction

Theorem 5.: There are infinitely many primes.

Proof by contradiction:

1. Suppose there are only finitely many primes, say $p_1 < p_2 < \ldots < p_r$.
2. Let $k = (p_1 * p_2 * \ldots * p_r) + 1$.
3. Then k when divided by any p_i has remainder 1. So none of the p_i's divide k.

Proof by contradiction

Theorem 5.: There are infinitely many primes.

Proof by contradiction:

1. Suppose there are only finitely many primes, say $p_1 < p_2 < \ldots < p_r$.
2. Let $k = (p_1 * p_2 * \ldots * p_r) + 1$.
3. Then k when divided by any p_i has remainder 1. So none of the p_i's divide k.
4. But $k > 1$ and k is not prime (since $k > p_r$), so k can be written as a product of primes (why?)

Proof by contradiction

Theorem 5.: There are infinitely many primes.

Proof by contradiction:

1. Suppose there are only finitely many primes, say $p_1 < p_2 < \ldots < p_r$.
2. Let $k = (p_1 * p_2 * \ldots * p_r) + 1$.
3. Then k when divided by any p_i has remainder 1. So none of the p_i's divide k.
4. But $k > 1$ and k is not prime (since $k > p_r$), so k can be written as a product of primes (why?)
   - Fundamental theorem of arithmetic: any natural number > 1 can be written as a (unique) product of primes.

Proof by contradiction

Theorem 5.: There are infinitely many primes.

Proof by contradiction:

1. Suppose there are only finitely many primes, say $p_1 < p_2 < \ldots < p_r$.
2. Let $k = (p_1 * p_2 * \ldots * p_r) + 1$.
3. Then k when divided by any p_i has remainder 1. So none of the p_i's divide k.
4. But $k > 1$ and k is not prime (since $k > p_r$), so k can be written as a product of primes (why?)
   - Fundamental theorem of arithmetic: any natural number > 1 can be written as a (unique) product of primes.
5. Now take any prime p in this product, then, p divides k. So, by 3. above, $p \notin \{p_1, \ldots, p_r\}$.
6. This contradicts 1. since we had assumed that $\{p_1, \ldots p_r\}$ was the set of all primes.

Proof by contradiction

Theorem 5.: There are infinitely many primes.

Proof by contradiction:

1. Suppose there are only finitely many primes, say $p_1 < p_2 < \ldots < p_r$.
2. Let $k = (p_1 * p_2 * \ldots * p_r) + 1$.
3. Then k when divided by any p_i has remainder 1. So none of the p_i's divide k.
4. But $k > 1$ and k is not prime (since $k > p_r$), so k can be written as a product of primes (why?)
   - Fundamental theorem of arithmetic: any natural number > 1 can be written as a (unique) product of primes.
5. Now take any prime p in this product, then, p divides k. So, by 3. above, $p \notin \{p_1, \ldots, p_r\}$.
6. This contradicts 1. since we had assumed that $\{p_1, \ldots p_r\}$ was the set of all primes. $\square$

A Non-constructive proof

Theorem 6.: There exist irrational numbers x and y such that x^y is rational.

A Non-constructive proof

Theorem 6.: There exist irrational numbers x and y such that x^y is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.

A Non-constructive proof

Theorem 6.: There exist irrational numbers x and y such that x^y is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.
- Let $x = y = \sqrt{2}$ and consider $z = \sqrt{2}^{\sqrt{2}}$.
- Case 1: If z is rational, we are done (why?)

A Non-constructive proof

Theorem 6.: There exist irrational numbers x and y such that x^y is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.
- Let $x = y = \sqrt{2}$ and consider $z = \sqrt{2}^{\sqrt{2}}$.
- Case 1: If z is rational, we are done (why?)
- Case 2: Else z is irrational.

A Non-constructive proof

Theorem 6.: There exist irrational numbers x and y such that x^y is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.
- Let $x = y = \sqrt{2}$ and consider $z = \sqrt{2}^{\sqrt{2}}$.
- Case 1: If z is rational, we are done (why?)
- Case 2: Else z is irrational.
  - Then consider $z^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$.

A Non-constructive proof

Theorem 6.: There exist irrational numbers x and y such that x^y is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.
- Let $x = y = \sqrt{2}$ and consider $z = \sqrt{2}^{\sqrt{2}}$.
- Case 1: If z is rational, we are done (why?)
- Case 2: Else z is irrational.
  - Then consider $z^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$.
  - Thus we have found two irrationals $x = z = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$ such that $x^y = 2$ is rational. $\square$

A Non-constructive proof

Theorem 6.: There exist irrational numbers x and y such that x^y is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.
- Let $x = y = \sqrt{2}$ and consider $z = \sqrt{2}^{\sqrt{2}}$.
- Case 1: If z is rational, we are done (why?)
- Case 2: Else z is irrational.
  - Then consider $z^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$.
  - Thus we have found two irrationals $x = z = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$ such that $x^y = 2$ is rational. $\square$

Indeed, note that the above proof is not constructive!

A Non-constructive proof

Theorem 6.: There exist irrational numbers x and y such that x^y is rational.

Proof:

- Consider $\sqrt{2}$. First show that $\sqrt{2}$ is irrational.
- Let $x = y = \sqrt{2}$ and consider $z = \sqrt{2}^{\sqrt{2}}$.
- Case 1: If z is rational, we are done (why?)
- Case 2: Else z is irrational.
  - Then consider $z^{\sqrt{2}} = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$.
  - Thus we have found two irrationals $x = z = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$ such that $x^y = 2$ is rational. $\square$

Indeed, note that the above proof is not constructive!

(H.W): Post a constructive proof of this theorem on piazza.

Types of proofs

1. $\neg(p \wedge q)$ is logically equivalent to $\neg p \vee \neg q$
2. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.
3. If 6 is prime, then $6^2 = 30$.
4. x is an even integer iff $x + x^2 - x^3$ is even.
5. There are infinitely many prime numbers.
6. There exist irrational numbers x, y such that x^y is rational.
7. For all $n \in \mathbb{N}$, $n! \leq n^n$.
8. There does not exist a (input-free) program which will always determine whether an arbitrary (input-free) program will halt.

Types of proofs

1. $\neg(p \wedge q)$ is logically equivalent to $\neg p \vee \neg q$

   – By truth tables
2. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.

   – Direct proof
3. If 6 is prime, then $6^2 = 30$. – Vacuous/trivial proof
4. x is an even integer iff $x + x^2 - x^3$ is even.

   – Both directions, by contrapositive ($A \to B = \neg B \to \neg A$)
5. There are infinitely many prime numbers.

   – Proof by contradiction
6. There exist irrational numbers x, y such that x^y is rational.

   – Non-constructive proof
7. For all $n \in \mathbb{N}$, $n! \leq n^n$.
8. There does not exist a (input-free) program which will always determine whether an arbitrary (input-free) program will halt.

Types of proofs

1. $\neg(p \wedge q)$ is logically equivalent to $\neg p \vee \neg q$

   – By truth tables

2. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.

   – Direct proof

3. If 6 is prime, then $6^2 = 30$. – Vacuous/trivial proof

4. x is an even integer iff $x + x^2 - x^3$ is even.

   – Both directions, by contrapositive $(A \to B = \neg B \to \neg A)$

5. There are infinitely many prime numbers.

   – Proof by contradiction

6. There exist irrational numbers x, y such that x^y is rational.

   – Non-constructive proof

7. For all $n \in \mathbb{N}$, $n! \leq n^n$. – next!

8. There does not exist a (input-free) program which will always determine whether an arbitrary (input-free) program will halt.