

CC

Complicações Computacionais

Rosália Rodrigues

21-04-2004



"Computer Science is no more about computers than astronomy is about telescopes."

"... is like referring to surgery as knife science."

Edsger Wybe Dijkstra
[1930 .. 2002]



*" Computer Science is the study of algorithms",
Knuth, 1968*

Donald Ervin **Knuth**

[n. 1938]



*" Computer Science is the study and
management of complexity", Dijkstra, 1969*

Existem registros de Algoritmos desde o tempo dos sumérios, acádios, das antigas China, Grécia, China, Índia, ...

- Algoritmo de **Euclides** [-325 .. -265]



"Para calcular o máximo divisor comum de dois números, subtraia o menor ao maior até ficarem iguais."

a	b
380	55
325	55
270	55
215	55
160	55
105	55
50	55
50	5
45	5
40	5
35	5
30	5
25	5
20	5
15	5
10	5
5	5

Algoritmo para o cálculo do Dia de Páscoa [Bula Papal de 1582]:

O Dia de Páscoa de um dado ano é o Domingo a seguir à primeira Lua Cheia, a partir de 21 de Março.

Para saber o Dia de Páscoa de um qualquer ano do Senhor:

Calcular o Número Dominical;

Calcular o Número de Ouro;

Calcular a Epacta;

Calcular a Correção Claviana;

Calcular a Lua de Janeiro;

Calcular a Lua de Março;

Calcular a Lua de Abril;

Calcular a Lua Pascal;

Dia Pascal \leftarrow (Lua Pascal - Número Dominical) $\text{mod } 7 + 1$;

Páscoa \leftarrow Lua Pascal + 8 - Dia Pascal;

Fim de Fevereiro \leftarrow 31 + 28 + (1 se bissexto);

Fim de Março \leftarrow Fim de Fevereiro + 31;

Se Páscoa \leq Fim de Março

Então Dia de Páscoa \leftarrow Páscoa - Fim de Fevereiro

Senão Dia de Páscoa \leftarrow Páscoa - Fim de Março.



- O termo Algoritmo



Abu Ja'far Muhammad ibn-Musa **Al-Khwarizmi**,
Bagdad [780 .. 845]

Algoritmo
Algarismo
Álgebra
(0)
...

... o que é um Algoritmo?

Definição 1:

Um Algoritmo é uma Solução de um Problema

- **Problema:** Dados $a, b \in \mathbb{N}$, calcular $\text{mdc}(a,b)$
- **Algoritmo:** Subtrair o menor ao maior, até ficarem iguais.

- **Problema:** Caixeiro Viajante

Dadas n cidades e a matriz das respectivas distâncias, calcular o circuito total mínimo.



- **Algoritmo:**

Gerar todas a Permutações de $(1, 2, 3, \dots, n)$;
calculando a soma das distâncias;
Escolher a menor.

Problemas e Algoritmos

... para 1 nanosegundo por permutação:



n	2^n (ns)	segundos	dias	anos
10	1024.	1.024×10^{-6}	1.18519×10^{-11}	3.24708×10^{-14}
20	1.04858×10^6	0.00104858	1.21363×10^{-8}	3.32501×10^{-11}
30	1.07374×10^9	1.07374	0.0000124276	3.40481×10^{-8}
40	1.09951×10^{12}	1099.51	0.0127258	0.0000348653
50	1.1259×10^{15}	1.1259×10^6	13.0312	0.0357021
60	1.15292×10^{18}	1.15292×10^9	13344.	36.5589
70	1.18059×10^{21}	1.18059×10^{12}	1.36643×10^7	37436.3
80	1.20893×10^{24}	1.20893×10^{15}	1.39922×10^{10}	3.83348×10^7
90	1.23794×10^{27}	1.23794×10^{18}	1.4328×10^{13}	3.92548×10^{10}
100	1.26765×10^{30}	1.26765×10^{21}	1.46719×10^{16}	4.01969×10^{13}

... isto é um Algoritmo?

Definição 2:

Um Algoritmo é uma Solução de um Problema,
mas só se terminar em tempo útil.

tempo útil ?

terminar ?

solução ?

problema ?

- **Problema :** Resolver a equação
$$x^n + y^n = z^n$$
com $x, y, z, n \in \mathbb{Z}, n > 2$
- **Algoritmo? Existe?**

Pierre de Fermat
[1601 .. 1665]



- *Equações Diofantinas* (soluções inteiras)

Diofanto de Alexandria [≈ 200 .. $\approx 200 + x$]



Caminhante! Aqui jaz Diofanto.
Os números dirão a duração da sua vida.
Cuja sexta parte foi ocupada por uma doce infância.
Decorrida mais uma duodécima parte da sua vida, o seu rosto cobriu-se com barba. Passado mais um sétimo da sua vida casou.
Cinco anos depois, nasceu-lhe o seu único filho, que apenas durou metade da vida do pai. Triste com a morte do seu filho, Diofanto viveu ainda quatro anos. Diz-me, Caminhante, que idade tinha Diofanto quando a morte o levou?

... gente que cria problemas!

Problemas e mais Problemas

- O 1º Problema de Hilbert
- O 2º Problema de Hilbert
- O 3º Problema de Hilbert
- O 4º Problema de Hilbert
- O 5º Problema de Hilbert
- O 6º Problema de Hilbert
- O 7º Problema de Hilbert
- O 8º Problema de Hilbert
- O 9º Problema de Hilbert
- O 10º Problema de Hilbert**
- ...
- O 23º Problema de Hilbert

- **10º Problem de Hilbert (1900):**
Existirá um “algoritmo” para encontrar soluções inteiras de Equações Diofantinas?
- ***Entscheidungsproblem* (1928):**
Existirá um “algoritmo” para **decidir** se uma afirmação pode ser demonstrada?

David Hilbert
[1862 .. 1943]



- Hilbert: Formalização total da Matemática:

Sistema Formal = {Axiomas} + {Regras de Inferência}
“Algoritmização” do processo dedutivo.

*“Hilbert’s idea was a success, ...
not for mathematical reasoning or deduction,
but for programming, for calculating, for computing.”*

Gregory J. Chaitin

Mas ...

Kurt Gödel

[1906 .. 1978]



Todo o sistema formal decidível (que contenha a teoria elementar dos números naturais) ou é inconsistente ou incompleto (1931).

... há coisas que não se podem decidir.

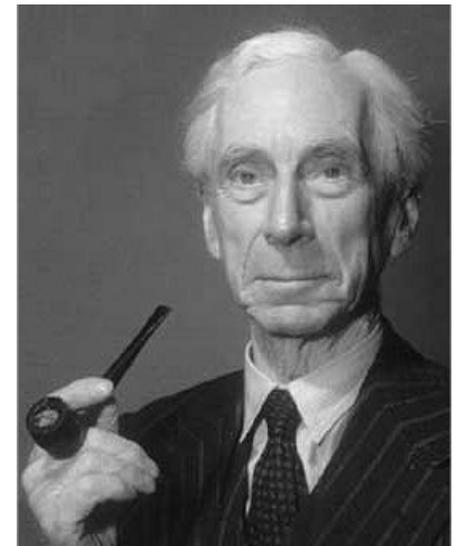
... há coisas que não se podem demonstrar.

A afirmação seguinte é Falsa!
A afirmação anterior é Verdadeira!

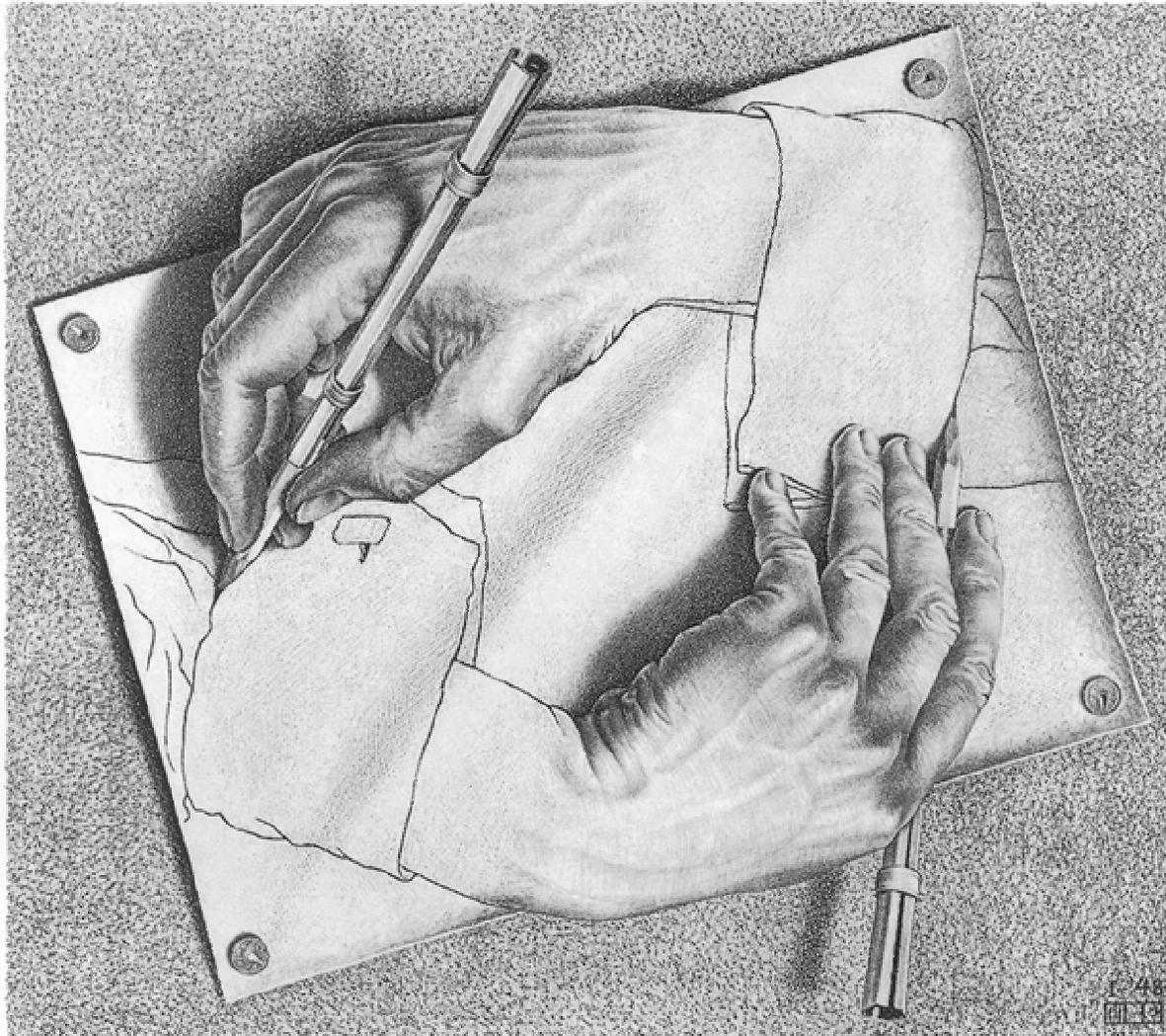
*"If I were a medical man, I should
prescribe a holiday to any patient who
considered his work important."*

Bertrand Arthur William **Russell**

[1872 .. 1970]



Paradoxos



Maurits Cornelis
Escher

[1898 .. 1972]

Hilbert (1928): Qualquer problema pode ser “resolvido” por um “algoritmo”?

Gödel (1931): Não pode!
Demonstrei com um Algoritmo Recorrente.

Turing (1936): Um Algoritmo é uma “máquina” ...

Alan Mathison Turing

[1912 .. 1954]



Resolução de uma Instância de um Problema:



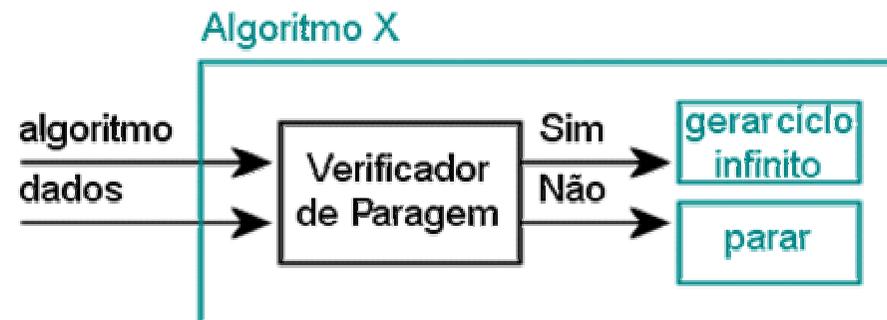
Mas será que a Máquina de Turing pára sempre?

Existirá um algoritmo (MT) para verificar se todo o algoritmo pára, para qualquer instância?

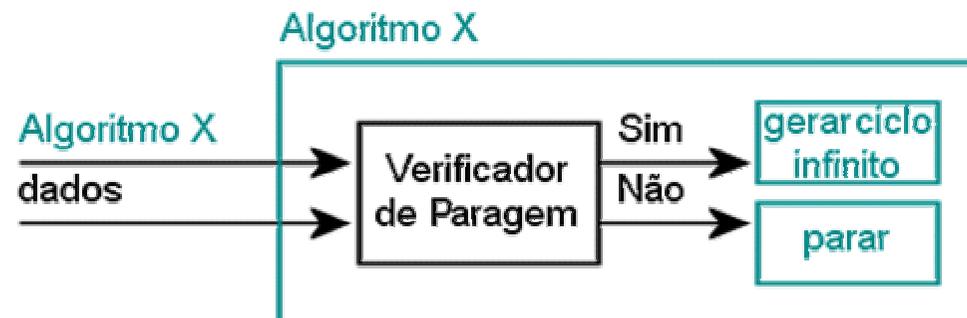


O Problema da Paragem

Se tal algoritmo existisse, poderíamos construir:



... e como o algoritmo de entrada é qualquer:



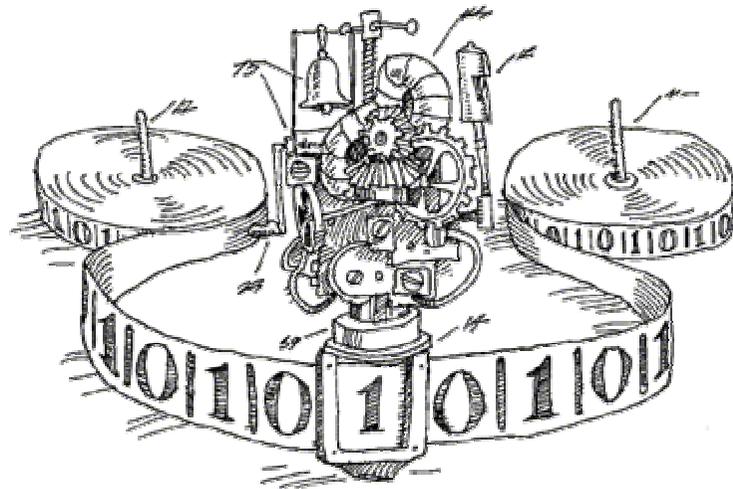


O Problema da Paragem é Indecidível

São Decidíveis os Problemas resolúveis por uma Máquina de Turing que pára sempre.

Definição 3:

Um Algoritmo é uma Máquina de Turing que pára.



*{ Um Problema resolúvel por um Computador
é resolúvel por uma Máquina de Turing }*

- Máquina de Turing (Alan Mathison Turing)
- Funções Recorrentes (Stephen Cole Kleene)
- Funções μ -recorrentes (Kurt Gödel)
- Cálculo- λ (Alonzo Church)
- Sistema de Post (Emil Leon Post)
- Lógica Combinatória (Moses Schönfinkel)

... todos cerca de 1936.

- Uma **Máquina de Turing** é um séptuplo ordenado,

$$M = (Q, \Sigma, \Gamma, \delta, q_0, \square, F)$$

onde:

Q é um conjunto finito de estados,

Σ é o conjunto finito de símbolos de entrada,

Γ é o conjunto finito de símbolos da Fita, onde $\Sigma \subseteq \Gamma$,

$\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$ é a função de transição,

$q_0 \in Q$ é o estado inicial,

$\square \in \Gamma \setminus \Sigma$ é o símbolo branco,

$F \subseteq Q$ é o conjunto dos estados finais ou de aceitação.

Definição 4:

Um Algoritmo para calcular o valor de uma função $f : C \rightarrow D$ é uma Máquina de Turing que, partindo de um $x \in C$ registado na Fita, pára com o valor exacto de $f(x) \in D$ registado na Fita.

Só estas funções são Computáveis.

- Numa Máquina de Turing **Não Determinista**,

$$\delta : Q \times \Gamma \longrightarrow 2^{Q \times \Gamma \times \{L, R\}}$$

A classe **P** :

Problemas resolúveis por uma Máquina de Turing, em tempo polinomial.

A classe **NP** :

Problemas resolúveis por uma Máquina de Turing, Não Determinista em tempo polinomial.

- Existirá, ou não existirá, alguma MT determinista capaz de resolver os problemas NP em tempo polinomial?
- Existirá mesmo algum problema NP que não seja P?

... não sabemos!

A grande questão:

P $\stackrel{?}{\neq}$ NP

{ Não vale dizer $N=1$ }

A Classe NP-completo {Os Intratáveis}:

Problemas NP tais que, se alguma vez algum deles for classificado como P, então $P = NP$.

(1965) Era moderna da Complexidade Computacional

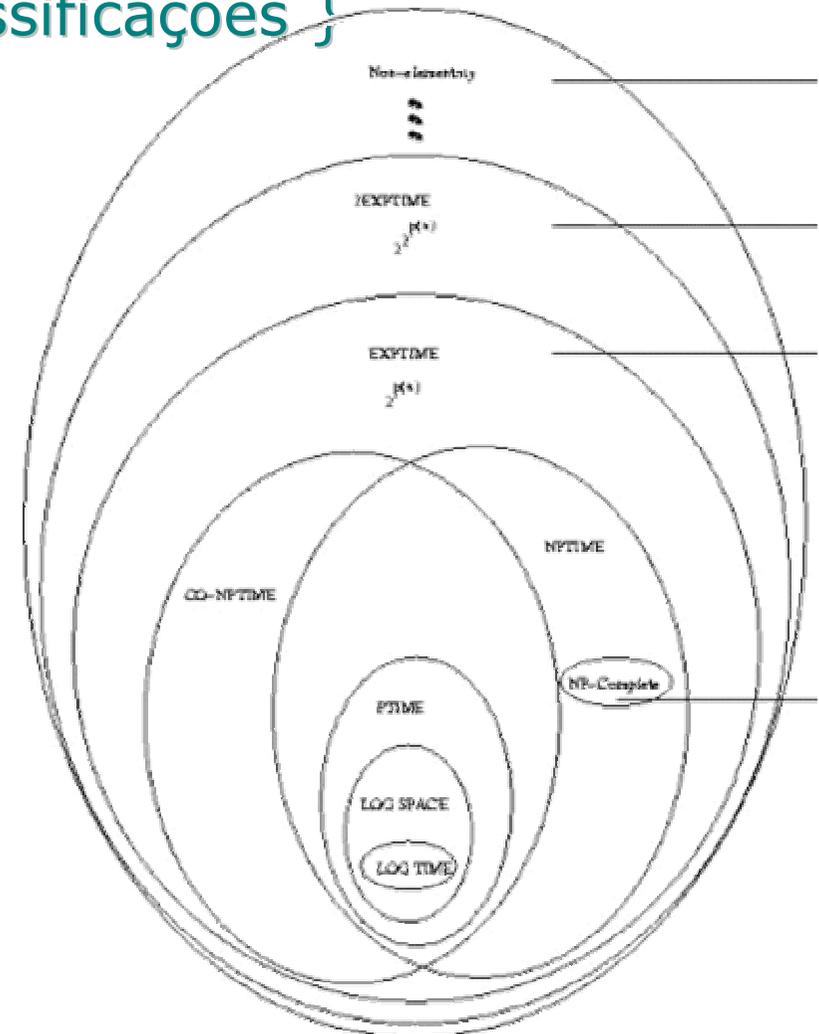
Hartmanis e Stearns

Definição formal de Complexidade Computacional, utilizando a Máquina de Turing como modelo.
Definição de Classes de Complexidade.

(anos 70) - Teoria da Complexidade

{ A década das Classificações }

Hartmanis
Stearns
Edmonds
Cook
Levin
Karp
Garey
Johnson
Papadimitriou
Yannakakis
...



Teoria da Aproximabilidade

Procura de uma solução quasi-óptima para Problemas Intratáveis.

Algoritmos de Aproximação.
Métodos Heurísticos.

1972, Garey, Graham e Ullman

1974, Garey e Johnson

Mas ...

obter boas aproximações para problemas NP-difíceis é tão difícil como calcular a sua solução exacta.

Complexidade Algorítmica



**Andrey Nikolaevich
Kolmogorov**

[1903 .. 1987]

Algorithmic Complexity
Information Complexity
Kolmogorov Complexity
Algorithmic Information Theory
K-complexity
Kolmogorov-Chaitin randomness
Stochastic Complexity
Descriptive Complexity
Minimum Description Length
Program-size Complexity
...

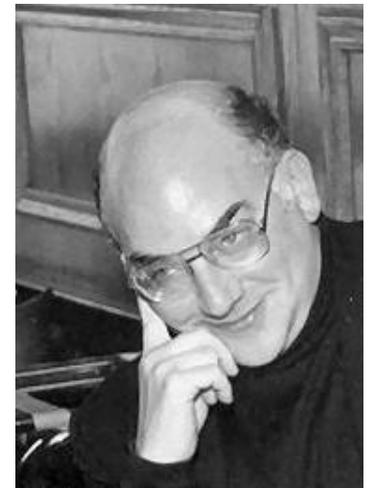


Ray J. Solomonoff

[n. 1926]

Gregory J. Chaitin

[n. \approx 1950]



A.N. Kolmogorov, V.A. Uspensky. "On the definition of algorithm".
Uspehi Math. Nauk, 1958, v. 13, No. 4, pp. 3-28.

Teoria da Complexidade Algorítmica (1960)

Complexidade = Quantidade de Informação
(tamanho da descrição)

Complexidade de um Problema
= Comprimento do menor algoritmo
(Máquina de Turing) que o resolva

Mas ... $K(x)$ não é Computável!

Complexidade de um Problema

= complexidade do Pior Caso

= complexidade da sua "pior" Instância

Como "avaliar" a Complexidade
de uma Instância particular de um Problema?

1986, Richard Karp

1994, Pekka Orponen

1996, Christos Papadimitriou

1999, Martin Mundhenk

1999, Mihalis Yannakakis

...

Mas ... também não é Computável!

Para onde vai a Complexidade?



Como (sobre)viver num mundo de Complexidades?

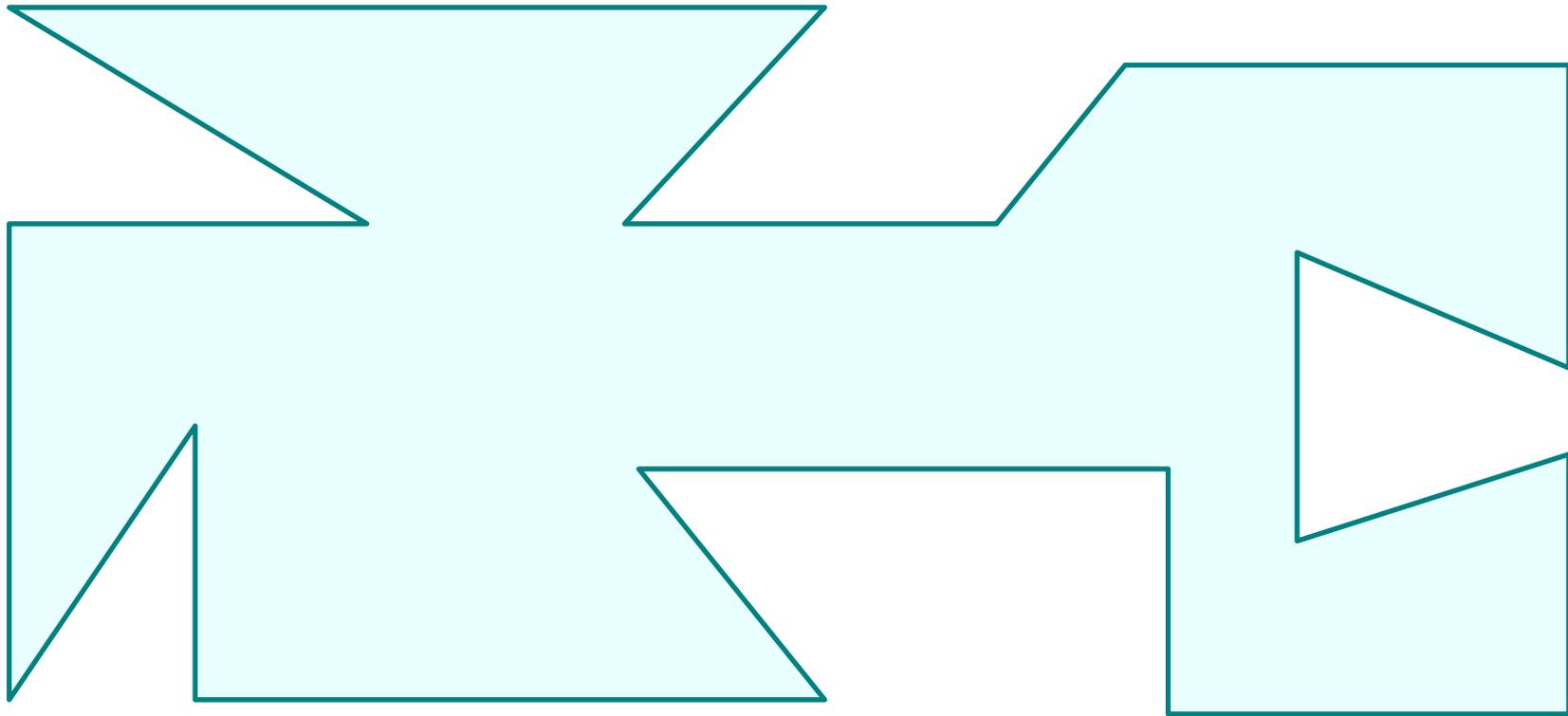
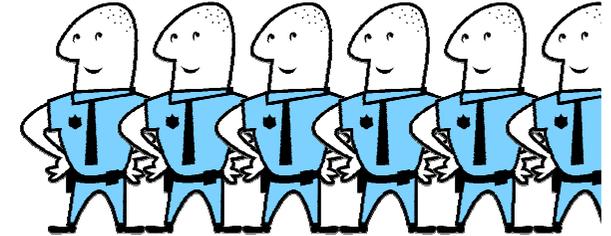
Como “tratar” Problemas Intratáveis?

- Construir algoritmos polinomiais para gerar “boas” soluções.
- Resolver (classes de) instâncias particulares.
- Tentar “reduzir” a um problema mais simples.

- Continuar a tentar ...
- Procurar outros modelos.
- ...

O Problema da Galeria de Arte

- Número mínimo de guardas? Onde?



O Problema da Galeria de Arte

"Porque é que eles não põem só um guarda à porta de saída?"



Soluções aproximadas inspiradas na Natureza:

- Simulação de Têmpera.
- Redes Neurais.
- Algoritmos Genéticos.
- Sistemas Formigueiro.
- Pesquisa Tabu.
- ...

Simulação de Têmpera



*"Nenhum Caixaieiro Viajante
deixou de sair de casa por
causa disso."*

A Complexidade das Instâncias

"Todas as Instâncias de um Problema Intratável são intratáveis, mas umas são mais intratáveis do que as outras."

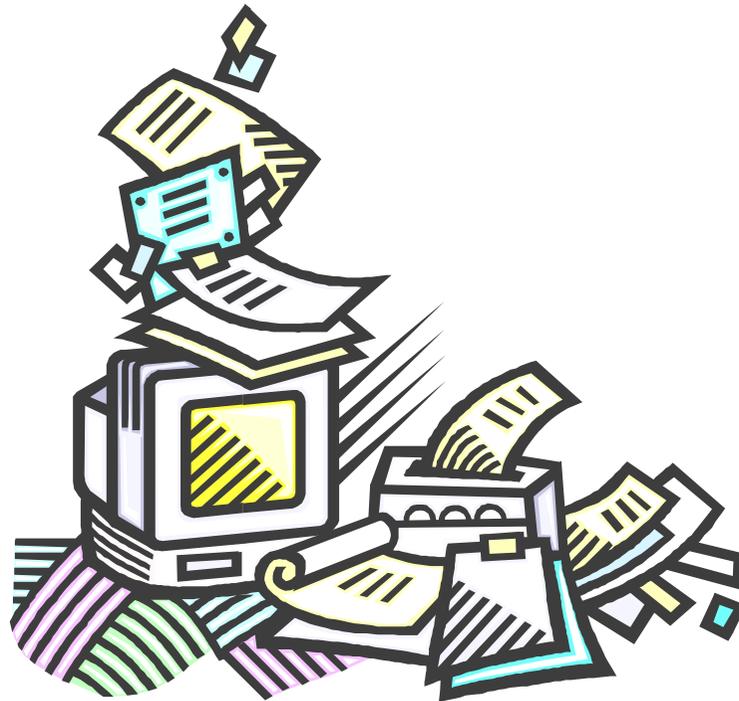


O Modelo Quântico de Computação



"Mas o Modelo tem mesmo de ser sempre a Máquina de Turing?"

... e os Computadores?



*“— I exaggerate only slightly —
the computer was invented in order to help
to clarify a philosophical question about the
foundations of mathematics.”*

Gregory J. **Chaitin**



*"Os Computadores servem
para criar Problemas."*