O TEOREMA DA INDEFINIBILIDADE DA VERDADE DE TARSKI

FERNANDO FERREIRA

Definição 1. *Um predicado numérico k-ário $P(x_1, \dots, x_k)$ diz-se* aritmeticamente definível *se existe uma fórmula $\phi(x_1, \dots, x_k)$ da linguagem da aritmética com as variáveis livres $x_1, \dots, x_k$ tal que, para todos $n_1, \dots, n_k$ em $\mathbb{N}$, se tem*

$$P(n_1, \dots, n_k) \text{ se, e somente se, } \models_{\mathbb{N}} \phi(\overline{n_1}, \dots, \overline{n_k}).$$

Uma função numérica (total ou parcial) diz-se aritmeticamente definível *se o seu gráfico é uma relação aritmeticamente definível.*

Nas condições acima, e descontando ambiguidades relativas à ordem das variáveis, diz-se que a fórmula ϕ define o predicado P. De modo análogo, se a função k-ária f é aritmeticamente definível, então existe uma fórmula $\phi(x_1, \dots, x_k, y)$ da linguagem da aritmética tal que, para todos $n_1, \dots, n_k, m$ em $\mathbb{N}$, se tem

$$f(n_1, \dots, n_k) = m \text{ se, e somente se, } \models_{\mathbb{N}} \phi(\overline{n_1}, \dots, \overline{n_k}, \overline{m}).$$

Nestas condições diz-se que ϕ define a função f.

Proposição 1. *Toda a função recursiva primitiva é aritmeticamente definível. Todo o predicado recursivo primitivo é aritmeticamente definível.*

Demonstração. A segunda asserção é consequência imediata da primeira. A primeira demonstra-se por indução na complexidade das funções recursivas primitivas.

Começamos por ver que as funções iniciais são aritmeticamente definíveis. A função unária constantemente igual a 0 é definível pela fórmula $x = x \wedge y = 0$. A função sucessor S é definível pela fórmula $y = x'$. Dado $k \geq 1$ e $1 \leq i \leq k$, a função projecção P_i^k é definível pela fórmula

$$x_1 = x_1 \wedge \cdots \wedge x_k = x_k \wedge y = x_i.$$

Suponhamos que a função k-ária f se obtém por *composição generalizada* a partir das funções recursivas primitivas $h, g_1, \dots, g_m$:

$$f(x_1, \dots, x_k) = h(g_1(x_1, \dots, x_k), \dots, g_m(x_1, \dots, x_k)).$$

Por hipótese de indução, $h, g_1, \dots, g_m$ são funções definíveis por certas fórmulas $\eta, \gamma_1, \dots, \gamma_m$ (respectivamente). Claramente, a função f é definível pela fórmula $\phi(x_1, \dots, x_k, y)$ abaixo:

$$\begin{cases} \exists z_1 \cdots \exists z_m (\gamma_1(x_1, \dots, x_k, z_1) \wedge \cdots \\ \qquad \wedge\, \gamma_m(x_1, \dots, x_k, z_m) \wedge \eta(z_1, \dots, z_m, y)). \end{cases}$$

Resta ver o caso em que uma função f se obtém por recursão primitiva a partir de funções g e h. Este caso não é imediato como os anteriores pois, *prima facie*, a linguagem da aritmética não parece talhada para lidar com definições recursivas. Não obstante:

Lema da função β de Gödel. *Existe uma função ternária β, aritmeticamente definível, com a seguinte propriedade: para toda a sequência finita de números naturais $n_0, n_1, \dots, n_j$ existe um par de números n, m tal que $\beta(n, m, 0) = n_0$, $\beta(n, m, 1) = n_1$, $\dots$, $\beta(n, m, j) = n_j$.*

Com a ajuda deste lema pode mostrar-se que f é aritmeticamente definível caso g e h o sejam. Vamos supor que f tem aridade $k+1$. Observamos, então, que $f(j, r_1, \dots, r_k) = r$ se, e somente se, existe uma sequência $n_0, \dots, n_j$ de números naturais com $n_j = r$ tal que (1) $n_0 = g(r_1, \dots, r_k)$; e (2) $n_{i+1} = h(i, n_i, r_1, \dots, r_k)$, para todo $i < j$. Tendo em conta esta observação e supondo que g e h são aritmeticamente definíveis pelas fórmulas $\gamma(x_1,\ldots,x_k,y)$ e $\eta(z,w,x_1,\ldots,x_k,y)$ (respectivamente) e que a função β é definível pela fórmula $B(u,v,z,w)$, um pouco de reflexão convence-nos que f é definível pela seguinte fórmula $\phi(z,x_1,\ldots,x_k,y)$:

$$\left\{\begin{array}{l} \exists u \exists v[B(u,v,z,y) \wedge \exists \check{w}(B(u,v,0,\check{w}) \wedge \gamma(x_1,\ldots,x_k,\check{w})) \wedge \\ \qquad \forall i < z \exists w \exists \tilde{w}(B(u,v,i,w) \wedge B(u,v,i',\tilde{w}) \wedge \eta(i,w,x_1,\ldots,x_k,\tilde{w}))]. \end{array}\right.$$

□

Deixamos a demonstração do lema da função β para o final do capítulo, assim com algumas observações importantes em torno da *forma* das fórmulas aritméticas que definem as funções recursivas primitivas.

Proposição 2. *Um predicado é aritmeticamente definível se, e somente se, está na hierarquia aritmética.*

Demonstração. Vê-se facilmente, por indução na complexidade, que para cada termo $t(x_1,\ldots,x_k)$ da linguagem da aritmética a função k-ária

$$(n_1,\ldots,n_k) \rightsquigarrow t(\overline{n_1},\ldots,\overline{n_k})^{\mathbb{N}}$$

é recursiva primitiva. Daqui sai que os predicados aritméticos definidos por fórmulas atómicas (i.e., da forma $t = q$ ou $t < q$, com t e q termos) são recursivos primitivos. As fórmulas da linguagem da aritmética obtêm-se a partir das fórmulas atómicas por meio dos conectivos Booleanos e dos quantificadores. Ora, como os predicados da hierarquia aritmética são fechados para as operações Booelanas e as quantificações, sai imediatamente que toda a fórmula aritmética define um predicado na hierarquia aritmética.

Os predicados em Σ_1 obtêm-se a partir dos predicados recursivos primitivos prefixando-os por meio duma quantificação existencial. Dado que os predicados recursivos primitivos são aritméticamente definíveis, sai imediatamente que os predicados Σ_1 também o são. Passando às negações, o mesmo acontece com os predicados em Π_1. Ora, todo o predicado da hierarquia aritmética obtém-se a partir dos predicados em Σ_1 e Π_1 por meio de quantificações. Visto que as linguagens do cálculo de predicados estão munidas de quantificadores, conclui-se que todos os predicados da hierarquia aritmética são aritmeticamente definíveis. □

Recordemos que uma *verdade aritmética* é um elemento de $\mathsf{Vd}_{\mathbb{N}}$, i.e., um elemento do conjunto das fórmulas fechadas da linguagem da aritmética que são verdadeiras no modelo *standard*.

Proposição 3. *Todo o conjunto da hierarquia aritmética é redutível ao conjunto dos números de Gödel das verdades aritméticas.*

Demonstração. Seja V o conjunto dos números de Gödel dos elementos de $\mathsf{Vd}_{\mathbb{N}}$. Considere-se X um conjunto da hierarquia aritmética. Pela Proposição anterior, seja $\phi(v_0)$ uma fórmula com a única variável livre v_0 tal que, para todo $n \in \mathbb{N}$, $n \in X$ sse $\phi^{v_0}_{\overline{n}} \in \mathsf{Vd}_{\mathbb{N}}$. Logo, $n \in X$ sse $\#(\phi^{v_0}_{\overline{n}}) \in V$. Claramente, a função $n \rightsquigarrow \#(\phi^{v_0}_{\overline{n}})$ é recursiva (se necessário for, apelando à Tese de Chuch), o que demonstra a redutibilidade desejada. □

Teorema da Indefinibilidade da Verdade de Tarski. *O conjunto (dos números de Gödel) das verdades aritméticas não é aritmeticamente definível.*

Demonstração. Se o conjunto V dos números de Gödel das verdades aritméticas fosse aritmeticamente definível então estaria num determinado nível Σ_n da hierarquia aritmética. Pela proposição anterior, então todo o conjunto da hierarquia aritmética seria redutível a um conjunto em Σ_n. Em particular, isto aconteceria para os conjuntos Π_n-completos, o que é absurdo. □

Nesta altura, já podemos adiantar uma versão do Primeiro Teorema da Incompletude de Gödel:

Primeiro Teorema da Incompletude (versão semântica). *O conjunto das verdades aritméticas não é recursivamente axiomatizável. Consequentemente, existem verdades aritméticas que não estão na teoria* PA.

Demonstração. Se o conjunto das verdades aritméticas fosse recursivamente axiomatizável então, pelo Teorema da Completude de Gödel, formaria um conjunto recursivamente enumerável. Seria, portanto, aritmeticamente definível. Isto contradiz o Teorema da Indefinibilidade da Verdade de Tarski.

Claramente, PA é recursivamente axiomatizável (use-se a Tese de Church) e $\mathsf{PA} \subseteq \mathsf{Vd}_{\mathbb{N}}$. Pelo que vimos acima, esta inclusão tem que ser própria. □

Como prometido, vamos demonstrar o lema da função β de Gödel. A demonstração baseia-se em resultados da teoria elementar dos números, os quais supomos conhecidos. Necessitamos do seguinte lema:

Lema 1. *Seja $j \neq 0$ um número natural. Se m é múltiplo de todos os números primos menores do que j, então os números $m+1$, $2m+1$, ..., $jm+1$ são primos entre si dois a dois.*

Demonstração. Suponhamos, com vista a um absurdo, que existem números i e k com $1 \leq i < k \leq j$ de tal modo que $im+1$ e $km+1$ não são primos entre si. Então existe pelo menos um número primo p que divide $im+1$ e $km+1$. Claro que p não pode dividir m. Por outro lado, p divide a diferença entre os dois números acima e, portanto, divide $(k-i)m$. Conclui-se que p divide $(k-i)$. Logo, p é um número primo menor que j. Assim, por hipótese, divide m. Isto é uma contradição. □

O outro resultado de que necessitamos é o Teorema Chinês dos Restos. Suponhamos que s_0, s_1, ..., s_j são inteiros positivos, primos entre si dois a dois. Nestas condições, o Teorema Chinês dos Restos assegura que, para qualquer sequência finita $n_0, n_1, \ldots, n_j$ de números naturais com $n_i < s_i$ $(i \leq j)$, existe um número $n < \Pi_{i=0}^{j} s_i$ tal que, para todo $i \leq j$, $\mathit{Resto}(n, s_i) = n_i$. Se usarmos a noção de classe de congruência, podemos formular este resultado da seguinte maneira: nas condições acima, $\mathbb{Z}_{\Pi_{i=0}^{j} s_i}$ está em bijecção com o produto cartesiano $\mathbb{Z}_{s_0} \times \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_j}$ por meio da função

$$n \rightsquigarrow (n \mod s_0,\ n \mod s_1\ , \ldots,\ n \mod s_j).$$

Definimos a função β de Gödel simplesmente por:

$$\beta(n, m, i) = \mathit{Resto}(n, m(i+1)+1).$$

Esta função tem a propriedade desejada. Com efeito, dada uma sequência finita de números naturais $n_0, n_1, \ldots, n_j$, podemos tomar um número m maior que $\max\{n_0, n_1, \ldots, n_j\}$ tal que $m+1$, $2m+1$, ..., $jm+1$, $(j+1)m+1$ são primos entre si dois a dois. Aplica-se agora o Teorema Chinês do Resto para se obter n.

Finalmente, terminamos com uma caracterização da forma das fórmulas aritméticas que definem os predicados Σ_1.

Definição 2. *Uma fórmula da linguagem da aritmética diz-se* rudimentar *se se pode obter a partir das fórmulas atómicas por intermédio dos conectivos Booleanos e de quantificações limitadas, i.e., quantificações da forma $\forall x(x < t \to \ldots)$ e $\exists x(x < t \wedge \ldots)$, onde t é um termo onde x não ocorre. Uma fórmula da linguagem da aritmética diz-se uma fórmula* $\exists$-rudimentar *se é da forma $\exists x\, \phi$, com ϕ uma fórmula rudimentar.*

Como é habitual, abreviamos as quantificações limitadas por $\forall x < t\, (\ldots)$ e $\exists x < t\, (\ldots)$. Analogamente, $\forall x \leq t\, (\ldots)$ e $\exists x \leq t\, (\ldots)$ abreviam as fórmulas limitadas $\forall x(x < t' \to \ldots)$ e $\exists x(x < t' \wedge \ldots)$ (respectivamente). É claro que as fórmulas $\exists$-rudimentares definem predicados em Σ_1. Também se tem o recíproco:

Proposição 4. *Os predicados em Σ_1 são definíveis por fórmulas $\exists$-rudimentares.*

Demonstração. Primeiramente, observa-se que as funções recursivas primitivas são definíveis por fórmulas $\exists$-rudimentares. Isso vê-se por inspecção da demonstração de que as funções recursivas primitivas são definíveis por fórmulas aritméticas com a ajuda de quatro propriedades simples de definibilidade e do facto de que a função β de Gödel é definida pela fórmula rudimentar $B(u, v, z, w)$ dada por:

$$\exists x \leq u \, [u = x(v(z+1)+1) + w \wedge w < v(z+1)+1].$$

As quatro propriedades mencionadas acima são acerca dos predicados definidos por fórmulas $\exists$-rudimentares: estes (1) contêm os predicados definíveis por fórmulas rudimentares; (2) são fechados para as quantificações existenciais; (3) são fechados para as conjunções; e (4) são fechados para as quantificações universais limitadas.

As quantificações "inertes" justificam (1). (2) sai do facto de que um complexo da forma $\exists x \exists y \, (\ldots)$ é aritmeticamente equivalente (i.e., equivalente no modelo *standard* $\mathbb{N}$) a um complexo da forma $\exists w \exists x < w \exists y < x \, (\ldots)$. Para ver (3), note-se que uma conjunção da forma $\exists x \, \phi \wedge \exists y \, \psi$ é logicamente equivalente a $\exists x \exists y \, (\phi \wedge \psi)$. Por fim, um complexo da forma $\forall x < t \, \exists y \, (\ldots)$ é aritmeticamente equivalente a $\exists w \forall x < t \exists y < w \, (\ldots)$.

Seja, agora, $P(x_1, \ldots, x_k)$ um predicado em Σ_1. Como sabemos, existe um predicado $(k+1)$-ário *recursivo primitivo* $Q(x_1, \ldots, x_k, y)$ tal que, para todos $n_1, \ldots, n_k \in \mathbb{N}$, $P(n_1, \ldots, n_k)$ se, e somente se, $\exists y Q(n_1, \ldots, n_k, y)$. Pelo que já vimos, existe uma fórmula $\exists$-rudimentar $\phi(x_1, \ldots, x_k, y)$ que define $Q(x_1, \ldots, x_k, y)$. Claramente, a fórmula $\exists y \phi(x_1, \ldots, x_k, y)$ define $P(x_1, \ldots, x_k)$ e é equivalente a uma fórmula $\exists$-rudimentar. $\square$