DOIS PROBLEMAS SOBRE GRAFOS

Paulo Cezar Pinto Carvalho
IMPA

INTRODUÇÃO

A figura abaixo mostra um mapa rodoviário de um país fictício. Neste artigo vamos examinar dois problemas relativos a este mapa:

1. Um funcionário, encarregado de verificar, periodicamente, o estado das estradas, deseja planejar a sua rota de inspeção. Idealmente, esta rota deveria se iniciar na capital e percorrer cada **estrada** exatamente uma vez, voltando, então, ao ponto de partida. Existe tal rota?

2. Um representante de vendas de uma companhia deseja planejar uma rota na qual ele visite cada **cidade** exatamente uma vez, voltando ao ponto de partida. Existe tal rota?

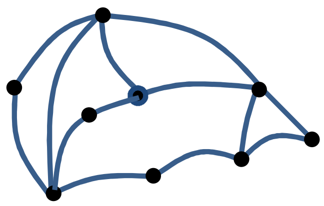

Fig. 1 - Mapa rodoviário de um país fictício

Há vários pontos em comum entre os dois problemas. Por exemplo: em ambos se deseja verificar a existência de um **circuito** (ou **ciclo**) no **grafo** determinado pelo mapa (um grafo é um par (V, A), em que V é o conjunto de **vértices** do grafo, e A é um conjunto de pares de vértices – os **arcos** do grafo). No primeiro problema, este circuito deve incluir exatamente uma vez cada arco do grafo. No segundo problema, o circuito deve incluir exatamente uma vez cada vértice do grafo. Embora os dois problemas sejam aparentemente semelhantes, há algumas diferenças fundamentais entre eles. Convidamos os leitores a refletir um pouco sobre cada um deles antes de prosseguir.

CIRCUITOS EULERIANOS

O primeiro problema – o do inspetor de estradas – foi estudado pela primeira vez por Euler (1707-1783). Por esta razão, um circuito que percorre cada arco de um grafo exatamente uma vez é chamado de **circuito euleriano** e um grafo que possui um tal circuito é chamado de **grafo euleriano**. A situação estudada por Euler ficou imortalizada como o *Problema das Pontes de Könisberg*, ilustrado na figura abaixo, e que possivelmente já é conhecido por muitos dos leitores. O objetivo é percorrer exatamente uma vez todas as sete pontes da cidade (hoje Kaliningrado), que conectam as duas ilhas entre si e com as margens do rio, voltando ao ponto de partida.

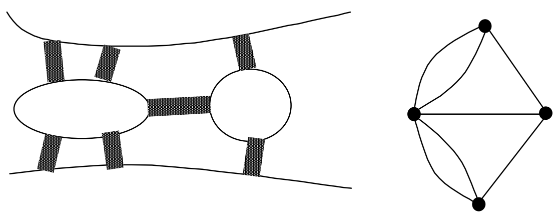

Fig. 2 – O Problema das Pontes de Könisberg

Em linguagem de grafos, trata-se de encontrar um circuito euleriano no grafo da figura acima, no qual os vértices representam as ilhas e as margens e os arcos são as pontes[1]. Euler mostrou a não-existência de tal circuito através de um argumento extremamente simples. Consideremos, por exemplo, a ilha da direita. Um circuito qualquer deve chegar à ilha e sair dela o mesmo número de vezes. Logo, para que exista um circuito euleriano, deve haver um número par de pontes com extremidade nesta ilha. Como existem três pontes nessas condições, concluímos que não é possível encontrar um circuito euleriano. De modo mais geral, temos o seguinte:

Teorema: *Existe um circuito euleriano em um grafo se e somente se o grafo é* ***conexo*** *(isto é, existe um caminho ligando qualquer par de vértices) e cada vértice tem* ***grau*** *par (ou seja, o número de arcos que nele incidem é par).*

O argumento acima mostra a necessidade de se ter grau em cada vértice para existir um circuito euleriano. É também óbvio que o grafo precisa ser conexo. A prova de que essas duas condições implicam na existência de um circuito euleriano pode ser feita por indução finita no número de arcos do grafo e é deixada como um exercício para o leitor.

[Sugestão: suponha a propriedade verdadeira para grafos com menos de n arcos e considere um grafo com n arcos, satisfazendo às duas condições. Começando em um vértice qualquer, percorra arcos do grafo, até voltar a um vértice já visitado (o caminho gerado possui, então, um ciclo). Retirando do grafo os arcos desse ciclo, obtém-se um ou mais grafos satisfazendo as duas condições e com menor número de arcos (portanto, com circuitos eulerianos, de acordo com a hipótese de indução). Basta explicar como "costurar" esses circuitos eulerianos ao ciclo descrito acima].

Podemos aplicar este teorema ao nosso problema de inspeção de estradas. Da mesma forma como no Problema das Pontes de Könisberg, não existe qualquer circuito euleriano no grafo determinado pelo mapa rodoviário, já que o vértice correspondente à capital tem grau 3. Assim, se o nosso inspetor de estradas recebesse de seu chefe a incumbência de elaborar um trajeto nas condições do problema 1, ele poderia facilmente convencê-lo da impossibilidade de fazê-lo. Como veremos a seguir, a situação do seu colega representante de vendas é bem pior...

CIRCUITOS HAMILTONIANOS

Um circuito passando exatamente uma vez por cada vértice de um grafo é chamado de **circuito hamiltoniano**, em homenagem ao matemático irlandês William Rowan Hamilton (1805-1865), que estudou este problema no grafo determinado pelas arestas de um dodecaedro regular (existe ou não um circuito hamiltoniano neste caso?). Um grafo que possui um circuito hamiltoniano é chamado de **grafo hamiltoniano.**

A situação do problema de verificar se um grafo é hamiltoniano é bem diferente da do problema anterior. Apesar de terem sido estudados por vários séculos, não há uma boa caracterização dos grafos hamiltonianos. Há diversas famílias de grafos para os quais existe um circuito hamiltoniano (um exemplo trivial é um grafo completo, em que cada vértice é ligado a todos os outros); também é possível estabelecer certas condições que implicam na não-existência de um circuito. Mas uma caracterização geral não foi encontrada e, à luz de certos avanços em teoria da computação das últimas décadas, parece improvável que ela seja encontrada algum dia.

[1] A rigor, neste caso temos um multi-grafo, já que certos pares de vértices são ligados por mais de um arco.

O problema de decidir se um grafo é hamiltoniano está na companhia de diversos problemas ilustres, com as seguintes características em comum:

- O problema possui uma assimetria fundamental: é muito fácil convencer alguém da existência de um circuito hamiltoniano em um grafo: basta exibir tal caminho. No entanto, é difícil, em geral, convencer alguém da não-existência de um tal circuito. Por exemplo, o grafo da figura abaixo (o leitor é capaz de reconhecê-lo?) tem um circuito hamiltoniano, de cuja existência o leitor fica imediatamente convencido pela figura. Já o grafo dado no início do artigo não tem circuito hamiltoniano, mas não existe um argumento simples e geral para demonstrar esse fato (assim, nosso amigo representante de vendas certamente terá mais trabalho para convencer seu chefe da impossibilidade de elaborar uma rota nas condições do problema 2 do que seu colega inspetor de estradas).

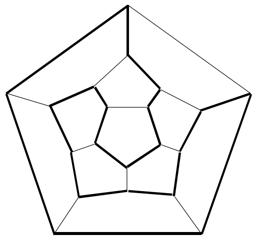

Fig. 3 – Um grafo hamiltoniano

- Não se conhece um algoritmo eficiente para verificar se um grafo é hamiltoniano (por eficiente, entendemos aqui um algoritmo em que o número de passos seja limitado por um polinômio no número de vértices do grafo). Além disso, parece improvável que um tal algoritmo possa algum dia ser encontrado, porque sua existência implicaria na existência de algoritmos eficientes para um grande número de outros problemas, para os quais também não se conhecem algoritmos eficientes. Estes problemas (incluindo o de verificar a existência de circuito hamiltoniano) formam uma classe de problemas chamados de **NP-completos**. Um outro problema famoso da classe é o de determinar o número mínimo de cores que podem ser usadas para colorir os vértices de um grafo de modo que vértices de mesma cor não sejam ligados por um arco.

O leitor poderá estar pensando assim: mas será que esta história de algoritmos eficientes tem relevância, numa era de computadores cada vez mais velozes? Afinal de contas, existe um algoritmo extremamente simples para verificar se um grafo possui um circuito hamiltoniano. Se existir um tal circuito, ele corresponderá a uma permutação (circular) dos vértices com a propriedade de que vértices consecutivos sejam ligados por um arco do grafo. Ora, para verificar a existência de circuito hamiltoniano basta gerar todas as permutações circulares dos vértices e testar se uma delas corresponde a um percurso no grafo.

É claro que este algoritmo funciona para grafos de tamanho moderado (ele poderia ser o recurso usado pelo nosso vendedor: como são apenas 9 cidades, ele teria que testar "apenas" 8! = 40.320 caminhos, o que seria feito com rapidez em um computador). Mas o que ocorre com grafos maiores? Vejamos, por exemplo, uma situação em que o número de cidades cresce para 50 (o que representaria um tamanho ainda bastante razoável para uma situação real). Neste caso, o computador deveria examinar 49! circuitos potenciais. Tentemos estimar a magnitude deste número. A forma mais simples é usar a fórmula de Stirling, que fornece a estimativa $n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$. Mas, neste caso, podemos usar estimativas mais elementares. Por exemplo, podemos usar apenas potências de 2. Temos:

$49! = \quad 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times ... \times 15 \times 16 \times ... \times 31 \times 32 \times \ldots \times 49 \; > 1 \times 2 \times 2 \times 4 \times 4 \times 4 \times 4 \times 8 \times ... \times \; 8 \times 16 \times ... \times 16 \times 32 \times \ldots \times 32 \; = \; 2^2 \text{ x } 4^4 \text{ x } 8^8 \text{ x } 16^{16} \text{ x } 32^{18} \; = \; 2^{2+8+64+90} = 2^{164}$.

Mas $2^{10} = 1024 > 10^3$. Logo $49! > 16.\ 10^{48}$.

Ora, um computador moderno pode realizar cerca de 200 milhões de operações por segundo. Se em cada operação ele conseguir testar um circuito, ele ainda assim precisará de mais de $16.\ 10^{48} / 2.\ 10^6 = 8 \times 10^{42}$ segundos, o que corresponde a aproximadamente a 2×10^{35} anos. Assim, trata-se claramente de uma missão impossível para o algoritmo de força bruta baseado na análise de cada permutação de vértices.

PROBLEMAS DIFÍCEIS QUE TAMBÉM SÃO ÚTEIS

O resultado da discussão acima pode parecer bastante desanimador: não parece haver bons métodos para verificar a existência de um circuito hamiltoniano e algoritmos de força bruta só funcionam para problemas com pequeno número de vértices (é bom que se diga que existe um meio termo: há estratégias que permitem resolver o problema acima para valores razoáveis de *n*, reduzindo substancialmente o número de possibilidades a serem examinadas; mesmo estes algoritmos, no entanto, tornam-se impráticos a partir de um certo ponto). O mesmo ocorre com todos os chamados problemas NP-completos.

No entanto, ao invés de ficarmos deprimidos com esta característica desses problemas, podemos explorá-la para uma importante finalidade em *criptografia*, que é a parte da Matemática que estuda métodos para criar e decifrar códigos. Para tal, é também muito importante a assimetria apontada acima (e que ocorre em todos os problemas NP-completos): é difícil encontrar um circuito hamiltoniano (ou mostrar que não existe um), mas é fácil testar se uma seqüência de vértices forma um circuito hamiltoniano.

Suponhamos que você seja cliente de um banco. Para ter acesso aos serviços, você usa o número de sua conta (que é público) e uma senha, que em princípio deve ser conhecida apenas por você. O procedimento mais simples seria ter a sua senha armazenada no sistema do banco. Mas aí você correria o risco de que ela fosse descoberta, por exemplo, por um funcionário desonesto. Em lugar disto, o sistema do banco armazena uma versão codificada da senha, que não precisa ficar em segredo. Esta codificação deve ser feita de tal forma que seja simples verificar se sua senha está correta (para que você seja autorizado a retirar dinheiro do caixa eletrônico), mas seja praticamente impossível recuperar a senha a partir da versão codificada.

Problemas NP-completos servem como uma luva para esta tarefa. Se quiséssemos usar o problema do circuito hamiltoniano, poderíamos agir mais ou menos da formadescrita a seguir. O cliente poderia escolher uma permutação dos números de 1 a 50, conhecida apenas por ele. A partir dessa informação, seria gerado um grafo, contendo necessariamente os arcos correspondentes ao circuito (os demais poderiam, por exemplo, ser gerados por um método aleatório, em que cada um dos possíveis arcos teria uma certa probabilidade de sere escolhido). Este grafo seria armazenado no sistema. A figura a seguir mostra uma representação de uma permutação dos números de 1 a 50 e um grafo, gerado aleatoriamente, que possui um ciclo hamiltoniano dado por esta permutação.

Fig. 4 – Um ciclo hamiltoniano e um grafo gerado a partir dele

Quando o cliente fosse utilizar sua conta, o sistema simplesmente verificaria se a permutação apresentada corresponde a um caminho no grafo. Como é improvável que um tal ciclo pudesse ser encontrado para um grafo deste tamanho, dificilmente um impostor conseguiria se fazer passar pelo cliente, ainda que conhecesse o grafo-problema. Na prática, são utilizados outros problemas NP-completos para se fazer codificação de senhas, mas a idéia é exatamente a mesma acima.

PALAVRAS FINAIS

Grafos são uma fonte inesgotável de problemas com enunciado simples mas que escondem, muitas vezes, uma sofisticada estrutura matemática. Neste artigo abordamos apenas alguns aspectos de dois desses problemas. Certamente voltaremos a falar em grafos em outros artigos desta revista. Para o leitor que deseja saber mais sobre o assunto, recomendamos os livros a seguir:

- Samuel Jurkievicz. . *Grafos – uma introdução.* OBMEP.
- Jaime Luiz Szwarcfiter. *Grafos e Algoritmos Computacionais*. Editora Campus.
- Oynstein Ore. *Graphs and Their Uses*. The Mathematical Association of America.