Proceeding Series of the Brazilian Society of Computational and Applied Mathematics
Preprint

Limites Inferiores para Cadeias Aditivas

Ian Maldonado Kühl[1] Alessandro Firmiano[2] João Paulo M. dos Santos[3]
Academia da Força Aérea-AFA, Pirassununga, SP

O conceito de Cadeia Aditiva baseia-se em uma lista de números em que o primeiro valor é igual a 1. Os demais valores da sequência são obtidos por etapas de adição dois a dois dos elementos anteriores e não necessariamente diferentes. Ao atingir um valor natural n, fica estabelecia uma cadeia de adição de n. Por exemplo, a sequência: $1, 2, 3, 6, 9, 9, 12, 24, 15$ é uma cadeia de adição para $n = 15$. Esta cadeia possui um elemento maior que o último elemento $n = 15$, no entanto, a remoção do valor 24 da sequência ainda configura uma cadeia de adição que válida. Logo, mesmo sendo uma cadeia aditiva não ordenada pelos valores naturais dos seus elementos, a cadeia ainda seria válida após a eliminação de valores maiores que o elemento **alvo**. Elementos duplicados são permitidos e alguns elementos da cadeia podem ser construídos de mais de uma maneira. No exemplo acima, $12 = 3 + 9$ e $12 = 6 + 6$. Neste resumo, as Cadeias Aditivas possuem elementos em ordem crescente e não possuem elementos duplicados, ou seja, são expressas da seguinte forma [2]:

$$1 = a_0 < a_1 < \cdots < a_r = n, \quad a_i = a_j + a_k, \quad i > j \geqslant k \geqslant 0. \tag{1}$$

A Cadeia Aditiva de n definida em (1) possui tamanho $l(n) = r$. A cadeia que possui o menor tamanho para o valor n é denominada de **Cadeia Ótima** (*optimal chain*). Calcular uma cadeia aditiva de comprimento mínimo não é uma tarefa fácil. Uma versão generalizada deste tipo de problema, em que se deve encontrar uma cadeia que forma simultaneamente cada uma de uma sequência de valores, é NP-completa [6]. Até o momento, não existe um algoritmo conhecido que possa calcular uma Cadeia Ótima para um determinado n com garantia de tempo razoável e de baixo custo computacional.

Uma aplicação imediata da Cadeia Aditiva (1) pode ser encontrada na área da Computação com problemas relacionados ao processo de exponenciação a^n de forma eficiente [4], pois, $l(n)$ pode representar o número de multiplicações necessárias. Um caso clássico é a aplicação da Cadeia Ótima $1, 2, 3, 6, 12, 24, 30, 31$ para minimizar a operação a^{31} determinando apenas sete multiplicações:

$$a^2 = a \cdot a,\ a^3 = a^2 \cdot a,\ a^6 = a^3 \cdot a^3,\ a^{12} = a^6 \cdot a^6,\ a^{24} = a^{12} \cdot a^{12},\ a^{30} = a^{24} \cdot a^6,\ a^{31} = a^{30} \cdot a.$$

Uma técnica para calcular cadeias aditivas relativamente curtas é o **Método Binário**. Nesta estratégia, uma cadeia aditiva para n é obtida recursivamente, a partir de uma cadeia para $\textbf{floor}\left(\frac{n}{2}\right)$. Caso n seja par, pode ser obtido em uma única soma adicional, pois, $n = 2 \cdot \textbf{floor}\left(\frac{n}{2}\right)$. Caso n seja ímpar, o método utiliza duas somas: $n - 1 = \textbf{floor}\left(\frac{n}{2}\right)$ e em seguida a adição de 1. O **Método do Fator** para encontrar cadeias aditivas é baseado na fatoração de n em números primos. Desta forma, se p é um fator primo de n, então a cadeia aditiva pode ser obtida iniciando com uma corrente para $\frac{n}{p}$ e, em seguida, concatenando uma cadeia para o primo p, modificado pela multiplicação de cada um dos elementos por $\frac{n}{p}$ [5].

[1] ianmaldonadokuhl@gmail.com
[2] firmianoafj@fab.mil.br
[3] jp2@alumni.usp.br

Em 1937, Edward G. Thurber estabeleceu as bases da atual notação para as Cadeias Aditivas, tais como, os conceitos de *small step* e *large step*. Contudo, tais definições não levam em consideração a análise sobre o peso de Hamming dos números abordados e, portanto, não são capazes de constituírem instrumento próprio para a análise de certas situações envolvendo Cadeias Aditivas. O objetivo deste trabalho é compreender como ocorre o aumento do peso de Hamming e a sua relação com as etapas definidas por Thurber. Uma conjectura conhecida por **Knuth-Stolarsky** estabelece um limite inferior para o comprimento das Cadeias Aditivas [7]. Para isto, considere as seguintes definições de Thurber para um dado inteiro positivo n:

$$\begin{cases} \lambda(n) = \lfloor \log_2(n) \rfloor \\ s(n) = l(n) - \lambda(n) \\ v(n) = \#\{1|(n)_2\}. \end{cases} \tag{2}$$

Com as definições em (2) é conjecturado que $v(n) \leqslant 2^{s(n)}$, ou seja, $l(n) \geqslant \lambda(n) + \lfloor \log_2 v(n) \rfloor$. Buscas realizadas por computadores não encontraram contradições com a conjectura para todo $n \leqslant 2^{64}$ [3]. Se for verdadeira, uma Cadeia Aditiva relativamente curta para $n = 223.696.213$, cuja representação binária é 1101010101010101010101010101 ($v(n) = 15$ e $s(n) = 6$) é dada por:

$1, 2, 3, 5, 10, 13, 23, 46, 92, 105, 210, 420, 840, 1680, 3360, 6720, 6825, 13650, 27300, 54600, 109200, 218400, 4320800, 873600, 1736003494400, 6988800, 13977600, 27955200, 55910400, 111820800, 223641600, 223696200, 223696213.$

O comprimento $l(n)$ de uma Cadeia Aditiva é um parâmetro complicado e muitas vezes difícil de ser computado [1], no entanto, pode ser provado que:

$$\log_2 n \leqslant l(n) \leqslant \lfloor \log_2(n) \rfloor + v(n) - 1. \tag{3}$$

Assim, conforme foi demonstrado por Brauer (1939), o comportamento de $l(n)$ é aproximadamente logarítmo, ou seja, $l(n) \sim \log_2 n$.

Referências

[1] H. Altman. **Internal Structure of Addition Chains: Well-Ordering**. Online. Acesso em 28/03/2022, `https://arxiv.org/pdf/1409.1627.pdf`. 2015.

[2] A. T. Brauer. "On Addition Chains". Em: **American Mathematical Society** 45(10) (1939), pp. 736–739. DOI: `10.1090/S0002-9904-1939-07068-7`.

[3] N. M. Clift. "Calculating Optimal Addition Chains". Em: **Computing V** 91(3) (2011), pp. 265–284. DOI: `10.1007/s00607-010-0118-8`.

[4] H. Dellac. "Question 49". Em: **L'Intermédiaire des Mathématiciens** (1894), p. 20.

[5] W. Hansen. "Zum Scholz-Brauerschen Problem". Em: **Journal für die reine und angewandte Mathematik** 202 (1959), pp. 129–136. URL: `http://eudml.org/doc/150404`.

[6] E. D. Knuth. **The Art of Computer Programming**. 1st. ed. Addison-Wesly, 2007. ISBN: 978-0321751041.

[7] K. B. Stolarsky. "A lower bound for the Scholz-Brauer problem". Em: **Canadian Journal of Mathematics** 21 (1969), pp. 675–683. DOI: `https://doi.org/10.4153/CJM-1969-077-x`.