Algoritmos certificadores e verificadores: testemunhas ausentes e provas computacionais*

Anne Rose Alves Federici Marinho
Vinícius Gusmão Pereira de Sá

Universidade Federal do Rio de Janeiro, Brasil
annefederici@gmail.com, vigusmao@dcc.ufrj.br

Um *algoritmo certificador* para um problema Π exibe, para uma instância x de Π, uma resposta y e uma *testemunha* w, possibilitando a verificação da corretude da resposta por meio de um *algoritmo verificador*, que recebe x, y e w como entrada. Algoritmos certificadores são em muitos casos preferíveis a algoritmos tradicionais (não-certificadores) porque permitem que acatemos as respostas obtidas como verdadeiras sem que precisemos confiar cegamente na *implementação* dos algoritmos que as encontraram, garantindo que as respostas não foram comprometidas por falhas na implementação.

Na literatura sobre algoritmos certificadores [2], busca-se em geral possibilitar uma verificação simples, de forma que a corretude do próprio verificador possa ser trivialmente comprovada, e eficiente, permitindo que a resposta seja verificada a partir da testemunha fornecida sem aumento significativo do tempo total de processamento. Há, no entanto, dois casos que fogem a esse padrão e que apresentam, ainda assim, interesse do ponto de vista de certificação/verificação. O primeiro caso é aquele em que conseguimos construir verificadores que prescindem de testemunhas, pois são capazes de efetuar a verificação de forma simples e eficiente diretamente da resposta obtida. O segundo é o caso em que a testemunha exibida permite uma verificação que não é formalmente eficiente, por demandar tempo exponencial, mas que, para instâncias pequenas, é computacionalmente viável, permitindo por exemplo a criação de provas computacionais para teoremas.

Ilustramos os dois casos acima, respectivamente, com algoritmos verificadores para o problema da seleção dos k maiores elementos [1] e o problema de reconhecimento de grafos de disco unitário [3].

References

[1] Blum, M., Floyd, R. W., Pratt, V. R., Rivest, R. L., Tarjan, R. E., Time bounds for selection, *Journal of Computer and System Sciences* 7 (4) (1973) 448–461.

[2] McConnell, R.M., Mehlhorn, S., Schweitzer, P., Certifying Algorithms, 2010. *Computer Science Review* 5(2) (2011) 119–161.

[3] McDiarmid, C., Müller, T., Integer realizations of disk and segment graphs, J. Comb. Theory, Series B 103(1) (2013) 114–143.

*Trabalho parcialmente financiado pelo CNPq e pela CAPES.