Finding an Addition Chain using Brauer's k algorithm

August 23, 2023

1 Introduction

This challenge asks us to provide an Addition Chain for a given number. An addition chain is a series of positive integers where each number (except the first) is the sum of two previous numbers in the chain (where these two numbers may be identical). The last number in the series has to be the given target number. The first number in the series is always 1. Addition chains are useful to optimize the runtime of exponentiation: rather than computing a^{15} (naively, this would amount to 15 multiplications; using the square-and-multiply-algorithm), we can get the number of multiplications down to seven. To further decrease the number of required multiplications, we can harness the addition chain $\{1, 2, 3, 6, 12, 15\}$ to compute: $a^2 = a * a$, $a^3 = a^2 * a$, $a^6 = a^3 * a^3$, $a^{12} = a^6 * a^6$, and finally $a^{15} = a^{12} * a^3$, requiring just five multiplications! Obviously, addition chains are only useful if they are sufficiently short (mind you, for our example $n = 15$, $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$ is also an addition chain!). Unfortunately, the problem of finding the *shortest* addition chain for a given number is NP-complete. But luckily, there are algorithms for finding *reasonably* short ones.

In the given challenge, we only have one register, meaning we need a special kind of chain in which each of the sums used to calculate its numbers uses the immediately previous number. Such a chain is called a *Brauer Chain.*

2 Brauer's k-ary algorithm

The challenge was solved using *Brauer's k-ary method.* In my description of how it works, I will rely on this random thesis that was linked in the Wikipedia article.

Brauer's method builds on the more primitive *binary method.* A number is expressed in binary, e.g. $11010_b = 26$. To obtain an addition chain, we process the binary representation from left to right. On the very left, we will encounter our first 1, and we simply add it to our chain. Now, how do we get from the 1_b

we already have to the 11_b including the next bit? We need to multiply by 2 for the bit shift to the left (10_b), and then add another 1 (11_b). From these two operations, we get our next to numbers to add to the chain: 2 and 3. Moving on to the third binary digit, we encounter a zero. To get from 11_b to 110_b, we need to multiply by two, obtaining our next number 6. Up next, another bit equal to 1; to get from 110_b to 1101_b, we need to again multiply by 2 and add 1, so we add 12 and 13 to our list. Lastly, another bit equal to 1, so we multiply by 2 and arrive at our final result 26, or 11010_b. Our complete addition chain then is $\{1, 2, 3, 6, 12, 13, 26\}$. Wha we did was basically adding each intermediate result obtained from the operations required to construct the original number bit by bit, from left to right. Since the binary representation of a number n has $log_2(n)$ bits, and each binary digit will add at most two numbers to our chain, an addition chain for n is of length at most $2 * log_2(n)$.

Brauer's k-ary method generalizes this idea: instead of processing a number in its binary representation, a suitable k is selected, and the number is processed in its base-2^k representation. That is, for each digit in this representation, we process k bits of the number's binary representation, all at once. Which k is most suitable is not immediately obvious, i.e., there is a non-linear relationship between the size of k and the length of our addition chain obtained using Brauer's method. Essentially, there is a trade-off: a larger k may shorten the length of the portion of the chain starting at 2^k, but this portion of the chain has to be preceded by the trivial portion of the chain having the form $\{1, 2, 3, 4, ..., 2^k\}$! More intricacies may follow if I should find the time! In particular, I think I might compute a small example with $k = 2$ and $k = 3$ to demonstrate. Or maybe I'll do a plot visualizing the trade-off between a longer trivial first portion of the chain but shorter second portion of the chain that emerges as k increases.