Matemática e Computação

Matemática Universitária Nº 9/10, dezembro de 1989

Responsáveis: Geovan T. dos Santos e Jonas de M. Gomes

Uma Técnica de Demonstração em Cálculo Formal

Paulo Viana

PUC/RJ
Pontifícia Universidade Católica do Rio de Janeiro

Dedicado ao Elon

"Desde os gregos, quem diz matemática diz demonstração; alguns mesmo duvidam que se encontrem, fora das matemáticas, demonstrações no sentido preciso e rigoroso que esta palavra recebeu dos gregos, e que a ela procuramos dar aqui. Pode-se dizer que este sentido não variou, uma vez que o que era para Euclides uma demonstração continua sendo uma para nós; e, em épocas em que a noção foi ameaçada de se perder, e quando deste fato a matemática se viu em perigo, foi entre os gregos que se procuraram os modelos". Desta maneira – colocando-se na continuidade de uma tradição milenar – começa o tratado "Elementos de Matemática", de Nicholas Bourbaki. Mais adiante Bourbaki torna mais preciso: "a originalidade essencial dos gregos consiste precisamente em um esforço consciente de dispor os raciocínios matemáticos em uma ordem tal que a seqüencia de um passo ao seguinte não deixe qualquer lugar a dúvida e alcance um consenso universal". Este sentido que os gregos desenvolveram de demonstração foi usado para construir o bloco ordenado de definições, axiomas e teoremas da Geometria Plana e Espacial, que foi sistematicamente registrado por Euclides e que, depois de tantos séculos, ainda nos enche de maravilha. O corpo de teoremas da Geometria foi estendido ao longo do tempo, neste processo utilizando-se sempre, como enfatizou Bourbaki, o mesmo conceito de demonstração. O seguinte teorema de Geometria Plana, por exemplo, foi descoberto no século XVIII.

Teorema do Círculo. *Em um triângulo qualquer os pontos médios de cada lado e os pés de todas as alturas situam-se no mesmo círculo.*

Para provar o teorema consideram-se, em um triângulo ABC, os pontos médios D, E e F dos lados AB, BC e AC, respectivamente, e considera-se, por exemplo, o ponto H, pé da altura que cai do ponto B. Por semelhança de triângulos a linha DF é paralela a BC, com o comprimento DF igual à metade do comprimento BC. O comprimento EH é também igual à metade do comprimento BC: com efeito, o ângulo BHC é reto, e logo H situa-se no segmento circular capaz de ângulos retos, que é um círculo com centro em E e diâmentro BC. Analogamente DE é paralela a AC, e logo o trapézio $DEFH$ é isósceles e, por isso, inscritível em círculo. Como H é o pé de uma altura arbitrária, o teorema se conclui, com uma demonstração classicamente perfeita.

Menos de vinte anos depois da publicação do primeiro volume dos "Elementos de Matemática", no entanto, começaram a surgir raciocínios que se diziam demonstrações, mas que usavam cálculos que não eram explicitados (e assim não poderiam ter sua validade conferida pelo leitor), pela razão de serem cálculos feitos por máquinas. A infâmia maior veio em 1977, quando Kenneth Appel e Wolfgang Haken mostraram que a primeira demonstração alegada para a Conjectura das Quatro Cores, feita por Alfred Kempe em 1878 e apontada como errônea por Percy Heawood em 1890, poderia ter a linha de raciocínio completada, e assim efetivamente demonstraram a conjectura. Esta conjectura declarava que quatro cores seriam suficientes para colorir qualquer mapa no plano. A pretensa demonstração de Kempe argumentava que um mapa que necessitasse de cinco cores para ser colorido deveria conter pelo menos uma dentre quatro configurações inevitáveis de países e que, para cada uma destas configurações, o número de países poderia ser diminuido sem afetar a necessidade de cinco cores no colorimento. Assim, qualquer mapa que necessitasse de cinco cores para ser colorido poderia ter o número de países reduzido e continuar exigindo cinco cores, isto é, não haveria um mapa necessitando de cinco cores com um número mínimo de países, e logo não poderia haver nenhum mapa que efetivamente precisasse de cinco cores. Para uma das quatro configurações inevitáveis, contudo, a demonstração de Kempe estava errada. A demonstração de Appel e Haken usava o mesmo raciocínio, mas tinha o número de configurações inevitáveis aumentado para quase 1500 e, para mostrar que, para cada uma delas, o número de países poderia ser reduzido, foi necessária a utilização de cerca de 1200 horas de computador. E assim, sem ferramenta teórica nova alguma, apenas com o refinamento de um antigo raciocínio acrescido de um poder de fogo computacional fantástico (para a época), foi estabelecida afirmativamente uma das mais famosas dúvidas que tiravam o sono dos matemáticos.

Houve muita polêmica na ocasião. Quem esperava uma demonstração cheia de sutilezas topológicas, que iluminasse alguma propriedade única do plano, encontrou uma enumeração seca de casos e a verificação mecânica de cada um e, na decepção, houve quem duvidasse do status de verdade da conjectura. Certamente a demonstração de Appel e Haken não esgotou a curiosidade sobre o assunto e mantém-se viva a procura de uma demonstração computacionalmente mais simples para o Teorema das Quatro Cores. Enquanto não aparece esta demonstração (que bem pode nem existir), não se deve abandonar, contudo, a certeza de que o teorema está demonstrado.

O exemplo de Appel e Haken foi só o caso mais sensacional de um tipo de demonstração que usa cálculos automáticos. Essas demonstrações vão se tornando cada vez mais habituais, já não despertando mais qualquer surpresa. Confrontado com uma demonstração dessas, e desejoso de verificá-la, um matemático só tem que repetir o cálculo em seu próprio computador – coisa que foi efetivamente realizada pela equipe de editores do *Illinois Journal of Mathematics* para aceitar como definitiva a demonstração de Appel e Haken. Com a idéia cada vez mais generalizada de ver o computador como um instrumento essencial do trabalho matemático (algo assim como a estabilidade financeira e uma boa biblioteca), este procedimento vai se tornando rotineiro. Na verdade, este uso já é tão comum que há o perigo de se esquecer que qualquer computador não é mais que uma sucessão de estados que , se instruidos convenientemente, podem representar qualquer objeto matemático que obedeça à implacável condição de finitude; tal esquecimento pode levar à ingênua superstição de que computadores são capazes, por exemplo, de somar números inteiros. Assim, parte do trabalho de Appel e Haken foi encontrar uma representação conveniente para os objetos que os interessavam, as configurações de mapas ou, equivalentemente, os grafos.

Atualmente tem sido feito um uso cada vez maior de programas que permitem representar em máquina, além de números e matrizes, – objetos tradicionalmente associados a cálculos em computadores, – outros objetos matemáticos tais como funções, séries de potências, frações contínuas, e assim por diante; tais programas lidam com estes objetos de um modo análogo ao que as calculadoras eletrônicas usam ao lidar com números, isto é, eles desempenham uma variedade de operações que os objetos matemáticos admitem – para funções reais de variável real, por exemplo, eles podem operar somas, produtos, composições, substituições, diferenciações, integrações, etc. Estes programas, como o MACSYMA, o REDUCE, o MAPLE, o MuMATH, são as ferramentas básicas para o Cálculo Formal[1], isto é, cálculo com objetos matemáticos não (necessariamente) numéricos. Outros programas, como o MACAULAY e o SCRATCHPAD, chegam a trabalhar com objetos como ideais em anéis de polinômios e suas relações (syzygies).

A possibilidade de operar funções em grande escala, sem depender de nervos e virtualmente livre de erros de cálculo, abriu uma vasta quantidade de perspectivas novas e os programas de C'alculo Formal foram usados em uma variedade enorme de aplicações, tais como o estudo em detalhe de movimentos lunares ou o teste de teorias cosmológicas. Em matemática o apareci-

[1] A denominação "Cálculo Formal" é tradução da terminologia francesa; a designação consagrada em inglês é "Computer Algebra" que, além de ser notacionalmente pior do que a francesa ("Computer Algebra" não é uma parte da Álgebra, como a denominação parece indicar), não se presta para tradução em português. Será já tarde demais para evitarmos uma terminologia anglicista e cacofônica?

mento destes programas influenciou (ou foi conseqüência de) uma tendência para raciocinar construtivamente mesmo em áreas em que os métodos eram, por tradição, puramente existenciais. Assim, por exemplo, a Geometria Algébrica, modernamente a plataforma de lançamento das mais ousadas abstrações, viu a introdução de raciocínios efetivos com o algoritmo de Buchberger para o cálculo de bases de Gröbner, que permite manipular ideais em anéis de polinômios da maneira mais concreta possível (ver [1]). As aplicações deste método são das mais variadas; tipicamente, o algoritmo permite decidir sobre questões em que hipóteses e teses tenham formulação polinomial – uma vastíssima gama de questões, sem dúvida, que inclui, por exemplo, teoremas de Geometria Plana como o Teorema do Círculo enunciado e demonstrado acima, como indicaremos a seguir. Para informações mais detalhadas sobre este tipo de aplicação a referência [2] pode ser consultada.

Para dar expressão polinomial ao enunciado fixamos um par de eixos cartesianos no plano e consideramos como variáveis as coordenadas dos pontos A, B, C, ... envolvidos. Observamos, em seguida, que as condições da hipótese e da tese têm expressão polinomial nestas variáveis: por exemplo, se fixarmos como coordenadas $A = (x_1, x_2)$, $B = (x_3, x_4)$, $C = (x_5, x_6)$, $D = (x_7, x_8)$, $H = (x_9, x_{10})$, então a condição de D ser o ponto médio de AB se expressa pelo par de equações lineares

$$h_1 : 2x_7 - x_1 - x_3 = 0$$

$$h_2 : 2x_8 - x_2 - x_4 = 0;$$

a condição de H estar em AC pela equação quadrática

$$h_3 : (x_9 - x_1)(x_6 - x_2) - (x_{10} - x_2)(x_5 - x_1) = 0;$$

a condição de perpendicularidade de AC e BH pela equação quadrática

$$h_4 : (X_6 - x_2)(x_4 - x_{10}) + (x_9 - x_3)(x_5 - x_1) = 0;$$

e assim por diante. Fixamos ainda coordenadas para o centro G do círculo que circunscreve DEF, e a condição da tese, de que H se situa neste círculo, tem ainda uma expressão quadrática h_t.

Queremos então decidir se a expressão h_t é conseqüência das expressões $h_1, h_2, \ldots$, isto é, se para todo vetor $(x_1, \ldots, x_{16})$ satisfazendo $h_1, h_2, \ldots$ ocorre que h_t também é satisfeita – em linguagem geométrica, queremos saber se h_t está no ideal da variedade definida por $h_1, h_2, \ldots$. Gostaríamos neste ponto de invocar o *Nullstellensatz*, o Teorema dos Zeros de Hilbert, que afirma que esta questão é equivalente a decidir se

$$h_t \in \sqrt{I(h_1, h_2, \ldots)}, \tag{1}$$

onde $I(h_1, h_2, \ldots)$ denota o ideal gerado por $h_1, h_2, \ldots$ em $k[x_1, \ldots]$ e $\sqrt{I}$ denota o radical de um ideal I; mas aí se coloca um problema: quem é k? Euclides, sem o saber, parecia pensar estar trabalhando com $k = R$, mas se quisermos usar o Teorema dos Zeros de Hilbert deveremos tomar k algebricamente fechado, por exemplo, $k = C$. Ocorre que os teoremas da Geometria Plana são verdadeiros para $k = R$ *ou* para $k = C$. O método que descreveremos agora, aplicando o algoritmo de Buchberger, decidirá a questão para $k = C$ e, se provarmos que neste caso (*) é verdadeira, então o teorema se deduz evidentemente também para $k = R \subset C$. Seria no entanto concebível, para algum teorema de Geometria Plana, mostrarmos que a inclusão correspondente a (*) é falsa para $k = C$ e, ainda assim, termos um teorema verdadeiro para $k = R$.

Finalmente aplicamos o algoritmo de Buchberger para decidir sobre (*) – uma questão finita; o algoritmo está implementado na maioria dos programas de Cálculo Formal, como o MACSYMA e o REDUCE, de modo que podemos simplesmente deixar o computador ligado e ir dormir, para acordar no dia seguinte com o teorema demonstrado.

Uma objeção óbvia de ordem estética se coloca: como comparar uma demonstração em estilo clássico como a apresentada antes, que requer habilidade e imaginação na escolha dos argumentos e que, quando consumada, nos parece iluminar e que certamente nos traz satisfação, com uma atividade puramente mecânica e banal como executar um programa pronto? É um sentimento análogo à frustração de um topólogo à notícia da demonstração de Appel e Haken para o Teorema das Quatro Cores.

Confrontamos esta objeção com duas defesas. A primeira é pragmática: está certo que um matemático queira desenvolver seu raciocínio elevando-se a abstrações rarefeitas, mas a Matemática também deve ser aplicada e aplicações necessitam de resultados. Hoje, sofremos por não ter uma demonstração esteticamente satisfatória do Teorema das Quatro Cores, mas antes sofríamos (quanto!) por não saber da validade da Conjectura das Quatro Cores. Questões de Geometria Plana mais complexas que o Teorema do Círculo ilustrado acima são efetivamente usadas em modelamento geométrico, devem ter sua validade decidida e, para isso, uma demonstração automática é tão boa quanto qualquer outra.

A segunda defesa é estética: o desenvolvimento de novos algoritmos sem dúvida traz tanta alegria quanto o desenvolvimento de novos teoremas e envolve argumentos de mesma natureza que os que estão implícitos no conceito de demonstração herdado de Euclides: mesmo porque uma idéia estreita de demonstração, que não admitisse cálculos verificados por máquinas, seria realmente um presente de grego.

Bibliografia

1. B.Buchberger, "Gröbner Basis: An Algorithmic Method in Polynomial Theory," in Multidimensional Systems Theory, N.K.Bose, 1985.
2. B.Kutzler, S.Stifler, *On the Application of the Buchberger's Algorithm to Automated Geometry Theorem Proving*, Journal of Symbolic Computation **2** (1986), 389-398.