RESOLVER ou VERIFICAR?

UMA PERGUNTA QUE VALE UM MILHÃO DE DÓLARES

Em 2000, o Instituto Clay para Matemática (EUA) elegeu sete problemas considerados centrais para o progresso da matemática, chamando-os 'Os problemas do milênio'. A solução de cada um deles vale um prêmio de US$ 1 milhão (cerca de R$ 2 milhões).

Neste artigo, apresentaremos ao leitor um desses problemas, que guarda semelhança com um quebra-cabeça de muitas peças: leva muito tempo para ser 'resolvido', mas pouquíssimo tempo para verificarmos se a resposta está 'correta' – basta uma olhada rápida.

Celina M. H. de Figueiredo
Programa de Engenharia de Sistemas e Computação, Instituto Alberto Luiz Coimbra de Pós-graduação e Pesquisa de Engenharia (Coppe), Universidade Federal do Rio de Janeiro

O computador é um aliado imprescindível para resolver os complexos problemas que surgem em biologia, química, física, economia, áreas nas quais pesquisadores se dedicam à modelagem e à simulação de problemas de larga escala com uso de computadores. Porém, há problemas que têm resistido à habilidade dos programadores.

À medida que resolvemos problemas cada vez maiores e mais complexos por meio de enorme poder computacional e algoritmos engenhosos, os problemas resistentes e desafiadores ganham destaque. Nesse sentido, a teoria que propõe o problema do milênio do qual trataremos aqui ajuda a entender as limitações computacionais fundamentais. Uma questão de interesse teórico explica a dificuldade prática de problemas formulados em toda a comunidade científica.

Campanha de vacinação Imagine que uma campanha de vacinação no estado do Rio de Janeiro precisa visitar cada uma das capitais dos seus 92 municípios. Para ajudar na visualização, apresentamos uma figura em que cada capital de município é representada por um ponto e na qual uma rodovia entre duas capitais de municípios está expressa por um segmento de reta.

Por restrições de custo, a equipe responsável deverá partir da cidade-sede da campanha, passar por cada uma das 92 capitais de municípios fluminenses e retornar à cidade de partida, realizando um circuito que usa as rodovias do estado e que visita cada capital de município – e isso é importante – apenas uma vez.

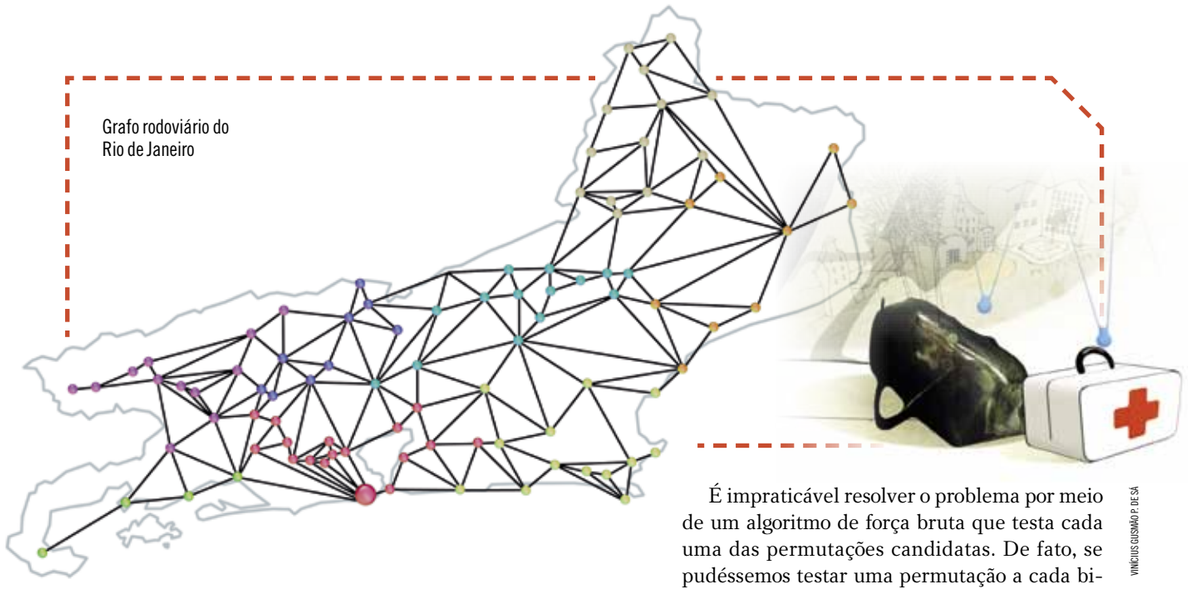
Será que esse circuito pode ser realizado no estado do Rio de Janeiro?

Esse circuito corresponde ao chamado problema do ciclo hamiltoniano, formulado, em 1856, pelo físico e matemático irlandês William Hamilton (1805-1865) e também conhecido como o 'problema do caixeiro viajante'.

Em matemática, costumamos dizer que as condições para a resolução de um problema podem ser de dois tipos: necessárias e/ou suficientes. Exemplo simples: é suficiente tirar 10 nas provas para passar em uma disciplina, mas não é necessário tirar notas tão altas. No entanto, é necessário fazer todas as provas de uma disciplina, mas isso não é suficiente para ser aprovado nela. No caso, a condição necessária e suficiente é, digamos, fazer todas as provas e tirar acima da nota mínima nelas.

Uma condição suficiente para que o circuito do vacinador exista é que, por cada cidade, passem muitas rodovias do estado. No entanto, essa condição não é necessária. Uma condição necessária é a inexistência do que denominaremos cidade-gargalo. Em outras palavras, não pode haver uma cidade pela qual passam todas as rodovias que conectam outras duas cidades. Porém, essa condição agora é necessária, mas não é suficiente para que exista o circuito.

Vejamos exemplos práticos. No estado do Rio de Janeiro, a cidade de Angra dos Reis é uma cidade-gargalo, porque toda rodovia conectando Paraty a qualquer outro município do estado passa por Angra dos Reis. Ao sair de Paraty, o vaci- >>>



VINÍCIUS GUSMÃO P. DE SÁ

nador teria que passar de novo por Angra dos Reis, o que inviabilizaria seu circuito. Note essa obrigatoriedade na figura. Há outras cidades-gargalo no estado: Cabo Frio, Resende e Campos dos Goytacazes.

Portanto, o circuito do vacinador é inviável no estado fluminense.

Pavimentando rodovias Considere agora uma campanha para recuperar a pavimentação das rodovias do estado. Novamente, por restrições de custo, a equipe responsável, saindo da cidade-sede da campanha, deve realizar um circuito que percorra cada rodovia exatamente uma vez, retornando ao ponto de partida.

Será que esse circuito pode ser realizado no estado do Rio de Janeiro?

Note que o circuito do vacinador visita cada cidade do estado exatamente uma vez, enquanto o do pavimentador percorre cada rodovia estadual uma só vez. No entanto, é possível que nosso vacinador tenha deixado de percorrer alguma rodovia do estado; por sua vez, nosso pavimentador talvez visite uma cidade do estado mais de uma vez. Mas, em nenhum dos dois casos, as regras das campanhas seriam violadas.

O circuito do vacinador corresponde a uma permutação do conjunto das cidades do estado, enquanto o circuito do pavimentador corresponde a uma permutação do conjunto das rodovias do estado**.** Vale aqui relembrar brevemente o conceito de permutação. Ele indica de quantas maneiras diferentes podemos arranjar objetos distintos de um conjunto. Por exemplo, as letras A, B e C podem ser arranjadas assim: ABC, ACB, BAC, BCA, CAB, CBA. Portanto, teríamos seis permutações, quantidade expressa matematicamente por 3! (lê-se, três fatorial), que representa 3 x 2 x 1.

Tanto no caso da vacinação quanto da pavimentação, procuramos o circuito desejado em um universo enorme, de aproximadamente 92! = 92 x 91 x 90 x ... x 3 x 2 x 1 circuitos possíveis. Esse é um número enorme, com 143 algarismos.

É impraticável resolver o problema por meio de um algoritmo de força bruta que testa cada uma das permutações candidatas. De fato, se pudéssemos testar uma permutação a cada bilionésimo de segundo, precisaríamos de mais de 3×10^{125} anos, muito mais que a idade estimada do universo ($1{,}4 \times 10^{10}$ anos).

Vértices e arestas Buscamos uma propriedade matemática do problema que reduza drasticamente o universo de busca dentro do enorme conjunto formado por todos os circuitos possíveis. O matemático suíço Leonhard Euler (1707-1783) resolveu definitivamente o problema do pavimentador ao publicar, em 1736, o que consideramos o primeiro artigo científico da área de teoria dos grafos (ver coluna 'Qual o problema?' em *CH* 233 e 235).

Naquele artigo, foi apresentada uma propriedade que caracteriza e que é, ao mesmo tempo, necessária e suficiente para a existência desse circuito do pavimentador: o número de rodovias que passam por cada cidade deve ser par.

Euler restringiu drasticamente nosso universo de busca dentro do conjunto formado por todas as possíveis permutações das rodovias. A poderosa condição de Euler fornece a solução após a simples verificação do grau das 92 cidades – grau, no caso, é o número de rodovias que passam pela cidade.

Euler, em 1736, modelou o circuito do pavimentador por meio de um problema em teoria dos grafos: cada cidade corresponde a um vértice, e cada rodovia entre duas cidades é representada por uma aresta que liga os dois vértices correspondentes. No estado do Rio de Janeiro, temos 92 capitais de municípios correspondendo a 92 vértices e temos rodovias que correspondem às arestas, conectando esses vértices como representado na figura.

O município de Carapebus**,** por exemplo, liga-se por rodovias a três outros municípios: Macaé, Conceição de Macabu e Quissamã. Pelo teorema de Euler, o vértice de grau ímpar que representa Carapebus impossibilita um circuito do pavimentador. Entretanto, caso encontremos outro estado onde todas as cidades tenham grau par, a condição fácil e poderosa de Euler garante que aquele estado admite um circuito do pavimentador.

Força bruta Para o problema do pavimentador, podemos decidir se o circuito existe ou não por meio da caracterização matemática simples encontrada por Euler: basta conferir se o número de rodovias que passa por cada cidade é par. Porém, para o problema do vacinador, conhecemos algumas condições necessárias e outras condições suficientes, mas ainda não temos uma caracterização simples que resolva o problema rapidamente. Isto é, não temos, como no caso do circuito do pavimentador, uma condição necessária e suficiente. Na verdade, nem sabemos sequer se tal caracterização existe.

Hoje, para o problema do vacinador, nos resignamos a buscar a resposta por meio de um algoritmo de força bruta que lista todos os possíveis candidatos a circuitos, listando os elementos do enorme conjunto formado por todas as possíveis permutações das cidades.

No entanto, caso alguém persistente (ou com muita sorte) alegue ter encontrado um circuito do vacinador, é fácil verificar que esse circuito satisfaz a restrição: basta conferir se cada cidade é visitada uma só vez e que cidades consecutivas no circuito sejam, de fato, conectadas por uma rodovia.

Emparelhando amizades Será que o problema do vacinador é intrinsecamente mais difícil que o problema do pavimentador? Será que há problemas cuja solução pode ser verificada facilmente, embora essa solução não possa ser encontrada facilmente?

Esse é o desafio central para a teoria da computação, capturado no problema do milênio P *versus* NP, ao qual nos referimos anteriormente.

Vejamos um exemplo prático. Considere uma turma – digamos, de 40 alunos – em um colégio. Cada aluno tem alguns amigos na turma. O problema do emparelhamento procura organizar a turma em 20 pares de alunos amigos entre as $40!/(20!2^{20})$ possíveis organizações em 20 pares de alunos**,** que é um número enorme, da ordem de 2^{78}, com 24 algarismos.

O problema do emparelhamento é um problema fundamental na área de complexidade computacional. É um problema cuja solução sugeriu a definição formal adotada para a chamada computação eficiente: um algoritmo é eficiente se sua execução consome um número de passos que cresce como uma potência fixa do tamanho dos dados da entrada.

Hoje, já se conhece um algoritmo eficiente que resolve o problema do emparelhamento em n^3 passos, para uma turma de n alunos. Para a nossa turma de $n = 40$ alunos, observe a drástica redução do número exponencial 2^{78} (24 algarismos) para o número polinomial $40^3 = 64.000$ (cinco algarismos) – usamos o termo polinomial como sinônimo de problema tratável, viável, eficiente, em contraste com exponencial, sinônimo de intratável, inviável, difícil.

O algoritmo que resolve uma entrada de tamanho n em n^3 passos é denominado algoritmo polinomial.

Problemas desafiadores Considere algumas variações do problema de emparelhamento: i) organizar a turma em grupos de três alunos amigos mútuos; ii) dividir a turma em três grupos de alunos amigos mútuos; iii) organizar os alunos em uma única mesa-redonda de forma que apenas amigos sentem-se lado a lado (essa variação é o problema do vacinador).

Esses problemas desafiadores compartilham uma propriedade: dada uma candidata a solução – um emparelhamento em grupos de três alunos, uma partição em três grupos de alunos ou uma alocação em uma única mesa-redonda –, podemos aprovar essa candidata por meio de um teste rápido, por meio de um algoritmo polinomial.

Porém, ainda não conhecemos – nem sabemos se existe – um algoritmo eficiente para resolver qualquer uma dessas variações. Cada qual define um problema matemático desafiador, e são temas de pesquisa avançada em matemática combinatória que levam os nomes: emparelhamento 3-dimensional, 3-coloração e ciclo hamiltoniano.

O desafio é encontrar alguma propriedade matemática que torne o problema tratável por meio de um algoritmo polinomial para buscar rapidamente soluções no imenso universo dos possíveis candidatos.

Solução difícil, verificação fácil A questão central para computação é: quão eficientemente um problema pode ser resolvido por meio de um algoritmo? Do ponto de vista computacional, distinguimos problemas fáceis e difíceis, usando o conceito de algoritmo polinomial.

Consideramos fáceis os problemas que podem ser resolvidos por meio de um algoritmo que consome um pequeno número de passos até chegar à solução, ou seja, esse número de passos cresce devagar, com uma potência fixa do tamanho dos dados da entrada – podemos imaginar aqui como exemplos: emparelhamento em pares de amigos ou o circuito do pavimentador.

Consideramos difíceis os problemas para os quais qualquer possível algoritmo consome um número extremamente grande de passos até >>>

RESOLVER É MAIS FÁCIL QUE VERIFICAR?

Em 1903, em um congresso da Sociedade Norte-americana de Matemática, o matemático Frank Cole (1861-1926) provou que o número $2^{67} - 1 = 147.573.952.589.676.412.927$ não é primo, exibindo a fatora-ção 193.707.721 x 761.838.257.287. Quando apresentou essa fatoração, Cole fez a multiplicação desses dois números enormes no quadro e em silêncio, sendo ao final aplaudido de pé. É simples – embora tedioso, se feito manualmente – calcular $2^{67} - 1$, multiplicar 193.707.721 por 761.838.257.287 e verificar que dão o mesmo número. Já encontrar essa fatoração é difícil. Cole disse que ele levou três anos trabalhando aos domingos.

P igual a NP? A teoria da complexidade computacional põe os problemas desafiadores – aqueles que resistem à classificação em fácil ou difícil (como o problema do vacinador) em uma única classe, na qual estão problemas igualmente difíceis, igualmente desafiadores.

Em computação, chamamos P (de tempo polinomial) a classe dos problemas que podem ser resolvidos por meio de um algoritmo polinomial. Chamamos NP (de certificado polinomial) a classe dos problemas em que todo candidato a solução pode ser aprovado ou rejeitado rapidamente (em tempo polinomial). A classe NP é uma classe maior, mais geral que a classe P. Todo problema que pertence à classe P também pertence à classe NP, porém não sabemos se as duas classes coincidem.

Dito isso, podemos afirmar que o problema do milênio em teoria da computação é decidir se vale a igualdade P = NP. Caso ela seja provada, isso significaria que qualquer problema que tem solução que pode ser verificada rapidamente tem também solução que pode ser encontrada rapidamente.

Para estudar a possível igualdade P = NP, os pesquisadores definiram um conjunto especial de problemas igualmente difíceis entre si e pelo menos tão difíceis quanto qualquer problema em NP. Esses problemas são chamados NP-completos, porque têm a seguinte propriedade: se alguém descobrir um algoritmo que resolva em tempo polinomial um problema NP-completo, então todos os outros problemas NP também poderão ser resolvidos em tempo polinomial, ou seja, serão P. Mas se alguém provar que é impossível resolver um problema NP-completo em tempo polinomial, então nenhum problema NP-completo poderá ser resolvido em tempo polinomial.

O problema do vacinador é um problema NP-completo. Portanto, caso alguém consiga um algoritmo polinomial para resolver o problema do vacinador, terá, na verdade, revolvido um problema que vale US$ 1 milhão, porque terá provado que P = NP. CH

retornar a resposta, ou seja, esse número de passos cresce rápido, como uma exponencial no tamanho dos dados da entrada – podemos imaginar aqui como candidatos: emparelhamento em 3 amigos mútuos ou o circuito do vacinador.

Muitos problemas desafiadores compartilham a seguinte propriedade: encontrar a solução parece ser difícil, embora verificar a solução seja fácil (ver 'Resolver é mais fácil que verificar?'). Na prática, isso se assemelha a um quebra-cabeça com, digamos, milhares de peças: é difícil 'resolvê-lo', mas é facílimo verificar se a 'solução' está correta, bastando, para isso, uma rápida olhada.

A intuição diz que encontrar a solução tem que ser mais difícil que simplesmente verificar a solução – mas nem sempre a intuição é um bom guia para a verdade. Para esses problemas desafiadores, candidatos a problemas difíceis, ainda não conhecemos algoritmos polinomiais e nem mesmo sabemos provar matematicamente a inexistência deles.

A autora trabalha na área de complexidade computacional dos problemas combinatórios e seus algoritmos aproximativos, randomizados e quânticos. É especialista na classificação de problemas desafiadores – em especial, da teoria dos grafos, tendo este ano classificado como NP-completo um problema proposto há 40 anos.

Sugestões para leitura

FORTNOW, L. 'The status of the P versus NP problem'. In: *Communications of the Association for Computing Machinery*, v. 52, n. 9, pp. 78-86, setembro de 2009.
APPLEGATE, D. L.; BIXBY, R. E.; CHVÁTAL, V.; COOK, W. J. *The Traveling Salesman Problem: a Computational Study* (Princeton: Princeton University Press, 2006).
KLEINBERG, J; TARDOS, E. *Algorithm Design* (Boston: Addison Wesley, 2005)
SZWARCFITER, J. L. *Grafos e Algoritmos Computacionais.* (Rio de Janeiro: Campus, 1988).

NA INTERNET

>> Prêmio Problemas do Milênio (em inglês): http://www.claymath.org/millennium/