Universidade de Brasília
Instituto de Ciências Exatas

Departamento de Ciência da Computação

117536 - Projeto e Análise de Algoritmos
Turma: B

Análise Assintótica e Corretude do Algoritmo KMP Utilizando PVS

Gabriel Levi - 16/0006490
Gabriel Nunes - 16/0006597

21 de outubro de 2019

1 Introdução

A verificação formal de algoritmo, no que tange ao seu comportamento assintótico e a corretude do algoritmo é interesse central da Ciência da Computação. Por vezes, a prova via argumentação, isto é, lápis e papel pode ser suficiente para que o escritor convença o leitor de que o algoritmo está correto. Contudo, esse modelo de prova se sustenta muita vezes em passos de pura intuição, assumições que ambas as partes enxergam como um axioma, e saltos lógicos que por mais naturais que pareçam escondem um conjunto não-trivial de conceitos. A ocorrência desses aspectos em uma formalização pode ocultar falhas que, de fato, provem a incorretude do algoritmo e desmonstre um comportamento assintótico pior do que o esperado.

Como forma de minimizar o exposto anteriormente, introduz-se os sistemas de verificação de provas. Os verificadores garantem que os passos realizados dentro de uma prova respeitem o conjunto de regras de sua lógica intrínseca. Então, dadas premissas corretas e um ponto factível onde se deseja chegar, qualquer passo intermediário tem que, necessariamente, estar correto. Obviamente, construções ruins de objetivos e premissas podem levar a provas, ainda sim, incorretas ou impossíveis. Podemos concluir então que os sistemas de verificação pressupõe que uma prova, ou pelo menos a ideia da mesma, já exista e o usuário interessado o utilize para demonstrar que de fato aquela construção vale.

Um dos verificadores, PVS - Prototype Verification System - é a linguagem de especificação e provador automatizado de teoremas que aqui será utilizado. PVS trabalha com implementações em distribuições de diferentes versões de LISP. Em um arquivo, o usuário define premissas - um algoritmo - e teoremas. O arquivo é dado como entrada para o provador que requisita as regras a serem aplicadas até que o teorema desejado seja provado. As regras reconhecidas pelo PVS tratam-se simplesmente de regras da lógica de primeira-ordem. O PVS permite também que uma prova possa ser revisitada em uma representação gráfica que revela cada passo bem como suas depedências.

O objetivo deste trabalho é analisar assintóticamente o custo de tempo e a corretude do algoritmo de *pattern matching* desenvolvido por Donald Knuth, James Morris e Vaughan Pratt (KMP) e publicado em 1977. A escolha do KMP como objeto de estudo se deu pelo seu grande conjunto de aplicações práticas e por se tratar de um algoritmo muito inteligente para um problema onde a solução ingênua pode facilmente ter comportamento

assintótico de ordem quadrática ou cúbica. A análise aqui feita apresentará a ideia de prova que será verificada via PVS. A formalização completa pode ser encontrada em `https://github.com/paa-2019-2/kmp-analysis`.

Esse documento se organizará, daqui em diante, primeiro por um capítulo de revisão teórica. Em seguida, no capitulo 3, a apresentação do algoritmo KMP apoiado por instâncias de entradas para melhor entendimento. O capitulo 4 apresentará a ideia abordada pelos autores para a análise de assintótica do algoritmo bem como argumentação sobre o pior e o melhor caso do mesmo. O capitulo 5 - Correção do algoritmo KMP - apresentará, como o capitulo anterior, a ideia abordada e sua argumentação. Por fim, o capitulo de conclusão, apresentará um resumo dos resultados aqui encontrados acompanhado de um meta-texto discorrendo sobre as principais dificuldades do trabalho com o verificador formal de provas.

2 Revisão teórica

Este capítulo apresentará conceitos importantes para o entedimento do que se segue nos capitulos posteriores. Caso sinta-se a vontade com o conceito, cujo o nome será enunciado no título de cada subseção, não há nenhum mal em pular. Cada um dos conceitos será apresentado de maneira simples mais preocupado com ser inteligível para o leitor do que com um profundo formalismo. Em compensação, uma boa bibliografia de apoio será indicada para aqueles interessados em se aprofundar ou que não acharam que o texto de uma ou mais subseções foi suficiente.

// Se não existir nada além de Notação Assintótica, converter pra uma seção de revisão sobre Notação assintótica.