

# Sobre a Demonstração do Teorema de Gödel

Luís Monteiro

Departamento de Informática  
Centro de Informática e Tecnologias da Informação

Seminários Centenário Kurt Gödel  
FCT/UNL, 6 de Novembro de 2006

# Enunciado dos teoremas da incompletude de Gödel

K. Gödel, *Acerca de proposições formalmente indecidíveis nos Principia Mathematica e sistemas relacionados*, 1931

## Primeiro teorema da incompletude de Gödel

Seja  $AP$  uma teoria de primeira ordem da aritmética de Peano. Existe uma proposição  $\varphi$  tal que, se  $AP$  for consistente- $\omega$ , nem  $\varphi$  nem a sua negação  $\neg\varphi$  são demonstráveis em  $AP$ .

(A proposição  $\varphi$  diz-se indecidível e  $AP$  diz-se incompleta.)

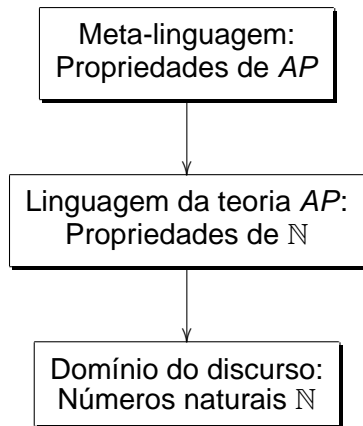
## Segundo teorema da incompletude de Gödel

Seja  $T$  uma teoria consistente, com um sistema decidível de axiomas e contendo a aritmética de Peano. Existe uma proposição  $Cons_T$  que exprime que  $T$  é consistente e que não é demonstrável em  $T$ .

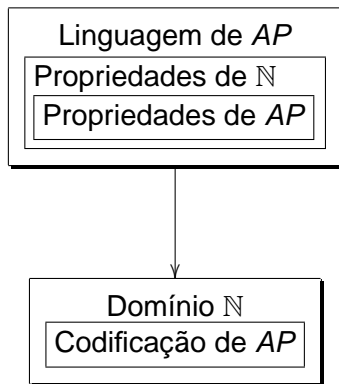
# Níveis de discurso

Linguagem-objecto e meta-linguagem

Há duas linguagens em jogo:



Linguagem de  $AP$  como meta-linguagem:



# Sistemas formais

O puzzle MU (D. Hofstadter, *Gödel, Escher, Bach: An Eternal Golden Braid*)

- Sobre palavras escritas com as letras  $M, I, U$  podem aplicar-se várias regras para obter novas palavras:
  - I. A toda a palavra terminada por  $I$  pode acrescentar-se  $U$  no fim.
  - II. Em qualquer palavra começada por  $M$  pode duplicar-se o que vier a seguir a  $M$ .
  - III. Qualquer sequência  $III$ , onde quer que ocorra, pode ser substituída por  $U$ .
  - IV. Qualquer sequência  $UU$ , onde quer que ocorra, pode ser apagada.
- Problema: Partindo da palavra  $MI$ , pode chegar-se a  $MU$ ?

# Sistemas formais

## O sistema formal MIU

**Símbolos:** As letras *M, I, U*.

**Fórmulas:** Todas as palavras com as letras *M, I, U*:

*MU UM UIM MUUMUU ...*

**Axiomas:** Apenas um, a fórmula *MI*.

**Regras:** A linha inferior **infere-se** da linha superior:

$$(I) \frac{xI}{xIU} \quad (II) \frac{Mx}{Mxx} \quad (III) \frac{xIIIy}{xUy} \quad (IV) \frac{xUUy}{xy}$$

**Demonstração:** Sucessão de fórmulas derivadas do axioma por aplicação das regras de inferência:

- |     |               |                       |
|-----|---------------|-----------------------|
| (1) | <i>MI</i>     | axioma                |
| (2) | <i>MII</i>    | de (1) pela regra II  |
| (3) | <i>MIII</i>   | de (2) pela regra II  |
| (4) | <i>MIIIIU</i> | de (3) pela regra I   |
| (5) | <i>MUIU</i>   | de (4) pela regra III |
| (6) | <i>MUIUUU</i> | de (5) pela regra II  |
| (7) | <i>MUIIU</i>  | de (6) pela regra IV  |

**Teorema:** A última fórmula de uma demonstração.  
As fórmulas de (1) a (7) são teoremas.

Duas actividades possíveis com o sistema MIU:

- Trabalhar no **interior do sistema**: produzir **teoremas**.

Exemplo:

TEOREMA *MUIIU*.

- Investigar **propriedades do sistema**: produzir **meta-teoremas**.

Exemplo:

META-TEOREMA *MU não pode resultar de MI visto que cada aplicação de uma regra nunca produz um número de I's que seja múltiplo de 3.*

Os teoremas de Gödel são meta-teoremas de *AP*.

# O sistema formal *AP* da aritmética de Peano

## Símbolos

Lógicos	$\neg$	$\Rightarrow$	$\forall$	
Aritméticos	$0$	$'$	$+$	$\times$ $=$
Variáveis	$v_1$	$v_2$	$\dots$	
Parênteses	$($	$)$		

# O sistema formal AP

## Termos e fórmulas

- Os números naturais representam-se pelos termos (**numerais**)

$$0 \quad 0' \quad 0'' \quad 0''' \quad \dots$$

- Para cada natural  $n$ ,

$\bar{n}$  abrevia o numeral  $0' \dots'$  ( $n$  pelicas)

- Outros termos:

$$(v_1 + v_3)' \times (v_2 + 0')$$

- Fórmulas:

$$\neg(\forall v_1)\neg(v_1 \times v_2 = v_3)$$

- Proposições:

$$(\forall v_1)(\forall v_2)v_1 + v_2 = v_2 + v_1$$

# O sistema formal $AP$

Axiomas (só alguns exemplos)

Lógicos:

- $p \Rightarrow q \Rightarrow p$
- $(\forall v)p(v) \Rightarrow p(t)$  para todo o termo  $t$ .

Aritméticos:

- $\neg(v' = 0)$
- $v' = w' \Rightarrow v = w$
- $v + 0 = v$
- $v + w' = (v + w)'$
- Para toda a fórmula  $p(v)$ ,

$$p(0) \Rightarrow (\forall v)(p(v) \Rightarrow p(v')) \Rightarrow (\forall v)p(v)$$

# O sistema formal AP

## Regras de inferência

*Modus Ponens*  $q$  é uma consequência de  $p$  e  $p \Rightarrow q$ .

$$\frac{p \quad p \Rightarrow q}{q}$$

*Generalização*  $(\forall v)p$  é uma consequência de  $p$ .

$$\frac{p}{(\forall v)p}$$

# O sistema formal $AP$

Demonstração, teorema, teoria

- **Demonstração**

Sucessão de fórmulas

$$p_0 \quad p_1 \quad p_2 \quad \cdots \quad p_n$$

em que cada fórmula é um axioma ou resulta da aplicação de uma regra de inferência a fórmulas anteriores na sequência.

- **Teorema**

Última fórmula de um demonstração.

- **Teoria**

Conjunto de todos os teoremas.

# O sistema formal $AP$

## Meta-propriedades de uma teoria

Propriedades que uma teoria pode ou não satisfazer:

- **Validade**

Todos os teoremas são válidos.

- **Completude**

Toda a fórmula válida é um teorema.

- **Consistência**

Não existe nenhuma fórmula  $q$  tal que  $q$  e  $\neg q$  sejam teoremas.

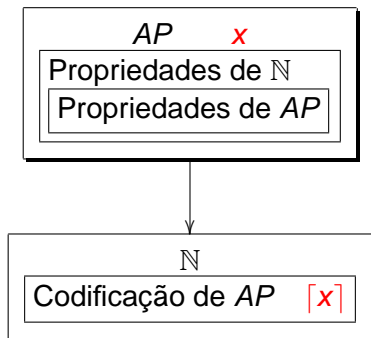
- **Consistência- $\omega$**

Não existe nenhuma fórmula  $q(v)$  tal que  $\neg q(\bar{n})$  para todo o  $n$  e  $(\exists v)q(v)$  sejam teoremas.

# Codificação de $AP$ em $\mathbb{N}$

## Números de Gödel

A codificação de  $AP$  em  $\mathbb{N}$  consiste em atribuir a cada entidade  $x$  de  $AP$  (símbolo, expressão, sucessão de expressões) um número  $[x]$ , chamado o seu **número de Gödel**.



# Números de Gödel

## Símbolos

Nos códigos dos símbolos não são utilizados múltiplos de 10.

$x$	$[x]$	$x$	$[x]$
$\neg$	1	$=$	8
$\Rightarrow$	2	$($	9
$\forall$	3	$)$	11
0	4	$v_1$	12
'	5	$v_2$	13
$+$	6	$v_3$	14
$\times$	7	$\vdots$	$\vdots$

# Números de Gödel

## Expressões e sucessões de expressões

### Expressões

Números de Gödel dos símbolos da expressão separados por 0

$$[0''] = 40505 \quad [v_1 = 0] = 120804$$

### Sucessões de expressões

Números de Gödel das expressões separados por 00

NOTA: Gödel utilizou uma codificação diferente, baseada na decomposição de um número em factores primos.

# Propriedade esprimível

## Internalização de propriedades externas

- Uma propriedade  $P(x_1, \dots, x_n)$  **de números naturais** é **exprimível** em AP se existir uma fórmula  $p(v_1, \dots, v_n)$  tal que para todos os números naturais  $m_1, \dots, m_n$ ,

$P(m_1, \dots, m_n)$  é verdade     sse      $p(\bar{m}_1, \dots, \bar{m}_n)$  é verdade.

- Uma propriedade **de símbolos, expressões e sucessões de expressões** é **exprimível** em AP se a correspondente propriedade dos seus números de Gödel for esprimível.

NOTA: Por simplicidade escrever-se-á  $p(m_1, \dots, m_n)$  omitindo as barras, confundindo números e numerais.

# Exemplos de propriedades esprimíveis

O artigo de Gödel define 46 propriedades

1.  $x$  é divisível por  $y$ .
2.  $p$  é um número primo.
3.  $p$  é o factor primo de ordem  $n$  de  $x$ .
6.  $y$  é o termo de ordem  $n$  da sucessão dos números que corresponde ao número  $x$ .
23.  $x$  é (o número de Gödel de) uma fórmula.
26. A variável  $v$  ocorre livre em  $x$ .
31.  $z$  é o resultado da substituição da variável  $v$  por  $y$  em  $x$ .
42.  $x$  é um axioma.
43.  $x$  é uma consequência imediata de  $y$  e  $z$ .
45.  $x$  é uma demonstração da fórmula  $y$ .
46.  $x$  é uma fórmula demonstrável.

# Exemplos de propriedades esprimíveis

## Demonstração e substituição

Notação para duas propriedades esprimíveis:

- A propriedade “ $x$  é uma demonstração de  $y$ ” é esprimível por  $d(v_1, v_2)$ :

$x$  é uma demonstração de  $y$      sse      $d(\lceil x \rceil, \lceil y \rceil)$ .

- A propriedade “a substituição do número  $m$  na variável livre de  $y$  dá  $z$ ” é esprimível por  $s(v_1, v_2) = v_3$ :

A propriedade anterior é verdadeira se, e só se,

$y$  tem a forma  $p(v_1)$

$z$  tem a forma  $p(m)$

$s(m, \lceil p(v_1) \rceil) = \lceil p(m) \rceil$  é verdade.

# Teorema de Tarski

A propriedade de ser uma fórmula verdadeira não é exprimível

Demonstração por redução ao absurdo:

- Suponhamos que  $verd(v_1)$  exprime a propriedade de que uma fórmula é verdadeira.
- Sejam  $p(v_1) = \neg verd(s(v_1, v_1))$  e  $m = \lceil p(v_1) \rceil$ .
- Tem-se  $s(m, m) = s(m, \lceil p(v_1) \rceil) = \lceil p(m) \rceil$ .
- Chega-se a uma contradição:

$$p(m) = \neg verd(s(m, m)) \text{ é } V$$

sse

$$\text{a fórmula de número } s(m, m) \text{ é } F$$

sse

$$p(m) \text{ é } F.$$

- Logo, a propriedade de verdade não é exprimível.

- A fórmula

$$p(m) = \neg \text{verd}(s(m, m))$$

afirma que a fórmula de número de Gödel  $s(m, m)$  é falsa.

- Mas a fórmula de número de Gödel  $s(m, m)$  é  $p(m)$ .
- Logo,  $p(m)$  afirma a sua própria falsidade:

$$p(m) = p(m) \text{ é falsa.}$$

# Um teorema de incompletude

Toda a teoria válida é incompleta

- Usa-se  $dem(v_1) = (\exists v_2)d(v_2, v_1)$  em vez de  $verd(v_1)$ .
- Põe-se de novo  $p(v_1) = \neg dem(s(v_1, v_1))$  e  $m = \lceil p(v_1) \rceil$ .
- Neste caso,  $p(m) = \neg dem(s(m, m))$  afirma que  $p(m)$  não é demonstrável.
- Tal como na demonstração do Teorema de Tarski, usando a validade da teoria conclui-se que  $p(m)$  não é demonstrável.
- Como  $p(m)$  afirma isso mesmo, é verdadeira.
- Mas então,  $\neg p(m)$  é falsa.
- O que implica que  $\neg p(m)$  não é demonstrável visto que a teoria é válida.
- Logo a teoria é incompleta, porque nem  $p(m)$  nem  $\neg p(m)$  são demonstráveis.

# Teoremas da incompletude de Gödel

## Demonstração

### Primeiro teorema da incompletude de Gödel

Seja  $AP$  uma teoria de primeira ordem da aritmética de Peano. Existe uma proposição  $\varphi$  tal que, se  $AP$  for consistente- $\omega$ , nem  $\varphi$  nem a sua negação  $\neg\varphi$  são demonstráveis em  $AP$ .

### Segundo teorema da incompletude de Gödel

Seja  $T$  uma teoria consistente, com um sistema decidível de axiomas e contendo a aritmética de Peano. Existe uma proposição  $Cons_T$  que exprime que  $T$  é consistente e que não é demonstrável em  $T$ .

Segue linhas semelhantes às demonstrações anteriores.