

O que é uma demonstração?*

Keith Devlin

Department of Mathematics and Computer Science
Colby College, Waterville, Maine 04901, E.U.A.

A cena é familiar. O melhor estudante na aula de matemática (que, naturalmente, tenciona seguir filosofia e gestão de empresas) entalou o professor ao fim de três semanas.

Estudante: Não percebo bem o que é ao certo uma demonstração.

Professor: É exactamente o que eu disse na aula. Uma demonstração é um raciocínio lógico, sólido, que estabelece a verdade da afirmação em estudo.

E: Mas como é que se sabe que um raciocínio é lógico e sólido? O que é que essas palavras significam?

P: Meu Deus, com certeza que tu consegues reconhecer um raciocínio lógico quando o vês, não consegues? Não ficaste convencido com algum dos exemplos que eu apresentei na aula?

E: Bem, eu fiquei convencido de que as demonstrações falsas que apresentou como exemplo eram realmente falsas. Em cada um dos casos, depois de ter chamado a atenção para o erro lógico, eu consegui perceber porque é que aquele raciocínio particular não era uma demonstração. Mas já não estou tão certo em relação aos exemplos que apresentou como sendo demonstrações válidas. Admito que não consegui encontrar nenhum erro lógico, e os raciocínios pareciam de facto bastante convincentes. Mas como é que podemos ter a certeza de que o raciocínio era sólido e de que não existia algum erro escondido que nos escapou a todos?

P: Bom, sabes, aquelas demonstrações já são conhecidas há centenas de anos, foram examinadas por montes de matemáticos muito inteligentes, e nunca ninguém descobriu nenhum erro. Com certeza que não podemos estar todos enganados, pois não?

E: Provavelmente não. Mas não significa isso que a noção de demonstração válida é uma noção socialmente definida, que o que torna uma demonstração válida é que a maioria dos matemáticos concordam que ela é válida?

P: Deus do céu, não. Para ser válida, uma demonstração tem que seguir as regras da lógica. Faz-se uma série de afirmações, cada uma das quais é consequência das anteriores de acordo com as regras da lógica.

E: Quais regras da lógica? Nunca nos disse quais são. A mim pareceu-me que, para cada um dos seus exemplos, apresentava uma série de afirmações em que cada uma parecia razoável, dadas as anteriores. Mas onde estavam as regras da lógica? Onde é que está a diferença entre o que fez na aula e um raciocínio político engenhoso?

P: Bem, claro que, para vos ser mais fácil seguir a demonstração, eu não escrevi todos os passos. Mas isso poderia ser feito. Os lógicos esclareceram isto no princípio deste século. Eles criaram uma linguagem formal em que se

* **O que é uma demonstração?** é reproduzido da coluna "Computers and Mathematics" (ed. Keith Devlin), *Notices of the American Mathematical Society*, Vol. 39, Nº9, Novembro 1992, com a autorização da American Mathematical Society.

escrevem as demonstrações, "cálculo dos predicados" é como lhe chamam, identificaram os axiomas básicos da lógica, especificaram as regras da dedução — acho que uma delas se chama "*modus ponens*" ou coisa parecida — e então obtém-se uma noção completamente rigorosa de demonstração. E, de facto, é tão rigorosa que em algumas áreas da matemática — não na minha, apresso-me a dizer — se pode programar um computador para ele fazer o trabalho em vez de nós, para gerar demonstrações ou verificá-las.

E: Portanto o que está a dizer é que qualquer uma das demonstrações vulgares que os matemáticos encontram todos os dias no seu trabalho pode ser reescrita de um modo formal que se enquadra nessa estrutura que os lógicos axiomatizaram.

P: Exacto.

E: Então porque é que não fez isso na aula? Porque é que não nos disse quais são os axiomas e as regras da lógica e não fez isso dessa maneira?

P: Meu Deus, isso seria impraticável. Se eu tentasse tornar mesmo a mais simples das demonstrações assim tão precisa, ela ficaria incrivelmente comprida, e absolutamente ilegível. Vocês nunca seriam capazes de a seguir. Seria muito menos convincente do que a versão que eu dei.

E: Quer dizer que nunca se escreve uma demonstração em lógica formal?

P: Sim, agora já estás a perceber. Em princípio, isso *podia* ser feito. Qualquer demonstração válida *podia* ser escrita completamente em lógica formal, e então estaria de acordo com a definição de demonstração dos lógicos.

E: Só que ficaria tão comprida que ninguém poderia realmente lê-la e verificar que estava correcta.

P: Exactamente.

E: Deixe-me ver se percebi. O que está a dizer é que, estritamente falando, uma demonstração é válida se estiver escrita em cálculo dos predicados e tiver uma estrutura correcta de acordo com as regras da lógica. Mas essas demonstrações são demasiado longas e complicadas para alguém as conseguir ler, e portanto nunca ninguém faz isso. O que acontece na prática é que uma demonstração é declarada válida se *pudesse*, em princípio, ser escrita desta maneira formal.

P: Sim, é mais ou menos isso.

E: Mas como é que sabe que a sua demonstração, aquela que escreve no quadro, podia ser escrita como uma demonstração formal se nunca faz realmente isso?

P: Bom, basta olhar para ela. A irracionalidade de $\sqrt{2}$, por exemplo. O raciocínio que eu apresentei é obviamente válido, e portanto sabes que podia ser traduzido para uma demonstração válida do cálculo dos predicados.

E: Mas como é que sabe, se nunca ninguém o fez?

P: (*Impaciente*). Bom, sabes, aqueles lógicos eram tipos inteligentes, e nós sabemos pelo trabalho deles que qualquer demonstração válida podia ser escrita dessa maneira, pelo menos em princípio.

E: Mas como é que sabe à partida que a sua demonstração é válida?

P: Ouve, eu tenho mais que fazer. Tu estás a andar em círculo. Claramente não percebeste o que é que se passa quando se prova qualquer coisa. Talvez a matemática não seja um bom assunto para ti. Já pensaste em escolher antes filosofia?

Fim da história. Mas não, claro, fim da discussão. E é uma discussão com uma importância crescente na última década, com a entrada em cena das demonstrações por computador, o desenvolvimento e a utilização de

demonstradores automáticos de teoremas, e as tentativas de arranjar processos de verificação de sistemas informáticos. O que é que entendemos exactamente por "demonstração"?

Parece que os matemáticos — e para evitar gerar demasiadas cartas de protesto, apresso-me a corrigir isto para "nós os matemáticos" — são um pouco esquizofrénicos quando se trata de responder a esta pergunta. Quando apertados pelo estudante persistente, refugiamo-nos na definição do lógico e defendemo-nos com o "traduzível em princípio". Mas na prática todos trabalhamos satisfeitos com o que é claramente uma noção socialmente determinada de demonstração. Embora possamos ter algumas dúvidas em relação a demonstrações particularmente longas e inovadoras, geralmente confiamos na nossa capacidade de distinguir um raciocínio válido de um errado. Além disso, temos tendência para pensar que realmente não se trata de matéria de opinião, e que, apesar de toda a sua concisão aparente, as demonstrações que construímos e publicamos são, num sentido absoluto, demonstrações *genuínas*. Eu seguramente penso assim. Mas também sei por experiência própria que a segurança que nós os matemáticos sentimos sobre o assunto não é facilmente explicável a pessoas fora deste campo, a quem, suspeito, realmente parece que nós simplesmente estamos a jogar um jogo segundo regras definidas por nós, escolhidas por alguma forma de votação secreta.

Até agora, a discussão sobre o que é que constitui uma demonstração aceitável teve lugar sobretudo na sala do café do departamento de matemática (ocasionalmente) e no salão de filosofia (intensamente). Mas aproxima-se o dia em que a discussão passará para os tribunais. Isso já esteve quase a acontecer em Inglaterra no ano passado, com o chamado caso VIPER, conforme explicado no artigo principal deste mês.¹ O autor é Donald MacKenzie, sociólogo da Universidade de Edimburgo. Juntamente com Alan Bundy, especialista em raciocínio automático do Departamento de Inteligência Artificial de Edimburgo, está actualmente envolvido num projecto de investigação sobre a natureza da demonstração, tanto como ela aparece nos departamentos matemáticos universitários como no tipo de situação industrial que ele descreve no seu artigo.

Deve também referir-se que a questão das demonstrações automáticas chegou às páginas do *New York Times* em 7 de Abril de 1992, com a notícia de um surpreendente trabalho (de Babai, Fortnow, Lund, Szegedy e Levin) sobre o problema da verificação de demonstrações formais longas. Um dos investigadores envolvidos, László Babai, escreveu um artigo expondo esse trabalho que foi publicado em duas partes pela *Newsletter* da Mathematical Association of America, FOCUS (Junho e Setembro, 1992).

(tradução de: João Filipe Queiró, Departamento de Matemática - Universidade de Coimbra)

¹ N. T. - O artigo referido intitula-se **Computers, Formal Proofs and the Law Courts** (*Notices of the American Mathematical Society*, vol. 39, nº 9, Novembro 1992, p. 1066-1069) e trata de um processo judicial iniciado por uma empresa britânica contra o Ministério da Defesa. Em causa estava a comercialização por este de um microprocessador, o VIPER, anunciado como o primeiro em que a correcção do *design* e a adequação às especificações eram "demonstradas". O caso não chegou aos tribunais por a empresa entretanto ter falido.