

O Referee Perfeito

Convidar a *Isabelle* para verificar as nossas contas pode ser uma maneira simpática de começar um longo dia de trabalho. Vamos descobrir, no entanto, um revisor implacável, capaz de encontrar a mais pequena falha de raciocínio. E que não vai aceitar um convite para jantar no fim da jornada.

Formalizar a matemática é um velho sonho dos profissionais no assunto. Desde Euclides, pelo menos, há a preocupação de escrever o conjunto de conhecimento já adquirido de uma forma simples, sistemática, puramente dedutiva. A princípio, a matemática consiste em duas partes: um conjunto de verdades *a priori*, os “axiomas” ou “postulados” e uma máquina de produção de verdades derivadas, a *lógica*. [1,2,3]

Para cumprir esta tarefa, precisamos de uma linguagem formal, como, por exemplo, escrever “ p e q ” na forma “ $p \wedge q$ ” ou então “ p implica q ” como apenas “ $p \rightarrow q$ ”. As vantagens do uso de uma linguagem formal são muitas: a primeira e mais óbvia é a clareza do que se está a dizer. Não há ambiguidade. Uma outra vantagem é tornar claros os raciocínios válidos, como por exemplo “se p é verdade e p implica q , então q é verdade”:

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

Um teorema, então, é um conjunto de hipóteses, uma implicação, e uma conclusão tal que sempre que as hipóteses forem verdadeiras, a conclusão também o será. Uma demonstração deste teorema é escrever, a partir das hipóteses, uma série de passos aceites (como o acima) até chegarmos à conclusão do teorema. Podemos programar um computador para, a partir das regras do jogo, tentar concluir um certo teorema. Constituirão o *input* do “provedor automático de teoremas” as hipóteses do teorema e a

conclusão desejada. Aguardamos um pouco e recebemos como *output* uma longa sequência de encadeamentos lógicos que é a demonstração desejada.

Esta abordagem sistemática da investigação matemática não é, definitivamente, muito popular entre os profissionais do assunto. O primeiro problema é que raríssimos matemáticos são capazes de escrever o seu próprio trabalho em linguagem formal, e sem isto não há nada que o computador possa fazer. O segundo é que a intuição é um ótimo guia: com os programas ora existentes, um simples exercício de Análise 1 demora uma semana a ser demonstrado.

A maior crítica, no entanto, não é esta. Quando usamos um computador para executar uma demonstração, esta pode ser tão longa que a verificação humana se torne inviável. Porque deveríamos então acreditar no computador? Será possível uma matemática intrinsecamente não humana, com teoremas tão complexos que só nos resta aceitar o veredicto último das máquinas? Sabemos que os computadores erram, frequentemente por erro do programador, mas em

O Teorema da Curva de Jordan

$$\forall C. \text{simple_closed_curvetop2 } C \rightarrow (\exists A B. \text{top2 } A \wedge \text{top2 } B \wedge \text{connected top2 } A \wedge \text{connected top2 } B \wedge A \neq \emptyset \wedge B \neq \emptyset \wedge A \cap B = \emptyset \wedge A \cap C = \emptyset \wedge B \cap C = \emptyset \wedge A \cup B \cup C = \text{euclid2})$$

Figura 1 – Formulação do Teorema da Curva de Jordan em linguagem formal. $\text{top2 } A$ significa que A é aberto na topologia usual de \mathbb{R}^2 , $\text{connected top2 } A$, que é conexo. O teorema afirma que uma curva simples fechada divide o plano \mathbb{R}^2 ($\text{euclid } 2$) em duas regiões abertas que com a própria curva (todas disjuntas dois a dois) formam o plano.

Frente

[O Referee Perfeito]

alguns casos por *bug* da própria arquitectura da máquina.

acialmente, devemos lembrar que os seres humanos são falíveis e a História está cheia de exemplos de teoremas provados cuja demonstração foi posteriormente desacreditada. Um exemplo particularmente importante é a demonstração do Teorema das Quatro Cores cujo erro na "demonstração" de Kempe (1879) só foi encontrado dez anos depois. Voltaremos em breve a este exemplo.

No entanto, o trabalho humano pode sempre ser verificado por outros seres humanos. (É por isto que os erros são finalmente encontrados). Quem verifica o trabalho dos computadores?

Existem vários sistemas automáticos para demonstração de teoremas, com algumas diferenças fulcrais entre si. *Isabelle*, *Hol Light* ou *Coq* são apenas

alguns *softwares* especialmente desenhados para esta função. A demonstração elaborada por um programa pode ser verificada por outro. Desta forma, o *referee* de um teorema provado por computador será um outro computador (esta é uma extensão natural do conceito de "revisão pelos pares"). Este procedimento já levou a pelo menos uma correcção: o *Hol Light* foi capaz de encontrar um erro da demonstração da conjectura de Robbins feita pelo provador *Reveal* em 1995. Aos seres humanos resta pagar a conta da electricidade.

Cada teorema formalizado entra numa biblioteca particular e pode ser usado em demonstrações posteriores, tal qual nós fazemos.

Além de provar teoremas, tais programas têm outra função: a de procurar *bugs* em *softwares*

desenhados para outros propósitos (como para a optimização da aerodinâmica de um avião) ou em arquitecturas de *hardware* (pelo menos um *bug* em microprocessadores da Intel foi descoberto desta forma). Considerando que alguns assuntos, como o controle de tráfego aéreo ou a distribuição de energia, são por demais críticos para

nos darmos ao luxo de errar e por demais extensos para serem deixados em mãos puramente humanas, verificadores automáticos são sempre bem-vindos.

O Teorema das Quatro Cores, referido acima, foi um dos primeiros teoremas provados com a ajuda intensiva de um computador, em 1976. Como a correcção da construção computacional de cada um dos quase dois mil casos em que o problema foi dividido não podia ser jamais verificada por um ser humano, muitos matemáticos não aceitaram a demonstração como definitiva. Recentemente, em 2005, um outro grupo de investigadores usando um provador automático, o *Coq*, reproduziu o resultado com uma verificação formal de cada passo, que a princípio pode ser verificada por qualquer um - mas sobretudo, por outro provador automático [4].

Outros teoremas recentemente formalizados são o Teorema da Curva de Jordan e o do Ponto Fixo de Brouwer. Na lista de actividades para os próximos anos está o Último Teorema de Fermat, demonstrado em 1994 - e assim vão os computadores criando o *genoma* matemático. [E3](#)

Figura 3 - Um Screenshot de uma demonstração no provador automático *Matita*.

Figura 2 - O Teorema das Quatro Cores: é possível colorir qualquer mapa plano, onde cada região é conexa (não há enclaves) tal que dois países adjacentes (que partilham uma aresta, não um único ponto) tenham cores distintas com apenas quatro

Referências

- [1] **Hales, Thomas C.** "Formal Proof" *Notices of the American Mathematical Society* 55(11), 1370-1380.
- [2] **Harrison, John.** "Formal Proof - Theory and Practice". *Notices of the American Mathematical Society* 55(11), 1395-1406.
- [3] **Wiedijk, Freek.** "Formal Proof - Getting Started". *Notices of the American Mathematical Society* 55(11), 1408-1414.
- [4] **Gonthier, Georges.** "Formal Proof- The Four Color Theorem". *Notices of the American Mathematical Society* 55(11), 1382-1393.