Provas e Programas

A influência da Lógica Matemática na Computação

Seminário de Pesquisa CIn-UFPE

Prof. Paulo Oliva, 30 de Março 2022

Componente React

```
class Square extends React.Component {
  constructor(props) {
    super(props);
    this.state = {
      value: null,
    };
  }

  render() {
    return (
      <button className="square" onClick={() => console.log('click')}>
        {this.props.value}
      </button>
    );
  }
}
```

Prova Matemática

proof of the infinity of primes

■ **Euclid's Proof.** For any finite set $\{p_1, \ldots, p_r\}$ of primes, consider the number $n = p_1 p_2 \cdots p_r + 1$. This n has a prime divisor p. But p is not one of the p_i: otherwise p would be a divisor of n and of the product $p_1 p_2 \cdots p_r$, and thus also of the difference $n - p_1 p_2 \cdots p_r = 1$, which is impossible. So a finite set $\{p_1, \ldots, p_r\}$ cannot be the collection of *all* prime numbers. □

A influência da lógica matemática na Computação

Lógica?

Em alguns países da América do Sul se fala português

O Brasil é um dos países da América do Sul 👎

No Brasil se fala português 👍

Em alguns países da América do Sul se fala português

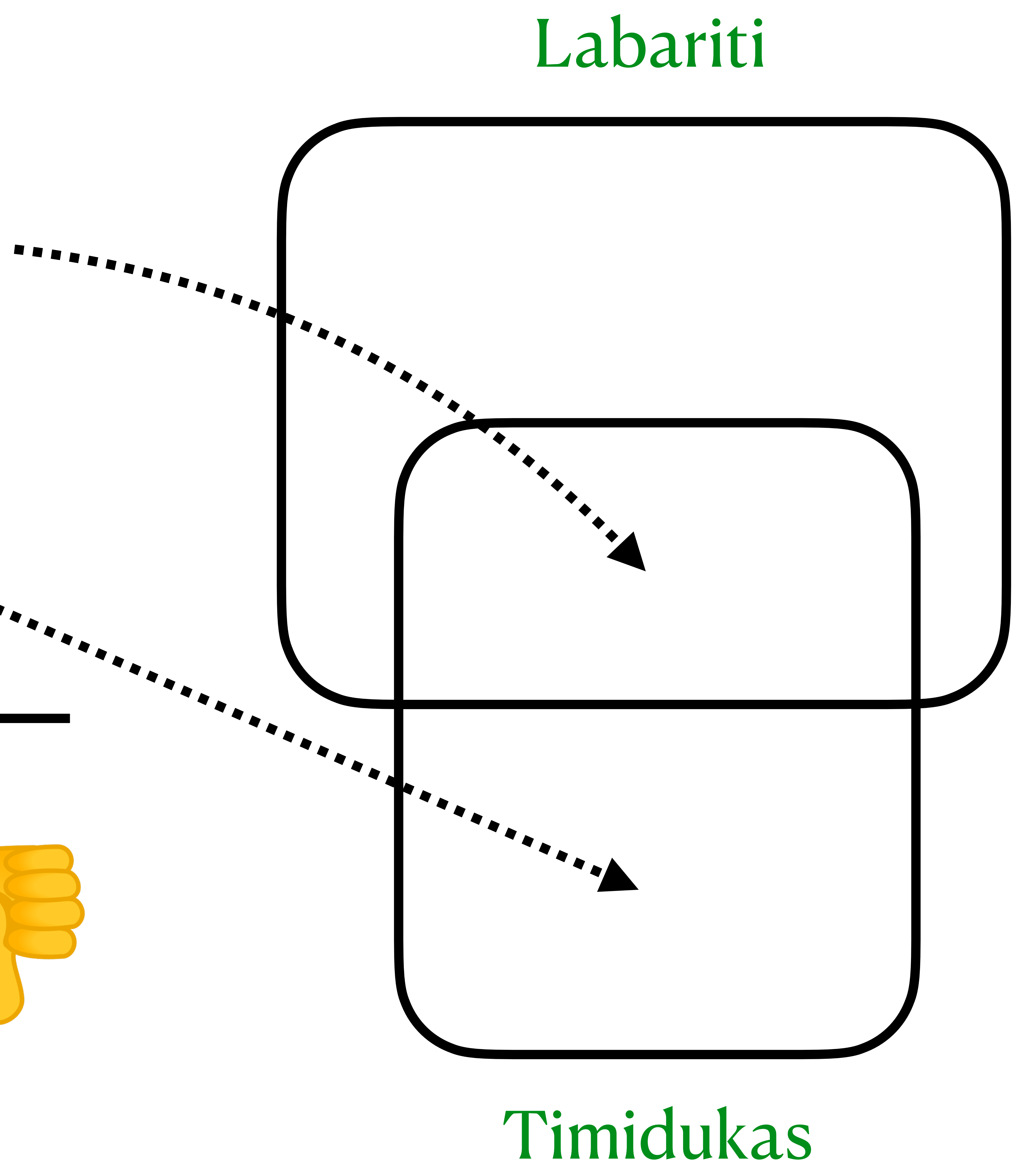
O Brasil é um dos países da América do Sul

No Brasil se fala português

Alguns Timidukas falam Labariti

Ginokilu é um Timiduka

Ginokilu fala Labariti



Aristotle's Syllogisms

	BARBARA		CELARENT
A	Every B is A.	E	No B is A.
A	Every C is B.	A	Every C is B.
A	Therefore, every C is A.	E	Therefore, no C is A.
	DARII		**FERIO**
A	Every B is A.	E	No B is A.
I	Some C is B.	I	Some C is B.
I	Therefore, some C is A.	O	Therefore, some C is not A.

A validade do argumento só depende da sua estrutura ou FORMA!

A validade do argumento só depende da sua forma!

Então...
Lógica matemática...

David Hilbert
(1862 - 1943)

“Is mathematics complete?
Is mathematics consistent?
Is mathematics decidable?”

Three of Hilbert’s 23 problems, 1900

Kurt Gödel
(1906 - 1978)

“Is mathematics complete?
Is mathematics consistent?

“NO!”

On formally undecidable propositions… , 1931

coding, self-reference, diagonalisation

“I’m lying”

“This sentence is false”

“This sentence is not provable”

David Hilbert
(1862 - 1943)

"Is there an **algorithm** that considers, as input, a statement and answers 'Yes' or 'No' according to whether the statement is universally valid?"

Decision problem, 1928

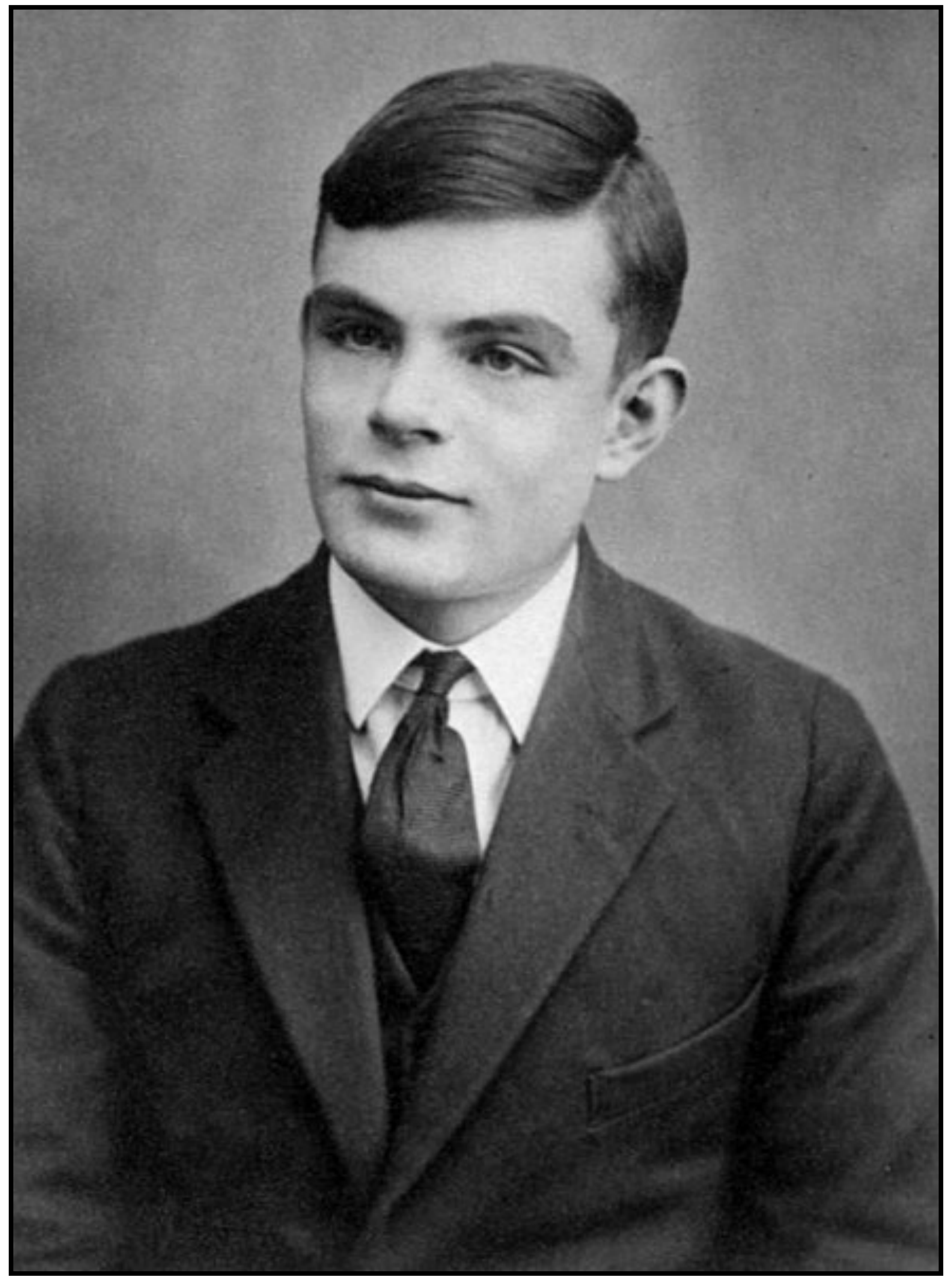
Entscheidungsproblem

Alonzo Church
(1903 - 1995)

“NO!”

A note on the Entscheidungsproblem , 1936

(Lambda calculus)



Alan Turing
(1912 - 1954)

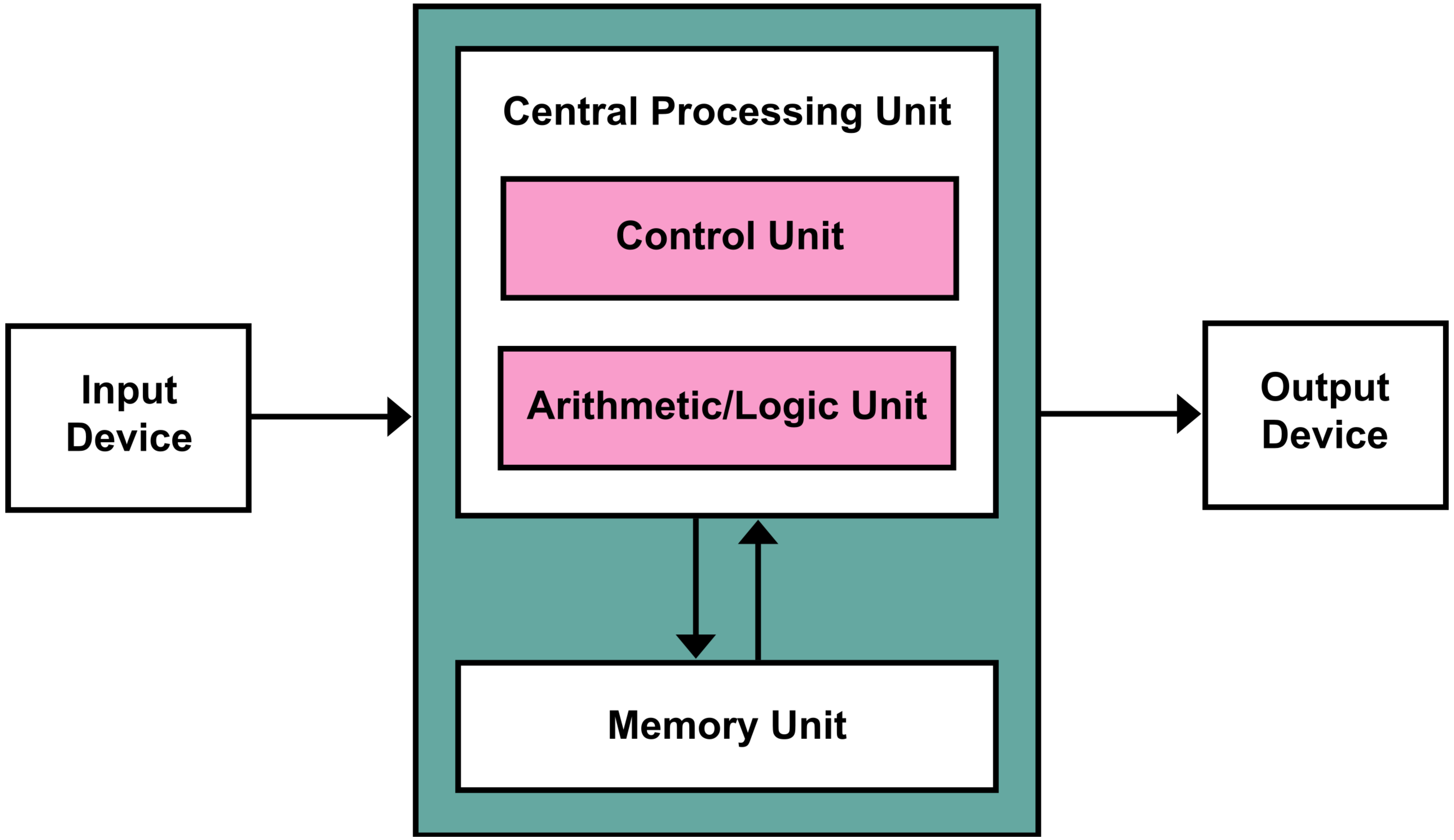
"NO!"

On computable numbers, with an Application to the Entscheidungsproblem, 1936

(Universal) Turing Machine

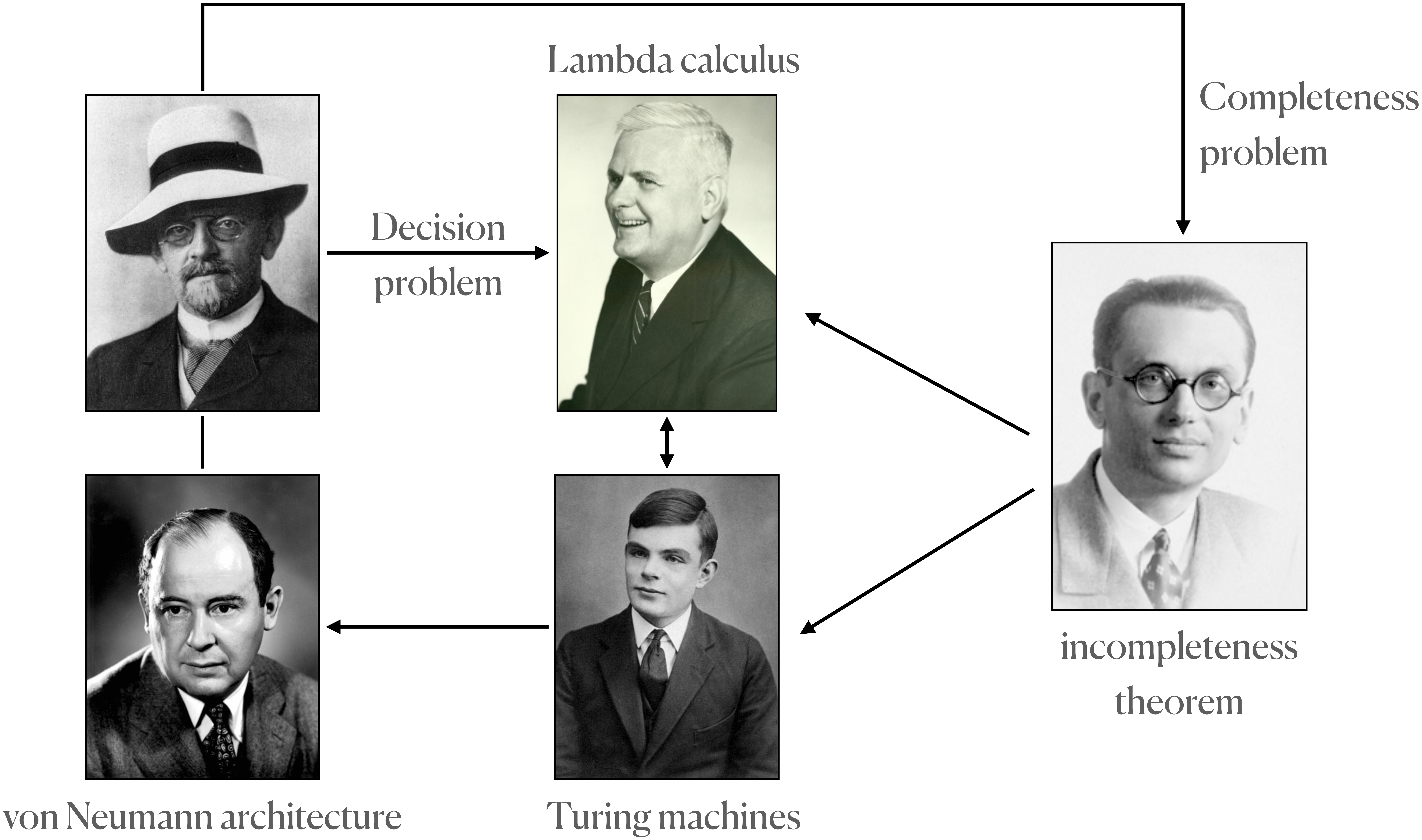
John von Neumann
(1903 - 1957)

von Neumann architecture, 1945



John von Neumann
(1903 - 1957)

- **Aluno de David Hilbert!**
- Set theory (*von Neumann paradox, 1929*)
- Proof theory (*consistency of arithmetic, 1930*)
- Quantum logic (1932)
- Ergodic theory (*mean ergodic theorem, 1932*)
- Game theory (*theorem of games, 1944*)
- Algorithms (*merge sort, 1945*)


Lambda calculus
Completeness problem
Decision problem
incompleteness theorem
von Neumann architecture
Turing machines

OK, os fundadores da Computação eram lógicos...

Coincidência?

Lógica

Computação

proof of the infinity of primes

■ **Euclid's Proof.** For any finite set $\{p_1, \ldots, p_r\}$ of primes, consider the number $n = p_1 p_2 \cdots p_r + 1$. This n has a prime divisor p. But p is not one of the p_i: otherwise p would be a divisor of n and of the product $p_1 p_2 \cdots p_r$, and thus also of the difference $n - p_1 p_2 \cdots p_r = 1$, which is impossible. So a finite set $\{p_1, \ldots, p_r\}$ cannot be the collection of *all* prime numbers. □

```
class Square extends React.Component {
  constructor(props) {
    super(props);
    this.state = {
      value: null,
    };
  }

  render() {
    return (
      <button className="square" onClick={() => console.log('click')}>
        {this.props.value}
      </button>
    );
  }
}
```

Lógica / Computação

1. Validade do raciocínio lógico só depende da forma (syntax)
   Um interpretador é capaz de validar a estrutura do programa
2. Provas complexas são baseadas em lemas que são re-usados
   Sistemas complexos são baseados em components reusáveis
3. Existe na verdade uma dualidade entre provas e programs
   Curry-Howard correspondence

Curry-Howard Correspondence?

L. E. J. Brouwer
(1881 - 1996)

- Matemático / Lógico Holandês
- Fundador da topologia moderna
- Fixed-point theory
- Fundador do **Intuitionism**
- Base para **Martin-Löf Type Theory**
- Had arguments with **David Hilbert**

L. E. J. Brouwer
(1881 - 1996)

Brouwer's fixed-point theorem

"For any continuous function f mapping a compact convex set to itself there exists a point x such that $f(x) = x$"

L. E. J. Brouwer
(1881 - 1996)

Brouwer's fixed-point theorem

"For any continuous function f mapping a compact convex set to itself there exists a point x such that $f(x) = x$"

Proof: Let $f\colon [0,1] \to [0,1]$.

Define $g(x) = f(x) - x$.

Then $g(0) = f(0) \geq 0$ and $g(1) = f(1) - 1 \leq 0$

By the **intermediate-value theorem**, there exists a point c such that $g(c) = 0 = f(c) - c$

O problema da lógica clássica…

$$\begin{array}{c} [\neg \exists x A] \\ \vdots \\ \text{contradição} \\ \hline \exists x A \end{array}$$

É impossível que não exista um x tal que A

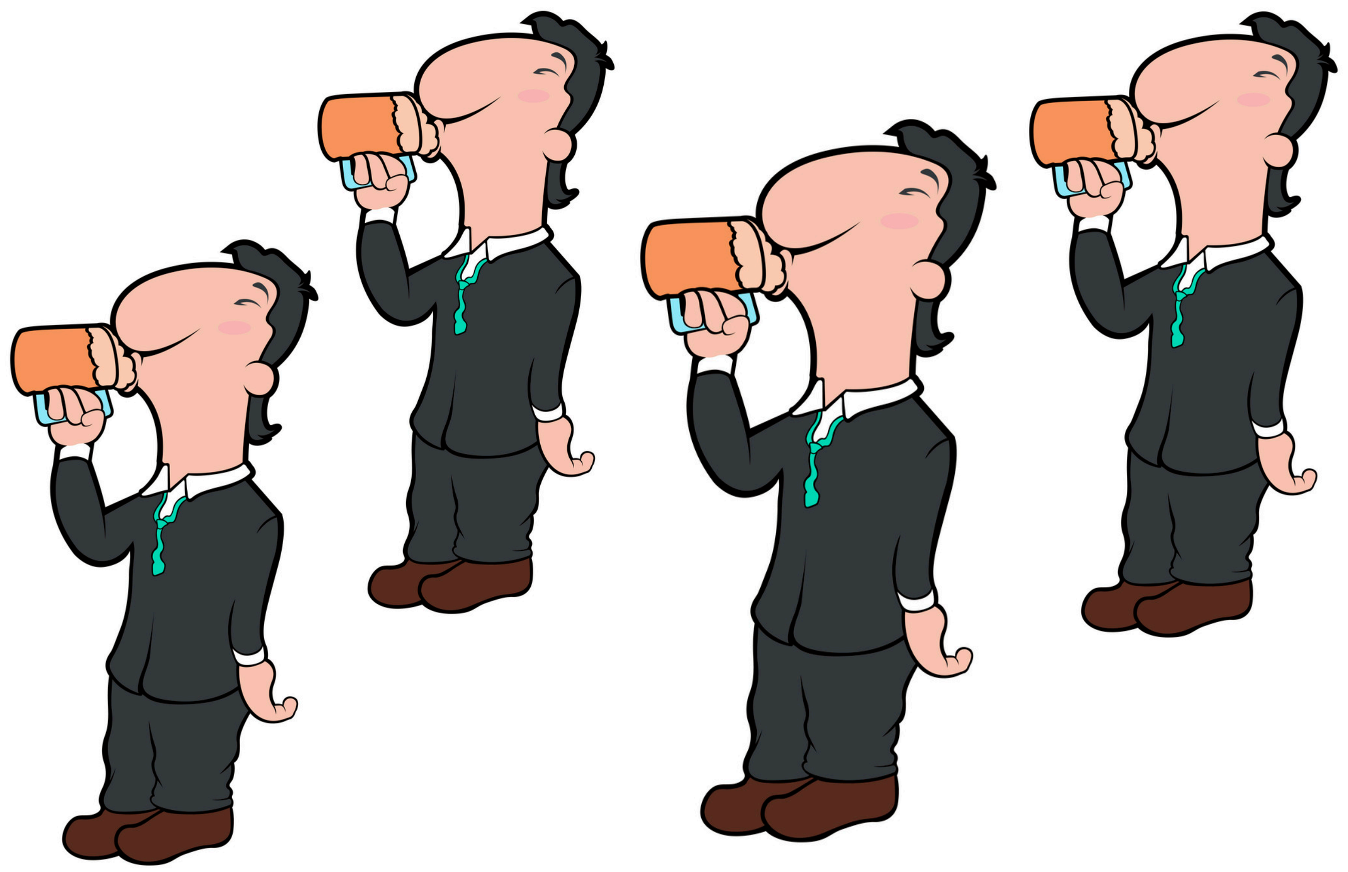
x tem que existir

$$\exists x(B(x) \rightarrow \forall y B(y))$$

existe uma pessoa

se ela bebe

tudo mundo bebe



$$A \lor \neg A$$

A é verdadeiro ou *A* é falso

$$A \vee \neg A$$

Riemann hypothesis é verdadeira	ou	Riemann hypothesis é falsa

$$A \lor \neg A$$

Sua comunicação com o banco online é segura

ou

É facilmente possível decifrar sua comunicação

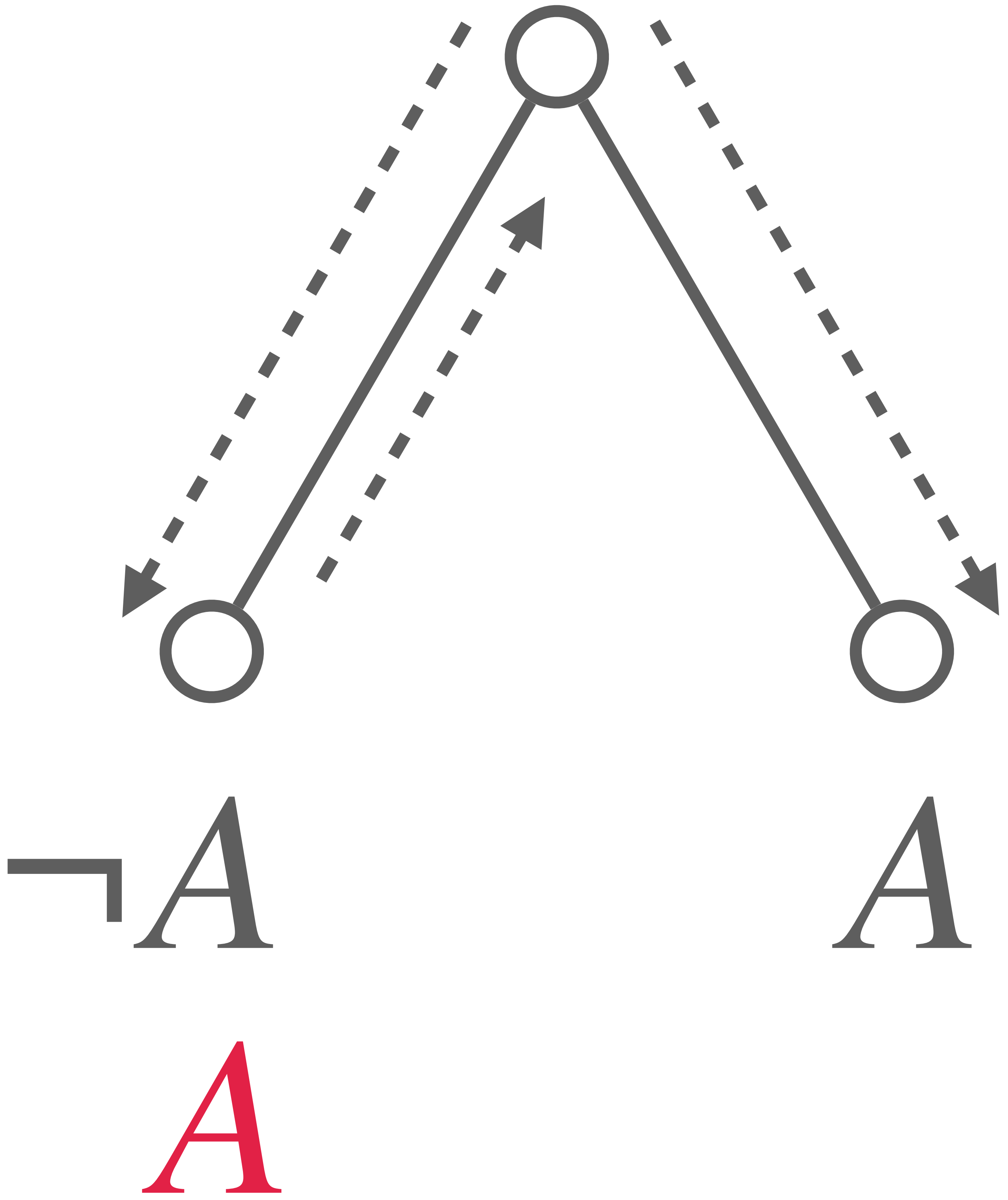
Interpretação da Lógica Clássica...

Classical Reasoning

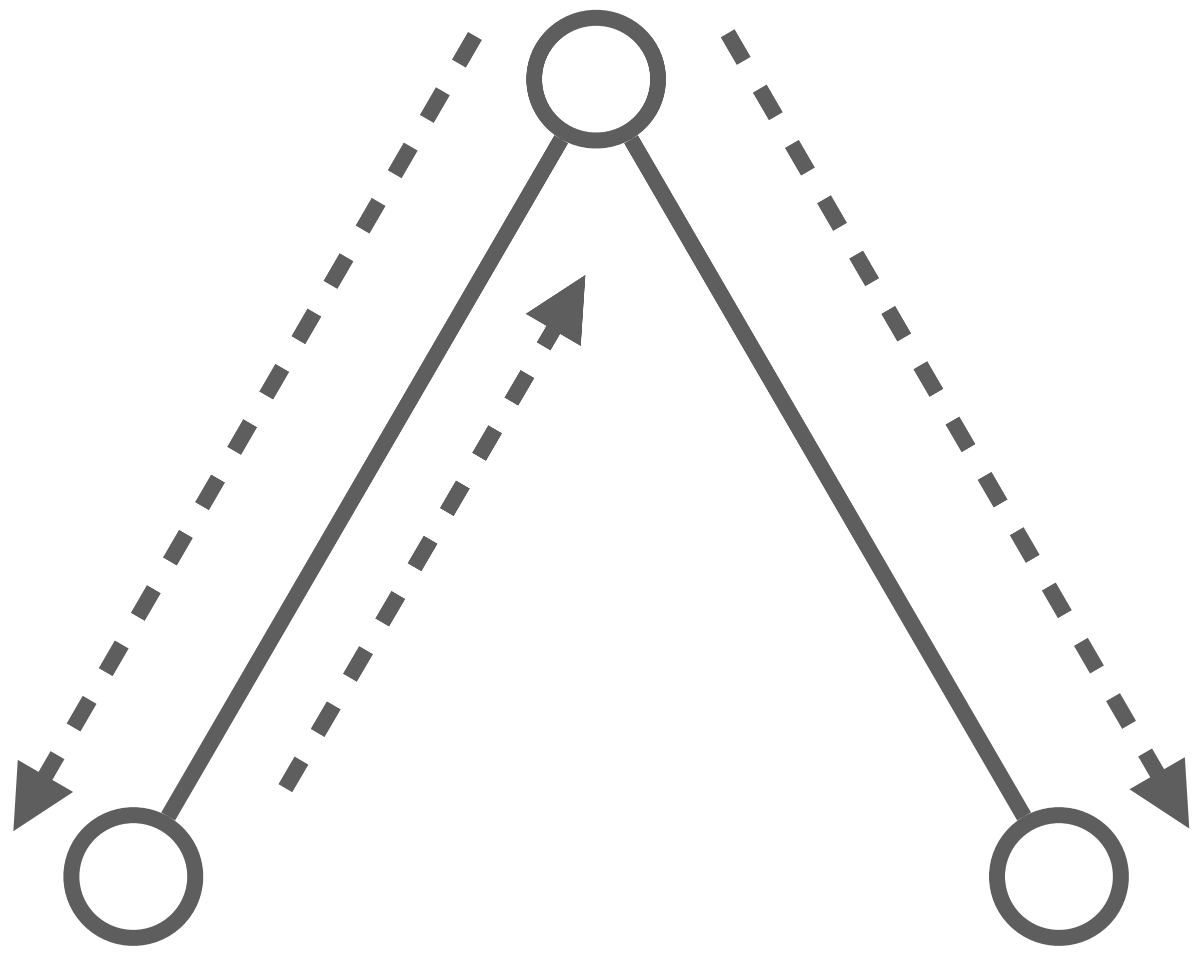
=

Backtracking

$$A \vee \neg A$$



$$\exists x(B(x) \to \forall y B(y))$$



$B(\text{joão}) \to \forall y B(y)$ $B(\text{maria}) \to \forall y B(y)$

$B(\text{joão})$ $\neg B(\text{maria})$

Interpretação Dialectica

Solução (parcial) para o "problema da consistência" do Hilbert!

Kurt Gödel
(1906 - 1978)

$$\forall x \exists y A(x, y)$$

$$\exists p \forall x A(x, p(x))$$

$$A(x, t(x))$$

$$\exists x(B(x) \to \forall y B(y))$$

$$\exists x \forall y(B(x) \to B(y))$$

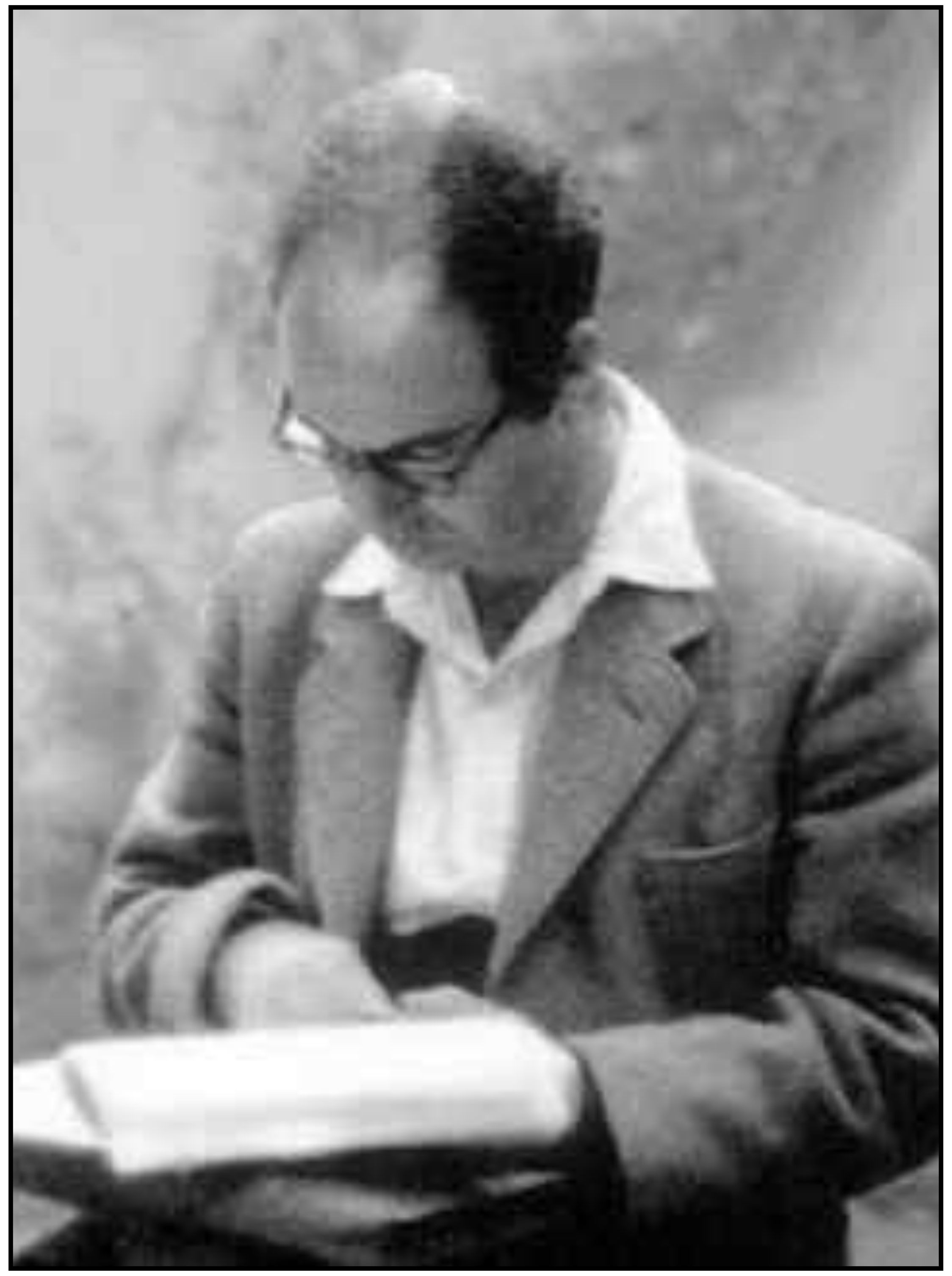
$$\forall p \exists x(B(x) \to B(p(x)))$$

$$\exists \phi \forall p(B(\phi p) \to B(p(\phi p)))$$

$$\exists \phi \forall p (B(\phi p) \rightarrow B(p(\phi p)))$$

$$\phi(p) = \begin{cases} \text{joão} & \text{if } B(p(\text{joão})) \\ p(\text{joão}) & \text{if } \neg B(p(\text{joão})) \end{cases}$$

$$B(\phi p) \rightarrow B(p(\phi p))$$



Georg Kreisel
(1923 - 2015)

"What more do we know if we have proved a theorem by restricted means than if we merely know that it is true?"

Unwinding of proofs program

Any proof in mathematics carries some form of construction or algorithm!

```
class Square extends React.Component {
  constructor(props) {
    super(props);
    this.state = {
      value: null,
    };
  }

  render() {
    return (
      <button className="square" onClick={() => console.log('click')}>
        {this.props.value}
      </button>
    );
  }
}
```

proof of the infinity of primes

■ **Euclid's Proof.** For any finite set $\{p_1, \ldots, p_r\}$ of primes, consider the number $n = p_1 p_2 \cdots p_r + 1$. This n has a prime divisor p. But p is not one of the p_i: otherwise p would be a divisor of n and of the product $p_1 p_2 \cdots p_r$, and thus also of the difference $n - p_1 p_2 \cdots p_r = 1$, which is impossible. So a finite set $\{p_1, \ldots, p_r\}$ cannot be the collection of *all* prime numbers. □

Seminário de Pesquisa CIn-UFPE

How to make Computing appeal more to Women

Prof. Claus Brabrand, Head of Center for Computing Education Research (CCER) at the IT University of Copenhagen

Data: 7 de abril, às 10h