

定理証明ツール Coq を使ったアッカーマン関数に関する性質の証明

1230345 出井 智也 【ソフトウェア検証・解析学研究室】

1 はじめに

アッカーマン関数は、原始再帰的でない再帰関数の例として知られ、また非常に値が大きくなることでも有名な関数である [1, アッカーマン関数], [2, pp.65–66]. これまで、アッカーマン関数についての研究は一部の計算機科学分野や数論での応用が主であり、その諸性質についての証明は非形式的なものが主であった. 本論文では、アッカーマン関数についての性質の一つを取り上げ、定理証明ツール Coq を用いて形式的に証明することを目的とする. 計算機科学の中の計算複雑性理論の分野では、指数時間 $O(2^n)$ や二重指数時間 $O(2^{2^n})$ を超える計算量階層が存在し、扱われる場合がある. その中でも特に大きな計算量として指数タワー $tower(2, n) = \underbrace{2^{2^{\cdot^{\cdot^2}}}}_n$ やアッカーマン関数 $A(n, n)$ が使われる. $A(n, n)$ が $tower(2, n)$ より漸近的に大きいことは既に知られているが、本論文ではそれを形式的に証明することを目標とする.

2 形式的証明と定理証明ツール

形式的証明とは、我々の用いる自然言語に起因する曖昧さを含む非形式的証明と違い、予め定められた公理と変換規則のみを用いて行われる証明あるいはその手法のことである. 証明すること自体に厳密な正しさが保証される反面、証明の記述や検証に多大な時間と労力を必要とする. そこで使われるのが、本研究で用いた Coq に代表される定理証明ツールである. Coq はカリー・ハワード同型対応を利用した型理論に基づく定理証明ツールであり、代数的な定理の証明に多く用いられる. Coq には専用 IDE が付随しており、本研究におけるコーディング・実行も CoqIDE 上で行った.

3 定義

3.1 アッカーマン関数

アッカーマン関数の定義は以下のように表される [1, アッカーマン関数].

$$A(x, y) = \begin{cases} y + 1 & x = 0, \\ A(x - 1, 1) & x > 0, y = 0, \\ A(x - 1, A(x, y - 1)) & \text{otherwise} \end{cases}$$

Coq で再帰関数を定義する際は構文的に停止性が保証されていないため上記の定義の 3 行目をそのまま与えることはできない. ここでは、Coq に与える定義として、[3] に掲載されていたものを使用した.

3.2 クヌースの矢印表記

クヌースの矢印表記は、1976 年にドナルド・クヌースによって考案されたハイパー演算子の表記法である

[1, 矢印表記], [2, pp.45–46]. 定義は以下の通り [1, 矢印表記].

$$\begin{aligned} a \uparrow^1 b &= a^b \\ a \uparrow^n 1 &= a \\ a \uparrow^{n+1} (b + 1) &= a \uparrow^n (a \uparrow^{n+1} b) \end{aligned}$$

Coq での定義は、[1, 矢印表記] に記載されていた定義を参考に、自然数の引数 a, n, b をとる再帰的な関数とした. ただし、 n は矢印の本数である. なお、[1, 矢印表記] の定義では $a \uparrow^1 b = a^b$ が再帰的定義の基底となっているが、Coq では自然数は 0 以上の整数と定義されているため、 $n = 0$ のときの定義がないと不都合が生じる. そのため、本研究では $a \uparrow^0 b = a \times b$ とした.

3.3 証明する命題

本研究では、[2, p.67] で非形式的な証明が与えられている命題「自然数 m, n について、 $m > 2$ のとき、 $A(m, n) = 2 \uparrow^{m-2} (n + 3) - 3$ 」及び $tower$ と矢印表記の関係 $tower(m, n) = m \uparrow^2 n$ を、Coq を使って証明する.

4 結果と考察

上記の定義に基づいて Coq を使った証明を試みた結果、5.3 で挙げた命題の証明に成功した. これによって、本論文の目標であった $A(n, n)$ と $tower(2, n)$ の関係は、矢印表記に関する命題 $(2 \uparrow^{n-2} (n + 3)) - 3 > 2 \uparrow^2 n$ として表すことができる. 十分大きな n に対してこの不等式が成り立つことは非形式的には自明であるから、本論文の目標は十分に達成したと考えられる. 最後に述べた不等式を形式的に証明することが今後の課題である. また、漸近的に真に $A(n, n)$ の方が大きいことを言うために、右辺に任意の正の定数を乗じてこの不等式が成立することを形式的に証明することも今後の課題である.

参考文献

- [1] 巨大数研究 Wiki | Fandom, <https://googology.fandom.com/ja/wiki/%E5%B7%A8%E5%A4%A7%E6%95%B0%E7%A0%94%E7%A9%B6Wiki>, 2023 年 2 月 6 日 10:21 閲覧
- [2] フィッシュ, "巨大数論 第 2 版", <https://gyafun.jp/ln/largenumber.pdf>
- [3] プログラミング Coq 7 章 停止性が明らかでない関数を定義するには, <https://www.iiijlab.net/activities/programming-coq/coqt7.html>, 2023 年 2 月 6 日 10:08 閲覧