Projeto e Análise de Algoritmos

Flávio L. C. de Moura

04 de julho de 2023

Praticamente todos os algoritmos estudados até aqui são polinomiais, i.e. o tempo de execução destes algoritmos no pior caso está em $O(p(n))$, onde $p(n)$ é um polinômio no tamanho da entrada n[1, 2]. Estes algoritmos formam a classe dos algoritmos que são considerados "eficientes". Os problemas que podem ser resolvidos por algoritmos polinomiais são chamados de "tratáveis". No entanto, vimos algoritmos cujos tempos de execução são exponenciais no tamanho da entrada, como por exemplo, busca em grafos utilizando força bruta. De fato, suponha que, dados um digrafo G e vértices u e v de G, queremos determinar quando existe um caminho de u para v em G. Utilizando um algoritmo força bruta, precisamos considerar todos os potenciais caminhos em G, e determinar quando algum deles é um caminho de u para v. Um potencial caminho é uma sequência de vértices de G de tamanho menor ou igual a $|V|$ (o número de vértices de G). O número de potenciais caminhos é $|V|^{|V|}$, e portanto exponencial.

Neste capítulo estudaremos uma classe de problemas para os quais as técnicas estudadas até aqui não se aplicam. Estes problemas não têm soluções polinomiais conhecidas, mas também não existe uma prova de que tais soluções não existam: esta é a famosa questão "P versus NP" que constitui um dos mais interessantes problemas em aberto na Computação. Formalmente, definimos um problema como a seguir:

Definição 1. *Um problema (abstrato) Q é uma relação binária que associa um conjunto I de instâncias a um conjunto S de soluções.*

Por exemplo, o problema PATH é uma relação que associa cada instância de um digrafo e dois vértices com um caminho que contém os dois vértices. O problema SHORTEST-PATH é uma relação que associa cada instância de um digrafo e dois vértices com um caminho mínimo que contém os dois vértices. Como caminhos mínimos não são necessariamente únicos, uma instância de um problema pode ter mais de uma solução. Neste capítulo trabalharemos essencialmente com *problemas de decisão*, que são problemas cujas respostas são sempre *sim* ou *não*:

Definição 2. *Um problema de decisão é uma relação binária sobre um conjunto I de instâncias e um conjunto binário (sim ou não) de soluções.*

Assim, podemos ver um problema de decisão como sendo uma função que associa instâncias em I ao conjunto de soluções $\{0, 1\}$. Por exemplo, o problema PATH é uma relação que associa, cada instância de um digrafo e dois vértices, com um caminho que contém os dois vértices. Este problema pode ser visto como um problema de decisão: Dados um digrafo G, e vértices u e v de G, determinar se existe um caminho de u para v em G.

Seja $\mathcal{C}$ uma classe de problemas caracterizados por uma propriedade, como por exemplo, possuir solução em tempo polinomial. Estamos interessados em identificar os problemas mais difíceis em $\mathcal{C}$, de tal forma que uma solução eficiente para algum destes problemas difíceis resulte em soluções eficientes para todos os outros problemas de $\mathcal{C}$. Na próxima seção estudaremos a classe P dos problemas que podem ser resolvidos deterministicamente em tempo polinomial.

1 A classe P

A classe P consiste dos problemas que podem ser resolvidos em tempo polinomial por um algoritmo determinístico.

Teorema 3. *PATH está em P*

Prova. Considere o seguinte algoritmo que recebe como entrada um digrafo G e vértices u e v.

1. Marque o vértice u
2. Enquanto existir aresta $(a, b) \in G$ com a marcado, e b não-marcado, marque b.
3. Se v está marcado retorne 1, caso contrário retorne 0.

   Análise do algoritmo: O *laço* (linha 2) pode ser executado segundo o algoritmo de busca em largura, por exemplo, que é linear no tamanho da representação do grafo G. As outras linhas do algoritmo são executadas apenas uma vez, portanto o algoritmo é polinomial.

□

1.1 Reduções em tempo polinomial

A ideia de *redutibilidade* entre dois problemas é que se um possui uma solução eficiente, então o outro também pode ser resolvido de forma eficiente. Adicionalmente, também podemos dizer que um problema não é mais fácil, e nem mais difícil, que outro também se aplica quando ambos são problemas de decisão. Por exemplo, considere um problema A que queremos resolver em tempo polinomial. Suponha que sabemos como resolver um outro problema B em tempo polinomial, e que temos um procedimento que transforma instâncias do problema A em instâncias do problema B com as seguintes características:

- A transformação é feita em tempo polinomial;
- As respostas são as mesmas para ambas as instâncias.

Chamamos este procedimento de *algoritmo de redução*, que nos fornece uma forma de resolver o problema A em tempo polinomial:

- Dada uma instância α do problema A, usamos o algoritmo de redução para transformá-la em uma instância β do problema B;
- Executamos o algoritmo polinomial para a instância β de B;
- Usamos a resposta de β como resposta de α.

Como cada um destes passos é realizado em tempo polinomial, todo o algoritmo também é realizado em tempo polinomial, e portanto temos uma forma de decidir A em tempo polinomial.

1.2 Linguagem formal

Um problema de decisão pode ser visto como um problema de reconhecimento de linguagem: seja U o conjunto de todas as entradas possíveis para o problema de decisão. Seja $L \subseteq U$, o conjunto de todas as entradas para as quais a resposta do problema é *sim*. Chamamos L a *linguagem* correspondente ao problema, e utilizamos os termos *problema* e *linguagem* de forma intercambiável. O problema de decisão deve então reconhecer se uma dada entrada pertence ou não à linguagem L.

Definição 4. *Seja Σ um conjunto finito (de símbolos) que chamaremos de alfabeto. O conjunto de todas as palavras (*strings*) que podem ser formadas com os símbolos de Σ é denotado por Σ^*. Uma linguagem L sobre Σ é qualquer subconjunto de Σ^*. O alfabeto vazio é denotado por ϵ, enquanto que a linguagem vazia é denotada por $\emptyset$.*

Diversas operações podem ser realizadas sobre linguagens: união, interseção, complemento, concatenação e fechamento. Do ponto de vista da teoria de linguagens formais, o conjunto das instâncias de qualquer problema de decisão Q é simplesmente o conjunto Σ^*, onde $\Sigma = \{0,1\}$. Como o problema Q é caracterizado pelas instâncias que produzem resposta 1 (*sim*), podemos ver a linguagem L sobre $\Sigma = \{0,1\}$ como sendo $L = \{x \in \Sigma^* \mid Q(x) = 1\}$.

Definição 5. *Dizemos que um algoritmo A aceita a palavra $x \in \{0,1\}^*$ se $A(x) = 1$, i.e. a resposta do algoritmo A ao receber a entrada x é igual a 1. A linguagem aceita pelo algoritmo A é o conjunto das palavras aceitas pelo algoritmo: $L = \{x \in \{0,1\}^* \mid A(x) = 1\}$. Dizemos que o algoritmo A rejeita a palavra x, se $A(x) = 0$.*

Note que, mesmo que a linguagem L seja aceita pelo algoritmo A, isto não significa que A rejeita uma palavra $x \notin L$ porque, por exemplo, A pode entrar em *loop*.

Definição 6. *Uma linguagem L é decidida pelo algoritmo A, se A aceita toda palavra em L, e rejeita toda palavra que não está em L. Uma linguagem L é aceita em tempo polinomial pelo algoritmo A, se A aceita L, e se existe uma constante k tal que para qualquer palavra $x \in L$ de comprimento n, o algoritmo A aceita x em tempo $O(n^k)$, para algum $k \geq 0$. Uma linguagem L é decidida em tempo polinomial pelo algoritmo A se existir uma constante não-negativa k tal que para qualquer palavra $x \in \{0,1\}^*$, o algoritmo decide em tempo $O(n^k)$ se $x \in L$.*

Assim, para aceitar uma linguagem, o algoritmo precisa apenas produzir uma resposta para toda palavra de L, mas para decidir uma linguagem, o algoritmo precisa aceitar ou rejeitar toda palavra em $\{0,1\}^*$. Como exemplo, o problema de decisão PATH corresponde a seguinte linguagem:

PATH $= \{\langle G, u, v, k\rangle : G = (V, E)$ é um grafo (não dirigido), $u, v \in V, k \geq 0$ é um inteiro, e existe um caminho de u para v em G contendo, no máximo, k arestas$\}$. Assim, a linguagem PATH pode ser aceita em tempo polinomial pelo seguinte algoritmo: Dada uma instância (G, u, v), o algoritmo executa BFS para computar o menor caminho de u para v, e então compara o número de arestas deste menor caminho com k. Se o menor caminho possui até k arestas então o algoritmo retorna 1, e para. Caso contrário, o algoritmo entra em *loop*. Note que este algoritmo não decide PATH. Neste caso, para decidir PATH basta que o algoritmo retorne 0 e pare, ao invés de entrar em *loop*. Para outros problemas, como o *problema da parada para máquinas de Turing*, existem algoritmos de aceitação, mas não de decisão.

Por fim, definimos a classe P em termos de linguagens:

$P = \{L \subseteq \{0,1\}^* :$ existe um algoritmo A que decide L em tempo polinomial$\}$

Definição 7. *Dizemos que uma linguagem L_1 é redutível polinomialmente à linguagem L_2, notação $L_1 \leq_p L_2$, se existe uma função computável em tempo polinomial $f : \{0,1\}^* \to \{0,1\}^*$ tal que para todo $x \in \{0,1\}^*$, $x \in L_1$ se, e somente se, $f(x) \in L_2$. A função f é chamada de* função de redução*, e o algoritmo polinomial F que computa a função f é chamado de* algoritmo de redução*.*

Observe que ao reduzirmos uma linguagem (ou problema) L_1 para outra linguagem (ou problema) L_2, queremos que cada instância de L_1 seja transformada em uma instância de L_2, isto é, se $x \in L_1$ então $f(x) \in L_2$. Adicionalmente, precisamos que elementos que não sejam instância de L_1 não sejam levados em L_2: $x \notin L_1$ então $f(x) \notin L_2$, o que é equivalente por contraposição a se $f(x) \in L_2$ então $x \in L_1$. Juntando estas duas informações temos a equivalência "$x \in L_1$ se, e somente se, $f(x) \in L_2$" da definição acima.

Reduções polinomiais são uma ferramenta poderosa que nos permitem provar que outras linguagens estão em P:

Lema 8. *Sejam $L_1, L_2 \in \{0,1\}^*$ linguagens tais que $L_1 \leq_p L_2$, então $L_2 \in P$ implica que $L_1 \in P$.*

Prova. Seja A_2 um algoritmo polinomial que decide a linguagem L_2, e F um algoritmo de redução polinomial que computa a função de redução f. Construiremos um algoritmo A_1 que decide L_1 da seguinte forma: dado $x \in \{0,1\}^*$, o algoritmo A_1 inicialmente usa F para transformar x em $f(x)$, e então usa o algoritmo A_2 para responder. Note que A_1 é polinomial já que tanto A_2 quanto F são polinomiais. □

Considere o problema 2-SAT, cujas instâncias são expressões lógicas formadas por conjunções de disjunções de dois literais, onde um literal é uma variável booleana ou a negação de uma variável booleana. Por exemplo, a expressão a seguir é uma instância de 2-SAT:

$$(x_1 \vee \neg x_2) \wedge (\neg x_1 \vee \neg x_3) \wedge (x_1 \vee x_2)$$

Uma solução da instância acima é uma designação de valores booleanos (0 ou 1) para as variáveis que satisfaçam a expressão, ou seja, que retornem 1. Por exemplo, a designação $x_1 = 1$, $x_2 = 1$ e $x_3 = 0$ satisfaz a expressão acima.

Teorema 9. *2-SAT $\in$ P.*

2 A classe NP

A classe NP consiste dos problemas que podem ser resolvidos em tempo polinomial por um algoritmo não-determinístico. A ideia é que inicialmente, o algoritmo advinhe uma solução (fase não-determinística), e em seguida esta solução deve ser verificada em tempo polinomial deterministicamente. Assim, a forma mais usual de apresentar a classe NP, consiste em considerar os problemas que podem ser verificados em tempo polinomial por um algoritmo determinístico [1, 2].

Como vimos, em alguns casos é possível evitar uma abordagem força bruta e encontrar soluções polinomiais para o problema em questão. Mas é fácil imaginar que isto nem sempre será possível. De fato, veremos que existem diversos problemas interessantes/importantes para os quais soluções polinomiais não foram encontradas até hoje, mas que ainda é possível verificar em tempo polinomial, dado um certificado.

Exemplo 10. *O problema de encontrar ciclos Hamiltonianos em (di)grafos tem sido estudado por muito tempo (mais de 100 anos!). Formalmente, um ciclo Hamiltoniano de um grafo $G = (V, E)$ é um ciclo simples que contém cada vértice de V, i.e. cada vértice de G é visitado uma única vez. Um (di)grafo que contém um ciclo Hamiltoniano é dito Hamiltoniano.*

Denotaremos por HAM-CYCLE o problema de encontrar ciclos Hamiltonianos em (di)grafos.

HAM-CYCLE = $\{\langle G\rangle : G$ é um (di)grafo Hamiltoniano $\}$

Podemos verificar uma possível solução em tempo polinomial: Suponha que um colega te diz que um (di)grafo G é Hamiltoniano, e como justificativa, fornece uma sequência de vértices na ordem que ele diz formar um caminho Hamiltoniano.

1. *Verifique que os vértices dados constituem o conjunto V dos vértices de G;*
2. *Verifique que cada par de vértices consecutivos da sequência dada corresponde a uma aresta de G.*

Como a verificação acima pode ser feita em tempo polinomial, temos que HAM-CYCLE $\in$ NP.

2.1 Algoritmos de Verificação

Definição 11. *Um algoritmo de verificação é um algoritmo A que recebe dois argumentos x e y, e verifica se $A(x, y) = 1$. Uma linguagem verificada por um algoritmo de verificação A é*
$L = \{x \in \{0,1\}^* : \exists y \in \{0,1\}^*$ *tal que* $A(x, y) = 1\}$

Intuitivamente, o algoritmo A verifica a linguagem L se, para cada $x \in L$, existe um certificado y tal que A é usado para provar que $x \in L$. Formalmente, a classe NP é a classe das linguagens que podem ser verificadas em tempo polinomial.

$$NP = \{L \subseteq \{0,1\}^* : \text{ existe um algoritmo determinístico } A \text{ que verifica } L \text{ em tempo polinomial}\}$$

Mais precisamente, $L \in$ NP se, e somente se, existe um algoritmo polinomial A e uma constante c tais que $L = \{x \in \{0,1\}^* : \exists y, |y| = O(|x|^c)$ tal que $A(x, y) = 1\}$.

Agora é fácil ver que HAM-CYCLE ∈ NP. Basta checar que o caminho dado (sequência de vértices) é uma permutação de V, isto é, cada vértice ocorre apenas uma vez, e que existe uma aresta em G para cada par de vértices consecutivos do caminho dado, e entre o primeiro e último vértices.

Estamos interessados em algoritmos que verificam se uma instância está ou não em uma linguagem. Por exemplo, dada uma instância (G, u, v) do problema de decisão PATH, e um caminho p de u para v, podemos facilmente verificar se p é um caminho em G.

A classe NP consiste dos problemas que podem ser verificados em tempo polinomial, i.e. dado um certificado, podemos verificar em tempo polinomial que este certificado é correto. Por exemplo, considerando o problema dos ciclos hamiltonianos em um (di)grafo $G = (V, E)$ com $n = |V|$, um certificado pode ser uma sequência $\langle v_1, v_2, \ldots, v_n \rangle$ de vértices que pode ser verificada em tempo polinomial. Para o problema 3-SAT, um certificado pode ser uma designação de valores para as variáveis da fórmula que pode ser verificado (se satisfaz ou não a fórmula dada) em tempo polinomial.

Exemplo 12. *Um clique em um grafo (não dirigido) é um subgrafo onde dois vértices quaisquer estão ligados por uma aresta. Um k-clique é um clique que contém k vértices. O problema CLIQUE consiste em determinar se um grafo contém um clique de um tamanho especificado:*

CLIQUE $= \{(G, k) : G$ *é um grafo com um k-clique*$\}$

***Afirmação**: CLIQUE* $\in$ *NP*

O clique é o certificado. Para a entrada $((G, k), c)$

1. *Verifique se c é um subconjunto de G.V de tamanho k;*
2. *Verifique se G contém todas as arestas que conectam vértices em c;*
3. *Se ambas as verificações podem ser feitas então retorne 1, caso contrário, retorne 0.*

Teorema 13. *3-SAT* $\leq_P$ *CLIQUE*

Prova. Nos grafos a serem construídos, cliques de um tamanho específico correspondem a designações satisfatíveis da fórmula. Seja φ uma fórmula com k cláusulas

$$\varphi = (a_1 \vee b_1 \vee c_1) \wedge (a_2 \vee b_2 \vee c_2) \wedge \ldots (a_k \vee b_k \vee c_k)$$

A redução f constrói a codificação $\langle G, k \rangle$ onde G é um grafo não dirigido dado por:

- Os vértices de G são organizados em k grupos de 3 vértices cada $t_1, t_2, \ldots, t_k$. Cada tripla t_i corresponde a uma das cláusulas de φ, e cada vértice na tripla corresponde a um literal da cláusula associada. Marque cada vértice de G com o literal correspondente em φ. As arestas de G conectam todos os vértices exceto:
  - vértices contraditórios, como x e $\neg x$;
  - vértices da mesma tripla.

Afirmação: φ é satisfatível se, e somente se, G possui um k-clique.

Suponha que φ é satisfatível, e portanto cada cláusula possui pelo menos um literal verdadeiro. Em cada tripla em G, selecionamos um vértice correspondente ao literal verdadeiro. Se mais de um literal for verdadeiro na mesma cláusula, escolhemos um deles aleatoriamente. Os vértices selecionados formam um k-clique: o número de vértices selecionados é k, cada par de vértices selecionado está ligado por uma aresta.

Suponha que G possui um k-clique. Nenhum par de vértices do clique ocorre na mesma tripla porque vértices da mesma tripla não são ligados por arestas. Portanto, cada tripla contém exatamente um dos vértices do k-clique. Designamos valores para as variáveis de φ de forma que cada literal que marca um vértice assume valor 1 (verdadeiro). Isto é possível porque vértices contraditórios não são ligados. Esta designação de variáveis satisfaz a fórmula φ porque cada tripla corresponde a um vértice do clique, e portanto cada cláusula de φ tem valor 1. □

Referências

[1] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms, Third Edition.* The MIT Press, 3rd edition, 2009.

[2] Michael Sipser. *Introduction to the Theory of Computation.* International Thomson Publishing, 1st edition, 1996.