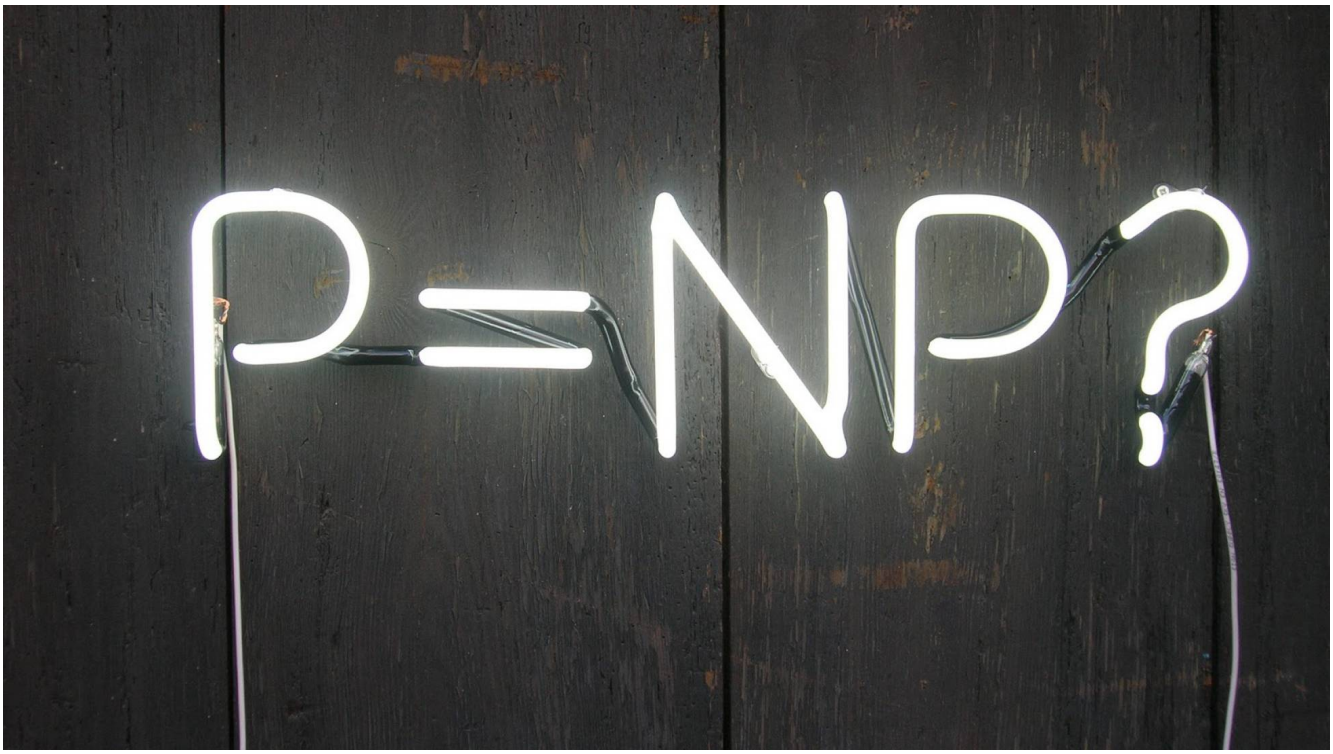
CIÊNCIA ›

O problema que os programadores não conseguiram resolver em 45 anos

Pergunta "P=NP?" tira os programadores do sério desde 1971

RICARDO PEÑA MARÍ

22 MAI 2017 - 21:54 CEST



Muitas pessoas se perguntam o que diabos se esconde por trás da pergunta P=NP?, e por que parece ser tão importante.

O que diabos se esconde por trás da pergunta 'P=NP?', e por que parece ser tão importante para os programadores? É uma pergunta ainda sem resposta desde 1971, ano em que foi formulada, que tira do sério os programadores. Se a resposta for P≠NP, as coisas ficariam mais ou menos na mesma, mas se for P=NP, estão muitas coisas mudariam e não necessariamente para melhor. Vamos ver por que.

MAIS INFORMAÇÕES

"O problema com a matemática não são as crianças, mas a forma como é ensinada"

Quando políticos dos EUA decidiram que o valor de pi era 3,2

Solucionado o mistério dos círculos de fadas da Namíbia

Detetives matemáticos

Boa parte das pessoas tende a pensar que os computadores podem resolver todos os problemas, e que os que não podem ser resolvidos hoje, o serão amanhã, porque sua potência de cálculo cresce continuamente. Os programadores sabem, por outro lado, que uma infinidade de problemas de cálculo não terá solução nunca (os chamados problemas indecidíveis), e que para outros problemas existem algoritmos que os resolvem, mas utilizando para isso tanto tempo de cálculo que para efeitos práticos é como se fossem irresolúveis (os chamamos problemas intratáveis). Os problemas que são resolvidos pelos computadores em um tempo razoável são chamados de polinomiais, e todos eles se agrupam na chamada classe P. São chamados assim porque seu tempo de cálculo é descrito por um polinômio no tamanho dos dados. Por exemplo, o problema de multiplicar duas matrizes de n fileiras e colunas pode ser resolvido utilizando menos de n3 multiplicações. Nenhum dos problemas intratáveis está na classe P.

investigam fraudes na loteria

Existe outra classe de problemas, a que chamamos de NP, cuja definição está dada de tal maneira que inclui todos os problemas da classe P, mas também muitos outros que se comportam de maneira intrigante. Um desses problemas é o chamado problema do representante comercial: dado um mapa de estradas, consiste em encontrar o caminho mais curto para se visitar n cidades de uma só vez e voltar ao ponto de origem. Para esses novos problemas da classe NP, os melhores algoritmos conhecidos têm um tempo de trabalho parecido ao dos problemas intratáveis, mas ninguém conseguiu demonstrar que não existem algoritmos polinomiais para eles. Ninguém conseguiu demonstrar também que são intratáveis. Estão, por assim dizer, em uma espécie de limbo informático: não se sabe se são polinomiais ou se são intratáveis. A teoria desenvolvida nos últimos anos chegou, entretanto, a alguma conclusão útil: definiu uma subclasse da classe NP, a subclasse dos problemas NP-completos, na qual são agrupados os problemas mais difíceis da classe NP, de tal forma que, se para qualquer um dos tais problemas se encontrar um algoritmo polinomial, então todos eles seriam resolvidos em tempo polinomial e, além disso, a classe NP seria rebaixada a P, ou seja, teríamos a igualdade P=NP. E mais, se fosse demonstrado que um só dos problemas NP-completos é intratável, então todos eles o seriam e teríamos a desigualdade P≠NP.

A criptografia atual depende de um problema da classe NP, da decomposição de um número em fatores, para o qual não temos algoritmos eficientes

As consequências desse último não seriam muitas: simplesmente deixaríamos de procurar algoritmos polinomiais para uma série de problemas interessantes, porque saberíamos com segurança que tais algoritmos não existem. Por outro lado, se fosse P=NP, teríamos encontrado algoritmos polinomiais para todos esses problemas. A parte boa disso é que poderíamos resolver, em bem pouco tempo, problemas do viajante com milhares de outras cidades e outras centenas de problemas úteis para os quais hoje temos algoritmos muito trabalhosos, e isso seria benéfico para a indústria, as comunicações e o desenvolvimento em geral. A parte ruim é que as senhas criptográficas seriam decifradas com muita facilidade, e muitas contas bancárias e comunicações cifradas ficariam expostas a vigaristas.

De fato, a criptografia atual depende de um problema da classe NP, o da decomposição de um número em fatores, para o qual não temos algoritmos eficientes. O mais eficiente de todos levou 18 meses para decompor em fatores um número de 200 cifras decimais, que são os habitualmente usados em criptografia. A segurança das senhas reside justamente nessa dificuldade, hoje insolúvel. Se fosse P=NP, então a decomposição em fatores passaria a ser um problema polinomial e poderia ser resolvido eficientemente. Para fundamentar a segurança de suas senhas a criptografia precisaria arquitetá-las na resolução de algum problema realmente intratável, porque todos os da classe NP teriam passado à categoria de eficientes.

Ricardo Peña Marí é professor da Universidade Complutense de Madrid.

Crônicas do Intangível é um espaço de divulgação sobre as ciências da computação, coordenado pela sociedade acadêmica SISTEDES (Sociedade de Engenharia de Software e de Tecnologias de Desenvolvimento de Software). O intangível é a parte não material dos sistemas informáticos (ou seja, o software), e aqui são contadas sua história e seu devir. Os autores são professores das universidades espanholas, coordenados por Ricardo Peña Marí (professor da Universidade Complutense de Madri) e Macario Polo Usaola (professor titular da Universidade de Castela-La Mancha).