Matemática Discreta

Escola de Artes, Ciências e Humanidades - USP
Profa Dra. Karla Lima
email:ksampaiolima@usp.br

Matemática Discreta

Ementa da disciplina:

- 1 - O que é uma prova?
  - Proposições
  - Axiomas
  - Deduções Lógicas
  - Exemplos de provas

- 2 - Indução Simples

- 3 – Indução Forte

- Trabalho 1

Matemática Discreta

Ementa da disciplina:

- 4 – Teoria dos Números I
  - Divisibilidade
  - Aritmetica Modular

- 5 – Teoria dos Números II
  - Alguns teoremas

- 6 – Relações

- Trabalho 2

Matemática Discreta

Ementa da disciplina:

- 7 – Somatórios, Aproximações e Assintótica

- 8 - Recorrências

- Trabalho 3

- Prova Final

Matemática Discreta

Avaliação e Bibliografia:

- Trabalhos + Avaliação Final

- Bibliografia

- Mathematics for Computer Science, Eric Lehman and Tom Leighton, 2004

Matemática Discreta

What is a Proof?

Matemática Discreta

What is a Proof?

Jury trial. Truth is ascertained by twelve people selected at random.

Word of God. Truth is ascertained by communication with God, perhaps via a third party.

Experimental science. The truth is guessed and the hypothesis is confirmed or refuted by experiments.

Inner conviction. "*My* program is perfect. I know this to be true."

Matemática Discreta

What is a Proof?

Mathematics its own notion of "proof". In mathematics, a *proof* is a verification of a *proposition* by a chain of *logical deductions* from a base set of *axioms*.

Matemática Discreta

1.1 Propositions

A *proposition* is a statement that is either true or false.

Matemática Discreta

1.1 Propositions

A *proposition* is a statement that is either true or false.

Proposition 1. $2 + 3 = 5$

Matemática Discreta

1.1 Propositions

A *proposition* is a statement that is either true or false.

Proposition 1. $2 + 3 = 5$

Proposition 2. $\forall\, n \in \mathbb{N} \quad n^2 + n + 41$ *is a prime number.*

Matemática Discreta

1.1 Propositions

Proposition 2. $\forall\, n \in \mathbb{N} \quad n^2 + n + 41$ *is a prime number.*

$$\text{“}n^2 + n + 41 \text{ is a prime number”}$$

Matemática Discreta

1.1 Propositions

Proposition 2. *$\forall\, n \in \mathbb{N} \quad n^2 + n + 41$ is a prime number.*

$$\text{“}n^2 + n + 41 \text{ is a prime number”}$$

n	$n^2 + n + 41$	prime or composite?
0	41	prime
1	43	prime
2	47	prime
3	53	prime
...	...	(all prime)
20	461	prime
39	1601	prime

Matemática Discreta

1.1 Propositions

Proposition 2. $\forall\, n \in \mathbb{N} \quad n^2 + n + 41$ *is a prime number.*

$\mathbf{n}$	$\mathbf{n^2 + n + 41}$	**prime or composite?**
0	41	prime
1	43	prime
2	47	prime
3	53	prime
$\ldots$	$\ldots$	(all prime)
20	461	prime
39	1601	prime

when $n = 40$, we get $n^2 + n + 41 = 40^2 + 40 + 41 = 41 \cdot 41$, which is not prime.

Matemática Discreta

1.1 Propositions

Proposition 3. $a^4 + b^4 + c^4 = d^4$ *has no solution when* $a, b, c, d \in \mathbb{N}^+$.

Matemática Discreta

1.1 Propositions

Proposition 3. $a^4 + b^4 + c^4 = d^4$ *has no solution when* $a, b, c, d \in \mathbb{N}^+$.

Here $\mathbb{N}^+$ denotes the *positive* natural numbers, $\{1, 2, 3, \ldots\}$. In 1769, Euler conjectured that this proposition was true. But the it was proven false 218 years later by Noam Elkies at the liberal arts school up Mass Ave. He found the solution $a = 95800, b = 217519, c = 414560, d = 422481$. We could write his assertion symbolically as follows:

Matemática Discreta

1.1 Propositions

Proposition 3. $a^4 + b^4 + c^4 = d^4$ *has no solution when* $a, b, c, d \in \mathbb{N}^+$.

Here $\mathbb{N}^+$ denotes the *positive* natural numbers, $\{1, 2, 3, \ldots\}$. In 1769, Euler conjectured that this proposition was true. But the it was proven false 218 years later by Noam Elkies at the liberal arts school up Mass Ave. He found the solution $a = 95800, b = 217519, c = 414560, d = 422481$. We could write his assertion symbolically as follows:

$$\exists\, a, b, c, d \in \mathbb{N}^+ \quad a^4 + b^4 + c^4 = d^4$$

Matemática Discreta

1.1 Propositions

Proposition 4. *$313(x^3 + y^3) = z^3$ has no solution when $x, y, z \in \mathbb{N}^+$.*

Matemática Discreta

1.1 Propositions

Proposition 4. $313(x^3 + y^3) = z^3$ *has no solution when* $x, y, z \in \mathbb{N}^+$.

This proposition is also false, but the smallest counterexample has more than 1000 digits. This counterexample could never have been found by a brute-force computer search!

Matemática Discreta

1.1 Propositions

Proposition 4. $313(x^3 + y^3) = z^3$ *has no solution when* $x, y, z \in \mathbb{N}^+$.

This proposition is also false, but the smallest counterexample has more than 1000 digits. This counterexample could never have been found by a brute-force computer search!

The symbols $\forall$ ("for all") and $\exists$ ("there exists") are called *quantifiers*.

Matemática Discreta

1.1 Propositions

Proposition 7. $\forall\, n \in \mathbb{Z} \quad (n \geq 2) \Rightarrow (n^2 \geq 4)$

Matemática Discreta

1.1 Propositions

Proposition 7. $\forall\, n \in \mathbb{Z} \quad (n \geq 2) \Rightarrow (n^2 \geq 4)$

This is an example of an *implication*, a proposition of the form $P \Rightarrow Q$.

Matemática Discreta

1.1 Propositions

Proposition 7. $\forall\, n \in \mathbb{Z} \quad (n \geq 2) \Rightarrow (n^2 \geq 4)$

This is an example of an *implication*, a proposition of the form $P \Rightarrow Q$.

the implication $P \Rightarrow Q$ is true when P is

false or Q is true.

Matemática Discreta

1.1 Propositions

Proposition 7. $\forall\, n \in \mathbb{Z} \quad (n \geq 2) \Rightarrow (n^2 \geq 4)$

This is an example of an *implication*, a proposition of the form $P \Rightarrow Q$.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Matemática Discreta

1.1 Propositions

"If pigs fly, then you will understand the Chernoff Bound."

Matemática Discreta

1.1 Propositions

“If pigs fly, then you will understand the Chernoff Bound.”

This is an example of an *implication*, a proposition of the form $P \Rightarrow Q$.

Matemática Discreta

1.1 Propositions

"If pigs fly, then you will understand the Chernoff Bound."

This is an example of an *implication*, a proposition of the form $P \Rightarrow Q$.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Matemática Discreta

1.1 Propositions

Proposition 8. $\forall\, n \in \mathbb{Z} \quad (n \geq 2) \Leftrightarrow (n^2 \geq 4)$

A proposition of the form $P \Leftrightarrow Q$ is read "P if and only if Q".

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Matemática Discreta

1.1 Propositions

Proposition 8. $\forall\, n \in \mathbb{Z} \quad (n \geq 2) \Leftrightarrow (n^2 \geq 4)$

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

$n = 3$ $\qquad$ $n = 1$ $\qquad$ $n = -3$

Matemática Discreta

1.2 Axioms

An *axiom* is a proposition that is assumed to be true, because you believe it is somehow reasonable. Here are some examples:

Axiom 1. *If* $a = b$ *and* $b = c$*, then* $a = c$.

Matemática Discreta

1.2 Axioms

An *axiom* is a proposition that is assumed to be true, because you believe it is somehow reasonable. Here are some examples:

A set of axioms is *consistent* if no proposition can be proved both true and false.

Matemática Discreta

1.2 Axioms

An *axiom* is a proposition that is assumed to be true, because you believe it is somehow reasonable. Here are some examples:

A set of axioms is *consistent* if no proposition can be proved both true and false.

A set of axioms is *complete* if every proposition can be proved or disproved.

Matemática Discreta

1.3 Logical Deductions

Logical deductions or *inference rules* are used to combine axioms and true propositions in order to form more true propositions.

One fundamental inference rule is *modus ponens*. This rule says that if P is true and $P \Rightarrow Q$ is true, then Q is also true. Inference rules are sometimes written in a funny notation. For example, modus ponens is written:

Matemática Discreta

1.3 Logical Deductions

Logical deductions or *inference rules* are used to combine axioms and true propositions in order to form more true propositions.

One fundamental inference rule is *modus ponens*. This rule says that if P is true and $P \Rightarrow Q$ is true, then Q is also true. Inference rules are sometimes written in a funny notation. For example, modus ponens is written:

$$\frac{\begin{array}{c} P \\ P \Rightarrow Q \end{array}}{Q}$$

Matemática Discreta

1.3 Logical Deductions

Logical deductions or *inference rules* are used to combine axioms and true propositions in order to form more true propositions.

One fundamental inference rule is *modus ponens*. This rule says that if P is true and $P \Rightarrow Q$ is true, then Q is also true. Inference rules are sometimes written in a funny notation. For example, modus ponens is written:

$$\frac{\begin{array}{c} P \\ P \Rightarrow Q \end{array}}{Q}$$

Matemática Discreta

1.3 Logical Deductions

Modus ponens is closely related to the proposition

$$(P \wedge (P \Rightarrow Q)) \Rightarrow Q.$$

"if P and $P \Rightarrow Q$ are true, then Q is true"

tautology,

Matemática Discreta

1.3 Logical Deductions

$((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$ and $((P \Rightarrow Q) \wedge \neg Q) \Rightarrow \neg P$

$$\begin{array}{c} P \Rightarrow Q \\ Q \Rightarrow R \\ \hline P \Rightarrow R \end{array} \qquad\qquad \begin{array}{c} P \Rightarrow Q \\ \neg Q \\ \hline \neg P \end{array}$$

Matemática Discreta

1.4 Examples of Proofs

1.4.1 A Tautology

Theorem 9. *The following proposition is a tautology:*

$$(X \Rightarrow Y) \quad \Leftrightarrow \quad (\neg Y \Rightarrow \neg X)$$

Matemática Discreta

1.4 Examples of Proofs

1.4.1 A Tautology

Theorem 9. *The following proposition is a tautology:*

$$(X \Rightarrow Y) \quad \Leftrightarrow \quad (\neg Y \Rightarrow \neg X)$$

"If you are wise, then you attend recitation."

Matemática Discreta

1.4 Examples of Proofs

1.4.1 A Tautology

Theorem 9. *The following proposition is a tautology:*

$$(X \Rightarrow Y) \quad \Leftrightarrow \quad (\neg Y \Rightarrow \neg X)$$

"If you are wise, then you attend recitation."

"If you do not attend recitation, then you are not wise."

Matemática Discreta

1.4 Examples of Proofs

1.4.1 A Tautology

Theorem 9. *The following proposition is a tautology:*

$$(X \Rightarrow Y) \quad \Leftrightarrow \quad (\neg Y \Rightarrow \neg X)$$

Proof. We show that the left side is logically equivalent to the right side for every setting of the variables X and Y.

Matemática Discreta

1.4 Examples of Proofs

1.4.1 A Tautology

Theorem 9. *The following proposition is a tautology:*

$$(X \Rightarrow Y) \quad \Leftrightarrow \quad (\neg Y \Rightarrow \neg X)$$

X	Y	$X \Rightarrow Y$	$\neg Y \Rightarrow \neg X$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Matemática Discreta

1.4 Examples of Proofs

1.4.1 A Tautology

Theorem 9. *The following proposition is a tautology:*

$$(X \Rightarrow Y) \quad \Leftrightarrow \quad (\neg Y \Rightarrow \neg X)$$

$$\frac{P \Rightarrow Q}{\neg Q \Rightarrow \neg P} \qquad\qquad \frac{\neg Q \Rightarrow \neg P}{P \Rightarrow Q}$$

Matemática Discreta

1.4 Examples of Proofs

1.4.2 A Proof by Contradiction

In logical terms, indirect proof relies on the following inference rule:

$$\frac{\neg P \Rightarrow \text{false}}{P}$$

Matemática Discreta

1.4 Examples of Proofs

1.4.2 A Proof by Contradiction

In logical terms, indirect proof relies on the following inference rule:

$$\frac{\neg P \Rightarrow \text{false}}{P}$$

tautology

P	$(\neg P \Rightarrow \text{false}) \Rightarrow P$
T	T
F	T

Matemática Discreta

1.4 Examples of Proofs

1.4.2 A Proof by Contradiction

Theorem 10. *$\sqrt{2}$ is an irrational number.*