COUNTING FIXED DEGREE $d \geq 2$ ADDITION CHAINS

THEOPHILUS AGAMA

ABSTRACT. We denote the length of an addition chain with fixed degree $d \geq 2$ leading to n by $l^d(n)$. We study the counting function

$$F_d(m, r) := \#\{n \in [d^m, d^{m+1}) \ : \ l^d(n) \leq m + r\}$$

establishing upper and lower bounds, which generalizes previous classical investigations of De Koninck, Doyon, and Verreault.

1. INTRODUCTION AND PREVIOUS WORKS

Addition chains are a simple, classical combinatorial model that encodes efficient ways to build a given integer by iterated additions. Formally, an *addition chain* for an integer $n \geq 1$ is a strictly increasing sequence

$$1 = a_0 < a_1 < \cdots < a_h = n$$

such that each a_k (for $k \geq 1$) is the sum of one or two previous terms $a_i + a_j$ with $i, j < k$. The minimal possible length r of an addition chain for n is denoted $\ell(n)$ and has been studied since the foundational work of Brauer and the early investigations surrounding the Scholz-Brauer problem (see, e.g., [4],[10], [14], [2]) which attempts to assert a universal truth of the inequality

$$\ell(2^n - 1) \leq n - 1 + \ell(n).$$

Extensive computational approaches have also been used to study optimal (minimal) length addition chains and the Scholz-Brauer problem, and there are a dozen articles treating the minimal length of an addition chain in this manner (see, eg, [17]).

[1]

Beyond intrinsic combinatorial interest, the lengths of an addition chain measure the multiplicative complexity of exponentiation, a quest that frequently arises in algorithmic number theory and cryptography [11],[12],[19].

The basic lower and upper bounds for $\ell(n)$ are elementary: the trivial doubling strategy shows $\ell(n) \leq \lfloor \log_2 n \rfloor + \nu(n) - 1$ (where ($\nu(n)$ is the number of ones in the binary expansion of n), while the binary length $\lfloor \log_2 n \rfloor$ gives the trivial lower bound. A stronger lower bound for $\ell(n)$ also exists in the literature (see, eg, [5]) and due to Schönhage, who proved in 1975

$$\ell(n) \geq \frac{\log n}{\log 2} + \frac{\log(\nu(n))}{\log 2} - 2.13$$

[1]For a concise historical account and additional information, see standard surveys and expository notes.

where $\nu(n)$ denotes the sum of all digits in the binary expansion of n. Over the decades, the literature has refined these estimates, studied extremal examples, and formulated conjectures (most notably the Scholz-Brauer conjecture [8] and many partial results [9] and lower bounds), and developed both constructive algorithms and combinatorial obstructions to short chains; key contributions include the work of Stolarski, Thurber, and others who obtained structural lower bounds and studied arithmetic patterns that force longer chains [6], [16], [21].

On the algorithmic side, the addition chains are a canonical model for exponentiation algorithms. Short chains are known to correspond to multiplication sequences that efficiently compute large powers [15]. This perspective motivated extensive algorithmic and complexity-theoretic work (for example, Pippengers work on exponentiation techniques and later algorithmic studies), and a number of dedicated algorithmic surveys and catalog methods of papers to generate short or near-optimal chains in practice. These algorithmic studies both inspired and benefited from the combinatorial work on chain structure because effective search heuristics depend on structural constraints such as allowed step-types in a chain.

Most past works have concentrated on the classical binary setting in which each step sums at most two earlier terms. Several authors have considered broader models. For example, addition-subtraction chains [18], g-ary chains [13], or more general vector addition chains [20] have shown that changing the allowed local arity can alter both the achievable lengths and the algorithmic landscape. However, a systematic asymptotic study of chains in which each new term is allowed to be the sum of *at most d earlier terms* for a fixed $d \geq 2$ (which we call *degree-d addition chains*) is comparatively undeveloped in the rigorous counting literature. The degree constraint interpolates between the classical binary model ($d = 2$) and the denser local combinatorial regimes (larger d). It is therefore natural to ask how the parameter d affects the minimum length in the worst case and the frequency of unusually short chains that produce integers in dyadic ranges.

Very recently, De Koninck, Doyon, and Verreault obtained sharp quantitative results for the classical $d = 2$ minimal-length counting problem. For the counting function
$$F(m, r) := \#\{n \in [2^m, 2^{m+1}) \ : \ \ell(n) \leq m + r\}$$
they proved matching exponential-type upper and lower bounds in ranges of r growing like $\frac{cm}{\log m}$ for $0 < c < \log 2$, refining long-standing distributional heuristics about how often integers admit chains significantly shorter than the trivial doubling baseline [3]. In particular, they obtained the following upper bound
$$F\left(m, \frac{cm}{\log m}\right) < \exp\left(cm + \frac{\epsilon m \log \log m}{\log m}\right)$$
and the lower bound
$$F\left(m, \frac{cm}{\log m}\right) > \exp\left(cm - \frac{c(1 + \epsilon)m \log \log m}{\log m}\right)$$
for all sufficiently large values of m and for any $\epsilon > 0$. Their arguments combine a careful decomposition of step types, structural inequalities that count step types,

ways to choose step types, as well as ways to choose integers to be added in each step, and a delicate combinatorial counting of admissible local configurations. Their work provides both the motivation and the technical blueprint for the present paper.

In this article, we generalize the De Koninck-Doyon-Verreault approach to the fixed-degree setting. For a fixed integer $d \geq 2$, we define $\ell^d(n)$ to be the minimal length of a degree-d addition chain for n, and we investigate the counting function

$$F_d(m, r) := \#\{n \in [d^m, d^{m+1}) \ : \ l^d(n) \leq m + r\}.$$

where $l^d(n)$ is the length that may or may not be minimal. In the case where we choose a minimal length, we can set $l^d(n) := \ell(n)$. Our main results give general exponential upper and lower bounds for $F_d(m, r)$ for a general r, with constants and sub-exponential correction factors that depend explicitly on d. In particular, we obtain the following results

Theorem 1.1. *Let $d \geq 2$ be a fixed integer and r a positive real number. For any $\epsilon > 0$ and for m sufficiently large*

$$F_d(m, r) \leq \exp\left(G(d) r \log(m + r) + (1 + \epsilon) H(d) r \log \log m + 4 \log(m + r) + O_d(r) \right)$$

where

$$G(d) := \frac{d - 1}{1 - \log_d(d - 1)}$$

and

$$H(d) := \frac{d}{1 - \log_d \gamma_d}.$$

Theorem 1.2. *Let $d \geq 2$ be a fixed integer and r a positive real number. For all m sufficiently large, we have*

$$F_d(m, r) \geq \exp\left(\mathcal{G} \frac{d - 1}{4} (\log m - \log \log r + \log \log d - \log d - c \frac{\log d}{\log r} - \frac{c'}{r}) \right)$$

for some absolute constant $c, c' > 0$ and where

$$\mathcal{G} := \min_{r > 0} \left\{ \frac{r}{d}, \frac{m \log d}{(d - 1) \log r + (d - 1) \log(1 - \frac{1}{d})} \right\}.$$

The proofs require d-ary analogs of the run-gap decompositions and new combinatorial estimates counting admissible sequences of step-classes when each step may be formed by summing up to d earlier terms; these combinatorial counts are more intricate than the binary case because the local arity expands the family of possible step-patterns, yet the same structural control suffices to obtain matching exponential asymptotics in the relevant parameter ranges.

2. Preliminaries and setup

Definition 2.1. Let $n \geq 3$ and $d \geq 2$ be a fixed positive integer. We say that the sequence of positive integers

$$s_0 = 1 < s_1 < \cdots < s_h = n$$

is an addition chain of fixed degree $d \geq 2$ leading to n of length h if for each $1 \leq i \leq h$ the representation

$$s_i = \sum_{\substack{i_j \in [0, i-1] \cap \mathbb{Z} \\ j \in [1, d] \cap \mathbb{N}}} s_{i_j}, \quad (s_{i_j} < s_i)$$

holds.

In other words, each term term in an addition chain with a fixed degree $d \geq 2$ is the sum of at most d previous terms in the chain, with repetition allowed. We call the shortest fixed degree $d \geq 2$ addition chain that leads to a target an *optimal degree d addition chain*. We denote the length of an optimal addition chain with fixed degree $d \geq 2$ leading to a target n with $\ell^d(n)$. We denote the length of the fixed degree chain $(d \geq 2)$ - whether or not it is optimal - by $l^d(n)$. The special case where the fixed degree $d = 2$ recovers the well-known concept of an addition chain first introduced in [2].

Example 2.2. Choose the target $n = 21$ and fix the degree $d = 3$. The sequence

$$s_0 = 1, s_1 = 2, s_2 = 4, s_3 = 8, s_4 = 16, s_5 = 21$$

is an addition chain with fixed degree $d = 3$, because $s_2 = 2s_1, s_3 = 2s_2, s_4 = 2s_3, s_5 = s_4 + s_2 + s_0$. However, it is not of minimal length. An example chain of fixed degree 3 and of minimal length is

$$s_0 = 1, s_1 = 3, s_2 = 9, s_3 = 21.$$

Example 2.3. Choose the target $n = 63$ and fix the degree $d = 4$. The sequence

$$s_0 = 1, s_1 = 2, s_2 = 4, s_3 = 8, s_4 = 16, s_5 = 32, s_6 = 56, s_7 = 63$$

is an addition chain with fixed degree $d = 4$, because $s_2 = 2s_1, s_3 = 2s_2, s_4 = 2s_3, s_5 = 2s_4, s_6 = s_5 + s_4 + s_3, s_7 = s_6 + s_2 + s_1 + s_0$. A chain of fixed degree 4 and of minimal length leading to 63 is given by

$$s_0 = 1, s_1 = 4, s_2 = 16, s_3 = 52, s_4 = 61, s_5 = 63.$$

We now provide definitions that adapt the notions of big steps and small steps for fixed degree d addition chains.

Definition 2.4. Let $d \geq 2$ be fixed, and let

$$s_0 = 1 < s_1 < \cdots < s_h = n$$

be any addition chain with fixed degree d. We define the sets

$$G := \{j \; : \; s_j = d \cdot s_{j-1}, 1 \leq j \leq h\}$$

and

$$K := \{j \; : \; s_j < d \cdot s_{j-1}, 1 \leq j \leq h\}.$$

We call G the *d-dilate steps* and K the *non d-dilate steps*, respectively, in the chain. We denote by $|G|$ and $|K|$ the number of d-dilate and non-d-dilate steps in the addition chain with fixed degree.

Example 2.5. Fix $d = 3$ and choose the target $n = 20$. We construct the addition chain with fixed degree $d = 3$ as follows

$$s_0 = 1, s_1 = 2, s_2 = 6, s_3 = 18, s_4 = 20$$

with $s_1 = 1 + 1, s_2 = 2 + 2 + 2, s_3 = 6 + 6 + 6, s_4 = 18 + 2$. In this case, we have

$$G = \{2, 3\} \quad \text{and} \quad K = \{1, 4\}$$

as the 3-dilate and non 3-dilate steps, respectively.

We set
$$F_d(m, r) := \#\{n \in [d^m, d^{m+1}) \ : \ l^d(n) \leq m + r\}.$$
In other words, the function $F_d(m, r)$ counts the number of integers $n \in [d^m, d^{m+1})$ as targets of a fixed degree $d \geq 2$ addition chains of length satisfying $l^d(n) \leq m + r$.

The function $F_d(m, r)$ is extremely important. It often naturally appears in most investigations that seek to count the number of integers that can be obtained as targets belonging to the interval $[d^m, d^{m+1})$ when constructing an addition chain of length at most $m + r$, because an upper bound for this function automatically serves as an upper bound for the count of those integers [1], [3].

3. Splitting steps into four classes

Let $d \geq 2$ be fixed and
$$s_0 = 1 < s_1 < \cdots < s_{\lfloor m+r \rfloor} = n$$
be a fixed degree $d \geq 2$ addition chain leading to $n \in [d^m, d^{m+1})$. We introduce the following partition into steps of the addition chain of fixed degree $d \geq 2$

- $\mathcal{A}_d := \{j \ : \ s_j = ds_{j-1}\}$ (d-dilate step)

- $\mathcal{B}_d := \{j \ : \ \lambda_d s_{j-1} \leq s_j < ds_{j-1}\}$ (d-large steps)

- $\mathcal{C}_d := \{j \ : \ (d - 1 + \delta)s_{j-1} \leq s_j < \lambda_d s_{j-1}\}$ (d-medium sized steps)

- $\mathcal{D}_d := \{j \ : \ s_j < (d - 1 + \delta)s_{j-1}\}$ (d-small steps)

where
$$\lambda_d = (d - 1) + \frac{1}{\alpha_d}$$
with
$$\alpha_d := \frac{1 + \sqrt{(d-1)^2 + 4}}{2}$$
and
$$\delta := \delta(m) = \frac{1}{\log m}.$$

We call the steps in $\mathcal{A}_d$ as d-dilate steps and those in $\mathcal{B}_d, \mathcal{C}_d, \mathcal{D}_d$ non-d-dilate steps. By denoting the respective cardinality by

$$\#\mathcal{A}_d = A_d, \#\mathcal{B}_d = B_d, \#\mathcal{C}_d = C_d, \#\mathcal{D}_d = D_d$$

we obtain
$$A_d + B_d + C_d + D_d = \lfloor m + r \rfloor.$$

The partition into step framework that has been introduced can be viewed as a generalization of that in [3]. We observe that in the case of the classical addition chain, we take the degree $d = 2$ and deduce the known partition into the step framework

$$\mathcal{A} := \{i \ : \ s_i = 2s_{i-1}\} \quad \text{(doubling steps)}$$

$$\mathcal{B} := \{i \ : \ \gamma s_{i-1} \leq s_i < 2s_{i-1}\} \quad \text{(large steps)}$$

where $\gamma := \frac{1+\sqrt{5}}{2}$ is the *golden* ratio

$$\mathcal{C} := \{i \ : \ (1+\delta)s_{i-1} \leq s_i < \gamma s_{i-1}\} \quad \text{(medium-size steps)}$$

where $\delta := \delta(m) \longrightarrow 0$ as $m \longrightarrow \infty$. In particular

$$\delta := \delta(m) = \frac{1}{\log m}$$

$$\mathcal{D} := \{i \ : \ s_i < (1+\delta)s_{i-1}\} \quad \text{(small steps)}.$$

4. Remark on the sizes of step classes

Lemma 4.1. *Let $d \geq 2$ be fixed and let*

$$s_0 = 1 < s_1 < \cdots < s_{\lfloor m+r \rfloor} = n$$

be a fixed degree $d \geq 2$ addition chain leading to $n \in [d^m, d^{m+1})$. Let G and K denote, as usual, the dilate and non dilate steps in the fixed degree chain. We have

$$n \leq d^{|G|}\gamma_d^{|K|}$$

where

$$\gamma_d := \frac{d - 1 + \sqrt{(d-1)^2 + 4}}{2}.$$

Proof. Suppose that $j \in K$, then $s_j \leq (d-1)s_{j-1} + s_{j-2}$. We set $s_j = xs_{j-1}$ for each $j \in K$. It is clear that $x < d$ for $j \in K$. We deduce

$$x^m d^v \leq (d-1)x^{m-1}d^v + x^{m-2}d^v$$

with $m + v = j$, where m and v are the number of non dilate and dilate steps, respectively, up to step j. We set

$$x^m d^v = (d-1)x^{m-1}d^v + x^{m-2}d^v$$

which is equivalent to the quadratic equation $x^2 - (d-1)x - 1 = 0$. We set

$$\gamma_d := \frac{d - 1 + \sqrt{(d-1)^2 + 4}}{2}$$

which is the positive integer solution for the quadratic equation. We deduce

$$s_j \leq \gamma_d^m d^v$$

with $m + v = j$. We get

$$n \leq d^{|G|} \gamma_d^{|K|}$$

□

We now control the total size of the non dilate steps in an addition chain of fixed degree $d \geq 2$ that leads to $n \in [d^m, d^{m+1})$ with length $l^d(n) \leq \lfloor m + r \rfloor$.

Lemma 4.2. *Let $s_0 = 1 < s_1 < \cdots < s_{\lfloor m+r \rfloor} = n$ be an addition chain of fixed degree $d \geq 2$ leading to $n \in [d^m, d^{m+1})$. Define the sets $\mathcal{A}_d, \mathcal{B}_d, \mathcal{C}_d, \mathcal{D}_d$ as above with their cardinality*

$$\#\mathcal{A}_d = A_d, \#\mathcal{B}_d = B_d, \#\mathcal{C}_d = C_d, \#\mathcal{D}_d = D_d.$$

We have

$$B_d + C_d + D_d \leq \frac{r}{1 - \log_d \gamma_d}.$$

Proof. Write

$$d^m \leq n \leq d^{A_d} \gamma_d^{B_d + C_d + D_d}$$

$$= d^{\lfloor m+r \rfloor} \left(\frac{\gamma_d}{d} \right)^{B_d + C_d + D_d}$$

$$\leq d^{m+r} \left(\frac{\gamma_d}{d} \right)^{B_d + C_d + D_d}$$

which implies that

$$1 \leq d^r \left(\frac{\gamma_d}{d} \right)^{B_d + C_d + D_d}$$

and the observed upper bound follows from this inequality. □

Lemma 4.3. *Let $s_0 = 1 < s_1 < \cdots < s_{\lfloor m+r \rfloor} = n$ be an addition chain of fixed degree $d \geq 2$ leading to $n \in [d^m, d^{m+1})$. Define the sets $\mathcal{A}_d, \mathcal{B}_d, \mathcal{C}_d, \mathcal{D}_d$ as above with their cardinality*

$$\#\mathcal{A}_d = A_d, \#\mathcal{B}_d = B_d, \#\mathcal{C}_d = C_d, \#\mathcal{D}_d = D_d.$$

We have

$$D_d \leq \frac{r - C_d(1 - \log_d \lambda_d)}{1 - \log_d(1 + \delta(d)) - \log_d(d-1)}$$

where $\delta(d) := \frac{\delta}{d-1}$.

Proof. Write

$$d^m \leq n \leq d^{A_d + B_d}(d - 1 + \delta)^{D_d} \lambda_d^{C_d}$$

$$= d^{\lfloor m+r \rfloor} \left(\frac{d-1+\delta}{d} \right)^{D_d} \left(\frac{\lambda_d}{d} \right)^{C_d}$$

$$\leq d^{m+r} \left(\frac{d-1+\delta}{d} \right)^{D_d} \left(\frac{\lambda_d}{d} \right)^{C_d}$$

which implies
$$1 \leq d^r \left(\frac{d-1+\delta}{d} \right)^{D_d} \left(\frac{\lambda_d}{d} \right)^{C_d}.$$

It follows that
$$0 \leq r \log d + D_d(\log(d-1+\delta) - \log d) + C_d(\log \lambda_d - \log d).$$

The upper bound for D_d can be deduced from the above inequality. $\qquad \square$

Remark 4.4. The inequality asserted in Lemma 4.3 suggests that there will always be a tradeoff between the number of d-small steps and d-medium-sized steps among the non dilate steps in an addition chain of fixed degree $d \geq 2$.

5. THE NUMBER OF WAYS TO PUT STEPS INTO THE FOUR CLASSES

In this section, we count the number of ways to put steps in a fixed degree $d \geq 2$ addition chain into the classes of steps $\mathcal{A}_d, \mathcal{B}_d, \mathcal{C}_d, \mathcal{D}_d$ introduced in the step.

Lemma 5.1. *Let $d \geq 2$ be fixed and set*
$$\alpha_d := \frac{1 + \sqrt{(d-1)^2 + 4}}{2}$$

and
$$\lambda_d := d - 1 + \frac{1}{\alpha_d}.$$

We have
$$\lambda_d \geq \alpha_d$$

for all $d \geq 2$. In particular, $\alpha_2 = \lambda_2 = \gamma$.

Proof. For all $d \geq 4$, we deduce
$$\begin{aligned} \alpha_d &= \frac{1 + \sqrt{(d-1)^2 + 4}}{2} \\ &< \frac{1 + \sqrt{2(d-1)^2}}{2} \\ &= \frac{(d-1)\sqrt{2} + 1}{2} \\ &\leq \frac{\sqrt{2}}{2} d < d - 1 < \lambda_d. \end{aligned}$$

The validity of the inequality can be checked for the cases $d = 2$ and $d = 3$. $\qquad \square$

Now, we observe a natural conspiracy between the steps in $\mathcal{B}_d$ and those in $\mathcal{C}_d \cup \mathcal{D}_d$. The observed phenomenon suggests that steps belonging to these classes communicate with each other in their position and pattern of appearance.

Lemma 5.2. *Let $j \in \mathcal{B}_d$, then $j - 1 \in \mathcal{C}_d \cup \mathcal{D}_d$. In particular, every d-large step in a fixed degree $d \geq 2$ addition chain must be preceded by a d-medium-sized step or a d-small step.*

8

Proof. Let $j \in \mathcal{B}_d$, then j is necessarily a non-dilate step. Therefore

$$s_j \leq \overbrace{s_{j-1} + \cdots + s_{j-1}}^{j-1 \text{ times}} + s_{j-2}.$$

Assume to the contrary $j - 1 \in \mathcal{A}_d \cup \mathcal{B}_d$. Then, by definition, we can write $\lambda_d s_{j-2} \leq s_{j-1} \leq d s_{j-2}$ which implies

$$\begin{aligned}
s_j &\leq (d-1)s_{j-1} + \frac{1}{\lambda_d}s_{j-1} \\
&= \left(d - 1 + \frac{1}{\lambda_d}\right)s_{j-1} \\
&\leq \left(d - 1 + \frac{1}{\alpha_d}\right)s_{j-1} = \lambda_d s_{j-1}
\end{aligned}$$

by virtue of the lemma 5.1. This deduction violates the assumption that $j \in \mathcal{B}_d$. $\square$

Let $S(A_d, B_d, C_d, D_d, m, r)$ denote the number of ways of splitting the steps in the fixed degree $d \geq 2$ addition chain of length $\lfloor m + r \rfloor$ into the classes of steps $\mathcal{A}_d, \mathcal{B}_d, \mathcal{C}_d, \mathcal{D}_d$. Standard combinatorial reasoning yields the upper bound

$$S(A_d, B_d, C_d, D_d, m, r) \leq \binom{\lfloor m+r \rfloor}{A_d, B_d, C_d, D_d} \leq \binom{m+r}{A_d, B_d, C_d, D_d} = \frac{(m+r)!}{A_d! B_d! C_d! D_d!}.$$

However, this bound is crude and can be easily improved using intermediate results. We observe that the number of ways to choose steps in $\mathcal{C}_d$ and $\mathcal{D}_d$ is at most

$$\binom{m+r}{C_d + D_d}\binom{C_d + D_d}{C_d} \leq \binom{m+r}{C_d + D_d}2^{C_d + D_r}.$$

By Lemma 5.2, the number of ways to choose steps in $\mathcal{B}_d$ is at most

$$\binom{C_d + D_d}{B_d} \leq 2^{C_d + D_d}.$$

By Lemma 4.3, we obtain the following upper bound

Lemma 5.3. *We have*

$$S(A_d, B_d, C_d, D_d, m, r) \leq \binom{m+r}{C_d + D_d}\exp(O_d(r)).$$

To be able to count a fixed degree $d \geq 2$ addition chain leading to $n \in [d^m, d^{m+1})$, we still need to count the number of ways to choose the integers to be added at each step in each class. Obviously, for dilate steps, there is a unique way to make this choice, because if $j \in \mathcal{A}_d$, then $s_j = d s_{j-1}$. Thus, we have nothing interesting to do for those choices of steps.

6. COUNTING INTEGERS TO BE ADDED AT EACH STEP

Lemma 6.1. *Let $s_0 = 1 < s_1 < \cdots < s_{\lfloor m+r \rfloor} = n$ be an addition chain of fixed degree $d \geq 2$ leading to $n \in [d^m, d^{m+1})$. Assume that the sets $\mathcal{A}_d, \mathcal{B}_d, \mathcal{C}_d, \mathcal{D}_d$ are each fixed. Denote by R_d the number of ways to choose integers to be added in steps that belong to $\mathcal{B}_d$. We have*

$$R_d \leq \exp(O(rd)) = \exp(O_d(r)).$$

Proof. Let $j \in \mathcal{B}_d$ and write

$$s_i = \sum_{\substack{i_j \in [0,i-1] \cap \mathbb{Z} \\ j \in [1,d] \cap \mathbb{N}}} s_{i_j}, \quad (s_{i_j} < s_i).$$

Set

$$s_{j_k} := \max_{\substack{j_i \in [0,j-1] \cap \mathbb{Z} \\ i \in [1,d] \cap \mathbb{Z}}} \{s_{j_i}\}$$

and

$$s_v := \min_{\substack{j_i \in [0,j-1] \cap \mathbb{Z} \\ i \in [1,d] \cap \mathbb{Z}}} \{s_{j_i}\}.$$

Because $j \in \mathcal{B}_d$, we must have $\lambda_d s_{j-1} \le s_j < (d-1)s_{j-1} + s_v$ which implies

(6.1)
$$\frac{1}{\alpha_d} s_{j-1} < s_v.$$

We observe that for each step u with $v < u < j$, we must have $u \in \mathcal{C}_d \cup \mathcal{D}_d$. Suppose that there exists a step u such that $u \notin \mathcal{C}_d \cup \mathcal{D}_d$, then $u \in \mathcal{A}_d \cup \mathcal{B}_d$. By definition, for this particular step u, it must satisfy the inequality $\lambda_d s_{u-1} \le s_u \le d s_{u-1}$. This implies $\lambda_d s_v \le s_u \le s_{j-1}$. We deduce

(6.2)
$$s_v \le \frac{1}{\lambda_d} s_{j-1}.$$

Combining inequality 6.1 and 6.2, we deduce

$$\frac{1}{\alpha_d} s_{j-1} < s_v \le \frac{1}{\lambda_d} s_{j-1}$$

which implies

$$\lambda_d < \alpha_d$$

thus violating the Lemma 5.1. It follows that the number of ways to choose each $j_i \in [0, j-1] \cup \mathbb{Z}$ with $i \in [1, d] \cup \mathbb{Z}$ for each $j \in \mathcal{B}_d$ is at most $(h_d(j))^d$ where

$$h_d(j) := \max_{t \ge 1} \{j - u \in \mathcal{C}_d \cup \mathcal{D}_d \ : \ 1 \le u \le t\}.$$

Equivalently, $h_d(j)$ counts the size of the largest interval $[j-t, j-1]$ such that each positive integer in this interval belongs to $\mathcal{C}_d \cup \mathcal{D}_d$ for each $j \in \mathcal{B}_d$. Now, let R_d denote the number of ways to choose integers to be added in steps that belong to $\mathcal{B}_d$. We deduce

$$R_d \le \prod_{j \in \mathcal{B}_d} (h_d(j))^d.$$

Using the *arithmetic-geometric mean* inequality (AGM), we deduce

$$\left(\prod_{j \in \mathcal{B}_d} (h_d(j))^d \right)^{\frac{1}{d B_d}} \le \frac{1}{B_d} \sum_{j \in \mathcal{B}_d} h_d(j)$$

$$\le \frac{C_d + D_d}{B_d}$$

10

where the latter inequality is a consequence of the lemma 5.2. It follows that

$$R_d \leq \prod_{j \in \mathcal{B}_d} (h_d(j))^d$$

$$\leq \left(\frac{C_d + D_d}{B_d} \right)^{dB_d}$$

$$= \exp(O(dB_d))$$

since the sets $\mathcal{A}_d, \mathcal{B}_d, \mathcal{C}_d, \mathcal{D}_d$ have been fixed. The result follows using the lemma 4.2. $\square$

We now turn our attention to counting the number of ways to choose integers to be added in steps that belong to $\mathcal{C}_d$.

Lemma 6.2. *Let $s_0 = 1 < s_1 < \cdots < s_{\lfloor m+r \rfloor} = n$ be an addition chain of fixed degree $d \geq 2$ leading to $n \in [d^m, d^{m+1})$. Assume that the sets $\mathcal{A}_d, \mathcal{B}_d, \mathcal{C}_d, \mathcal{D}_d$ are each fixed. Let W_d denote the number of ways to choose integers to be added in steps that belong to $\mathcal{C}_d$. We have*

$$W_d \leq (\log m)^{(1+\epsilon)dC_d} \exp(O(rd \log d))$$

for any $\epsilon > 0$.

Proof. Let $j \in \mathcal{C}_d$. By definition

$$\lambda_d s_{j-1} > s_j \geq (d - 1 + \delta)s_{j-1}$$

where $\delta := \delta(m) = \frac{1}{\log m}$. Write

$$s_j = \sum_{\substack{j_i \in [0, j-1] \cap \mathbb{Z} \\ i \in [1,d] \cap \mathbb{N}}} s_{j_i}, \quad (s_{j_i} < s_j).$$

Let $\delta(d) := \frac{\delta}{d-1}$. For each s_{j_i} in the sum, we can write

$$s_{j_i} \geq s_j - (d-1)\frac{(1 + \delta(d))^{-1}}{d - 1}s_j$$

$$= s_j - (1 + \delta(d))^{-1}s_j$$

$$= s_j - (1 - \delta(d) + \delta(d)^2 - \delta(d)^3 + \cdots)$$

$$\geq s_j \delta(d).$$

This implies that each summand s_{j_i} must satisfy the inequality $\delta(d)s_j \leq s_{j_i} \leq s_j$. Now, let

$$u_d(j) := \#\{s_{j_i} \ : \ \delta(d)s_j \leq s_j, \ j \in \mathcal{A}_d \cup \mathcal{B}_d \cup \mathcal{C}_d\}.$$

Taking $\delta(d) > 0$ sufficiently small (equivalently taking m sufficiently large), we have

$$(1 + \delta(d))^{u_d(j)} \leq \frac{1}{\delta(d)}.$$

In this regime

$$u_d(j) \leq -\frac{\log(\delta(d))}{\log(1 + \delta(d))}$$

$$\leq -\frac{\log(\delta(d))}{\delta(d)}$$

11

for each $j \in C_d$. This is the worst number of choices for summands s_{j_i} with $j_i \in \mathcal{A}_d \cup \mathcal{B}_d \cup \mathcal{C}_d$ for each step $j \in \mathcal{C}_d$. Similarly, let

$$\eta_d(j) := \#\{s_{j_i} \ : \ \delta(d)s_j \leq s_{j_i} \leq s_j, \ j_i \in \mathcal{D}_d\}.$$

The number of ways to choose integers to be added in steps $j \in \mathcal{C}_d$ is

$$W_d = \prod_{j=1}^{C_d} \left(u_d(j) + \eta_d(j) \right)^d.$$

Using the *arithmetic-geometric mean* inequality (AGM), we can write

$$
\begin{aligned}
W_d &= \prod_{j=1}^{C_d} \left(u_d(j) + \eta_d(j) \right)^d \\
&\leq \left(\frac{1}{C_d} \sum_{j=1}^{C_d} (u_d(j) + \eta_d(j)) \right)^{dC_d} \\
&\leq \left(-2\frac{\log(\delta(d))}{\delta(d)} + \frac{1}{C_d} \sum_{j=1}^{C_d} \eta_d(j) \right)^{dC_d}.
\end{aligned}
$$

Since $\eta_d(j)$ counts elements of $\mathcal{D}_d$ and each $\eta_d(j) \leq -2\frac{\log(\delta(d))}{\delta(d)}$ for each $j \in C_d$, we deduce

$$\sum_{j=1}^{C_d} \eta_d(j) \leq -2\frac{\log(\delta(d))}{\delta(d)} D_d.$$

Thus

$$
\begin{aligned}
W_d &\leq \left(-2\frac{\log(\delta(d))}{\delta(d)} + \frac{-2D_d}{C_d}\frac{\log(\delta(d))}{\delta(d)} \right)^{dC_d} \\
&= \left(-2\frac{\log(\delta(d))}{\delta(d)} \right)^{dC_d} \left(1 + \frac{D_d}{C_d} \right)^{dC_d}.
\end{aligned}
$$

Because the sets $\mathcal{A}_d, \mathcal{B}_d, \mathcal{C}_d, \mathcal{D}_d$ have been fixed, there exists an absolute fixed constant $\beta > 0$ such that $A_d = \beta B_d$. Hence

$$
\begin{aligned}
W_d &\leq \left(-2\frac{\log(\delta(d))}{\delta(d)} \right)^{dC_d} \left(1 + \frac{1}{\beta} \right)^{dC_d} \\
&= \left(-2\frac{\log(\delta(d))}{\delta(d)} \right)^{dC_d} \exp\left(dC_d \log(1 + \frac{1}{\beta}) \right) \\
&\leq (2(d-1))^{dC_d} (\log m)^{(1+\epsilon)dC_d} \exp(O(rd)) \\
&= (\log m)^{(1+\epsilon)dC_d} \exp(O(rd\log d)).
\end{aligned}
$$

$\square$

Finally, we count the number of ways to choose the integers to be added in steps that belong to $\mathcal{D}_d$.

Lemma 6.3. *Let $s_0 = 1 < s_1 < \cdots < s_{\lfloor m+r \rfloor} = n$ be an addition chain of fixed degree $d \geq 2$ leading to $n \in [d^m, d^{m+1})$. Assume that the sets $\mathcal{A}_d, \mathcal{B}_d, \mathcal{C}_d, \mathcal{D}_d$ are each fixed. Let T_d denote the number of ways to choose integers to be added in steps that belong to $\mathcal{D}_d$. We have*

$$T_d \leq \exp\left((d-1)D_d \log(m+r) + O(D_d) \right).$$

Proof. Let $j \in \mathcal{D}_d$ and write

$$s_j = \sum_{\substack{j_i \in [0, j-1] \cap \mathbb{Z} \\ i \in [1,d] \cap \mathbb{N}}} s_{j_i}, \quad (s_{j_i} < s_j).$$

We observe that each $j \in \mathcal{D}_d$ corresponds to the tuple with summands s_{j_i} as entries such that the sum of all entries gives s_j; therefore, there are at least D_d such tuples. Again, each of the tuples must be chosen from the d-dimension box $\overbrace{\lfloor m+r \rfloor \times \cdots \times \lfloor m+r \rfloor}^{d \text{ fold}}$. Because the sets $\mathcal{A}_d, \mathcal{B}_d, \mathcal{C}_d, \mathcal{D}_d$ are each fixed, there exists a fixed constant $1 > \beta > 0$ such that $D_d = \beta \lfloor m+r \rfloor$. Thus

$$T_d \leq \binom{\lfloor m+r \rfloor^d}{D_d}$$

$$\leq \left(\frac{e(\lfloor m+r \rfloor)^d}{D_d} \right)^{D_d}$$

$$= \exp\left(D_d(1 + d\log(m+r) - \log D_d) \right)$$

$$= \exp\left(dD_d \log(m+r) + D_d - D_d \log D_d \right)$$

$$= \exp\left((d-1)D_d \log(m+r) + O(D_d) \right).$$

$\square$

7. The generalized upper bound

In this section, we assemble the intermediate results obtained in the previous sections to obtain a general upper bound for the number of fixed degree $d \geq 2$ addition chains leading to a target $n \in [d^m, d^{m+1})$ of length $l^d(n) \leq \lfloor m+r \rfloor$. The upper bound we will derive is general in two ways, namely it extends a known upper bound to the case where terms can be generated by adding at most $d \geq 2$ previous terms and that the length of the chain is arbitrary. Consequently, the choice of r may not be limited as in [3], which handles the special case $d = 2$ for the minimum length addition chains. However, we can still specialize our upper bound in the case of a standard addition chain (classical).

Lemma 7.1. *Let $d \geq 2$ be a fixed integer, m be a positive integer, and r a positive real number. Let $N(A_d, B_d, C_d, D_d, m, r)$ denote the number of fixed degree $d \geq 2$ addition chains that lead to $n \in [d^m, d^{m+1})$ for fixed sets $\mathcal{A}_d, \mathcal{B}_d, \mathcal{C}_d, \mathcal{D}_d$. For any $\epsilon > 0$, we have*

$$N(A_d, B_d, C_d, D_d, m, r) \leq \exp\left((d-1)D_d \log(m+r) + (1+\epsilon)dC_d \log m + O_d(r) \right).$$

Proof. Using Lemma 5.3, 6.1, 6.2, 6.3, we deduce

$$N(A_d, B_d, C_d, D_d, m, r) \leq \binom{m+r}{C_d + D_d} \exp(O(rd))$$

$$\times \exp\bigg((d-1)D_d \log(m+r) + (1+\epsilon)dC_d \log\log m + O_d(r) \bigg).$$

The upper bound can be easily deduced from the preceding inequality. $\qquad\square$

Using Lemma 4.2 and Lemma 4.3, we can recast the inequality in Lemma 7.1 in the form

$$N(A_d, B_d, C_d, D_d, m, r) \leq \exp\bigg((d-1)\bigg(\frac{r - C_d(1 - \log_d \lambda_d)}{1 - \log_d(1 + \delta(d)) - \log_d(d-1)} \bigg) \log(m+r)$$

$$+ (1+\epsilon)d\frac{r}{1 - \log_d \gamma_d} \log\log m + O_d(r) \bigg).$$

Using this form of the upper for the number of fixed degree $d \geq 2$ addition chains with fixed sets of step classes, we deduce a generalized upper bound for the number of distinct fixed degree $d \geq 2$ addition chains leading to targets $n \in [d^m, d^{m+1})$ of length $l^d(n) \leq m + r$.

Theorem 7.2. *Let $d \geq 2$ be a fixed integer and r a positive real number. For any $\epsilon > 0$ and for m sufficiently large*

$$F_d(m, r) \leq \exp\bigg(G(d)r\log(m+r) + (1+\epsilon)H(d)r\log\log m + 4\log(m+r) + O_d(r) \bigg)$$

where

$$G(d) := \frac{d-1}{1 - \log_d(d-1)}$$

and

$$H(d) := \frac{d}{1 - \log_d \gamma_d}.$$

Proof. By definition, we have

$$F_d(m, r) := \#\{n \in [d^m, d^{m+1}) \ : \ l^d(n) \leq m + r\}.$$

In other words, the function $F_d(m, r)$ counts the number of integers $n \in [d^m, d^{m+1})$ as targets of a fixed degree $d \geq 2$ addition chains of length satisfying $l^d(n) \leq m + r$. Now, we deduce

$$F_d(m, r) \leq \sum_{A_d, B_d, C_d, D_d \leq \lfloor m+r \rfloor} N(A_d, B_d, C_d, D_d, m, r)$$

$$\leq (m+r)^4 N(A_d, B_d, C_d, D_d, m, r)$$

The claimed upper bound can be obtained by replacing with the upper bound for $N(A_d, B_d, C_d, D_d, m, r)$ in Lemma 7.1. $\qquad\square$

We now turn our attention to establishing a lower bound for the number of distinct integers as targets in the interval $[d^m, d^{m+1})$ of an addition chain of length at most $m + r$. The proof here is constructive and a slightly adapted version in the case of the classical addition chains treated in [3]. The lower bound here again is general in two ways: it accounts for the fixed degree context $d \geq 2$, and the chain length here may or may not be minimal.

Theorem 8.1. *Let $d \geq 2$ be a fixed integer and r a positive real number. For all m sufficiently large, we have*

$$F_d(m, r) \geq \exp\left(\mathcal{G} \frac{d-1}{4} (\log m - \log \log r + \log \log d - \log d - c\frac{\log d}{\log r} - \frac{c'}{r}) \right)$$

for some absolute constant $c, c' > 0$ and where

$$\mathcal{G} := \min_{r > 0} \left\{ \frac{r}{d}, \frac{m \log d}{(d-1) \log r + (d-1) \log(1 - \frac{1}{d})} \right\}.$$

Proof. Let $d \geq 2$ be a fixed integer and choose non-negative integers k and u such that

$$(d-1)ku \leq m$$

and

$$d^u + k(d-1) - (d-1)u \leq r$$

with

$$d^u + k(d-1) = r$$

and choose non-negative integers $s_1, \ldots, s_{(k-1)(d-1)}$ (repetition allowed) such that

$$\sum_{j=1}^{(d-1)(k-1)} s_j + (d-1)ku = m.$$

We now construct a fixed degree $d \geq 2$ addition chain that leads to an integer $n \in [d^m, d^{m+1})$ with a maximum length $m + r$. We will subsequently count the number of ways to do this construction. We start the fixed degree $d \geq 2$ addition chain with

$$a_0 = 1, a_1 = 2, \ldots, a_{d^u-2} = d^u - 1.$$

Next, we choose $(k-1)(d-1) + 1$ integers $V_1, \ldots, V_{(k-1)(d-1)+1}$ from the interval $[d^{u-1}, d^u]$ and continue the fixed degree chain $d \geq 2$ as follows:

$$a_{d^u-1} \qquad\qquad = V_1$$
$$\cdots$$
$$\cdots$$
$$a_{d^u-1+s_1+u} \qquad\qquad = d^{s_1+u} V_1$$
$$a_{d^u+u+s_1} \qquad\qquad = d^{s_1+u} V_1 + V_2$$
$$\cdots$$
$$\cdots$$
$$a_t \quad = d^{\sum_{j=1}^{(k-1)(d-1)} s_j + (k-1)(d-1)u} V_1 + \cdots + V_{(k-1)(d-1)+1}$$

15

where

$$t \leq d^u + \sum_{j=1}^{(k-1)(d-1)} s_j + (d-1)(k-1)u + k(d-1)$$

$$= d^u + k(d-1) - (d-1)u + \sum_{j=1}^{(k-1)(d-1)} s_j + (d-1)ku$$

$$\leq m + r$$

by virtue of the setup. This construction yields a fixed degree addition chain that leads to an integer $n \in [d^m, d^{m+1})$. We note that this construction may not lead to every integer $n \in [d^m, d^{m+1})$. Furthermore, each distinct degree $d \geq 2$ chain constructed in this way leads to a unique integer $n \in [d^m, d^{m+1})$. We deduce

$$F_d(m,r) \geq \left(d^u \left(1 - \frac{1}{d}\right) \right)^{(k-1)(d-1)} \binom{m - (d-1)ku + (d-1)(k-1) - 1}{(d-1)(k-1)}$$

where

$$\left(d^u \left(1 - \frac{1}{d}\right) \right)^{(k-1)(d-1)}$$

is the least number of ways to choose non-negative integers $V_1, \ldots, V_{(k-1)(d-1)+1}$ in the interval $[d^{u-1}, d^u]$ and

$$\binom{m - (d-1)ku + (d-1)(k-1) - 1}{(d-1)(k-1)}$$

is the number of non-negative integer solutions to the Diophantine equation

$$\sum_{j=1}^{(k-1)(d-1)} s_j = m - (d-1)ku.$$

We further deduce

$$F_d(m,r) \geq \left(d^u \left(1 - \frac{1}{d}\right) \right)^{(k-1)(d-1)} \left(\frac{\frac{m}{u}\left(1 - \frac{d}{(d-1)k}\right)}{(d-1)(k-1)} \right)^{(k-1)(d-1)}$$

$$= \left(\frac{d^{u-1}}{k-1} \cdot \frac{m}{u} \left(1 - \frac{d}{(d-1)k}\right) \right)^{(d-1)(k-1)}$$

$$= \exp\left((d-1)(k-1)(\log m - \log u + (u-1)\log d - \log(k-1) \right.$$

$$\left. + \log(1 - \frac{d}{(d-1)k}) \right).$$

We set $E(k) := (k-1)\log m + H(k)$ where

$$H(k) := -(k-1)\log u + (k-1)(u-1)\log d + (k-1)\log\left(1 - \frac{d}{(d-1)k}\right) - (k-1)\log(k-1).$$

To find the value of k maximizing $H(k)$, we set $H'(k) = 0$ and deduce

$$0 = H'(k) = -\log u + (u-1)\log d - \frac{1}{(d-1)k - d} + \frac{1}{k} + \log\left(1 - \frac{d}{(d-1)k}\right) - \log(k-1) - 3.$$

By rearranging the terms, we obtain the transcendental equation

$$\log k = (u-1)\log d - \log u - \frac{1}{(d-1)k-d} + \frac{1}{k} + \log\left(1 - \frac{d}{(d-1)k}\right) - 3$$

Thus, the value of k maximizing $H(k)$ must satisfy

$$e^{\log k} = k \approx e^{(u-1)\log d} \approx e^{\log(r-(d-1)k)}$$

which is equivalent to

$$k \approx r - (d-1)k \implies k \approx \left\lfloor \frac{r}{d} \right\rfloor.$$

Also, from the constraint $(d-1)ku \le m$ and

$$u = \frac{\log(r-(d-1)k)}{\log d}$$

we obtain the feasible bound on k via the inequality

$$(d-1)ku \le (d-1)k\frac{\log(r-(d-1)k)}{\log d} \le m$$

and we obtain

$$k \le \frac{m\log d}{(d-1)\log(r-(d-1)k)} \approx \frac{m\log d}{(d-1)\log r + (d-1)\log(1-\frac{1}{d})}.$$

Now, we choose

$$k_0 := \left\lceil \min\left\{\frac{r}{2d}, \frac{m\log d}{2(d-1)\log r + 2(d-1)\log(1-\frac{1}{d})}\right\}\right\rceil.$$

Thus

$$k_0 - 1 \ge \frac{1}{4}\min\left\{\frac{r}{d}, \frac{m\log d}{(d-1)\log r + (d-1)\log(1-\frac{1}{d})}\right\}.$$

Using this lower bound for $k_0 - 1$, we deduce

$$F_d(m,r) \ge \exp\left(\mathcal{G}\frac{d-1}{4}(\log m - \log\log r + \log\log d - \log d - c\frac{\log d}{\log r} - \frac{c'}{r})\right)$$

for some absolute constant $c, c' > 0$ and where

$$\mathcal{G} := \min_{r>0}\left\{\frac{r}{d}, \frac{m\log d}{(d-1)\log r + (d-1)\log(1-\frac{1}{d})}\right\}.$$

$\square$

We obtain as a consequence the following lower bound for the number of integers $n \in [d^m, d^{m+1})$ obtained by constructing degree $d \ge 2$ addition chains of length $l^d(n) \le (1+c)m$ for a fixed constant c with $0 < c < 1$.

Corollary 8.2. *Let $d \ge 2$ be a fixed integer. Define*

$$F_d(m) := \#\{n \in [d^m, d^{m+1}) \ : \ l^d(n) \le (1+c)m, \ 0 < c < 1\}.$$

For all sufficiently large m, we have

$$F_d(m) \ge \exp\left(\frac{m\log d}{4} - \frac{m(\log\log m)(\log d)}{4\log m} + O(\frac{m}{\log m}\log d)\right).$$

Proof. We take $r := cm$ for a fixed c with $0 < c < 1$ in Theorem 8.1. $\square$

References

1. P. Erdős, *Remarks on number theory III. On addition chains*, Acta Arithmetica, vol. 6, Instytut Matematyczny Polskiej Akademii Nauk, 1960, 77–81.

2. A. Scholz, *253, Jber. Deutsch. Math. Verein. II*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 47, 1937, 41–42.

3. J.M. De Koninck, N. Doyon and W. Verreault *On the minimal length of addition chains*, Functiones et Approximatio Commentarii Mathematici, vol. 1:1, Adam Mickiewicz University, Faculty of Mathematics and Computer Science, 2025, 1–23.

4. A. Brauer, *On addition chains*, Bulletin of the American mathematical Society, vol. 45:10, 1939, 736–739.

5. A. Schönhage, *A lower bound for the length of addition chains*, Theoretical Computer Science, vol. 1:1, Elsevier, 1975, 1–12.

6. E. G. Thurber, *The Scholz–Brauer problem on addition chains*, Pacific Journal of Mathematics, vol. 49:1, Mathematical Sciences Publishers, 1973, 229–242.

7. C. T. Whyburn, *A note on addition chains*, Proceedings of the American Mathematical Society, vol. 16, 1965, 1134.

8. W. R. Utz, *A note on the Scholz–Brauer problem in addition chains*, Proceedings of the American Mathematical Society, vol. 4:3, 1953, 462–463.

9. A. Tall, *The Scholz conjecture is true for infinitely many integers with $\iota(2n) = \iota(n)$*, Integers, vol. 24, 2024, p. 2.

10. W. Hansen, *Zum Scholz-Brauerschen Problem*, Journal f'ur die reine und angewandte Mathematik, vol. 202, Walter de Gruyter, 1959, 129–136.

11. P. Downey, B. Leong, and R. Sethi, *Computing sequences with addition chains*, SIAM Journal on Computing, vol. 10:3, SIAM, 1981, 638–646.

12. C. Negre, T. Plantard, and J. M. Robert, *Efficient modular exponentiation based on multiple multiplications by a common operand*, 2015 IEEE 22nd Symposium on Computer Arithmetic, IEEE, 2015, 144–151.

13. Yara Elias and Pierre McKenzie, *On generalized addition chains*, Integers, vol. 14, 2014, p. 1.

14. AA Gioia, MV. Subbarao, and M. Sugunamma, *The Scholz-Brauer problem in addition chains*, 1962.

15. Yacobi, Yacov, *Exponentiating faster with addition chains*, Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1990, 222–229.

16. E. G Thurber, *On addition chains l (mn)* l (n)-b and lower bounds for c (r)*, Duke Math. J., vol. 40, 1973, 907–913.

17. N.M Clift, *Calculating optimal addition chains*, Computing, vol. 91:3, Springer, 2011, 265–284.

18. H. Volger, *Some results on addition/subtraction chains*, Information Processing Letters, vol. 20:3, Elsevier, 1985, 155–160.

19. F. Morain and J. Olivos, *Speeding up the computations on an elliptic curve using addition-subtraction chains*, RAIRO-Theoretical Informatics and Applications, vol. 24:6, EDP Sciences, 1990, 531–543.

20. P. De Rooij, *Efficient exponentiation using precomputation and vector addition chains*, Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1994, 389–399.

21. K. B. Stolarsky, *A lower bound for the Scholz–Brauer problem*, Canadian Journal of Mathematics, vol. 21, Cambridge University Press, 1969, 675–683.

Departement de mathematiques et de statistique, Universite Laval, Quebec, Canada
E-mail address: thaga1@ulaval.ca/Theophilus@aims.edu.gh/emperordagama@yahoo.com