Matemática Universitária Nº 12, dezembro de 1990, 23–41

Combinatória e Indemonstrabilidade, ou o 13º Trabalho de Hércules

Walter A. Carnielli* e Michael Rathjen

Instituto de Matemática - UNICAMP
Caixa Postal 6065
13.081 - Campinas, SP
e
Instituto de Lógica e Fundamentos da Matemática
Universidade de Münster, RFA.

Introdução: Os Paradoxos, Gödel e a máquina DIN–DIN

A idéia de demonstrar que algo "não se pode demonstrar" é em si mesma fascinante, e em raras ocasiões os estudantes e mesmo os matemáticos profissionais têm oportunidade de encontrar fenômenos matemáticos desse tipo. Em geral, tais argumentos só ocorrem nas provas de impossibilidade de solução dos "problemas clássicos gregos" (trissecção de ângulo, quadratura do círculo e duplicação do volume do cubo, usando apenas régua e compasso).

O objetivo deste trabalho é explicar, de maneira clara e simples, como é possível compreender o fenômeno de que certos resultados combinatórios finitos, que são corretos, não podem ser demonstrados na Aritmética formal (isto é, na Aritmética de Peano). Para isto a idéia principal está nas chamadas "funções de crescimento muito rápido", tão rápido, como veremos, que escapam ao poder de prova da Aritmética.

---

*Este artigo foi escrito enquanto W. A. Carnielli visitava a Universidade de Münster, como bolsista da Fundação Alexander von Humboldt. Queremos agradecer ao revisor deste trabalho pelas cuidadosas observações feitas.

Nosso tema está ligado ao grande debate sobre os fundamentos da Matemática travado no primeiro terço do século, envolvendo as figuras de David Hilbert, Kurt Gödel e seus seguidores. Em particular, desempenham papel central nesse debate os famosos teoremas de Gödel, ainda muito pouco compreendidos pelos matemáticos. Mostramos a seguir uma versão dramática do 1º teorema da incompletude de Gödel, e esperamos explicar ao leitor sem nenhum conhecimento prévio de Lógica Matemática, como tudo isso se relaciona.

Os teoremas de incompletude de Gödel, de 1931, representam de certa forma o fim da idade romântica da Matemática. Antes de Gödel, fazia parte de um amplo projeto de trabalho liderado por David Hilbert, conhecido como Programa de Hilbert, acreditar que todo problema matemático fosse solúvel. Nas próprias palavras de Hilbert, num congresso em Münster, em 1925: "Se existe um problema, ache a solução; você pode encontrá-la apenas pensando, pois não há *ignorabimus* em matemática".

De forma bastante simplificada, podemos colocar em dois pontos o que Hilbert e sua escola propunham:

1) Axiomatizar todo o corpo de conhecimento matemático (inclusive com objetivo de provar que todo problema matemático fosse solúvel).

2) Provar, por meios *estritamente finitários*, que a axiomática em 1) é consistente.

Por meios estritamente finitários entende-se aqui métodos de prova que não façam apelo ao infinito atual como infinito completado (em contrapartida ao infinito potencial). Em termos simples, Hilbert propunha que as teorias poderiam se referir ao infinito simbolicamente, mas a consistência deveria ser provada por métodos combinatórios, sem que se usasse a noção de infinito como um processo terminado.

Na verdade, a noção de "meios finitários só foi plenamente entendida bem depois da proposta de Hilbert. Do ponto de vista moderno, podemos identificar "finitário com "computável ou "recursivo no sentido das funções recursivas, tratadas em qualquer livro texto básico em ciências da computação. Alguns autores vão mais longe, a ponto de identificar os "meios estritamente finitários" de Hilbert às funções primitivas recursivas, uma sub-classe bem mais restrita das funções computáveis.

Os esforços para levar a efeito 2) deram origem à chamada *teoria da prova*[1]. A preocupação em provar a consistência da Matemática, e prová-la com os métodos que pareciam mais seguros (isto é, por meios estritamente finitários), era compreensível após a crise desencadeada pela descoberta, no começo do século, de que paradoxos podiam ser expressos matematicamente. Em particular, o conhecido Paradoxo de Russell[2] despertou suspeitas sobre os conceitos *impredicativos* ou *circulares* em Matemática.

Um conceito C é *impredicativo* quando sua definição faz uso de uma totalidade à qual C já pertence. O Paradoxo de Russell propunha que se toda propriedade define um conjunto, então a propriedade de "não pertencer a si mesmo", definiria um conjunto R, a saber, o "conjunto de todos os conjuntos que não pertencem a si mesmos". Como R é um conjunto, se ele pertence a si mesmo, isto é, se $R \in R$, então não é um elemento de R, isto é, $R \notin R$. Analogamente se $R \notin R$, então $R \in R$, o que significa: $R \in R$ se e somente se $R \notin R$, uma contradição.

O conjunto proposto por Russell é impredicativo, já que sua definição leva em conta todos os conjuntos, inclusive R. *No entanto, nem todos os conceitos impredicativos levam a contradições,* pelo menos a contradições imediatas: a definição usual de *supremo, de um conjunto de números reais* por exemplo, como "o menor dos limites superiores", define o supremo a partir da totalidade à qual ele pertence, e aparentemente não leva a contradição. Dessa forma, um problema central nos fundamentos da Matemática é saber quais procedimentos impredicativos levam a paradoxos que resultem em contradição.

Os paradoxos, em si, são muito *mais antigos* do que o debate desencadeado por Russell; talvez uma das indicações mais eloqüentes da importância deles para os fundamentos da Matemática seja o fato notável de que a preocupação em evitá-los foi

[1]Na verdade, fazia parte também do Programa de Hilbert uma proposta de eliminação dos elementos ideais em Matemática. Esta parte do Programa foi de certa maneira realizada. Uma boa introdução à teoria da prova com todos os detalhes é o livro de Pohlers [12].

[2]Uma discussão detalhada do Programa de Hilbert, dos Teoremas de Gödel, e de como isso se relaciona com a teoria da computabilidade pode ser encontrada em [5]. Os principais paradoxos formuláveis matematicamente e suas conseqüências são também discutidos nesse livro.

uma das causas do Programa de Hilbert, e uma sutil formulação Matemática do Paradoxo do Mentiroso, conhecido já dos antigos gregos, foi seu fim.

Gödel foi capaz de mostrar que:

1º Teorema de Incompletude: Em todo sistema formal consistente S, com um mínimo de Aritmética, é possível formalizar uma sentença **U** tal que **U** possa ser interpretada intuitivamente como a afirmação de que ela própria é indemonstrável em S.

Essa sentença **U** é formalmente indemonstrável em S, e portanto ela expressa um fato verdadeiro. Contrariando o que Hilbert acreditava, **U** constitui um legítimo *ignorabimus* em Matemática! Em segundo lugar, Gödel mostrou também que:

2º Teorema da Incompletude: A prova da consistência para sistemas formais (nas condições que Hilbert queria) não pode ser formalizada dentro do próprio sistema[2].

Um exemplo literário que ilustra a idéia desenvolvida por Gödel (no 1º Teorema de Incompletude) é o seguinte: um conhecido político que havia mentido durante toda sua vida pública, antes de retirar-se da carreira política, afirmou o seguinte, tentando salvar sua memória: "Eu sempre menti em toda minha carreira, e esse é um fato que pode ser provado".

Seus adversários quiseram provar que ele realmente havia mentido a vida toda. No entanto, depararam-se com um problema: se inclusive essa última frase fosse falsa, ou ele não havia mentido a vida toda, ou esse fato não poderia ser provado. Seus companheiros, por outro lado, tentando argumentar que ele não havia mentido a vida toda, encontraram um problema semelhante: como a única esperança era argumentar que a última frase fosse verdadeira, o que seria admitir que se poderia provar que ele houvera realmente mentido sempre.

Portanto o fato **U**: "ele sempre mentiu" é tal que nem **U** e nem $\neg$**U** (onde o símbolo "$\neg$" significa "negação") podem ser provados, mas é contudo verdadeiro, porque ele sempre mentiu, inclusive ao afirmar que U poderia ser provado![3] A prova formal desse teorema baseia-se no fato de que todas as noções envolvidas podem ser expressas aritmeticamente, isto é, com os "meios estritamente finitários" que Hilbert exigia. No fundo o aspecto mais importante desse processo é que a aritmetização acaba referindo-se a si mesma.

Uma outra tentativa de ilustrar esse aspecto, evitando-se a questão aritmética e enfatizando-se a questão da auto-referência é o seguinte exemplo, adaptado livremente de um quebra-cabeças proposto pelo lógico R. Smullyan, que chamaremos de "máquina DIN–DIN". A máquina DIN–DIN imprime, numa fita, combinações arbitrárias dos símbolos D, I, N e –. Algumas combinações especiais são chamadas *sentenças*: são elas quaisquer seqüências do tipo I–X, ID–X, NI–X e NID–X, onde X é uma seqüência arbitrária. Dizemos que o mecanismo que faz DIN–DIN imprimir seqüências na fita é um *sistema formal*. Por outro lado, uma *interpretação* (ou um *modelo*) do sistema formal consiste em atribuir um *sentido* às sentenças e um *valor–verdade* ("verdadeiro" ou "falso") a tal sentido, da seguinte maneira:

1) I–X significa "X é imprimível", e é verdadeira se e somente se X aparece (mais cedo ou mais tarde) impresso na fita.

2) ID–X significa "X–X é imprimível" (isto é, o dobro de X é imprimível) e é verdadeira see X–X aparece (mais cedo ou mais tarde) impresso na fita.

3) NI–X significa "X não é imprimível", e é verdadeira see X nunca aparece impresso na fita.

4) NID–X significa "X–X não é imprimível", e é verdadeira see X–X nunca aparece impresso na fita.

Pode-se ver aí claramente que a interpretação (que associa "imprimível" a I, "dobro" a D, e "não" a N) é uma proprie-

[3]Este exemplo é particularmente interessante pela seguinte razão: se $\mathbf{Pr}(x)$ é o predicado de "provabilidade" em **PA**, e $\ulcorner\psi\urcorner$ é o número de Gödel de ψ, a sentença proferida é da forma:

$$\psi \longleftrightarrow \neg\mathbf{Pr}(\ulcorner\psi\urcorner) \wedge \mathbf{Pr}(\ulcorner\neg\mathbf{Pr}(\ulcorner\psi\urcorner)\urcorner).$$

Pode-se mostrar que para $\mathbf{U} := \neg\mathbf{Pr}(\ulcorner\psi\urcorner)$, valem:

(i) **U** é verdadeira,

(ii) $\mathbf{PA} \nvdash \mathbf{U}$,

(iii) $\mathbf{PA} \nvdash \neg\mathbf{U}$.

dade *fora* da máquina, que "fala sobre" a máquina, ao contrário da noção de sistema formal, que de certa forma "é a própria" máquina. Fazemos ainda uma hipótese adicional ao sistema formal:

Hipótese de correção: Quando DIN–DIN imprime sentenças, essas sentenças são verdadeiras. Isso não significa que DIN–DIN imprime *somente* sentenças, nem que ela imprime *todas* as sentenças verdadeiras possíveis, mas apenas que DIN–DIN não imprime sentenças falsas.

Considere agora a sentença NID–NID; essa sentença é verdadeira see o dobro de NID, isto é, NID–NID, nunca aparece impresso na fita, ou, em outras palavras, a sentença NID–NID afirma que *ela própria* é verdadeira see não é imprimível. Temos então que, ou ela é falsa e imprimível, ou é verdadeira e não imprimível. O primeiro caso não pode ocorrer, pela Hipótese de correção; portanto NID–NID é um exemplo de sentença *verdadeira mas que* DIN–DIN *não pode imprimir*!

O 2º Teorema de Incompletude leva em conta que a asserção "S é consistente" também pode ser formulada em termos aritméticos dentro de S, digamos pela fórmula $\mathbf{CON}(S)$, e que pode-se demonstrar a implicação $\mathbf{CON}(S) \longrightarrow \mathbf{U}$. Portanto, se $\mathbf{CON}(S)$ pode ser demonstrada em S, $\mathbf{U}$ também será. Dessa forma, os teoremas de Gödel mostram que *existem* problemas insolúveis em Matemática, em particular na Aritmética, e que a consistência das teorias matemáticas não pode ser formalizada usando seus próprios recursos, em particular a consistência da Aritmética não pode ser provada usando próprios recursos aritméticos ou "estritamente finitários".

Como podemos ver, uma das idéias básicas por trás dos argumentos de Gödel é a auto-referência usada diabolicamente, como no Paradoxo do Mentiroso: se alguém afirma "Eu estou mentindo agora", sua afirmação é verdadeira ou falsa? Ou mais simplesmente, a sentença "Esta sentença é falsa", é verdadeira ou falsa?

2. A Prova de Gentzen

No entanto, apesar dos Teoremas de Gödel, Gerhard Gentzen, um assistente de Hilbert em Göttingen, conseguiu obter em 1936 uma prova da consistência da teoria dos números. A prova de Gentzen, embora não salvasse o Programa de Hilbert, foi extremamente importante porque conseguiu mostrar que os "meios não-finitários" necessários à prova da consistência localizavam-se exatamente no esquema de indução. Meios não-finitários eram claramente necessários, já que Gödel mostrara que somente por meios finitários tal prova seria impossível. Em particular, Gentzen mostrou que a consistência da teoria dos números sem o esquema de indução pode ser facilmente demonstrada por meios finitários. Como conseqüência, o aparentemente inocente esquema da indução da Aritmética torna-se o principal suspeito por eventual conspiração contra a consistência da Matemática.

Gentzen inventou o cálculo de *dedução natural*[4], uma formulação do cálculo de predicados radicalmente diferente da usual (do tipo "axiomas + regras de derivação", chamada de "axiomática do tipo Hilbertiano"). A nova idéia embutida na dedução natural é que as regras para os operadores lógicos podem ser divididas em dois tipos: as regras de "introdução" e as de "eliminação". Assim, por exemplo, regras de "$\wedge$-introdução" e "$\wedge$-eliminação" são, respectivamente,

$$\frac{A, B}{A \wedge B} \quad \text{e} \quad \frac{A \wedge B}{A, B}$$

significando "se A e B são verdadeiras, o conectivo $\wedge$ pode ser introduzido fazendo $A \wedge B$ verdadeira", e "se $A \wedge B$ é verdadeira, o conectivoO$\wedge$ pode ser eliminado, fazendo A e B ambas verdadeiras". Formulando-se regras desse tipo para os conectivos $\vee$, $\wedge$, $\longrightarrow$ $\neg$ e para os quantificadores $\forall$, $\exists$ obtém-se um cálculo lógico com grande ênfase na *simetria* das provas.

Pouco mais tarde, Gentzen formulou uma nova versão desse cálculo conhecido como *cálculo de seqüentes*. Uma regra importante desse cálculo é a *regra do corte*, formulada como segue:

$$\frac{\Gamma;\ A \quad \Gamma;\ \neg A}{\Gamma}.$$

Essa regra significa que, se alguma das fórmulas do conjunto Γ, ou a fórmula A for verdadeira, e por outro lado uma das fórmulas

[4]Uma formulação similar foi proposta independentemente pelo lógico polonês Jáskowski.

de Γ, ou $\neg$ **A**, é verdadeira, então a fórmula verdadeira deve estar em Γ (pois, caso contrário, **A** e $\neg$ **A** teriam que ser verdadeiras).

A regra do corte tem uma característica muito importante: ela é a única regra do cálculo onde uma componente (no caso a fórmula **A**) pode ser *eliminada*. Assim, se a regra do corte foi usada, conhecendo-se somente o final da prova, não é possível saber se alguma fórmula foi introduzida na prova e em algum momento cancelada. Em outras palavras, a regra do corte concentra todo o *indeterminismo* das provas, como veremos.

Gentzen conjecturou que poderia ser possível transformar toda prova lógica numa certa *forma normal*, onde a regra do corte pudesse ser dispensada. Essa conjectura foi provada no conhecido "Hauptsatz" ou "Teorema Principal" (também chamado "Teorema de Eliminação do Corte"). Como conseqüência do "Hauptsatz" pode-se obter a *propriedade da subfórmula*: em todo sistema livre de corte, todas as fórmulas usadas numa prova estão presentes no seqüente (isto é, na asserção final). Dessa forma, em sistemas livres de corte, se duas pessoas provam independentemente um resultado matemático, essas provas não podem ser muito diferentes!

Esse resultado aproxima então, tanto quanto possível, o ato de provar de um ato *mecânico*. Não é surpresa, portanto, que um tal resultado, ou variante dele, como o Teorema de Herbrand, obtido por Herbrand em sua tese de doutorado em 1931, constitua peça fundamental na teoria da prova automática de teoremas. De fato, a linguagem PROLOG, por exemplo, é uma implementação de parte do cálculo de seqüentes, misturado com técnicas de controle, ainda que esse fato passe às vezes despercebido em ciência da computação.

O método de dedução natural de Gentzen influenciou fortemente o desenvolvimento do método dos *tableaux semânticos* introduzido por Beth e outros métodos de prova conhecidos como "provas por refutação de contra-exemplos".

3. Ordinais e Provas

Gentzen mostrou que para provar a consistência da teoria dos números (que de agora em diante denotaremos por **PA** ou *Aritmética de Peano*) é necessário fazer apelo a um princípio envolvendo ordinais. Os ordinais transfinitos são objetos que se fundamentam na relação de ordem. Uma *relação de ordem* sobre um conjunto X é qualquer relação binária $\leq$ que satisfaça, para quaisquer $x, y, z \in X$ as seguintes condições:

1) reflexidade ($x \leq x$)
2) antissimetria ($x \leq y$ e $y \leq x$ implica $x = y$)
3) transitividade ($x \leq y$ e $y \leq z$ implica $x \leq z$).

Dizemos nesse caso que X é *ordenado* por $\leq$. Se, ademais, todo subconjunto Y de X tem um primeiro elemento em relação a $\leq$ (isto é, existe $y_0 \in Y$ tal que $y_0 \leq x$ para todo $x \in Y$) dizemos que X é *bem-ordenado* por $\leq$.

Um *segmento inicial* definido por $a \in X$ é o conjunto $S(a) = \{x \in X : x \leq a \text{ e } x \neq a\}$

Um *ordinal* é um tipo especial de conjunto bem-ordenado α, tal que para todo $\beta \in \alpha$ o segmento inicial $s(\beta)$ coincide com β. Assim, por exemplo, cada ordinal finito n pode ser visto como o conjunto $\{0, 1, \ldots, n-1\}$.

É fácil mostrar que todo segmento inicial de um ordinal é também um ordinal.

Dois conjuntos X e Y, ordenados respectivamente por $\leq$ e $\preceq$, são chamados, *ordem-isomorfos* se existe uma bijeção $f: X \longleftarrow Y$ tal que $a \leq b$ see $f(a) \preceq f(b)$.

Pode-se provar que todo conjunto bem-ordenado é ordem-isomorfo a um único ordinal. Dessa forma, os ordinais podem ser vistos como *representantes* dos conjuntos bem-ordenados, via ordem-isomorfismo.

Se α é um ordinal, o conjunto $\alpha \cup \{\alpha\}$ é um outro ordinal que não é ordem-isomorfo a nenhum de seus segmentos iniciais; denotamo-lo, então, por $\alpha + 1$.

Analogamente, se $\alpha_1, \alpha_2, \ldots \alpha_n, \ldots$ é uma sequência infinita crescente de ordinais, pode-se provar, usando axiomas especiais para conjuntos, que a união $\bigcup_{i \in \mathbf{N}} \alpha_i$ é também um ordinal.

Mostramos, a seguir, como se definem os ordinais até ϵ_o, baseando-se nas operações de "somar um e "tomar limites de sequências (que significa, intuitivamente, terminar um processo infinitário, colecionando ordinais em outro ordinal maior):

1) Primeiro, temos a seqüência de números naturais

$$0, 1, 2, \ldots, n, \ldots.$$

2) Num segundo estágio imaginamos esse processo terminado, o que dá origem ao ordinal ω.

3) Num terceiro estágio, continuamos:

$$\omega, \omega + 1, \omega + 2, \ldots, \omega + n, \ldots.$$

4) No próximo passo, imaginando esse processo terminado, obtemos o ordinal $\omega \cdot 2$.

5) Analogamente,

$$\omega \cdot 2, \omega \cdot 2 + 1, \omega \cdot 2 + 2, \ldots$$

até obtermos $\omega \cdot 3$ como o ordinal que significa o término deste processo.

Obtemos, assim, imaginando cada processo terminado,

$$\omega, \omega \cdot 2, \omega \cdot 3, \ldots, \omega \cdot n, \ldots$$

e, imaginando *este* processo terminado, obtemos ω^2.

Repetindo todo o processo a partir de ω^2, obtemos:

$$\omega^2, \omega^2 + 1, \omega^2 + 2, \ldots, \omega^2 + \omega, \ldots, \omega^2 + \omega \cdot 2 + 1, \ldots$$

terminando o processo com ω^3.

Imaginando agora a seguinte seqüência terminada:

$$\omega, \omega^2, \omega^3, \ldots, \omega^n, \ldots$$

obtemos ω^ω, e repetindo sempre a mesma idéia, imaginando a próxima seqüência terminada:

$$\omega, \omega^\omega, \omega^{\omega^\omega}, \ldots,$$

obtemos o ordinal $\varepsilon_o = \omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}$ como uma torre infinita de ω's.

Vamos denotar por ω_n uma torre formada pela potência de base ω e expoente formado por sua vez como uma torre de $(n-1)$ ω's:

$$\omega_n = \left.\omega^{\omega^{\cdot^{\cdot^{\cdot^{\omega}}}}}\right\} n \text{ vezes.}$$

De forma precisa, definimos tais ordinais como: $\omega_o = 1$, $\omega_{n+1} = \omega^{\omega_n}$. Note que, por exemplo, ω_3 é $\omega^{(\omega^\omega)}$ e não $(\omega^\omega)^\omega$.

Todos os ordinais definidos "imaginando o processo terminado" são os *ordinais limites*, os outros são os *ordinais sucessores*.

Se assumirmos o esquema da *indução transfinita* como válida, na forma: "Se para uma propriedade $\mathbf{A}$ vale $\mathbf{A}(0)$, e se valendo $\mathbf{A}(\alpha)$ para todo $\alpha < \beta$ implica que vale $\mathbf{A}(\beta)$, então vale $\mathbf{A}(\gamma)$ para todo $\gamma < \varepsilon_o$", pode-se demonstrar a consistência de **PA**[5].

A idéia é a seguinte: é possível associar um código ordinal $\text{Ord}(p) < \varepsilon_o$ a cada prova p em **PA** de tal maneira que se p é a prova de uma inconsistência, existe sempre p' tal que p' também é a prova de uma inconsistência e $\text{Ord}(p') < \text{Ord}(p)$. Se supusermos que este processo de "descida" deve terminar em um número finito de passos, tal prova de inconsistência é impossível. A hipótese "este processo de descida termina em um número finito de passos" equivale a supor uma boa-ordem de tipo transfinito nos números naturais, e este é precisamente o ponto onde meios infinitários são necessários e onde ordinais entram na estória.

Baseados nos ordinais acima, podemos definir funções que crescem *muito* rápido. Uma das maneiras de se obter funções assim é a seguinte definição indutiva:

$$F_o(n) = n + 1$$

$$F_{\alpha+1}(n) = F_\alpha^{n+1}(n) \quad \text{(isto é, } F_\alpha \text{ composta } n+1 \text{ vezes) se } \alpha \text{ é ordinal sucessor,}$$

$$F_\alpha(n) = F_{\alpha(n)}(n), \quad \text{onde } \alpha(n) \text{ é o } n\text{-ésimo passo da seqüência que definiu } \alpha, \text{ se } \alpha \text{ é ordinal limite.}$$

[5] Na realidade é necessário muito menos que isso: basta supor este princípio para sentenças **A** que denotam predicados computáveis.

Para se ter uma idéia de como essas funções crescem rapidamente, para $\alpha = 0, 1, 2, 3$ temos:

$$F_o(n) \geq n,$$

$$F_1(n) \geq 2n,$$

$$F_2(n) \geq 2^n,$$

$$F_3(n) \geq \left. 2^{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}} \right\} n \text{ "2's" empilhados, e } n \text{ no topo.}$$

Não é difícil calcular que $2^{2^{2^{13}}} > 10^{10^{1000}}$ ou seja, 1 seguido de 10^{1000} zeros. Calculando que num livro de 1000 páginas cabem no máximo 10^7 zeros, precisaríamos de 10^{993} desses livros, certamente mais papel do que existe no mundo. Mas esse número é microscópico comparado com $F_3(13) \cdots$.

A função F_{ε_o} cresce de tal maneira rapidamente que o ordinal ε_o "marca o limite da demonstrabilidade em **PA**", isto é, se alguma prova é correta em **PA**, ela deve poder ser analisada por meio de ordinais menores que ε_o.[6] Por outro lado, se uma certa propriedade combinatória envolver funções que crescem mais rapidamente que F_{ε_o} então esta propriedade combinatória *não* pode ser *demonstrada em* **PA**, embora possa ser verdadeira. Esse fato é a chave de muitas provas conhecidas sobre indemonstrabilidade de propriedades combinatórias.

Resultados desse tipo sobre indemonstrabilidade constituem exemplos do grande hiato que existe entre o tratamento axiomático de um conceito (por exemplo, provas em **PA**) e o tratamento conjuntista (por exemplo, provas na teoria de conjuntos usual). Basicamente, quando trabalhamos com um conceito do ponto de vista conjuntista, estamos provando propriedades de uma *determinada construção* relativa ao conceito (como, por

[6] O ordinal que marca o limite da provabilidade de uma teoria **T** pode ser visto também como "o primeiro ordinal não demonstrável em **T** que consegue provar a consistência de **T**". As definições e o cálculo de tais ordinais fazem parte da chamada *análise ordinal*.

exemplo, os números naturais tomados como conjuntos), enquanto que quando o consideramos do ponto de vista axiomático (como, por exemplo, os números naturais em PA) estamos provando propriedades *gerais*, sem nos comprometermos com uma determinada construção.

Existe, por isso, interesse em estudar subsistemas da teoria de conjuntos[7], em especial os que envolvem quantificação sobre *conjuntos* de números naturais (chamados sistemas de segunda ordem)[8].

4. A Batalha Entre Hércules e a Hidra

Os resultados de Gödel, especialmente o 1º Teorema, colocaram uma dúvida natural para os matemáticos: seria possível que um problema aberto, como por exemplo o "Teorema" de Fermat ou a Conjectura de Goldbach, fossem indecidíveis? Ou, pelo menos, que se encontrasse uma sentença indecidível mas que tivesse um pouco mais de interesse matemático? Essa questão foi parcialmente resolvida em 1977, quando J. Paris e L. Harrington descobriram que basta uma pequena modificação no teorema de Ramsey, caso finito, para que se obtenha uma asserção combinatória finita, que embora verdadeira quando interpretada em termos de conjuntos, é indemonstrável em **PA**.

A versão que Paris e Harrington consideram (PH) é a seguinte: dizemos que um conjunto finito de números naturais é *largo* se $|s| > min(s)$. Por exemplo, $\{5, 9, 979, 10^{10}\}$ não é largo, mas $\{1, 4\}$ é. Os conjuntos da forma $\{1, 2, \ldots, k\}$ são trivialmente largos; dizemos então que S é *não-trivialmente largo* se S é largo mas não dessa forma.

Uma r-*coloração para* k-*conjuntos* é uma função dos conjuntos com k elementos em $r = \{0, 1, 2, \ldots, r-1\}$.

(PH): Para todo r, k existe n suficientemente grande tal que para qualquer coloração dos k-conjuntos de $B = \{k+1, k+$

---

[7] Uma grande variedade de subsistemas da teoria de conjuntos é estudada em [13]. Um exemplo de análise ordinal para um subsistema importante da teoria de conjuntos é feita em [14].

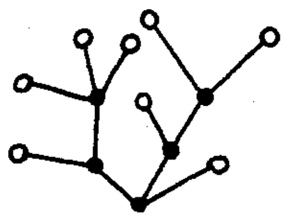
[8] Harvey Friedman (ver [10]) tem obtido resultados espetaculares em um programa de trabalho conhecido como *Matemática reversa*. Este programa consiste basicamente em isolar e estudar detalhadamente subsistemas de segunda ordem "fabricados sob medida" para certas áreas da Matemática.

$2, \ldots, n\}$ existe um k-conjunto $M \subset B$ não trivialmente largo e monocromático.

O Teorema de Paris-Harrington foi provado por meios semânticos, e sua prova não deixa muito claro qual é o aspecto combinatório envolvido que se recusa a ser demonstrável[9].

Um segundo exemplo de incompletude em **PA** que nos interessa discutir aqui é uma contrapartida Matemática de um episódio mitológico. A Hidra era uma criatura de nove cabeças, contra a qual todos os heróis fracassavam, porque de cada cabeça cortada brotavam outras duas. Coube a Hércules, filho de Zeus, a tarefa de derrotar a Hidra como um dos seus doze trabalhos, os quais, realizados, lhe deram o dom da imortalidade.

Suponhamos que por alguma razão olímpica, Hércules, agora já imortal, seja incumbido de combater uma outra Hidra, mais perigosa que a primeira. A Hidra agora é um monstro finito, em forma de árvore, constituída de uma *raiz* e de um número finito de *pescoços* (ou *nós*). Os nós superiores são as cabeças. Hércules deve vencê-la cortando todos os nós, até cortar a raiz.



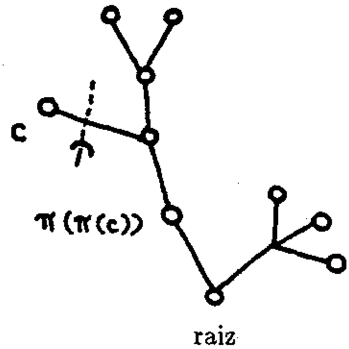
raiz

Essa Hidra, contudo, tem propriedades regenerativas surpreendentes: se denotamos por $\pi(c)$ o (único) *predecessor* de um nó c, e por $\pi(\pi(c))$ o predecessor de $\pi(c)$, a Hidra tem a seguinte propriedade:

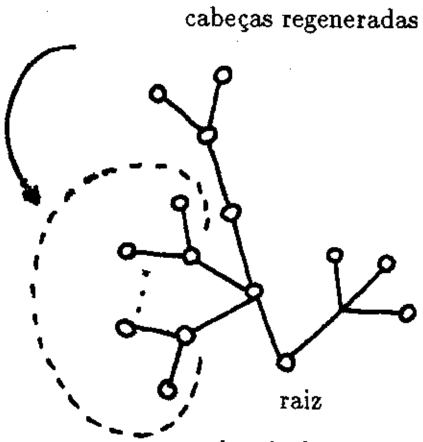
Para qualquer nó c, ela pode gerar em $\pi(\pi(c))$ um número *arbitrário* de cópias do que sobrou a partir de $\pi(c)$, caso $\pi(\pi(c))$ não seja a raiz.

[9] A prova original de Paris e Harrington pode ser encontrada em **[11]**. Em **[3]** temos um exemplo de outro princípio combinatório *à la* Ramsey, cujos casos finitos podem ser demonstrados em PA, mas cujo caso infinito é incompatível com o Axioma da Escolha, embora seja consistente com todos os demais axiomas de ZF.

Caso $\pi(\pi(c))$ ou $\pi(c)$ seja a raiz, não há possibilidade de regeneração.



antes do corte



depois do corte

Como pode Hércules vencê-la?

Na verdade, pode-se demonstrar que a Hidra perde sempre, independente de qualquer estratégia que Hércules utilize, mas tal fato não pode ser demonstrado em PA.

Uma prova completamente sintática, que deixa claro todo o processo combinatório envolvido, pode ser feita atribuindo-se ordinais às Hidras, e mostrando-se que a asserção "Hércules vence contra qualquer Hidra" equivale à indução transfinita sobre o ordinal ε_o.[10]

Para se ter uma idéia de como ordinais transfinitos se relacionam com objetos finitos (no caso, as Hidras) definimos explicitamente a correspôndencia $o(H)$ que associa a cada Hidra um ordinal:

1) Se H tem um único nó (i.e., somente a raiz) então $o(H) = 0$.

2) Se H tem mais que um nó, existem sub–Hidras $H_1, H_2, \ldots, H_n$ cujas raízes são os nós sucessores à raíz de H. Se $o(H_1), \ldots, o(H_n)$ são ordinais asociados a estas sub–Hidras, definimos, supondo $o(H_1) \geq o(H_2) \geq, \ldots \geq o(H_n)$:

$$o(H) = w^{o(H_1)} + \ldots + w^{(H_n)}$$

É claro que $o(H) < \varepsilon_o$, e pode-se compreender como asserções relativas aos ordinais $< \varepsilon_o$ transformaram-se em asserções a respeito das Hidras.

5. Indemonstrabilidade em Subsistemas da Aritmética

De uma certa forma, pode-se medir a *complexidade* de uma fórmula aritmética pela quantidade de quantificadores que ela contém. Assim, dizemos que uma fórmula é do tipo $\sum_k$ se ela for do tipo

$$(\exists x_1)(\forall x_2)\ldots(Qx_k)R(x_1, x_2, \ldots, x_k)$$

onde $Q = \exists$ se k é ímpar. $Q = \forall$ se k é par, e R é um predicado computável. Trocando-se cada quantificador $\forall$ por $\exists$ e vice-versa define-se, dualmente, as fórmulas de tipo Π_k. Por exemplo a Conjectura dos Números Primos Gêmeos, que afirma que existem infinitos primos da forma $p + 2$, para p primo, é do tipo Π_2:

$$(\forall n)(\exists p)(p > n \wedge p \text{ primo} \wedge (p+2) \text{ primo}).$$

Nosso objetivo nesta última parte é apresentar as idéias de um trabalho em conjunto (ver [4]), onde mostramos que em cada

[10] A prova a que nos referimos aqui é uma adaptação da prova de [1] sobre a indemonstrabilidade da convergência das seqüências de Goodstein. Detalhes podem ser encontrados em [2].

classe de complexidade Σ_k (ou, equivalentemente, Π_k) existe um resultado combinatório independente da Aritmética restrita àquela classe.

Suponhamos que associamos a cada Hidra uma *altura*, de tal maneira que Hidras que contenham somente a raiz tenham altura 0, e em geral a altura seja o número de nós (excluindo a raiz) no maior ramo.

Em [4] mostramos que é possível refinar a batalha entre Hércules e a Hidra, de tal maneira que se restringimos a altura máxima de Hidra H_k à $k, (k > 0)$, pode-se provar que se H_k segue uma estratégia de regeneração "não muito complicada" (em termos formais, uma estratégia primitiva recursiva) então, para todo $k \geq 1$:

1) Hércules vence H_{k+1},

2) esse fato pode ser demonstrado em $\mathbf{PA}_{k+1}$ (onde $\mathbf{PA}_n$ significa a Aritmética de Peano onde o esquema de indução só pode ser utilizado em fórmulas do tipo $\sum_n$) mas

3) não pode ser demonstrado em $\mathbf{PA}_k$.

A idéia intuitiva desenvolvida é no fundo uma aplicação do método diagonal que surgiu quando Cantor inventou sua prova do não-enumerabilidade dos números reais, e foi depois largamente utilizada em Matemática, em especial na teoria da computabilidade.

Vamos aplicar essa idéia a certos *pontos fixos* envolvendo os ordinais introduzidos na Seção 3.

Como vimos, ω^2 pode ser imaginado como

$$\omega^2 = \omega + \omega + \omega + \ldots ;$$

$$\text{daí} \qquad \omega + \omega^2 = \omega + (\omega + \omega + \omega + \ldots) = \omega^2$$

Portanto ω^2 é o primeiro ponto fixo da operação $\omega + x$, isto é,

$$\omega + x = x \longleftrightarrow x = \omega^2.$$

Concluímos, então que embora ω^2 possa ser "construído" usando produto em ω's (simplesmente como $\omega^2 = \omega.\omega$) ele não pode ser construído usando-se somente a soma de ω's, pois ele é ponto fixo da soma. Em outras palavras, sua caracterização por meio de soma envolve o fato de que ele teria que ser *reconhecido* como completo *antes* que estivesse completo !

Analogamente, podemos mostrar que

$$\omega_n.x = x \longleftrightarrow x = \omega_{n+1},$$

o que mostra que ω_{n+1} (torre com $n+1$ ω's) é o primeiro ponto fixo não nulo desta operação. Portanto ele não pode ser construído com recursos da Aritmética de ω_n (isto é, com as operações de soma, produto, e potência iterada na forma de torre com altura n).

Por último, $\omega^x = x \longleftrightarrow x = \varepsilon_o$, como pode-se ver facilmente (de modo completamente similar ao caso ω^2). Vemos portanto que ε_o é o primeiro ponto fixo desta operação.

Podemos demonstrar que cada um desses pontos fixos marca o limite da teoria $\mathbf{PA}_n$ (em termos precisos, o ordinal da teoria $\mathbf{PA}_n$ é ω_{n+1}). Em particular, podemos demonstrar que cada asserção "Hércules vence as Hidras H_n de altura restrita a n" necessita dos recursos aritméticos de ω_n para ser provada. Esse resultado vale para qualquer resultado combinatório que envolva funções que cresçam pelo menos tão rapidamente quanto F_{ω_n}. Temos daí outra idéia intuitiva sobre por quê **PA** necessita dos recursos de ε_o para provar sua própria consistência: como cada ω_{n+1} está fora do alcance de $\mathbf{PA}_n$, e como **PA** pode ser vista como o limite de $\mathbf{PA}_n$, então **PA** está fora do alcance do limite de ω_{n+1} (isto é, fora do alcance de ε_o).

Por enquanto, os únicos exemplos conhecidos (pelo menos por nós) são as infinitas batalhas de Hércules contra as Hidras H_n, mas em princípio é possível que outros resultados combinatórios interessantes possam ser encontrados.

BIBLIOGRAFIA

1. Buchholz, W. e Wainer, S., *Provably computable functions and the fast growing hierarchy, in "Logic and Combinatorics"*, S.G. Simpson, editor, Contemporary Mathematics 65 (1987), 179–198.
2. Carnielli, W. A., *Indemonstrabilidade em combinatória*, Manuscrito.
3. Carnielli, W. A., e Di Prisco, C. A., *Polarized partition relations of higher dimension*, A aparecer (disponível como "Relatório Interno IMECC-UNICAMP").

4. Carnielli, W. A., e Rathjen, M., *Hydrae and subsystems of arithmetic*, manuscrito.
5. Epstein, R. L. e Carnielli, W. A., "Computability: Computable Functions, Logic and the Foundations of Mathematics," Wadsworth & Brooks/Cole Mathematics Series, 1989.
6. Gentzen, G., *Untersuchungen über das Logische Schliessen I, II*, Mathematische Zeitschrift **39** (1934/35), 176–210, 405–431.
7. Gentzen, G., *Die Widerspruchsfreiheit der reinen Zahlentheorie*, Mathematische Annalen **112** (1936), 493–565.
8. Gentzen, G., *Beweisbarkeit und Unbeweisbarkeit von Anfangsfällen der transfiniten Induktion in der reinen Zahlentheorie*.
9. Gödel, K., *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme*, Monatshefte Math. Phys. **38** (1931), 173–198.
10. Harrington, L. *et allia*, "Harvey Friedman's Research on The Foundations of Mathematics," Studies in Logic and the Foundations of Mathematics, North Holland, 1985.
11. Paris, J. e Harrington, L., *A mathematical incompleteness in Peano Arithmetic*, in Handbook of Mathematical Logic, J. Barwise, editor, North-Holland (1978), 1133–1142.
12. Pohlers, W., "Proof Theory," Lecture Nots in Mathematics, Springer-Verlag, 1989.
13. Rathjen, M., *Untersuchungen zu Teilsystemen der Zahlentheorie zweiter Stufe und der Mengenlehre mit einer zwischen* $\Delta^1_2 - CA$ *und* $\Delta^1_2 - CA+$ **BI** *liegenden Beweisstärke*, Tese de Doutorado, Münster.
14. Rathjen, M., *Proof-theoretic analysys of* KPM, a aparecer (disponível como "Interner Bericht, Münster Universität"..
15. Raggio, A.R., *The* 50^{th} *anniversary of Gentzen's Thesis*, in "Methods and Applications of Mathematical Logic", Carnielli, W. A. e de Alcantara, L. P., editores, Contemporary Mathematics **69** (1988), 93–97.