Lógica Aplicada à Computação

Prof. Vivek Nigam Aula 2 – História da Lógica

Um pequeno teste de lógica

Um **escravo**, por desobediência foi aprisionado e condenado à morte. O **senhor** resolveu ser gentil com escravo e disse-lhe: Deixo-te escolher a maneira como vai morrer. Se disseres uma frase verdadeira, serás decapitado. Se disseres uma frase falsa, serás enforcado.

O **escravo** disse –"Vou morrer enforcado." Com esta afirmação o escravo escapou da morte. Por que?

O que veremos hoje

- A história da lógica;
- Entender a importância da lógica para a computação;
 - "Lógica esta para a Computação como o Cálculo para a Matemática." (M. Vardi)
- Revisão de Conceitos Elementares da Matemática (Parte I);

Conjuntos

Agenda

História da Lógica

- Primeira Era: Lógica Simbólica;
- Segunda Era: Lógica Algebraica;
- Terceira Era: Lógica Matemática;
- Quarta Era: Lógica Computacional.
- Revisão de Conceitos Elementares da Matemática

A palavra *trivial* se refere à palavra *trivium* que por sua vez se refere ao currículo fundamental:

A palavra *trivial* se refere à palavra *trivium* que por sua vez se refere ao currículo fundamental:

- Gramática
- Retórica
- Lógica

A palavra *trivial* se refere à palavra *trivium* que por sua vez se refere ao currículo fundamental:

- Gramática
- Retórica
- Lógica

Para dominar outras matérias, como a **aritimética**, precisa-se primeiro dominar as matérias acima.

O que é lógica?

O que é lógica?

Várias definições:

- A habilidade de determinar argumentos corretos sistematicamente;
- Lógica é o estudo das inferências (raciocínios) válidas;
- Uma sequência de argumentos que podem ser verificados;
- Raciocínio ao contrário de intuição;
- A dedução de afirmações a partir de um conjunto de afirmações.

O que é lógica?

Várias definições:

- A habilidade de determinar argumentos corretos sistematicamente;
- Lógica é o estudo das inferências (raciocínios) válidas;
- Uma sequência de argumentos que podem ser verificados;
- Raciocínio ao contrário de intuição;
- A dedução de afirmações a partir de um conjunto de afirmações.

Inicialmente usada pelos Sofistas em debates formais para saber quem ganhou um argumento sem a menor dúvida.

Retórica versus Lógica

Agenda

- História da Lógica
 - Primeira Era: Lógica Simbólica;
 - Segunda Era: Lógica Algébrica;
 - Terceira Era: Lógica Matemática;
 - Quarta Era: Lógica Computacional.
- Revisão de Conceitos Elementares da Matemática

Uso da linguagem natural (Grego, Português, Inglês, etc)

Uso da linguagem natural (Grego, Português, Inglês, etc)

Todos os homens são mortais.

Socrates é um homen.

Portanto Socrates é mortal.

Uso da linguagem natural (Grego, Português, Inglês, etc)

Todos os homens são mortais.

Socrates é um homen.

Portanto Socrates é mortal.

Problema: Linguagens naturais são ambíguas!

Fernando viu Maria usando óculos escuros.

Uso da linguagem natural (Grego, Português, Inglês, etc)

Todos os homens são mortais.

Socrates é um homen.

Portanto Socrates é mortal.

Problema: Linguagens naturais são ambíguas!

Fernando viu Maria usando óculos escuros.

Paradoxo: Esta sentença é falsa.

Descoberta de Provas Matemáticas – Método Axiomático

Descoberta de Provas Matemáticas – Método Axiomático

Euclides na sua obra Elementos descreve como deduzir teoremas sobre a geometria a partir de axiomas.

Estes axiomas são basicamente os mesmo usados até agora: Geometria Euclidiana.

Agenda

- História da Lógica
 - Primeira Era: Lógica Simbólica;
 - Segunda Era: Lógica Algebraica;
 - Terceira Era: Lógica Matemática;
 - Quarta Era: Lógica Computacional.
- Revisão de Conceitos Elementares da Matemática

George Boole (1847) tentou formalizar argumentos lógicos usando conceitos vindos da algebra:

$$a * (b + c) = a * b + a * c$$

$$a \cap (b \cup c) = a \cap b \cup a \cap c$$

George Boole (1847) tentou formalizar argumentos lógicos usando conceitos vindos da algebra:

$$a*(b+c) = a*b+a*c \qquad \qquad a\cap(b\cup c) = a\cap b\cup a\cap c$$

Boole formalizou várias regras de inferência usando somente simbolos matemáticos assim como feito na algebra.

Origem da Lógica Booleana: Usada na Eng. Eletrônica no desenho de circuitos eletrônicos.

George Boole (1847) tentou formalizar argumentos lógicos usando conceitos vindos da algebra:

$$a*(b+c) = a*b+a*c \qquad \qquad a\cap(b\cup c) = a\cap b\cup a\cap c$$

Boole formalizou várias regras de inferência usando somente simbolos matemáticos assim como feito na algebra.

Origem da Lógica Booleana: Usada na Eng. Eletrônica no desenho de circuitos eletrônicos.

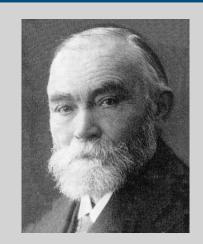
Problema: Boole foi longe demais. Tentou formalizar a divisão algo que não existe em lógica.

Outro Problema: Como formalizar para todos, por exemplo?

Outro Problema: Como formalizar para todos, por exemplo?

Gottlob Frege (1848 – 1925) foi o primeiro a formular *precisamente* a diferença entre variáveis e constantes. Introduziu simbolos para quantificadores:

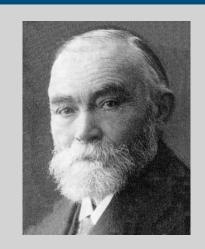
$$\forall x. \exists y. p(x) \Rightarrow q(x, y)$$



Outro Problema: Como formalizar para todos, por exemplo?

Gottlob Frege (1848 – 1925) foi o primeiro a formular *precisamente* a diferença entre variáveis e constantes. Introduziu simbolos para quantificadores:

$$\forall x. \exists y. p(x) \Rightarrow q(x, y)$$

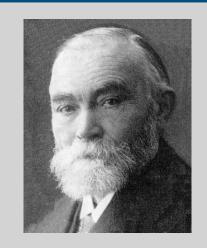


Frege propos utilizar a lógica matemática como uma linguagem da matemática.

Outro Problema: Como formalizar para todos, por exemplo?

Gottlob Frege (1848 – 1925) foi o primeiro a formular *precisamente* a diferença entre variáveis e constantes. Introduziu simbolos para quantificadores:

$$\forall x. \exists y. p(x) \Rightarrow q(x, y)$$



Frege propos utilizar a lógica matemática como uma linguagem da matemática.

A lógica simbólica começou a ajudar a resolver problemas fundamentais da matemática.

Agenda

- História da Lógica
 - Primeira Era: Lógica Simbólica;
 - Segunda Era: Lógica Algébrica;
 - Terceira Era: Lógica Matemática;
 - Quarta Era: Lógica Computacional.
- Revisão de Conceitos Elementares da Matemática

Com o avanço da matemática, novos paradoxos surgiram – assim como no uso de linguagens naturais.

Com o avanço da matemática, novos paradoxos surgiram – assim como no uso de linguagens naturais.

Cauchy provou que para todas sequências infinitas de funções contínuas:

$$f_1(x), f_2(x), f_3(x), \dots$$

a soma:

$$f(x) = \sum_{i=1}^{\infty} f_i(x)$$

também é contínua.

Contudo Abel descobriu um contra-exemplo!

Com o avanço da matemática, novos paradoxos surgiram – assim como no uso de linguagens naturais.

Cauchy provou que para todas sequências infinitas de funções contínuas:

$$f_1(x), f_2(x), f_3(x), \dots$$

a soma:

$$f(x) = \sum_{i=1}^{\infty} f_i(x)$$

também é contínua.

Contudo Abel descobriu um contra-exemplo!

Lógica pode ajudar a resolver essas contradições.

David Hilbert, o mais prominente matemático do seu tempo, propos um programa muito ambicioso para formalizar toda a matemática usando lógica. O seu objetivo foi de acabar de vez todas as contradições na matemática.



David Hilbert, o mais prominente matemático do seu tempo, propos um programa muito ambicioso para formalizar toda a matemática usando lógica. O seu objetivo foi de acabar de vez todas as contradições na matemática.



"Wir müssen wissen, wir werden wissen."

Ele propos 23 problemas os quais ele imaginou ocupariam os matemáticos pelas próximas décadas.

David Hilbert, o mais prominente matemático do seu tempo, propos um programa muito ambicioso para formalizar toda a matemática usando lógica. O seu objetivo foi de acabar de vez todas as contradições na matemática.



"Wir müssen wissen, wir werden wissen."

Ele propos 23 problemas os quais ele imaginou ocupariam os matemáticos pelas próximas décadas.

Entre eles, achar um sistema formal que seja capaz de dizer se uma afirmação é verdadeira ou não.

A Morte do Programa do Hilbert (1931)

A Morte do Programa do Hilbert (1931)



Kurt Gödel

A Morte do Programa do Hilbert (1931)



Kurt Gödel

 Primeiro Teorema de Incompletude: Para todo sistema capaz de modelar a aritmética, não pode ser ao mesmo tempo consistente e completo.

A Morte do Programa do Hilbert (1931)



Kurt Gödel

- Primeiro Teorema de Incompletude: Para todo sistema capaz de modelar a aritmética, não pode ser ao mesmo tempo consistente e completo.
- Segundo Teorema de Incompletude: Para todo sistema capaz de modelar a aritmética, se o sistema inclui uma afirmação sobre sua consistência, então o sistema é inconsistente.

A Morte do Programa do Hilbert (1936)



Alan Turing



Alonzo Church

A Morte do Programa do Hilbert (1936)



Alan Turing



Alonzo Church

 Indecibilidade: Eles mostraram que existem problemas para os quais não existe nenhum algoritmo capaz de resolver!

A Morte do Programa do Hilbert (1936)



Alan Turing



Alonzo Church

 Indecibilidade: Eles mostraram que existem problemas para os quais não existe nenhum algoritmo capaz de resolver!

Ao invés da lógica se tornar a base para toda a matemática, como Hilbert sonhou, se tornou um ramo importante dela.

Agenda

- História da Lógica
 - Primeira Era: Lógica Simbólica;
 - Segunda Era: Lógica Algebraica;
 - Terceira Era: Lógica Matemática;
 - Quarta Era: Lógica Computacional.
- Revisão de Conceitos Elementares da Matemática

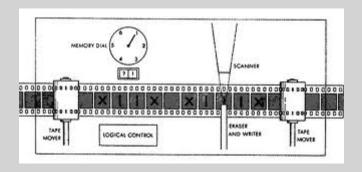


Alan Turing (1912 – 1954): O pai da computação.



Alan Turing (1912 – 1954): O pai da computação.

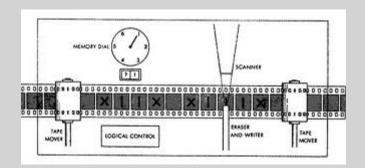
Para provar a existência de problemas indecidíveis, Turing propôs um modelo de uma máquina abstrata capaz de cálcular funções computáveis (Tese de Church-Turing): máquina de Turing.





Alan Turing (1912 – 1954): O pai da computação.

Para provar a existência de problemas indecidíveis, Turing propôs um modelo de uma máquina abstrata capaz de cálcular funções computáveis (Tese de Church-Turing): máquina de Turing.



A influência de Turing é considerável. Ele participou na construção dos primeiros computadores. Ele imaginava que os computadores podem ser tão poderosos capazes de pensar como humanos. (O teste de Turing.) A teoria de complexidade de algoritmos se baseia na noção de máquinas de Turing.

Lógica aparece em todos os lugares da Computação

- Circuitos Booleanos
- Complexidade de algorítmos: NP versus P
- Base de dados: linguagens como SQL
- Especificação e Verificação de Sistemas
- Inteligência Artificial
- Linguagens de Programação
- Segurança

Exercício: Paradoxos

Paradoxo do Barbeiro: Numa pequena cidade do interior vive um barbeiro, muito conhecido dos moradores da cidade, que barbeia todas (e somente aquelas) pessoas moradoras da cidade que não se barbeiam sozinhas. Ora, o barbeiro é um morador da cidade. Coloca-se a questão: quem faz a barba do barbeiro?

Exercício: Paradoxos

Paradoxo do Berry: Proposto em 1906. Existe um número finito de símbolos (letras, sinais de pontuação, etc.) na língua portuguesa. Então, existe um número finito de expressões em nossa língua que contem menos de 200 símbolos, mesmo contando as repetições. Há, portanto, um número finito de inteiros positivos que podem ser denotados por expressões da língua portuguesa que contem menos de 200 símbolos. Agora consideremos a sentença:

"O menor inteiro positivo que não se consegue denotar numa expressão em português com menos de 200 símbolos".

Agenda

- História da Lógica
 - Primeira Era: Lógica Simbólica;
 - Segunda Era: Lógica Algebraica;
 - Terceira Era: Lógica Matemática;
 - Quarta Era: Lógica Computacional.
- Revisão de Conceitos Elementares da Matemática

É um a coleção de elementos.

```
\{a, b, c\}, \mathbb{N} = \{1, 2, 3, 4, \ldots\}, \{azul, vermelho, laranja\}
```

É um a coleção de elementos.

```
\{a, b, c\}, \mathbb{N} = \{1, 2, 3, 4, \ldots\}, \{azul, vermelho, laranja\}
```

A relação x pertence ao conjunto A é escrita como $x \in A$.

```
a \in \{a, b, c\}, \quad 37 \in \mathbb{N}, \quad \text{azul} \in \{\text{azul}, \text{vermelho}, \text{laranja}\}
```

É um a coleção de elementos.

```
\{a, b, c\}, \mathbb{N} = \{1, 2, 3, 4, \ldots\}, \{azul, vermelho, laranja\}
```

A relação x pertence ao conjunto A é escrita como $x \in A$.

```
a \in \{a, b, c\}, \quad 37 \in \mathbb{N}, \quad \text{azul} \in \{\text{azul}, \text{ vermelho}, \text{ laranja}\}
```

A relação x não pertence ao conjunto A é escrita como $x \notin A$.

```
d \notin \{a, b, c\}, -43 \notin \mathbb{N}, \text{ rosa } \notin \{\text{azul, vermelho, laranja}\}
```

É um a coleção de elementos.

```
\{a, b, c\}, \mathbb{N} = \{1, 2, 3, 4, \ldots\}, \{azul, vermelho, laranja\}
```

A relação x pertence ao conjunto A é escrita como $x \in A$.

```
a \in \{a, b, c\}, \quad 37 \in \mathbb{N}, \quad \text{azul} \in \{\text{azul}, \text{ vermelho}, \text{ laranja}\}
```

A relação x não pertence ao conjunto A é escrita como $x \notin A$.

```
d \notin \{a, b, c\}, -43 \notin \mathbb{N}, \text{ rosa } \notin \{\text{azul, vermelho, laranja}\}
```

Um conjunto pode ser membro de um outro conjunto:

$${a,b,c} \in {\{a,b,c\}, \{a,c\}, \{c\}\}}$$

É um a coleção de elementos.

```
\{a, b, c\}, \mathbb{N} = \{1, 2, 3, 4, \ldots\}, \{azul, vermelho, laranja\}
```

A relação x pertence ao conjunto A é escrita como $x \in A$.

```
a \in \{a, b, c\}, \quad 37 \in \mathbb{N}, \quad \text{azul} \in \{\text{azul}, \text{ vermelho}, \text{ laranja}\}
```

A relação x não pertence ao conjunto A é escrita como $x \notin A$.

```
d \notin \{a, b, c\}, -43 \notin \mathbb{N}, \text{ rosa } \notin \{\text{azul, vermelho, laranja}\}
```

Um conjunto pode ser membro de um outro conjunto:

$${a,b,c} \in {\{a,b,c\}, \{a,c\}, \{c\}\}}$$

Notação: Indicamos em geral um conjunto com letras maiúsculas, e.g., A, B, C, ... e elementos com letras minúsculas, e.g., a, b, c, ... A exceção é quando um elemento é um conjunto, neste caso usamos letras maiúsculas.

Existem várias formas de descrever um conjunto:

Existem várias formas de descrever um conjunto:

• Simplesmente escrevendo os seus elementos:

```
\{a,b,c\} – Quando o conjunto é finito.
\{1,2,3,\ldots\} – Quando o conjunto é infinito e é claro qual a sua lei de formação.
```

Existem várias formas de descrever um conjunto:

• Simplesmente escrevendo os seus elementos:

```
\{a,b,c\} – Quando o conjunto é finito.
\{1,2,3,\ldots\} – Quando o conjunto é infinito e é claro qual a sua lei de formação.
```

Explicitando sua propriedade:

```
\{x \mid x \text{ tem a propriedade } P\}
\{x \mid x \in \mathbb{N} \text{ e } x > 10\} = \{11, 12, 13, ...\}
\{x \mid x \text{ \'e divisor inteiro de } 3\} = \{-3, -1, 1, 3\}
```

Alguns conjuntos especiais:

Alguns conjuntos especiais:

• Conjunto unitário: que tem somente um elemento.

```
\{a\} \{\{1,2,3\}\}
```

Alguns conjuntos especiais:

• Conjunto unitário: que tem somente um elemento.

$$\{a\}$$
 $\{\{1,2,3\}\}$

 Conjunto vazio: que n\u00e3o possui nenhum elemento. Duas formas de escrever: {} ou \u00d6.

$$\{x \mid x \neq x\} = \emptyset$$

 $\{x \mid x \text{ \'e impar e m\'ultiplo de } 2\} = \emptyset$

Alguns conjuntos especiais:

• Conjunto unitário: que tem somente um elemento.

$$\{a\}$$
 $\{\{1,2,3\}\}$

 Conjunto vazio: que n\u00e3o possui nenhum elemento. Duas formas de escrever: {} ou \u00d6.

$$\{x \mid x \neq x\} = \emptyset$$
$$\{x \mid x \text{ \'e impar e m\'ultiplo de 2}\} = \emptyset$$

A cardinalidade de um conjunto, escrito |A|, é o número de elementos que ele contém.

Relação Subconjunto: Se A e B são conjuntos, dizemos que A é um subconjunto de B, escrito A ⊆ B se todo o elemento de A é um elemento de B. Escrevemos A ⊂ B se existe um elemento de B que não pertence a A.

Relação Subconjunto: Se A e B são conjuntos, dizemos que A é um subconjunto de B, escrito A ⊆ B se todo o elemento de A é um elemento de B. Escrevemos A ⊂ B se existe um elemento de B que não pertence a A.

$$\{a,b\} \subset \{a,b,c,d\}$$
$$\{a,b\} \subseteq \{a,b,c,d\}$$

Relação Subconjunto: Se A e B são conjuntos, dizemos que A é um subconjunto de B, escrito A ⊆ B se todo o elemento de A é um elemento de B. Escrevemos A ⊂ B se existe um elemento de B que não pertence a A.

$$\{a,b\} \subset \{a,b,c,d\}$$
$$\{a,b\} \subseteq \{a,b,c,d\}$$

• Conjuntos Iguais: Dois conjuntos $A \in B$ são iguais, escrito A = B, se $A \subseteq B \in B \subseteq A$.

$${a,b,c,d} = {a,c,d,b}$$

 ${a,a,b,c,d} = {a,c,d,b}$

Relação Subconjunto: Se A e B são conjuntos, dizemos que A é um subconjunto de B, escrito A ⊆ B se todo o elemento de A é um elemento de B. Escrevemos A ⊂ B se existe um elemento de B que não pertence a A.

$$\{a,b\} \subset \{a,b,c,d\}$$
$$\{a,b\} \subseteq \{a,b,c,d\}$$

• Conjuntos Iguais: Dois conjuntos $A \in B$ são iguais, escrito A = B, se $A \subseteq B \in B \subseteq A$.

$${a,b,c,d} = {a,c,d,b}$$

 ${a,a,b,c,d} = {a,c,d,b}$

Perceba que todos os conjutos contém o conjunto vazio. Quer dizer, a afirmação é sempre verdadeira: $\emptyset \subset A$.

• **União**: Dado dois conjuntos $A \in B$ a sua união, escrito $A \cup B$, é o conjunto contendo os elementos de A ou B ou ambos.

$$A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$$

 $\{a, b, c\} \cup \{a, 1, 2\} = \{a, b, c, 1, 2\}$

• **União**: Dado dois conjuntos $A \in B$ a sua união, escrito $A \cup B$, é o conjunto contendo os elementos de A ou B ou ambos.

$$A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$$

 $\{a, b, c\} \cup \{a, 1, 2\} = \{a, b, c, 1, 2\}$

• Interseção: A interseção de dois conjuntos $A \in B$, escrito $A \cap B$, é o conjunto contendo os elementos que pertencem a A e a B.

$$A \cap B = \{x \mid x \in A \text{ e } x \in B\}$$
$$\{a, b, c\} \cap \{a, 1, 2\} = \{a\}$$
$$\{a, b, c\} \cap \emptyset = \emptyset$$

• **União**: Dado dois conjuntos $A \in B$ a sua união, escrito $A \cup B$, é o conjunto contendo os elementos de A ou B ou ambos.

$$A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$$

 $\{a, b, c\} \cup \{a, 1, 2\} = \{a, b, c, 1, 2\}$

• Interseção: A interseção de dois conjuntos $A \in B$, escrito $A \cap B$, é o conjunto contendo os elementos que pertencem a A e a B.

$$A \cap B = \{x \mid x \in A \text{ e } x \in B\}$$
$$\{a, b, c\} \cap \{a, 1, 2\} = \{a\}$$
$$\{a, b, c\} \cap \emptyset = \emptyset$$

Se o conjunto A é uma coleção de conjuntos, *i.e.*, $A = \{A_1, A_2, \dots, A_n\}$, definimos:

$$\bigcup A = A_1 \cup A_2 \cup \cdots \cup A_n$$
$$\bigcap A = A_1 \cap A_2 \cap \cdots \cap A_n$$

• **Diferença**: A diferença de dois conjuntos $A \in B$, escrito $A \setminus B$ ou A - B, é o conjunto contendo os elementos que pertencem a A mas que não pertencem a B.

$$A \setminus B = \{x \mid x \in A \text{ e } x \notin B\}$$

 $\{a, b, c\} \setminus \{a, 1, 2\} = \{b, c\}$

• **Diferença**: A diferença de dois conjuntos $A \in B$, escrito $A \setminus B$ ou A - B, é o conjunto contendo os elementos que pertencem a A mas que não pertencem a B.

$$A \setminus B = \{x \mid x \in A \text{ e } x \notin B\}$$

 $\{a, b, c\} \setminus \{a, 1, 2\} = \{b, c\}$

• **Produto Cartesiano**: Dado dois conjuntos $A \in B$ o seu produto cartesiano, escrito $A \times B$, é o conjunto:

$$A \times B = \{(x, y) \mid x \in A \in y \in B\}$$
$$\{a, b, c\} \times \{a, 1\} = \{(a, a), (a, 1), (b, a), (b, 1), (c, a), (c, 1)\}$$

• **Diferença**: A diferença de dois conjuntos $A \in B$, escrito $A \setminus B$ ou A - B, é o conjunto contendo os elementos que pertencem a A mas que não pertencem a B.

$$A \setminus B = \{x \mid x \in A \text{ e } x \notin B\}$$

 $\{a, b, c\} \setminus \{a, 1, 2\} = \{b, c\}$

• **Produto Cartesiano**: Dado dois conjuntos $A \in B$ o seu produto cartesiano, escrito $A \times B$, é o conjunto:

$$A \times B = \{(x, y) \mid x \in A \in y \in B\}$$
$$\{a, b, c\} \times \{a, 1\} = \{(a, a), (a, 1), (b, a), (b, 1), (c, a), (c, 1)\}$$

• Conjunto de Partes: O conjunto de partes de um conjunto A, escrito $\mathcal{P}(A)$, é o conjunto contendo todos os subconjuntos de A.

$$\mathcal{P}(A) = \{C \mid C \subseteq A\}$$

$$\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{a, b\}, \{a, c\}, \{a, b, c\}\}$$

Exercício: Conjuntos

Sejam $A = \{1, 2, 4, 8\}$ e $B = \{1, 2, 9, 0\}$

- \bullet $A \cap B$
- \bullet $A \setminus B$
- \bullet $A \cup B$

Para quaisquer conjuntos A, B, C, classifique em verdadeiro ou falso as afirmações abaixo. Tente prová-las ou fornecer um contra-exemplo.

•
$$\emptyset \subseteq (A \cap B)$$

- $\emptyset \subseteq (A \cup B)$
- \bullet $A \in (A \cup B)$
- \bullet $A \subseteq (A \cup B)$

$$\bullet$$
 $(A \cup B) \subseteq A$

$$\bullet$$
 $(A \cap B) \subseteq A$

$$\bullet$$
 $(A \cap B) \subseteq (A \cap B)$

$$\bullet \ (A \cap B \cap C) \subseteq (A \cap B)$$

Seja $A = \{x \mid x \in \mathbb{N} \text{ e } x < 5\}$. Quantos elementos tem $\mathcal{P}(A)$?