The Proof Of The Scholz-Brauer Conjecture

Xiao-Wei Li
(xiaowei-li@foxmail.com)

Abstract

A proof of the Scholz-Brauer conjecture. The method uses a comparative analysis of approaches to overcome a long-standing difficulty. Its significance lies in advancing the analysis in this area and providing a new analytical tool.

Keywords

Scholz-Brauer conjecture, proof, comparative analysis.

Introduction

In computational complexity theory there is an easily understood conjecture — the Scholz-Brauer conjecture, which has a history of over sixty years. This conjecture concerns algorithms for computing x^n for a given positive integer x. Regardless of the size of the two numbers, each multiplication is counted as one step. Among all possible algorithms that obtain x^n from x, the least number of steps is denoted by $\alpha(n)$.

The Scholz-Brauer conjecture states that for every positive integer n, there are:

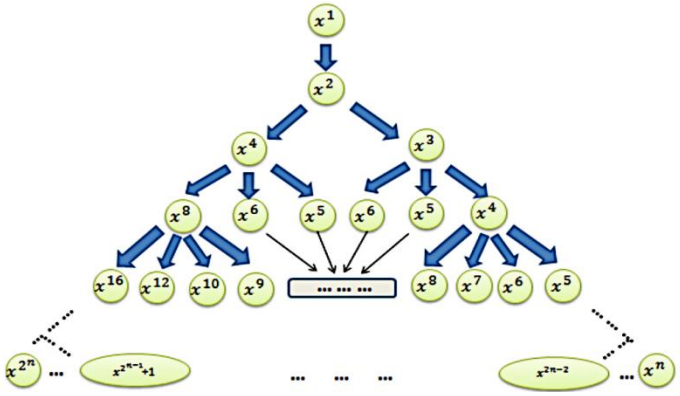
$$\alpha(2^n-1)\leq\alpha(n)+n-1$$

Method

Proof. At first, we note: $f(n)=x^n$, $g(n)=x^{2^n-1}$, $\beta(n)=\alpha(2^n-1)$

The Scholz-Brauer conjecture is equivalent to the following problem. Find the shortest path (from x^1 to x^n) in the Graph A.

Graph A.



Then ,the steps of the shortest path (from x^1 to x^n) is the value of the function $\alpha(n)$. We can find that every path in the graph A has something in common. Now we

choose any path in the graph, we can find that they have the same form as the following :

$$x^1 \to x^2 \to x^{m_3} \to \ldots \to x^{m_i} \to \ldots \to x^{m_n}; \quad i \in \{1,2,\ldots...,n\}$$

It's obvious that we can find these:

$$①x^{m_{i+1}} > x^{m_i}$$

$$②x^{m_{i+1}} = x^{m_i} \times x^{m_j}; \quad j \in \{1,2,3,\ldots...,i\}$$

According to the analysis of the graph above , the program of the shortest road can be described as the following :

$$x^1 \to x^2 \to x^{m_3} \to \ldots \to x^{m_i} \to \ldots \to x^{m_{\alpha(n)}} \to x^n;$$

$$i \in \{1,2,\ldots...,\alpha(n)\}; \quad x^{m_1} = x^1; \quad x^{m_2} = x^2$$

The operations (to get x^n) step by step are presented as follows :

$$f(n) = f(t)f(n-t); t \in \{1,2,\ldots...,n-1\} \Longleftrightarrow f(x+y) = f(x)f(y)$$

In a given path-selection process, the set of available values expands as the number of steps increases, yet the value actually chosen at each step is not fixed. Denote the value taken at the i-th step by w_i. For instance, at the first step only $f(1)$ is available, so $w_1=1$, i.e. $f(1)=f(w_1)$, representing x^1.

Thus, the first operation is $f(w_1)f(1)=f(1+w_1)=f(2)$, which in concrete terms means $x^1 \cdot x^{w_1} = x^{1+w_1} = x^2$. After this operation, the value taken at the second step is denoted by w_2. At the second step, the available choices form the set $\{f(1), f(1+w_1)\}$, i.e. $f(w_2) \in \{f(1), f(1+w_1)\}$ (the specific choice is not predetermined).

The second operation can then be written as $f(w_2)f(1+w_1)=f(1+w_1+w_2)$, which corresponds to $x^{w_2} \cdot x^{1+w_1} = x^{1+w_1+w_2}$. Although we know that $w_1=1$, the value of w_2 varies with the chosen path, so we must express it algebraically.

Similarly, denote the value taken at the third step by w_3 , The available choices are now $\{f(1), f(1+w_1), f(1+w_1+w_2)\}$,i.e. $f(w_3) \in \{f(1), f(1+w_1), f(1+w_1+w_2)\}$ .The third operation is $f(w_3)f(1+w_1+w_2)=f(1+w_1+w_2+w_3)$, meaning $x^{w_3} \cdot x^{1+w_1+w_2} = x^{1+w_1+w_2+w_3}$.

Proceeding in this manner, at the $\alpha(n)$-th step the value taken is denoted by $w_{\alpha(n)}$, and the available set is $\{f(1), f(1+w_1), f(1+w_1+w_2), \cdots, f(1+w_1+w_2+\cdots+w_{\alpha(n)-1})\}$, i.e. $f(w_{\alpha(n)}) \in \{f(1), f(1+w_1), f(1+w_1+w_2), \cdots, f(1+w_1+w_2+\cdots+w_{\alpha(n)-1})\}$. The $\alpha(n)$ -th

operation is then $f(w_{\alpha(n)})f(1+w_1+w_2+\cdots+w_{\alpha(n)-1})=f(1+w_1+w_2+w_3+\cdots+w_{\alpha(n)})$, which in explicit form is $x^{w_{\alpha(n)}}\cdot x^{1+w_1+w_2+\cdots+w_{\alpha(n)-1}}=x^{1+w_1+w_2+w_3+\cdots+w_{\alpha(n)}}$.

In summary, after the $\alpha(n)$-th operation we obtain $x^{1+w_1+w_2+w_3+\cdots+w_{\alpha(n)}}$. Since this equals x^n, we have $n=1+w_1+w_2+w_3+\cdots+w_{\alpha(n)}$. The above procedure is summarised as follows.

So. The shortest path to get x^n can be written down like this :

$$\begin{cases} f(w_1)f(w_1)=f(w_1+w_1) \\ f(w_2)f(w_1+w_1)=f(w_1+w_1+w_2) \\ f(w_3)f(w_1+w_1+w_2)=f(w_1+w_1+w_2+w_3) \\ \vdots \\ f(w_{\alpha(n)-1})f\left(w_1+\sum_1^{\alpha(n)-2}w_i\right)=f\left(w_1+\sum_1^{\alpha(n)-1}w_i\right) \\ f(w_{\alpha(n)})f\left(w_1+\sum_1^{\alpha(n)-1}w_i\right)=f(n) \end{cases}$$

From the above calculation, we can get the following conclusions:

$$n=w_1+\sum_1^{\alpha(n)}w_i\,;\quad w_1=1$$

Also , compare to the formula of the shortest road ,we know

$$\begin{cases} m_1=w_1 \\ m_2=w_1+w_1 \\ \vdots \\ m_{\alpha(n)}=w_1+\sum_1^{\alpha(n)-1}w_i \end{cases}$$

Of course, we can also use the following form to request $g(n)$.

$$f(n)=f(t)f(n-t)$$

If we have identified a way of operations . By this operation, steps to obtain $g(n)$ will be not less than the minimum step . Because there are various operation , one of the operations can be found out and we define it as a sub-operation.

Now , one sub-operation is defined by:

$$g(n)=g(t)[g(n-t)]^{2^t}\Longleftrightarrow g(x+y)=g(x)[g(y)]^{2^x}$$

We marked the function of the steps which are got by the sub-operation above as $\gamma(n)$. So , here is :

$$\beta(n)\leq\gamma(n)$$

Now , we need to prove the following conclusion:

$$\gamma(n)=\alpha(n)+n-1$$

According to the approach which we have used in $f(n)$, we can write $g(n)$ like this :

$$\begin{cases} g(w_1)[g(w_1)]^{2^{w_1}}=g(w_1+w_1) \\ g(w_2)[g(w_1+w_1)]^{2^{w_2}}=g(w_1+w_1+w_2) \\ g(w_3)[g(w_1+w_1+w_2)]^{2^{w_3}}=g(w_1+w_1+w_2+w_3) \\ \vdots \\ g(w_{\alpha(n)-1})\left[g\left(w_1+\sum_1^{\alpha(n)-2} w_i\right)\right]^{2^{w_{\alpha(n)-1}}}=g\left(w_1+\sum_1^{\alpha(n)-1} w_i\right) \\ g(w_{\alpha(n)})\left[g\left(w_1+\sum_1^{\alpha(n)-1} w_i\right)\right]^{2^{w_{\alpha(n)}}}=g(n) \end{cases}$$

From the above calculation, we can get the following conclusions:

$$n=w_1+\sum_1^{\alpha(n)} w_i ; \quad w_1=1; \quad g(w_1)=f(w_1)$$

Also , compare to the formula of the shortest road ,we know:

$$\begin{cases} m_1=w_1 \\ m_2=w_1+w_1 \\ \vdots \\ m_{\alpha(n)}=w_1+\sum_1^{\alpha(n)-1} w_i \end{cases}$$

We can find that if we want to get $g(w_1+w_1)$,we should pay attention to the two parts.

The first part, we should note a few steps to get $[g(w_1)]^{2^{w_1}}$ required.

Part1. $g(w_1)\rightarrow[g(w_1)]^2\rightarrow[[g(w_1)]^2]^2\rightarrow\cdots\rightarrow[g(w_1)]^{2^{w_1}}$,The steps are : $\boldsymbol{w_1}$

Part2. $g(w_1),[g(w_1)]^{2^{w_1}}\rightarrow g(w_1)[g(w_1)]^{2^{w_1}}$,The steps are : **1**

According to the analogy of this process ,we can get this :

$$\gamma(n)=\alpha(n)+\sum_1^{\alpha(n)} w_i$$

And because we have known this reason : $n=w_1+\sum_1^{\alpha(n)} w_i$; $w_1=1$,we can get this conclusion :

$$\gamma(n)=\alpha(n)+\sum_1^{\alpha(n)} w_i =\alpha(n)+n-w_1=\alpha(n)+n-1$$

Because of $\beta(n)\leq\gamma(n)$, we can get this conclusion :

$$\beta(n)\leq\alpha(n)+n-1$$

This is all about the proof of the Scholz-Brauer conjecture.