AIMS Mathematics, 11(6): 16235–16263.
DOI: 10.3934/Math.2026667
Received: 15 March 2026
Revised: 19 May 2026
Accepted: 29 May 2026
Published: 08 June 2026

https://www.aimspress.com/journal/Math

Research article

Addition-multiplication chains with one small step

S. Tarek[1], **Hatem M. Bahig**[2,*] **and M. Anwar**[1]

[1] Department of Mathematics, Faculty of Science, Ain Shams University, Cairo, Egypt

[2] College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia

* **Correspondence:** Email: hmibrahim@imamu.edu.sa.

Abstract: An addition-multiplication chain of length l for a positive integer n is a monotonic increasing sequence $1 = a_0 < a_1 < \ldots < a_l = n$ of positive integers, such that for each $1 \leq i \leq l$, we have $a_i = a_j + a_k$ or $a_i = a_j \times a_k$, where $0 \leq k \leq j \leq i-1$. In this paper, we establish upper bounds for each element in any AM-chain based on the number of squaring steps and the distribution of non-squaring steps preceding the given element. Moreover, we get additional upper bounds independent of the distribution of non-squaring steps. These bounds yield a new upper bound for the number of non-squaring steps in any AM-chain. Finally, we determine all AM-chains that include exactly one small step and, as a consequence, compute the shortest lengths $\ell_{AM}(.)$ of certain integers.

Keywords: addition chains; addition-multiplication chains; shortest length; small step
Mathematics Subject Classification: 11Y55, 68Q25, 68R01

1. Introduction

An addition chain [1–3] of length l for a positive integer n is a monotonic increasing sequence $1 = a_0 < a_1 < \ldots < a_l = n$, such that for each $1 \leq i \leq l$, we have $a_i = a_j + a_k$ for some $k \leq j < i$. The shortest length of an addition chain for n is denoted by $\ell_A(n)$. The concept of an addition chain is closely related to the number of multiplications needed to compute x^n, since exponents are added when multiplying powers with the same base. Numerous studies have explored addition chains as a means of representing the computational difficulty of evaluating integers and polynomials [1, 3, 4].

Various proposals in the literature aim to extend or generalize addition chains in different ways. For example, q-addition chains [5], k-chains [6], and addition sequences (*i.e.,* addition chains for a set of numbers) [3, 7, 8].

One of the generalizations of addition chains is the $\mathbb{B}$-chain introduced by Dobkin and Lipton [9] to investigate the complexities associated with evaluating polynomials and integers. A $\mathbb{B}$-chain of length

l for a positive integer n is a sequence $1 = a_0, a_1, \ldots, a_l = n$, such that for each $1 \leq i \leq l$, we have $a_i = a_j \circ a_k$, where $k \leq j < i$, $\mathbb{B}$ is a finite set of binary operations, and $\circ \in \mathbb{B}$. If $\mathbb{B} \equiv \{+, -\}$, the $\mathbb{B}$-chain is called an addition-subtraction chain [10, 11]. If $\mathbb{B} \equiv \{+, \times\}$, the $\mathbb{B}$-chain is called an addition-multiplication chain (simply an AM-chain) [3, 12, 13].

The study of addition chains is motivated by number-theoretic computations such as exponentiation, where minimizing the number of multiplications optimizes cryptographic algorithms. For example, to compute the exponentiation x^{15}, one may use the shortest addition chain for the exponent $n = 15$, namely $1, 2, 3, 6, 12, 15$. This yields the sequence $x^2, x^3, x^6, x^{12}, x^{15}$, and hence x^{15} can be evaluated using only five multiplications instead of the fourteen multiplications required by the naive method. Computing the exponentiation x^n is one of the most important operations in public-key cryptosystems [2]. However, the problem of computing a shortest addition chain is NP-hard [1]. Therefore, from a practical perspective, since n is very large, considerable attention has been devoted to the fast generation of short, not necessarily shortest, addition chains. More precisely, the focus is often on efficient computation of the exponentiation without directly generating a short addition chain [4]. A similar perspective applies to the generation of shortest AM-chains, although the computational complexity of generating a shortest AM-chain remains an open problem [3, 9].

This paper focuses on theoretical results concerning AM-chains.

Formally, let n be a positive integer. An AM-chain of length l for n is a monotonic increasing sequence $1 = a_0 < a_1 < \ldots < a_l = n$, with the property that for each $1 \leq i \leq l$, we have $a_i = a_j \overset{+}{\times} a_k$, *i.e.,*

$$a_i = a_j + a_k \text{ or } a_i = a_j \times a_k, \text{ where } 0 \leq k \leq j \leq i - 1. \tag{1.1}$$

The shortest length of all AM-chains for n is denoted by $\ell_{AM}(n)$.

Note that

$$\ell_{AM}(n) \leq \ell_A(n),$$

since every addition chain is a valid AM-chain. The use of multiplication allows for strictly shorter chains in many cases.

A step $a_i = a_j + a_k$ or $a_i = a_j \times a_k$, where $0 \leq k \leq j \leq i - 1$, can be classified in two ways:

(1) Based on the indices j and k:

- The ith step $a_i = a_j \times a_k$, $0 \leq k \leq j < i$, is called
  - $\times$-star step (multiplicative star step) if $j = i - 1$,
  - $\times$-doubling step (squaring step) if $j = k = i - 1$,
  - $\times$-nondoubling step (multiplicative non-squaring step) if $k \leq i - 2$.

  Clearly, a multiplicative non-squaring step can include a multiplicative star step.
- The ith step $a_i = a_j + a_k$, $0 \leq k \leq j < i$, is called
  - $+$-star step (additive star step) if $j = i - 1$,
  - $+$-doubling step (doubling step) if $j = k = i - 1$,
  - $+$-nondoubling step (additive non-doubling step) if $k \leq i - 2$.

  Similarly, an additive non-doubling step can include an additive star step.

Each step in an AM-chain can be classified as either a squaring step or a non-squaring step. The non-squaring step is either multiplicative non-squaring, additive non-doubling, or doubling. Therefore, any AM-chain that contains d squaring steps and $p = (l - d)$ non-squaring steps has length

$$l = d + p.$$

(2) Based on the values a_i and a_{i-1}:
Let λ_{AM} be a function defined on the set of positive integers as follows:

$$\lambda_{AM}(1) = 0$$

$$\lambda_{AM}(x) = \lfloor \log_2 \log_2 x \rfloor + 1 \text{ for } x \geq 2, \tag{1.2}$$

If $\lambda_{AM}(a_i) = \lambda_{AM}(a_{i-1}) + 1$, then step i is called a big step; otherwise, $\lambda_{AM}(a_i) = \lambda_{AM}(a_{i-1})$, and it is called a small step.

The length l of an AM-chain can be expressed as:

$$l = \lambda_{AM}(n) + S_{AM}(a_0, a_1, \ldots, a_l),$$

where for $1 \leq i \leq l$, $S_{AM}(a_0, a_1, \ldots, a_i)$, or simply $S_{AM}(a_i)$ indicates how many small steps are present in the chain up to a_i, and $\lambda_{AM}(n)$ indicates how many big steps are present in the chain. Thus, the length of shortest AM-chain for n can be obtained by minimizing $S_{AM}(n)$.

The only AM-chains with no small steps are those of the form

$$1, 2, 2^2, 2^{2^2}, \ldots, 2^{2^A}.$$

In other words, the only integers $n > 1$ satisfying $\ell_{AM}(n) = \lambda_{AM}(n)$ are those of the form $n = 2^{2^A}$, where $A \geq 0$.

Remark 1.1. *(On the definition of λ_{AM} and small steps) The definition of λ_{AM} for $x \geq 2$ is slightly different from that in [12]. In [12], for $x \geq 2$,*

$$\lambda'_{AM}(x) = \lfloor \log_2 \log_2 x \rfloor \tag{1.3}$$

Thus, according to Eq (1.3), the first step is considered small in any AM-chain, while it is considered a big step using Eq (1.2). For example, the chain $1, 2, 4$ has one small step and one big step using Eq (1.3), whereas it has two big steps in the present work, i.e., Eq (1.2).

This normalization (using Eq (1.2)) ensures that $S_{AM}(n) = 0$ precisely for integers of the form $n = 2^{2^A}$, which are maximal for their AM-chain length. In general, $S_{AM}(n)$ measures how far n lies below the largest integer attainable with the same number of big steps. Note that using Eq (1.3) [12], integers of the form $n = 2^{2^A}$ have one small step.

This justification improves the structural parallelism and provides a more natural interpretation of small and big steps while remaining compatible with earlier results; see Table 1. The table shows the similarity between the lengths of the shortest addition chains (A-chains) and the shortest AM-chains based on Eq (1.2). It provides a natural parallel with addition chains and integer complexity, where

the defect similarly quantifies deviation from maximal growth at fixed complexity, yielding a cleaner and more consistent framework.

Table 1. Comparison of the lengths of the shortest A-chains and AM-chains (based on Eqs (1.2) and (1.3)) in the cases of zero and one small step, demonstrating how $\lambda_{AM}(n)$, *i.e.*, Eq (1.2), aligns with $\lambda_A(n)$ for addition chains.

	A-chain [1]	AM-chain and Eq (1.2)	AM-chain and Eq (1.3)
lower bound of the shortest length	$\ell_A(n) \geq \lambda_A(n) = \lfloor \log n \rfloor$	$\ell_{AM}(n) \geq \lambda_{AM}(n)$ using Eq (2.1)	$\ell_{AM}(n) \geq \lambda'_{AM}(n) + 1$ using Eq (2.1)
the length of shortest chains with no small steps	$n = 2^x$, $x \geq 0$ $\ell_A(n) = x = \lambda_A(n)$	$n = 2^{2^x}$, $x \geq 0$ $\ell_{AM}(n) = x + 1 = \lambda_{AM}(2^{2^x})$ using Eq (2.2)	–
the length of shortest chains with one small step	$n = 2^x + 2^y$, $x > y \geq 0$ $\ell_A(n) = x + 1 = \lambda_A(n) + 1$	n as in Theorem 1.2 (new results) $\ell_{AM}(n) = \lambda_{AM}(n) + 1$	$n = ^{2^x}$, $x \geq 0$ $\ell_{AM}(n) = x+1 = \lambda'_{AM}(n)+1$

This paper presents three new contributions on AM-chains.

(1) In Section 3, we establish an upper bound for each element in any AM-chain based on the number of squaring steps and the distribution of non-squaring steps preceding the given element. We also establish an improved bound on the total number of non-squaring steps in any AM-chain. Moreover, we get an additional upper bound independent of the distribution of non-squaring steps. These results improve the bounds obtained by [13].

(2) In Section 5, we determine all AM-chains that include exactly one small step. We also determine all integers whose shortest AM-chains contain one small step.

(3) In Section 6, we compute the shortest length $\ell_{AM}(.)$ of certain numbers, such as $2^{2^A+2^B+2^C}$ and $3^{2^A+2^B}$. These results extend the work of [12, 13].

The following theorem identifies all AM-chains with exactly one small step.

Theorem 1.1. *An AM-chain with one small step has one of the following forms:*

(1) $1, 2, 3, \ldots, 3^{2^\alpha}$, $\alpha \geq 0$,

(2) $1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+1, \ldots,\ \left(2^{2^\alpha}+1\right)^{2^\tau}$, $\alpha \geq 1,\ \tau \geq 0$,

(3) $1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+2^{2^\beta}, \ldots,\ \left(2^{2^\alpha}+2^{2^\beta}\right)^{2^\tau}$, $\alpha > \beta \geq 0,\ \tau \geq 0$,

(4) $1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^\beta}, \ldots,\ 2^{2^{\alpha+\tau}+2^{\beta+\tau}}$, $\alpha > \beta \geq 0,\ \tau \geq 0$,

(5) $1,\ 2,\ 3,\ 4, \ldots,\ 4^{2^\tau}$, $\tau \geq 0$,

(6) $1,\ 2,\ 3,\ 5, \ldots,\ 5^{2^\tau}$, $\tau \geq 0$,

(7) $1,\ 2,\ 3,\ 6, \ldots,\ 6^{2^\tau}$, $\tau \geq 0$,

(8) $1,\ 2,\ 3, \ldots,\ 3^{2^\alpha},\ 3^{2^\alpha+2^{\alpha-1}}, \ldots,\ 3^{2^{\alpha+\tau}+2^{\alpha+\tau-1}} = 27^{2^{\alpha+\tau-1}}$, $\alpha \geq 1,\ \tau \geq 0$,

(9) $1,\ 2,\ 3,\ 9,\ 18,\ldots,\ 18^{2^\tau},\ \tau \geq 0,$

(10) $1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^{\alpha-1}},\ldots,\ 2^{2^{\alpha+\tau}+2^{\alpha+\tau-1}},\ 2^{2^{\alpha+\tau+1}+2^{\alpha+\tau-2}},\ldots,\ 2^{2^{\alpha+\tau+\delta+1}+2^{\alpha+\tau+\delta-2}},$
$\alpha,\ \tau \geq 1,\ \delta \geq 0,$

(11) $1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^{\alpha-1}},\ 2^{2^{\alpha+1}+2^\alpha},\ 2^{2^{\alpha+2}},\ldots,\ 2^{2^{\alpha+\tau+2}},\ \alpha \geq 1,\ \tau \geq 0,$

(12) $1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+1,\ 2^{2^{\alpha+1}}+2^{2^\alpha},\ldots,\ \left(2^{2^{\alpha+1}}+2^{2^\alpha}\right)^{2^\tau},\ \alpha \geq 1,\ \tau \geq 0,$

(13) $1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+1,\ 2^{2^{\alpha+1}},\ldots,\ 2^{2^{\alpha+\tau+1}},\ \alpha \geq 1,\ \tau \geq 0,$

(14) $1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+2^{2^\beta},\ 2^{2^{\alpha+1}}+2^{2^\alpha+2^\beta},\ldots,\ \left(2^{2^{\alpha+1}}+2^{2^\alpha+2^\beta}\right)^{2^\tau},\alpha > \beta \geq 0,\ \tau \geq 0,$

(15) $1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+2^{2^\beta},\ 2^{2^{\alpha+1}},\ldots,\ 2^{2^{\alpha+\tau+1}},\alpha > \beta \geq 0,\ \tau \geq 0,$

(16) $1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^\beta},\ 2^{2^{\alpha+1}+2^\beta},\ldots,\ 2^{2^{\alpha+\tau+1}+2^{\beta+\tau}},\ \alpha > \beta \geq 0,$

(17) $1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^\beta},\ 2^{2^{\alpha+1}},\ldots,\ 2^{2^{\alpha+\tau+1}},\ \alpha > \beta \geq 0,\ \tau \geq 0,$

(18) $1,\ 2,\ 3,\ 6,\ 18,\ldots,\ 18^{2^\tau},\ \tau \geq 0,$

(19) $1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^{\alpha-1}},\ 2^{2^{\alpha+1}+2^{\alpha-1}},\ 2^{2^{\alpha+2}},\ldots,\ 2^{2^{\alpha+\tau+2}},\ \alpha \geq 1,\ \tau \geq 0.$

Theorem 1.1 shows all possible AM-chain forms that contain exactly one small step. By filtering out non-shortest AM-chains and grouping mathematically equivalent forms, we get the following theorem.

Theorem 1.2. *(Integers whose shortest AM-chains contain one small step)*
An integer $n > 1$ satisfies $\ell_{AM}(n) = \lambda_{AM}(n) + 1$ if and only if n is one of the following forms:

(1) $3^{2^\alpha},\ \alpha \geq 0,$

(2) $\left(2^{2^\alpha}+1\right)^{2^\tau},\ \alpha \geq 1,\ \tau \geq 0,$

(3) $\left(2^{2^\alpha}+2^{2^\beta}\right)^{2^\tau},\ \alpha > \beta \geq 0,\ \tau \geq 0,$

(4) $2^{2^\alpha+2^\beta},\ \alpha > \beta \geq 0,$

(5) $27^{2^\alpha},\ \alpha \geq 0,$

(6) $\left(2^{2^{\alpha+1}}+2^{2^\alpha+2^\beta}\right)^{2^\tau},\alpha > \beta \geq 0,\ \tau \geq 0.$

This paper is organized as follows. Section 2 provides the necessary background for this work. In Section 3, we establish a new upper bound for each element in an AM-chain that includes d squaring steps. We also find a new upper bound for the number of non-squaring steps in an AM-chain, which will be utilized to prove Theorem 1.1. In Section 4, we analyze AM-chains that contain d squaring steps. In Section 5, we use the bounds obtained to provide the proof of Theorems 1.1 and 1.2. In Section 6, we utilize Theorem 1.1 to determine the shortest length $\ell_{AM}(.)$ of certain integers. Section 7 includes the conclusion and future work.

2. Preliminaries

This section presents some well-known results that are required in this paper.

Bahig [12] showed the following results regarding $\ell_{AM}(n)$:

$$\ell_{AM}(n) \geq \log_2 \log_2 n + 1, \ n \geq 2. \tag{2.1}$$

$$\ell_{AM}(2^{2^n}) = n + 1, \ n \geq 0. \tag{2.2}$$

$$\ell_{AM}(x^{2^n}) \geq n + \log_2(\lfloor \log_2 x \rfloor) + 2, \ v(x) > 1, \ n \geq 0. \tag{2.3}$$

$$\ell_{AM}(y^{2^n}) = n + q + 2, \quad \text{where } y \text{ has one of the following forms:}$$
$$2^{2^q} + 1, \ 2^{2^q} + 2^{2^t}, \text{ and } 2^{2^q} \times 2^{2^t}, \ n \geq 0, \ 0 \leq t \leq q, \tag{2.4}$$

where $v(x)$ is the number of 1's in the binary representation of x.

In [13], Bahig and Mahran proved that for an AM-chain $a_0, a_1, \ldots, a_l = n$ that includes d squaring steps and s small steps, we have

$$n \leq 2^{2^{l-d} F_{l-d+3}}, \tag{2.5}$$

$$s + 1 \leq l - d \leq 3.271s + 3.271, \tag{2.6}$$

where F_m is the mth Fibonacci number defined by $F_0 = 0$, $F_1 = 1$, and

$$F_{m+2} = F_{m+1} + F_m \text{ for all } m \geq 0.$$

Remark 2.1. *Let* $1, 2, \ldots, a_i = 2^{2^i}, a_{i+1} = 2^{2^{i+1}}$, *be an AM-subchain. The step* $i + 1$ *cannot be big if it is non-squaring.*

3. New upper bounds

In this section, we improve the upper bounds in both Eqs (2.5) and (2.6).

Theorem 3.1. *Let* $1, 2, a_2, \ldots, a_l$ *be an AM-chain of length* l, *with* $a_2 = 4$, *that includes* d *squaring steps and* $p = l - d$ *non-squaring steps. Then,*

$$\log_2(a_l) \leq 2^{d-1} \times F_{p+2}. \tag{3.1}$$

Proof. We prove the theorem by induction on l.

For $l = 2$, we have the chain $1, 2, 4$, with $p = 1$, and $d = 1$. Since $\log_2(4) = 2 \leq 2^0 \times F_3 = 1 \times 2 = 2$, Eq (3.1) holds for $l = 2$.

For $l = 3$, we have four chains:

$$1, 2, 4, 16; \quad 1, 2, 4, 8; \quad 1, 2, 4, 6; \quad \text{and } 1, 2, 4, 5.$$

For the first chain, we have $p = 1$, $d = 2$, and Eq (3.1) holds since $\log_2(a_3) = \log_2(16) = 4 \leq 2^1 \times F_3 = 2 \times 2 = 4$. For the other three chains, we have $p = 2$, $d = 1$, and Eq (3.1) holds since $\log_2(a_3) \leq \log_2(8) = 3 \leq 2^0 \times F_4 = 1 \times 3 = 3$. Thus, Eq (3.1) is true for $l = 3$.

Let Eq (3.1) be true for $l = 3, \ldots, k$. Next, we prove Eq (3.1) at $l = k + 1$.

If step $k+1$ is squaring, then

$$\log_2(a_{k+1}) = 2\log_2(a_k) \le 2\left(2^{d-2} \times F_{p+2}\right) = 2^{d-1} \times F_{p+2}.$$

If the step $k+1$ is non-squaring, then $a_{k+1} \le a_k \times a_{k-1}$. Now, we have two cases: either the step k is squaring or non-squaring.

If it is squaring, then

$$\log_2(a_{k+1}) \le 3\log_2(a_{k-1}) \le 3\left(2^{d-2} \times F_{p+1}\right) = 2^{d-1} \times \frac{3}{2}F_{p+1} \le 2^{d-1} \times F_{p+2},$$

where we used the inequality $\frac{3}{2}F_n \le F_{n+1}$, which holds for all $n \ge 2$ and also for $n = 0$.

If step k is non-squaring, then we apply the inductive hypothesis to both a_k and a_{k-1}:

$$\log_2(a_{k+1}) \le \log_2(a_k) + \log_2(a_{k-1}) \le \left(2^{d-1} \times F_{p+1}\right) + \left(2^{d-1} \times F_p\right) = 2^{d-1} \times F_{p+2}.$$

□

Theorem 3.2. *Let $1, 2, a_2, \ldots, a_l$ be an AM-chain of length l, with $a_2 = 3$, that includes d squaring steps and $p = l - d$ non-squaring steps. Then,*

$$\log_2(a_l) \le 2^d\left(F_{p-1}\log_2(3) + F_{p-2}\right). \tag{3.2}$$

Proof. We prove the theorem by induction on l.

For $l = 2$, we have the chain $1, 2, 3$, with $p = 2$, and $d = 0$. Since $\log_2(a_2) = \log_2(3) \le 2^0\left(F_1\log_2(3) + F_0\right) = \log_2(3)$, Eq (3.2) is true for $l = 2$.

For $l = 3$, we have four chains:

$$1, 2, 3, 9; \quad 1, 2, 3, 6; \quad 1, 2, 3, 5; \quad \text{and } 1, 2, 3, 4.$$

For the first chain, we have $p = 2$, $d = 1$, and Eq (3.2) holds since $\log_2(a_3) = \log_2(9) = 2\log_2(3) \le 2^1\left(F_1\log_2(3) + F_0\right) = 2\log_2(3)$. For the other three chains, we have $p = 3$, $d = 0$, and Eq (3.2) holds since $\log_2(a_3) \le \log_2(6) = \log_2(3) + 1 \le 2^0\left(F_2\log_2(3) + F_1\right) = \log_2(3) + 1$.

Let Eq (3.2) be true for $l = 3, \ldots, k$. Next, we prove it at $l = k+1$. There are two cases:
Case (1) is when the step $k+1$ is squaring. Thus,

$$\log_2(a_{k+1}) = 2\log_2(a_k) \le 2\left(2^{d-1}\left(F_{p-1}\log_2(3) + F_{p-2}\right)\right) = 2^d\left(F_{p-1}\log_2(3) + F_{p-2}\right).$$

Thus, Eq (3.2) holds for $k+1$.
Case (2) is when the step $k+1$ is non-squaring. Thus, $a_{k+1} \le a_k \times a_{k-1}$. We now have two subcases:

Case (2.1) is when the step k is squaring. In this case, we have

$$\begin{aligned}\log_2(a_{k+1}) \le \log_2(a_k) + \log_2(a_{k-1}) = 3\log_2(a_{k-1}) &\le 3\left(2^{d-1}\left(F_{p-2}\log_2(3) + F_{p-3}\right)\right)\\ &= 2^d\left(\frac{3}{2}F_{p-2}\log_2(3) + \frac{3}{2}F_{p-3}\right)\\ &\le 2^d\left(F_{p-1}\log_2(3) + F_{p-2}\right), \quad p \ge 5,\end{aligned}$$

where we used the inequality $\frac{3}{2}F_n \leq F_{n+1}$, which holds for all $n \geq 2$ and also for $n = 0$. We now show that the above inequality also holds for the remaining values of p, *i.e.,* $p = 3$, and 4.

If $p = 3$, we have

$$\frac{3}{2}F_1 \log_2(3) + \frac{3}{2}F_0 \leq F_2 \log_2(3) + F_1 \iff \frac{3}{2}\log_2(3) \leq \log_2(3) + 1 \iff \frac{1}{2}\log_2(3) \leq 1,$$

which holds since $\log_2(3) \leq 2$ (equivalent to $3 \leq 4$).

If $p = 4$, we have

$$\frac{3}{2}F_2 \log_2(3) + \frac{3}{2}F_1 \leq F_3 \log_2(3) + F_2 \iff \frac{3}{2}\log_2(3) + \frac{3}{2} \leq 2\log_2(3) + 1 \iff \frac{1}{2} \leq \frac{1}{2}\log_2(3),$$

which holds since $1 \leq \log_2(3)$ (equivalent to $2 \leq 3$).

Thus, for Case (2.1), Eq (3.2) holds for $k + 1$.

Case (2.2) is when the step k is non-squaring. In this case, Eq (3.2) is true for $k + 1$ since

$$\begin{aligned}
\log_2(a_{k+1}) &\leq \log_2(a_k) + \log_2(a_{k-1}) \\
&\leq 2^d \left(F_{p-2}\log_2(3) + F_{p-3}\right) + 2^d \left(F_{p-3}\log_2(3) + F_{p-4}\right) \\
&= 2^d \left((F_{p-2} + F_{p-3})\log_2(3) + (F_{p-3} + F_{p-4})\right) \\
&= 2^d \left(F_{p-1}\log_2(3) + F_{p-2}\right).
\end{aligned}$$

Thus, Eq (3.2) is true for $k + 1$. □

The next corollary finds upper bounds for the number of small steps and non-squaring steps in an AM-chain by applying Theorems 3.1 and 3.2.

Corollary 3.1. *Let* $1, 2, a_2, \ldots, a_l = n$ *be an AM-chain of length l, which includes d squaring steps,* $p = l - d$ *non-squaring steps, and s small steps.*

If $a_2 = 4$, *then*

$$s + 1 \leq p \leq 3.271s + 1.$$

Otherwise (i.e., $a_2 = 3$*),*

$$s + 1 \leq p \leq 3.271s + 1.1855.$$

Proof. Since the first step is big and non-squaring, and all subsequent squaring steps are big, we have

$$s + 1 \leq p.$$

If $a_2 = 4$, we have $\log_2(a_l) \leq 2^{d-1} \times F_{p+2}$. Therefore,

$$2^{\lambda_{AM}(n)-1} \leq \log_2(a_l) \leq 2^{d-1} \times F_{p+2},$$

where we used the fact that $2^{2^{\lambda_{AM}(n)-1}} \leq a_l$.

Using the fact that $F_m \leq 2\varphi^{m-3}$, which holds for all $m \geq 2$ and also for $m = 0$, where $\varphi = \frac{1+\sqrt{5}}{2}$, and $l = d + p = \lambda_{AM}(n) + s$, we get

$$2^{\lambda_{AM}(n)-1} \leq \left(2^{\lambda_{AM}(n)+s-p-1}\right)\left(2\varphi^{p-1}\right).$$

Dividing by $2^{\lambda_{AM}(n)-1}$, we get

$$1 \leq 2^{s+1} \times \left(\frac{\varphi}{2}\right)^{p} \times \varphi^{-1}.$$

Taking $\log_2$, we get

$$0 \leq s + 1 + p \log_2\left(\frac{\varphi}{2}\right) - \log_2(\varphi).$$

Consequently,

$$p \leq \frac{s}{\log_2\left(\frac{2}{\varphi}\right)} + \frac{1 - \log_2(\varphi)}{\log_2\left(\frac{2}{\varphi}\right)}.$$

Thus,

$$p \leq 3.271s + 1.$$

In the case of $a_2 = 3$, we have $\log_2(a_l) \leq 2^d \left(F_{p-1} \log_2(3) + F_{p-2}\right)$. Therefore,

$$2^{\lambda_{AM}(n)-1} \leq \log_2(a_l) \leq 2^d \left(F_{p-1} \log_2(3) + F_{p-2}\right).$$

Assume for now that $p \geq 4$; we will handle the remaining cases afterward.

Using the fact that $F_m \leq 2\varphi^{m-3}$, which holds for all $m \geq 2$ and also for $m = 0$, and $l = d + p = \lambda_{AM}(n) + s$, we get

$$2^{\lambda_{AM}(n)-1} \leq 2^{\lambda_{AM}(n)+s-p+1} \left(\varphi^{p-4} \log_2(3) + \varphi^{p-5}\right) \quad p \geq 4.$$

Dividing by $2^{\lambda_{AM}(n)-1}$, we get

$$1 \leq 2^{s+2} \times \left(\frac{\varphi}{2}\right)^{p} \left(\varphi^{-4} \log_2(3) + \varphi^{-5}\right), \quad p \geq 4.$$

Taking $\log_2$, we get

$$0 \leq s + 2 + p \times \log_2\left(\frac{\varphi}{2}\right) + \log_2\left(\varphi^{-4} \log_2(3) + \varphi^{-5}\right), \quad p \geq 4.$$

Thus,

$$p \leq \frac{s}{\log_2\left(\frac{2}{\varphi}\right)} + \frac{\log_2\left(\varphi^{-4} \log_2(3) + \varphi^{-5}\right) + 2}{\log_2\left(\frac{2}{\varphi}\right)}, \quad p \geq 4.$$

Hence,

$$p \leq 3.271s + 1.1855, \quad p \geq 4. \tag{3.3}$$

Now we consider the case $1 \leq p \leq 3$. Note that $s = 0$ if and only if $p = 1$, and since the AM-chain starts with $1, 2, 3$, we get $p \geq 2$; hence, $s \geq 1$. For $(p, s) = (2, 1)$ and $(3, 1)$, Eq (3.3) holds, so it remains valid for all $p \geq 2$ and can be written as

$$p \leq 3.271s + 1.1855, \quad p \geq 2. \tag{3.4}$$

□

Note that whether $a_2 = 4$ or 3, Eq (3.4) holds for any AM-chain.

4. AM-chains with d squaring steps

The purpose of this section is to investigate AM-chains containing d squaring steps and to determine upper bounds for their elements. Theorems 3.1 and 3.2 give upper bounds based only on the number of squaring steps. We now prove two stronger results, Theorems 4.1 and 4.2, which demonstrate that both the number of squaring steps and the distribution of non-squaring steps preceding a given element in an AM-chain play a key role in determining its maximum value.

In this section, we use D to denote a block of consecutive squaring steps, and $\overline{D}$ to denote a block of consecutive non-squaring steps. The notations $|D|$ and $\left|\overline{D}\right|$ refer to the number of steps in each block. We use D_i, to denote the i^{th} squaring block, and similarly $\overline{D}_i$ to denote the i^{th} non-squaring block.

In any AM-chain $1, 2, a_2, a_3, \ldots, a_l$, the sub-AM-chain $a_2, a_3, \ldots, a_l$ can be divided into a combination of D and $\overline{D}$ blocks.

Since we seek to find the maximum value for an element in an AM-chain after a_2, we can maximize the outcome of a non-squaring step by multiplying the current element, say a_i, by the previous one, a_{i-1}; *i.e.,* $a_{i+1} = a_i \times a_{i-1}$ ($\times$-star step). If there is a block of consecutive steps of $\times$-stars, we denote this block by T.

We note that the addition operation does not need not to be considered when finding the maximum value for an element, since a +-doubling step $a_{i+1} = a_i + a_i,\ i \geq 1$, can be considered as a multiplicative non-squaring step since $a_{i+1} = a_i + a_i = a_i \times a_1,\ i \geq 1$.

By replacing each non-squaring step with an $\times$-star step, each $\overline{D}$ block can be replaced by a T block. In this case, we have $\left|\overline{D}\right| = |T|$.

Theorem 4.1. *Let $1, 2, a_2, \ldots, a_l$ be an AM-chain of length l, with $a_2 = 4$, that includes d squaring steps and $l - d$ non-squaring steps. Assume that the $l - d - 1$ non-squaring steps following a_2 are partitioned into r blocks $\overline{D}_1, \ldots, \overline{D}_r$, such that between any two $\overline{D}$ blocks, there is a D block. Then,*

$$a_l \leq 2^{2^{d-r} \times \prod_{i=1}^{r} F_{\left|\overline{D}_i\right|+3}}, \tag{4.1}$$

where $\sum_{i=1}^{r} \left|\overline{D}_i\right| = l - d - 1$, and F_i is the ith Fibonacci number.

Proof. To find an upper bound of a_l, we replace each $\overline{D}$ block by a T block, since for $i \geq 2$ a non-squaring step $a_i = a_j + a_k$ or $a_j \times a_k \leq a_{i-1} \times a_{i-2}$, where $1 \leq k \leq i-2$, $1 \leq j \leq i-1$. Thus, we have four possible arrangements (cases) for T, and D.
Case (1):

$$1, 2, 4, T_1, D_1, T_2, \ldots, D_{r-1}, T_r.$$

The first block T_1 has the form

$$2^{F_4}, 2^{F_5}, \ldots, 2^{F_{|T_1|+3}}.$$

The second block D_1 has the form

$$2^{2\times F_{|T_1|+3}}, 2^{2^2\times F_{|T_1|+3}}, \ldots, 2^{2^{|D_1|}\times F_{|T_1|+3}}.$$

The third block T_2 has the form

$$2^{2^{|D_1|-1}\times F_{|T_1|+3}\times F_4}, 2^{2^{|D_1|-1}\times F_{|T_1|+3}\times F_5}, \ldots, 2^{2^{|D_1|-1}\times F_{|T_1|+3}\times F_{|T_2|+3}}.$$

Following this process, we finally obtain the block T_r:

$$\begin{aligned} &2^{2^{\left(\sum_{i=1}^{r-1}|D_i|\right)-(r-1)}\times\left(\prod_{i=1}^{r-1}F_{|T_i|+3}\right)\times F_4},\ 2^{2^{\left(\sum_{i=1}^{r-1}|D_i|\right)-(r-1)}\times\left(\prod_{i=1}^{r-1}F_{|T_i|+3}\right)\times F_5},\ldots,\\ &2^{2^{\left(\sum_{i=1}^{r-1}|D_i|\right)-(r-1)}\times\left(\prod_{i=1}^{r-1}F_{|T_i|+3}\right)\times F_{|T_r|+3}}=2^{2^{d-r}\times\prod_{i=1}^{r}F_{|T_i|+3}}, \end{aligned} \tag{4.2}$$

where $\sum_{i=1}^{r-1}|D_i| = d-1$. Thus,

$$a_l \le 2^{2^{d-r}\times\prod_{i=1}^{r}F_{\left|\overline{D}_i\right|+3}}.$$

Case (2):

$$1, 2, 4, T_1, D_1, T_2, \ldots, D_{r-1}, T_r, D_r.$$

Using Eq (4.2), the last block D_r is

$$\begin{aligned} &2^{2^{\left(\sum_{i=1}^{r-1}|D_i|\right)-(r-1)+1}\times\left(\prod_{i=1}^{r}F_{|T_i|+3}\right)},\ 2^{2^{\left(\sum_{i=1}^{r-1}|D_i|\right)-(r-1)+2}\times\left(\prod_{i=1}^{r}F_{|T_i|+3}\right)},\ldots,\\ &2^{2^{\left(\sum_{i=1}^{r-1}|D_i|\right)-(r-1)+|D_r|}\times\left(\prod_{i=1}^{r}F_{|T_i|+3}\right)}=2^{2^{d-r}\times\prod_{i=1}^{r}F_{|T_i|+3}}, \end{aligned}$$

where $\sum_{i=1}^{r}|D_i| = d-1$. Thus,

$$a_l \le 2^{2^{d-r}\times\prod_{i=1}^{r}F_{\left|\overline{D}_i\right|+3}}.$$

Case (3):

$$1, 2, 4, D_1, T_1, D_2, \ldots, D_r, T_r.$$

The first block D_1 has the form

$$2^{2^2}, 2^{2^3}, \ldots, 2^{2^{|D_1|+1}}.$$

The second block T_1 has the form

$$2^{2^{|D_1|}\times F_4}, 2^{2^{|D_1|}\times F_5}, \ldots, 2^{2^{|D_1|}\times F_{|T_1|+3}}.$$

The third block D_2 has the form

$$2^{2^{|D_1|+1}\times F_{|T_1|+3}}, 2^{2^{|D_1|+2}\times F_{|T_1|+3}}, \ldots, 2^{2^{|D_1|+|D_2|}\times F_{|T_1|+3}}.$$

The fourth block T_2 has the form

$$2^{2^{|D_1|+|D_2|-1}\times F_{|T_1|+3}\times F_4}, 2^{2^{|D_1|+|D_2|-1}\times F_{|T_1|+3}\times F_5}, \ldots, 2^{2^{|D_1|+|D_2|-1}\times F_{|T_1|+3}\times F_{|T_2|+3}}.$$

Continuing in this pattern, we get the block T_r:

$$2^{2^{\left(\sum_{i=1}^{r}|D_i|\right)-(r-1)}\times\left(\prod_{i=1}^{r-1}F_{|T_i|+3}\right)\times F_4}, 2^{2^{\left(\sum_{i=1}^{r}|D_i|\right)-(r-1)}\times\left(\prod_{i=1}^{r-1}F_{|T_i|+3}\right)\times F_5},\ldots,$$

$$2^{2^{\left(\sum_{i=1}^{r}|D_i|\right)-(r-1)}\times\left(\prod_{i=1}^{r-1}F_{|T_i|+3}\right)\times F_{|T_r|+3}}=2^{2^{d-r}\times\prod_{i=1}^{r}F_{|T_i|+3}},$$

where $\sum_{i=1}^{r}|D_i|=d-1$. Thus,

$$a_l\le 2^{2^{d-r}\times\prod_{i=1}^{r}F_{|\overline{D}_i|+3}}.$$

Case (4):

$$1,2,4,D_1,T_1,D_2,\ldots,D_r,T_r,D_{r+1}.$$

Case (4) has the same result as Case (3), using the same argument used to prove Case (2) from Case (1). Thus, $a_l\le 2^{2^{d-r}\times\prod_{i=1}^{r}F_{|\overline{D}_i|+3}}$ in all cases. □

Remark 4.1. *(Addition-chain analogue of Theorem 4.1) The addition-chain version of Theorem 4.1 holds as well. Let* $1,2,a_2,\ldots,a_l$ *be an addition chain of length l that includes d doubling steps and* $l-d$ *non-doubling steps. Assume that the* $l-d$ *non-doubling steps are partitioned into r blocks* $\overline{D}_1,\ldots,\overline{D}_r$*, such that between each two* $\overline{D}$ *blocks there is a D block. Then,*

$$a_l\le 2^{d-r}\prod_{i=1}^{r}F_{|\overline{D}_i|+3},$$

where $\sum_{i=1}^{r}|\overline{D}_i|=l-d$*, and* F_i *denotes the ith Fibonacci number.*

Theorem 4.2. *Let* $1,2,a_2,\ldots,a_l$ *be an AM-chain of length l, with* $a_2=3$*, that includes d squaring steps and* $l-d$ *non-squaring steps. Assume that the* $l-d-2$ *non-squaring steps following* a_2 *are partitioned into r blocks* $\overline{D}_1,\ldots,\overline{D}_r$*, such that between each two* $\overline{D}$ *blocks there is a D block. If* $a_3=3^2$*, then*

$$a_l\le 3^{2^{d-(r-1)}\times\prod_{i=1}^{r}F_{|\overline{D}_i|+3}}.$$

Otherwise (i.e., $a_3\ne 3^2$*),*

$$a_l\le 3^{2^{d-(r-1)}\times F_{|\overline{D}_1|+1}\times\prod_{i=2}^{r}F_{|\overline{D}_i|+3}}\times 2^{2^{d-(r-1)}\times F_{|\overline{D}_1|}\times\prod_{i=2}^{r}F_{|\overline{D}_i|+3}},\tag{4.3}$$

where $\sum_{i=1}^{r}\left|\overline{D}_i\right|=l-d-2$.

Proof. If $a_3=3^2$, then the proof is similar to the proof of Theorem 4.1 by replacing the base 2 with 3. Thus, $a_l\le 3^{2^{d-(r-1)}\times\prod_{i=1}^{r}F_{|\overline{D}_i|+3}}$.

Otherwise, $a_3\ne 3^2$. By replacing each $\overline{D}$ block by a T block, we have two possible arrangements (cases) for T and D:

Case (1):

$$1,2,3,T_1,D_1,T_2,\ldots,D_{r-1},T_r.$$

The first block T_1 has the form

$$3^{F_2}\times 2^{F_1},3^{F_3}\times 2^{F_2},\ldots,3^{F_{|T_1|+1}}\times 2^{F_{|T_1|}}.$$

The second block D_1 has the form

$$3^{2\times F_{|T_1|+1}}\times 2^{2\times F_{|T_1|}}, 3^{2^2\times F_{|T_1|+1}}\times 2^{2^2\times F_{|T_1|}}, \ldots, 3^{2^{|D_1|}\times F_{|T_1|+1}}\times 2^{2^{|D_1|}\times F_{|T_1|}}.$$

The third block T_2 has the form

$$3^{2^{|D_1|-1}\times F_{|T_1|+1}\times F_4}\times 2^{2^{|D_1|-1}\times F_{|T_1|}\times F_4}, 3^{2^{|D_1|-1}\times F_{|T_1|+1}\times F_5}\times 2^{2^{|D_1|-1}\times F_{|T_1|}\times F_5}, \ldots,$$
$$3^{2^{|D_1|-1}\times F_{|T_1|+1}\times F_{|T_2|+3}}\times 2^{2^{|D_1|-1}\times F_{|T_1|}\times F_{|T_2|+3}}.$$

If we follow this process, finally, we will obtain the block T_r:

$$3^{2^{\left(\sum_{i=1}^{r-1}|D_i|\right)-(r-1)}\times F_{|T_1|+1}\times\left(\prod_{i=2}^{r-1}F_{|T_i|+3}\right)\times F_4}\times 2^{2^{\left(\sum_{i=1}^{r-1}|D_i|\right)-(r-1)}\times F_{|T_1|}\times\left(\prod_{i=2}^{r-1}F_{|T_i|+3}\right)\times F_4},$$
$$3^{2^{\left(\sum_{i=1}^{r-1}|D_i|\right)-(r-1)}\times F_{|T_1|+1}\times\left(\prod_{i=2}^{r-1}F_{|T_i|+3}\right)\times F_5}\times 2^{2^{\left(\sum_{i=1}^{r-1}|D_i|\right)-(r-1)}\times F_{|T_1|}\times\left(\prod_{i=2}^{r-1}F_{|T_i|+3}\right)\times F_5}, \ldots,$$
$$3^{2^{\left(\sum_{i=1}^{r-1}|D_i|\right)-(r-1)}\times F_{|T_1|+1}\times\left(\prod_{i=2}^{r}F_{|T_i|+3}\right)}\times 2^{2^{\left(\sum_{i=1}^{r-1}|D_i|\right)-(r-1)}\times F_{|T_1|}\times\left(\prod_{i=2}^{r}F_{|T_i|+3}\right)}.$$

where $\sum_{i=1}^{r-1}|D_i| = d$. Thus,

$$a_l \le 3^{2^{d-(r-1)}\times F_{|\overline{D}_1|+1}\times\prod_{i=2}^{r}F_{|\overline{D}_i|+3}}\times 2^{2^{d-(r-1)}\times F_{|\overline{D}_1|}\times\prod_{i=2}^{r}F_{|\overline{D}_i|+3}}.$$

Case (2):

$$1, 2, 3, T_1, D_1, T_2, \ldots, D_{r-1}, T_r, D_r.$$

This implies the same result as in Case (1). □

Remark 4.2. *Note that setting $r = 1$ in Theorems 4.1 and 4.2 recovers Theorems 3.1 and 3.2, respectively, exactly. This shows that the earlier bounds represent the maximal growth scenario, which occurs when all non-squaring steps are contiguous.*

5. Proofs of Theorems 1.1 and 1.2

5.1. Proof of Theorem 1.1

Using Corollary 3.1 and setting the number of small steps $s = 1$, we obtain the possible total number of non-squaring steps $p \in \{2, 3, 4\}$. By studying all possible AM-chains with p non-squaring steps, we derive the nineteen AM-chain forms. Table 2 shows the structural constraints for each case.

Table 2. Classification of valid numerical pathways by p.

p	Structural Constraints & Examples
2	For $p = 2$, the two non-squaring steps are entirely accounted for by the initial step and a small step S. In this case, the small step may occur immediately after $1, 2$, hence $S = 3$, or it may occur after a squaring block, consequently $S \in \{2^{2^\alpha} + 1, 2^{2^\alpha} + 2^{2^\beta}, 2^{2^\alpha+2^\beta}\}$, where $\alpha > \beta \geq 0$, resulting in Cases I through IV of Theorem 1.1. Examples: $1, 2, 3, 9, 81$; and $1, 2, 4, 16, 64$.
3	For $p = 3$, exactly one big non-squaring step B must be introduced after the chain $1, 2$ and a small step S. We show that if $S = 3$, then either $B \in \{4, 5, 6\}$, yielding Cases V, VI, and VII, respectively; or $B \in \{3^{2^\alpha+2^{\alpha-1}}, 18\}$ after a squaring block, yielding Cases VIII and IX, respectively. Alternatively, if S follows an initial squaring block, then either $B \in \{2^{2^{\alpha+1}} + 2^{2^\alpha}, 2^{2^{\alpha+1}}, 2^{2^{\alpha+1}} + 2^{2^\alpha+2^\beta}, 2^{2^{\alpha+1}+2^\beta}\}$, yielding Cases XII, XIII, XIV, XV, XVI, and XVII, respectively; or $B \in \{2^{2^{\alpha+\tau+1}+2^{\alpha+\tau-2}}, 2^{2^{\alpha+2}}\}$ after an intermediate squaring block, yielding Cases X and XI, respectively. Examples: $1, 2, 3, 5, 25$; $1, 2, 3, 9, 27, 729$; $1, 2, 4, 16, 17, 256$; and $1, 2, 4, 16, 64, 4096, 65536$.
4	For $p = 4$, two big non-squaring steps (B_1 and B_2) are required after the chain $1, 2$ and a small step S. We show that we have two valid chains. The first one is when $S = 3$, $B_1 = 6$, and $B_2 = 18$, resulting in Case XVIII, and the other is when $S = 2^{2^\alpha+2^{\alpha-1}}$, $B_1 = 2^{2^{\alpha+1}+2^{\alpha-1}}$, and $B_2 = 2^{2^{\alpha+2}}$, resulting in Case XIX. Examples: $1, 2, 3, 6, 18$; and $1, 2, 4, 8, 32, 256$.

We now prove the theorem.

Let p denote the number of non-squaring steps. By substituting $s = 1$ into Eq (3.4), we get $p = 2, 3, 4$. Thus, we have three main cases based on p.

Case (1): $p = 2$.

Since every small step is a non-squaring step, the two non-squaring steps are:

- the first step, occurring at $i = 1$, and
- the small step S, which occurs after a step with $i > 1$.

There are two subcases:

Case (1.1):

$$1, 2, S, \ldots .$$

The only choice for S is 3; hence, we get the AM-chain

$$1, 2, 3, \ldots, 3^{2^\alpha}, \ \alpha \geq 0. \tag{5.1}$$

Eq (5.1) corresponds to the Case (I) in Theorem 1.1.

Case (1.2):

$$1, 2, \ldots, 2^{2^\alpha}, S, \ldots .$$

The only choices for S are

$$2^{2^\alpha}+1,\ 2^{2^\alpha}+2^{2^\beta},\ \text{and}\ 2^{2^{\alpha+2^\beta}},\ \text{where}\ \alpha>\beta\geq 0.$$

Therefore, we have the following chains for Case (1.2) (with one small step):

$$1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+1,\ldots,\ \left(2^{2^\alpha}+1\right)^{2^\tau},\ \alpha\geq 1,\ \tau\geq 0, \tag{5.2}$$

$$1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+2^{2^\beta},\ldots,\ \left(2^{2^\alpha}+2^{2^\beta}\right)^{2^\tau},\ \alpha>\beta\geq 0,\ \tau\geq 0, \tag{5.3}$$

and

$$1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^{\alpha+2^\beta}},\ldots,\ 2^{2^{\alpha+\tau}+2^{\beta+\tau}},\ \alpha>\beta\geq 0,\ \tau\geq 0. \tag{5.4}$$

Eqs (5.2, 5.3, 5.4) correspond to the Cases (II, III, IV) in Theorem 1.1.

Case (2): $p=3$.

Since every small step is a non-squaring step, the three non-squaring steps are:

- the first step, occurring at $i=1$,
- the small step S, and
- the remaining non-squaring step B, which must be big.

Figure 1 shows all possible AM-chains when $p=3$.

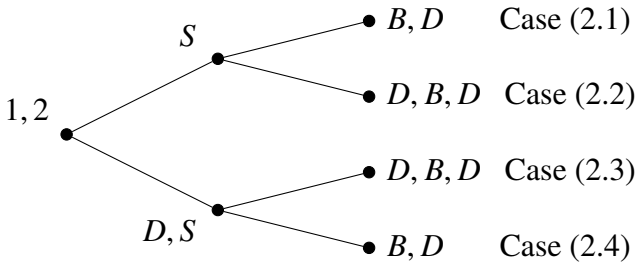

Figure 1. All four possible cases for AM-chains containing (after $1,2$) exactly one small step S and exactly one big non-squaring step B. The symbol D represents a block of consecutive squaring steps.

.

Case (2.1):

$$1,\ 2,\ S,\ B,\ D. \tag{5.5}$$

In this case, $S=3$. Hence, the only possible values of B are 4, 5, and 6. Therefore, we get the following three chains:

Case (2.1.1):

$$1,\ 2,\ 3,\ 4,\ldots,\ 4^{2^\tau}, \tag{5.6}$$

Eq (5.6) corresponds to Case (V) in Theorem 1.1.

Case (2.1.2):

$$1,\ 2,\ 3,\ 5,\ldots,\ 5^{2^\tau}, \tag{5.7}$$

Eq (5.7) corresponds to Case (VI) in Theorem 1.1.

Case (2.1.3):

$$1,\ 2,\ 3,\ 6, \ldots,\ 6^{2^{\tau}},\ \text{where } \tau \geq 0. \tag{5.8}$$

Eq (5.8) corresponds to Case (VII) in Theorem 1.1.

Case (2.2):

$$1,\ 2,\ S,\ D,\ B,\ D. \tag{5.9}$$

The only possible value for S is 3. Then, we have

$$1,\ 2,\ 3, \ldots,\ 3^{2^{\alpha}},\ B, \ldots\ ,\ \alpha \geq 1.$$

We note that $\lambda_{AM}\left(3^{2^{\alpha}}\right) = \alpha+1$. Therefore, in order to have a big step for B, we have $\lambda_{AM}(B) = \alpha+2$. If $\alpha = 1$, the only possible values for B are

$$B = 3^2 \times 3,$$

and

$$B = 3^2 \times 2.$$

If $\alpha \geq 2$, the only possible value for B is

$$B = 3^{2^{\alpha}} \times 3^{2^{\alpha-1}} = 3^{2^{\alpha}+2^{\alpha-1}},$$

where, $\lambda_{AM}\left(3^{2^{\alpha}+2^{\alpha-1}}\right) = \alpha + 2$, since

$$2^{2^{\alpha+2}} = 16^{2^{\alpha}} > \left(3 \times 3^{\frac{1}{2}}\right)^{2^{\alpha}} = 3^{2^{\alpha}} \times 3^{2^{\alpha-1}} = \left(3 \times 3^{\frac{1}{2}}\right)^{2^{\alpha}} > 4^{2^{\alpha}} = 2^{2^{\alpha+1}}.$$

Otherwise, we get

$$B \leq 3^{2^{\alpha}} \times 3^{2^{\alpha-2}} = \left(3 \times 3^{2^{-2}}\right)^{2^{\alpha}} < (3.95)^{2^{\alpha}} < 4^{2^{\alpha}} = 2^{\alpha+1},$$

and hence $\lambda_{AM}\left(3^{2^{\alpha}+2^{\alpha-2}}\right) = \alpha + 1$, which is a contradiction.

Therefore, we get two subcases:

Case (2.2.1):

$$1,\ 2,\ 3, \ldots,\ 3^{2^{\alpha}},\ 3^{2^{\alpha}+2^{\alpha-1}}, \ldots,\ 3^{2^{\alpha+\tau}+2^{\alpha+\tau-1}} = 27^{2^{\alpha+\tau-1}},\ \alpha \geq 1,\ \tau \geq 0. \tag{5.10}$$

Eq (5.10) corresponds to Case (VIII) in Theorem 1.1.

Case (2.2.2):

$$1,\ 2,\ 3,\ 9,\ 18, \ldots,\ 18^{2^{\tau}},\ \tau \geq 0. \tag{5.11}$$

Eq (5.11) corresponds to Case (IX) in Theorem 1.1.

Case (2.3):

$$1,\ 2,\ D,\ S,\ D,\ B,\ D. \tag{5.12}$$

Similar to Case (1.2), the only choices for S are

$$2^{2^\alpha}+1,\ 2^{2^\alpha}+2^{2^\beta},\ \text{and}\ 2^{2^\alpha+2^\beta},\ \text{where}\ \alpha>\beta\geq 0.$$

Therefore, Case (2.3) has the following three subcases:

$$\begin{aligned}
&\text{Case (2.3.1):}\ \ 1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+1,\ \ldots,\left(2^{2^\alpha}+1\right)^{2^\tau},\ B_1,\ \ldots,\ \alpha,\ \tau\geq 1,\\
&\text{Case (2.3.2):}\ \ 1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+2^{2^\beta},\ \ldots,\ \left(2^{2^\alpha}+2^{2^\beta}\right)^{2^\tau},\ B_2,\ \ldots,\\
&\qquad\qquad \alpha>\beta\geq 0,\ \tau\geq 1,\\
&\text{Case (2.3.3):}\ \ 1,\ 2,\ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^\beta},\ldots,\ 2^{2^{\alpha+\tau}+2^{\beta+\tau}},\ B_3,\ \ldots,\ \alpha>\beta\geq 0,\ \tau\geq 1.
\end{aligned}$$

Since

$$\lambda_{AM}\left(\left(2^{2^\alpha}+1\right)^{2^\tau}\right)=\lambda_{AM}\left(\left(2^{2^\alpha}+2^{2^\beta}\right)^{2^\tau}\right)=\lambda_{AM}\left(2^{2^{\alpha+\tau}+2^{\beta+\tau}}\right)=\alpha+\tau+1,$$

we have

$$\lambda_{AM}(B_1)=\lambda_{AM}(B_2)=\lambda_{AM}(B_3)=\alpha+\tau+2.$$

If $\alpha\geq 2$ in either Cases (2.3.1) and (2.3.2), we get

$$B_i<\left(2^{2^\alpha+1}\right)^{2^\tau+2^{\tau-1}}=2^{2^{\alpha+\tau}+2^{\alpha+\tau-1}+2^\tau+2^{\tau-1}}<2^{2^{\alpha+\tau+1}},\qquad i=1,\ 2,$$

and hence $\lambda_{AM}(B_i)<\alpha+\tau+2,\ i=1,\ 2$, which is a contradiction.

For $\alpha=1$, Cases (2.3.1) and (2.3.2) are reduced to the following chains:

$$1,\ 2,\ 4,\ 5,\ \ldots,\ 5^{2^\tau},\ B_1,\ \ldots\quad(\tau\geq 1),$$

$$1,\ 2,\ 4,\ 6,\ \ldots,\ 6^{2^\tau},\ B_2,\ \ldots\quad(\tau\geq 1).$$

which is impossible since for $i=1,2$ and $\tau\geq 1$, we have

$$B_i\leq(6\sqrt{6})^{2^\tau}<16^{2^\tau},$$

which implies that $\lambda_{AM}(B_i)<\tau+3$, which is a contradiction.

Then, Cases (2.3.1) and (2.3.2) are impossible.

If $\beta\leq\alpha-2$ in Case (2.3.3), we get

$$B_3\leq 2^{2^{\alpha+\tau}+2^{\alpha+\tau-1}+2^{\alpha+\tau-2}+2^{\alpha+\tau-3}}<2^{2^{\alpha+\tau+1}},$$

which is a contradiction. Then, $\beta>\alpha-2$, hence, the only possible value for β is $\beta=\alpha-1$.

If $\tau\geq 2$, the only possible value of B_3 is

$$B_3=2^{2^{\alpha+\tau}+2^{\alpha+\tau-1}}\times 2^{2^{\alpha+\tau-1}+2^{\alpha+\tau-2}}=2^{2^{\alpha+\tau+1}+2^{\alpha+\tau-2}},$$

since otherwise we get

$$B_3\leq 2^{2^{\alpha+\tau}+2^{\alpha+\tau-1}}\times 2^{2^{\alpha+\tau-2}+2^{\alpha+\tau-3}}<2^{2^{\alpha+\tau+1}}.$$

If $\tau = 1$, the only possible values of B_3 are

$$B_3 = 2^{2^{\alpha+1}+2^{\alpha}} \times 2^{2^{\alpha}+2^{\alpha-1}} = 2^{2^{\alpha+2}+2^{\alpha-1}},$$

and

$$B_3 = 2^{2^{\alpha+1}+2^{\alpha}} \times 2^{2^{\alpha}} = 2^{2^{\alpha+2}}.$$

Otherwise, we get

$$B_3 \leq 2^{2^{\alpha+1}+2^{\alpha}} \times 2^{2^{\alpha-1}} < 2^{2^{\alpha+2}},$$

which is a contradiction.

Therefore, we get two subcases:

Case (2.3.3.1):

$$1,\ 2, \ldots,\ 2^{2^{\alpha}},\ 2^{2^{\alpha}+2^{\alpha-1}}, \ldots,\ 2^{2^{\alpha+\tau}+2^{\alpha+\tau-1}},\ 2^{2^{\alpha+\tau+1}+2^{\alpha+\tau-2}}, \ldots,\ 2^{2^{\alpha+\tau+\delta+1}+2^{\alpha+\tau+\delta-2}}, \tag{5.13}$$

where $\alpha,\ \tau \geq 1, \delta \geq 0$.

Eq (5.13) corresponds to Case (X) in Theorem 1.1.

Case (2.3.3.2):

$$1,\ 2, \ldots,\ 2^{2^{\alpha}},\ 2^{2^{\alpha}+2^{\alpha-1}},\ 2^{2^{\alpha+1}+2^{\alpha}},\ 2^{2^{\alpha+2}}, \ldots,\ 2^{2^{\alpha+\tau+2}},\ \alpha \geq 1,\ \tau \geq 0. \tag{5.14}$$

Eq (5.14) corresponds to Case (XI) in Theorem 1.1.

Case (2.4):

$$1,\ 2,\ D,\ S,\ B,\ D. \tag{5.15}$$

Similar to Case (1.2), the only choices for S are

$$2^{2^{\alpha}} + 1,\ 2^{2^{\alpha}} + 2^{2^{\beta}},\ \text{and}\ 2^{2^{\alpha}+2^{\beta}},\ \text{where}\ \alpha > \beta \geq 0.$$

Therefore, Case (2.4) has the following three subcases:

$$\begin{aligned}
&\text{Case (2.4.1):}\quad 1,\ 2, \ldots,\ 2^{2^{\alpha}},\ 2^{2^{\alpha}} + 1,\ B_4, \ldots,\ \alpha \geq 1,\\
&\text{Case (2.4.2):}\quad 1,\ 2, \ldots,\ 2^{2^{\alpha}},\ 2^{2^{\alpha}} + 2^{2^{\beta}},\ B_5, \ldots,\ \alpha > \beta \geq 0,\\
&\text{Case (2.4.3):}\quad 1,\ 2, \ldots,\ 2^{2^{\alpha}},\ 2^{2^{\alpha}+2^{\beta}},\ B_6, \ldots,\ \alpha > \beta \geq 0.
\end{aligned}$$

We note that

$$\lambda_{AM}\left(2^{2^{\alpha}}\right) = \lambda_{AM}\left(2^{2^{\alpha}} + 1\right) = \lambda_{AM}\left(2^{2^{\alpha}} + 2^{2^{\beta}}\right) = \lambda_{AM}\left(2^{2^{\alpha}+2^{\beta}}\right) = \alpha + 1.$$

Therefore, we have

$$\lambda_{AM}(B_4) = \lambda_{AM}(B_5) = \lambda_{AM}(B_6) = \alpha + 2.$$

This result will be used to reject some possible values for B_4, B_5, and B_6.

We now consider Case (2.4.1). We prove that the only possible values for B_4 are

$$B_4 = \left(2^{2^{\alpha}} + 1\right) \times 2^{2^{\alpha}} = 2^{2^{\alpha+1}} + 2^{2^{\alpha}}, \tag{5.16}$$

and

$$B_4 = 2^{2^\alpha} \times 2^{2^\alpha} = 2^{2^{\alpha+1}}, \tag{5.17}$$

since the other possible values make B_4 a small step.

Suppose that B_4 is an additive step. Then, we get

$$B_4 \leq 2^{2^\alpha+1} + 2 < 2^{2^\alpha+2} \leq 2^{2^{\alpha+1}}.$$

Hence, B_4 cannot reach $2^{2^{\alpha+1}}$ as an additive step, and must therefore be a multiplicative step.

If B_4 is a multiplicative star step not of the form given in Eq (5.16), then

$$B_4 \leq (2^{2^\alpha} + 1) \times 2^{2^{\alpha-1}} = 2^{2^\alpha+2^{\alpha-1}} + 2^{2^{\alpha-1}} < 2^{2^\alpha+2^{\alpha-1}+1} \leq 2^{2^{\alpha+1}}.$$

Therefore, $\lambda_{AM}(B_4) < \alpha + 2$.

On the other hand, if B_4 is not a multiplicative star step and is not equal to the value in Eq (5.17), then

$$B_4 \leq 2^{2^\alpha} \times 2^{2^{\alpha-1}} < 2^{2^{\alpha+1}},$$

and again we have $\lambda_{AM}(B_4) < \alpha + 2$.

Hence, Case (2.4.1) can be divided into the following two subcases:

Case (2.4.1.1):

$$1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha} + 1,\ 2^{2^{\alpha+1}} + 2^{2^\alpha}, \ldots,\ \left(2^{2^{\alpha+1}} + 2^{2^\alpha}\right)^{2^\tau},\ \alpha \geq 1,\ \tau \geq 0. \tag{5.18}$$

Eq (5.18) corresponds to Case (XII) in Theorem 1.1.

Case (2.4.1.2):

$$1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha} + 1,\ 2^{2^{\alpha+1}}, \ldots,\ 2^{2^{\alpha+\tau+1}},\ \alpha \geq 1,\ \tau \geq 0. \tag{5.19}$$

Eq (5.19) corresponds to Case (XIII) in Theorem 1.1.

We now consider Case (2.4.2). Similar to Case (2.4.1), the only possible values for B_5 in Case (2.4.2) are

$$B_5 = (2^{2^\alpha} + 2^{2^\beta}) \times 2^{2^\alpha} = 2^{2^{\alpha+1}} + 2^{2^\alpha+2^\beta},$$

and

$$B_5 = 2^{2^\alpha} \times 2^{2^\alpha} = 2^{2^{\alpha+1}}.$$

Hence, Case (2.4.2) can be divided into the following two subcases:

Case (2.4.2.1):

$$1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha} + 2^{2^\beta},\ 2^{2^{\alpha+1}} + 2^{2^\alpha+2^\beta}, \ldots,\ \left(2^{2^{\alpha+1}} + 2^{2^\alpha+2^\beta}\right)^{2^\tau}, \alpha > \beta \geq 0,\ \tau \geq 0. \tag{5.20}$$

Eq (5.20) corresponds to Case (XIV) in Theorem 1.1.

Case (2.4.2.2):

$$1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha} + 2^{2^\beta},\ 2^{2^{\alpha+1}}, \ldots,\ 2^{2^{\alpha+\tau+1}}, \alpha > \beta \geq 0,\ \tau \geq 0. \tag{5.21}$$

Eq (5.21) corresponds to Case (XV) in Theorem 1.1.

We now consider Case (2.4.3). B_6 can be a multiplicative or additive step. If B_6 is a multiplicative star step, then the possible values of B_6 are

$$B_6 = 2^{2^\alpha+2^\beta} \times 2^{2^\alpha} = 2^{2^{\alpha+1}+2^\beta},$$

or

$$B_6 = 2^{2^\alpha+2^{\alpha-1}} \times 2^{2^{\alpha-1}} = 2^{2^{\alpha+1}}.$$

Note that B_6 cannot be

$$B_6 \leq 2^{2^\alpha+2^{\alpha-1}} \times 2^{2^{\alpha-2}} < 2^{2^{\alpha+1}};$$

since $\lambda_{AM}(B_6) < \alpha + 2$, which is a contradiction.

Similar to Case (2.4.1), if B_6 is not a multiplicative star step, the only possible value for it is

$$B_6 = 2^{2^\alpha} \times 2^{2^\alpha} = 2^{2^{\alpha+1}}.$$

Note that B_6 cannot be

$$B_6 \leq 2^{2^\alpha} \times 2^{2^{\alpha-1}} < 2^{2^{\alpha+1}}.$$

If B_6 is an additive step, we have

$$B_6 < 2^{2^\alpha+2^\beta+1} \leq 2^{2^{\alpha+1}}.$$

It follows that there are two different values of B_6. Thus, Case (2.4.3) has the following two subcases:

Case (2.4.3.1):

$$1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^\beta},\ 2^{2^{\alpha+1}+2^\beta}, \ldots,\ 2^{2^{\alpha+\tau+1}+2^{\beta+\tau}},\ \alpha > \beta \geq 0,\ \tau \geq 0. \tag{5.22}$$

Eq (5.22) corresponds to Case (XVI) in Theorem 1.1.

Case (2.4.3.2):

$$1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^\beta},\ 2^{2^{\alpha+1}}, \ldots,\ 2^{2^{\alpha+\tau+1}},\ \alpha > \beta \geq 0,\ \tau \geq 0. \tag{5.23}$$

Eq (5.23) corresponds to Case (XVII) in Theorem 1.1.

Case (3): $p = 4$.

Since every small step is a non-squaring step, the four non-squaring steps consist of the following:

- the first step (occurring at $i = 1$),
- the small step S, and
- two non-squaring steps B_1 and B_2, which must both be big steps.

Figure 2 shows all possible AM-chains when $p = 4$.

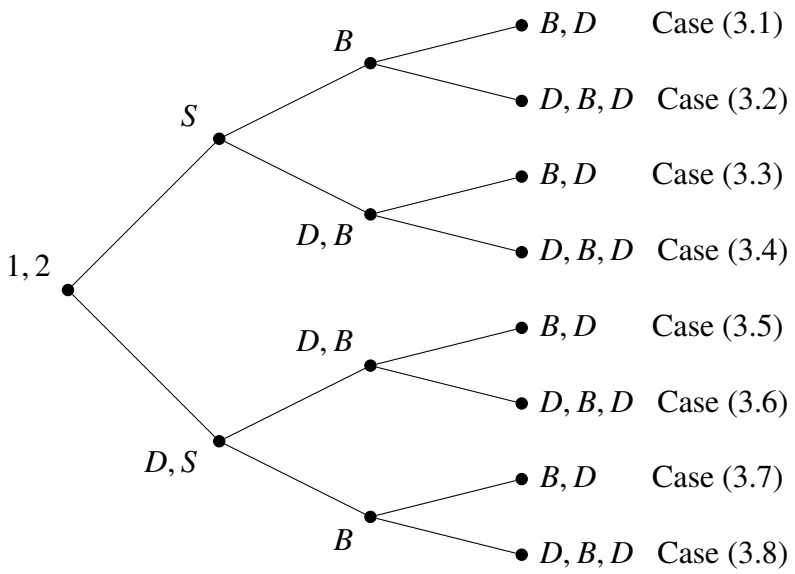

Figure 2. All eight possible cases for AM-chains containing (after 1, 2) exactly one small step S and exactly two big non-squaring steps B. The symbol D represents a block of consecutive squaring steps.

Case (3.1):

$$1,\ 2,\ S,\ B,\ B,\ D.$$

Using Case (2.1), the only possible AM-chain is

$$1,\ 2,\ 3,\ 6,\ 18, \ldots,\ 18^{2^\tau}\ ,\ \tau \geq 0. \tag{5.24}$$

Eq (5.24) corresponds to Case (XVIII) in Theorem 1.1.

Case (3.2):

$$1,\ 2,\ S,\ B,\ D,\ B,\ D.$$

Using Case (2.1), the only possible subchains are

$$\text{Case (3.2.1):}\quad 1,\ 2,\ 3,\ 4, \ldots,\ 4^{2^\tau},\ B_7, \ldots,\ \tau \geq 1,$$

$$\text{Case (3.2.2):}\quad 1,\ 2,\ 3,\ 5, \ldots,\ 5^{2^\tau},\ B_8, \ldots,\ \tau \geq 1,$$

$$\text{Case (3.2.3):}\quad 1,\ 2,\ 3,\ 6, \ldots,\ 6^{2^\tau},\ B_9, \ldots,\ \tau \geq 1.$$

We note that $\lambda_{AM}\left(4^{2^\tau}\right) = \lambda_{AM}\left(5^{2^\tau}\right) = \lambda_{AM}\left(6^{2^\tau}\right) = \tau + 2$. Therefore, $\lambda_{AM}(B_i) = \tau + 3,\ i = 7, 8, 9.$

Next, we show that all of these subchains are impossible, since all possible values for $B_i,\ i = 7, 8, 9$, are small.

Since

$$B_i \leq 6^{2^\tau + 2^{\tau-1}} = \left(6\sqrt{6}\right)^{2^\tau} < 14.7^{2^\tau} < 16^{2^\tau} = 2^{2^{\tau+2}},\ i = 7, 8, 9,$$

we get that $\lambda_{AM}(B_i) < \tau + 3,\ i = 7, 8, 9$.

Case (3.3):

$$1,\ 2,\ S,\ D,\ B,\ B,\ D.$$

Using Case (2.2), the only possible subchain is

$$1,\ 2,\ 3, \ldots,\ 3^{2^\alpha},\ 3^{2^\alpha+2^{\alpha-1}},\ B, \ldots,\ \alpha \geq 1.$$

As we know, $\lambda_{AM}\left(3^{2^\alpha+2^{\alpha-1}}\right) = \alpha + 2$, and

$$B \leq 3^{2^{\alpha+1}+2^{\alpha-1}} = \left(3 \times 3^{\frac{1}{4}}\right)^{2^{\alpha+1}} < 4^{2^{\alpha+1}} = 2^{2^{\alpha+2}}.$$

Therefore, $\lambda_{AM}(B) < \alpha + 3$. Thus, B cannot be a big step. Hence, this case is impossible.

Case (3.4):

$$1,\ 2,\ S,\ D,\ B,\ D,\ B,\ D.$$

Using Case (2.2), the only possible subchains are

$$\begin{aligned}
&\text{Case (3.4.1):} \quad 1,\ 2,\ 3, \ldots,\ 3^{2^\alpha},\ 3^{2^\alpha+2^{\alpha-1}}, \ldots,\ 3^{2^{\alpha+\tau}+2^{\alpha+\tau-1}},\ B_{10}, \ldots,\ \alpha \geq 1,\ \tau \geq 1,\\
&\text{Case (3.4.2):} \quad 1,\ 2,\ 3,\ 9,\ 18, \ldots,\ 18^{2^\tau},\ B_{11}, \ldots,\ \tau \geq 1.
\end{aligned}$$

As we can see, $\lambda_{AM}\left(3^{2^{\alpha+\tau}+2^{\alpha+\tau-1}}\right) = \alpha + \tau + 2$, and $\lambda_{AM}\left(18^{2^\tau}\right) = \tau + 3$.
Since

$$\begin{aligned}
B_{10} &\leq 3^{2^{\alpha+\tau+1}+2^{\alpha+\tau-2}} = \left(3^2 \times 3^{\frac{1}{4}}\right)^{2^{\alpha+\tau}} < 12^{2^{\alpha+\tau}} < 2^{2^{\alpha+\tau+2}},\ \text{and}\\
B_{11} &\leq 18^{2^\tau+2^{\tau-1}} = \left(18 \times \sqrt{18}\right)^{2^\tau} < 2^{2^{\tau+3}},
\end{aligned}$$

we get $\lambda_{AM}(B_{10}) < \alpha + \tau + 3$, and $\lambda_{AM}(B_{11}) < \tau + 4$. Thus, B_{10} and B_{11} cannot be big. Hence, these subcases are impossible.

Case (3.5):

$$1,\ 2,\ D,\ S,\ D,\ B,\ B,\ D.$$

Using Case (2.3), the only possible subchains are

$$1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^{\alpha-1}}, \ldots,\ 2^{2^{\alpha+\tau}+2^{\alpha+\tau-1}},\ 2^{2^{\alpha+\tau+1}+2^{\alpha+\tau-2}},\ B_{12}, \ldots,\ \alpha \geq 1,\ \tau \geq 1,$$

and

$$1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^{\alpha-1}},\ 2^{2^{\alpha+1}+2^\alpha},\ 2^{2^{\alpha+2}},\ B_{13}, \ldots,\ \alpha \geq 1.$$

Since

$$B_{12} \leq 2^{2^{\alpha+\tau+1}+2^{\alpha+\tau}+2^{\alpha+\tau-1}+2^{\alpha+\tau-2}} < 2^{2^{\alpha+\tau+2}},$$

and

$$B_{13} \leq 2^{2^{\alpha+1}+2^\alpha} \times 2^{2^{\alpha+2}} < 2^{2^{\alpha+3}},$$

both B_{12} and B_{13} cannot be big steps. Hence, this case is impossible.

Case (3.6):

$$1,\ 2,\ D,\ S,\ D,\ B,\ D,\ B,\ D.$$

Similar to Case (3.5), this case is impossible.

Case (3.7):

$$1,\ 2,\ D,\ S,\ B,\ B,\ D.$$

Using Case (2.4), the only possible subchains are

$$\begin{aligned}
&\text{Case (3.7.1):} \quad 1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+1,\ 2^{2^{\alpha+1}}+2^{2^\alpha},\ B_{14}, \ldots,\ \alpha \geq 1,\\
&\text{Case (3.7.2):} \quad 1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+1,\ 2^{2^{\alpha+1}},\ B_{15}, \ldots,\ \alpha \geq 1,\\
&\text{Case (3.7.3):} \quad 1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+2^{2^\beta},\ 2^{2^{\alpha+1}}+2^{2^\alpha+2^\beta},\ B_{16}, \ldots,\ \alpha > \beta \geq 0,\\
&\text{Case (3.7.4):} \quad 1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha}+2^{2^\beta},\ 2^{2^{\alpha+1}},\ B_{17}, \ldots,\ \alpha > \beta \geq 0,\\
&\text{Case (3.7.5):} \quad 1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^\beta},\ 2^{2^{\alpha+1}},\ B_{18}, \ldots,\ \alpha > \beta \geq 0,\\
&\text{Case (3.7.6):} \quad 1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^\beta},\ 2^{2^{\alpha+1}+2^\beta},\ B_{19}, \ldots,\ \alpha > \beta \geq 0.
\end{aligned}$$

We note that

$$\lambda_{AM}\left(2^{2^{\alpha+1}}+2^{2^\alpha}\right) = \lambda_{AM}\left(2^{2^{\alpha+1}}\right) = \lambda_{AM}\left(2^{2^{\alpha+1}}+2^{2^\alpha+2^\beta}\right) = \lambda_{AM}\left(2^{2^{\alpha+1}+2^\beta}\right) = \alpha+2,$$

and

$$B_i < 2^{2^{\alpha+1}+2^\alpha+2} \leq 2^{2^{\alpha+2}},\ \text{for } i = 14, \ldots, 17.$$

Therefore,

$$\lambda_{AM}(B_i) < \alpha+3,\ \text{for } i = 14, \ldots, 17.$$

Hence, all $B_i,\ \text{for } i = 14, \ldots, 17$, cannot be big steps. Therefore, all subcases from Case (3.7.1) to Case (3.7.4) are impossible.

In Case (3.7.5), we have

$$B_{18} \leq 2^{2^{\alpha+1}+2^\alpha+2^{\alpha-1}} < 2^{2^{\alpha+2}}.$$

Therefore,

$$\lambda_{AM}(B_{18}) < \alpha+3.$$

Thus, B_{18} cannot be a big step, and that makes Case (3.7.5) impossible.

In Case (3.7.6), if $\beta \leq \alpha-2$, we get

$$B_{19} \leq 2^{2^{\alpha+1}+2^{\alpha-2}} \times 2^{2^\alpha+2^{\alpha-2}} = 2^{2^{\alpha+1}+2^\alpha+2^{\alpha-1}} < 2^{2^{\alpha+2}}.$$

Therefore, $\beta > \alpha-2$. Since $\alpha > \beta$, the possible value of β is $\alpha-1$.

If $\beta = \alpha-1$, the only possible value of B_{19} is

$$B_{19} = 2^{2^{\alpha+1}+2^{\alpha-1}} \times 2^{2^\alpha+2^{\alpha-1}} = 2^{2^{\alpha+2}};$$

otherwise, we get

$$B_{19} < 2^{2^{\alpha+2}},$$

which is a contradiction. Hence, we get the AM-chain:

$$1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^{\alpha-1}},\ 2^{2^{\alpha+1}+2^{\alpha-1}},\ 2^{2^{\alpha+2}}, \ldots,\ 2^{2^{\alpha+\tau+2}},\ \alpha \geq 1,\ \tau \geq 0. \tag{5.25}$$

Eq (5.25) corresponds to Case (XIX) in Theorem 1.1.

Case (3.8):

$$1,\ 2,\ D,\ S,\ B,\ D,\ B,\ D.$$

If the number of squaring steps after 2 is α, we get the AM-chain:

$$1,\ 2, \ldots, 2^{2^\alpha},\ S,\ B_{20}, \ldots,\ B_{21}, \ldots\ .$$

Therefore, $\lambda_{AM}(S) = \alpha + 1$, and $\lambda_{AM}(B_{20}) = \alpha + 2$. The maximum value for S is $S = 2^{2^\alpha+2^{\alpha-1}}$. Therefore, the maximum value for B_{20} is $B_{20} = 2^{2^{\alpha+1}+2^{\alpha-1}}$. If we have τ squaring steps after B_{20}, then we get

$$1,\ 2, \ldots,\ 2^{2^\alpha},\ 2^{2^\alpha+2^{\alpha-1}},\ 2^{2^{\alpha+1}+2^{\alpha-1}}, \ldots,\ 2^{2^{\alpha+\tau+1}+2^{\alpha+\tau-1}},\ B_{21}, \ldots$$

where $\alpha \geq 1,\ \tau \geq 1$. We note that $\lambda_{AM}(2^{2^{\alpha+\tau+1}+2^{\alpha+\tau-1}}) = \alpha + \tau + 1$. Also, we have

$$B_{21} \leq 2^{2^{\alpha+\tau+1}+2^{\alpha+\tau}+2^{\alpha+\tau-1}+2^{\alpha+\tau-2}} < 2^{2^{\alpha+\tau+2}}.$$

Hence,

$$\lambda_{AM}(B_{21}) < \alpha + \tau + 3,$$

which makes B_{21} a small step. Hence, this case is impossible.

This completes the proof of the theorem. □

5.2. Proof of Theorem 1.2

To prove Theorem 1.2, we must establish that an integer n has a shortest AM-chain with exactly one small step (i.e. $\ell_{AM}(n) = \lambda_{AM}(n) + 1$) if and only if n belongs to one of six primary families.

Proof. Assume that an integer n has a shortest AM-chain with exactly one small step. By Theorem 1.1, the chain must be one of the 19 exhaustive cases. We know that the only AM-chain that contains zero small steps has the form $1, 2, 2^2, 2^{2^2}, \ldots, 2^{2^A}$, for some $A \geq 0$. Consequently, if the integer $n \neq 2^{2^A}$, then $\ell_{AM}(n) > \lambda_{AM}(n)$, *i.e.*, $\ell_{AM}(n) \geq \lambda_{AM}(n)+1$. Since we assume that the integer n has a shortest AM-chain with exactly one small step, n cannot be one of the integers generated by Cases (V), (XI), (XIII), (XV), (XVII), and (XIX). All of these cases terminate at an integer of the form $n = 2^{2^A}$. Consequently, n must correspond to one of the remaining 13 cases.

The remaining 13 cases of Theorem 1.1 either terminate in, or can be consolidated into, the following six primary families of integers:

(1) $3^{2^\alpha},\ \alpha \geq 0,$

(2) $\left(2^{2^\alpha} + 1\right)^{2^\tau},\ \alpha \geq 1,\ \tau \geq 0,$

(3) $\left(2^{2^\alpha}+2^{2^\beta}\right)^{2^\tau},\ \alpha>\beta\geq 0,\ \tau\geq 0,$

(4) $2^{2^\alpha+2^\beta},\ \alpha>\beta\geq 0,$

(5) $27^{2^\alpha},\ \alpha\geq 0,$

(6) $\left(2^{2^{\alpha+1}}+2^{2^\alpha+2^\beta}\right)^{2^\tau},\ \alpha>\beta\geq 0,\ \tau\geq 0.$

It is clear that families (1) through (6) cover cases (I)–(III), (IV), (VIII), and (XIV), respectively. We now demonstrate that the remaining seven cases are also encompassed by these six families. Since $5=\left(2^{2^1}+1\right)$, the second family (2) explicitly covers the integers generated by Case (VI). Similarly, since $6=\left(2^{2^1}+2^{2^0}\right)$ and $18=\left(2^{2^2}+2^{2^0}\right)$, the third family (3) encompasses the integers generated by Cases (VII), (IX), and (XVIII). Furthermore, the third family (3) also covers the integers generated by Case (XII). We note that the expression for Case (XII), $\left(2^{2^{\alpha+1}}+2^{2^\alpha}\right)^{2^\tau}$, where $\alpha\geq 0,\ \tau\geq 0$, can be strictly rewritten in the general form of the third family (3), $\left(2^{2^x}+2^{2^y}\right)^{2^\tau}$, where $x>y\geq 0,\ \tau\geq 0$, by substituting $x=\alpha+1$ and $y=\alpha$. Additionally, the fourth family (4) covers the integers generated by Cases (X) and (XVI). For example, the expression for Case (X), $2^{2^{\alpha+\tau+\delta+1}+2^{\alpha+\tau+\delta-2}}$, where $\alpha\geq 1,\ \tau\geq 1,\ \delta\geq 0$), can be expressed in the general form of the fourth family (4), $2^{2^x+2^y}$, where $x>y\geq 0$, by substituting $x=\alpha+\tau+\delta+1$ and $y=\alpha+\tau+\delta-2$. Similarly, family (4) encompasses Case (XVI). Thus, n must belong to one of these six families.

Conversely, assume that an integer n belongs to one of the six primary families listed above. Because each of these families corresponds directly to one or more of the cases established in Theorem 1.1, there exists an AM-chain for n that contains exactly one small step. Therefore, $\ell_{AM}(n)\leq\lambda_{AM}(n)+1$. We must ensure that this is the shortest possible chain (i.e., $\ell_{AM}(n)>\lambda_{AM}(n)$). As established, the only integers n that admit a chain of length $\lambda_{AM}(n)$, *i.e.,* no small steps, are strictly those of the form 2^{2^A}. Furthermore, none of the integers generated by the six primary families can be expressed in the form 2^{2^A}. This completes the proof. □

6. Shortest AM-chains

Finding $\ell_A(n)$ and generating a shortest or short addition chain have attracted the interest of many researchers [7, 14–22]. Similarly, for AM-chain [12, 13].

In this section, we prove some new results about $\ell_{AM}(n)$.

Theorem 1.2 shows that

$$\ell_{AM}\left(2^{2^A+2^B}\right)=\lambda_{AM}\left(2^{2^A+2^B}\right)+1=A+2,\quad \text{where } A>B>0.$$

Now, we find $\ell_{A.M}\left(2^{2^A+2^B+2^C}\right)$, where $A>B>C>0$.

Theorem 6.1. $\ell_{AM}\left(2^{2^A+2^B+2^C}\right)=A+3$, *where* $A>B>C>0$.

Proof. Using Eq (2.1), we have

$$\ell_{AM}\left(2^{2^A+2^B+2^C}\right)\geq\log_2\left(\log_2\left(2^{2^A+2^B+2^C}\right)\right)+1>A+1.$$

If $\ell_{AM}\left(2^{2^A+2^B+2^C}\right) = A+2$, then a shortest AM-chain must contain one small step. Therefore, $2^{2^A+2^B+2^C}$ must be one of the cases in Theorem 1.2. Since $2^{2^A+2^B+2^C}$ is an even number, we exclude all odd cases. Therefore, the possible cases are

$$\left(2^{2^\alpha}+2^{2^\beta}\right)^{2^\tau},\ \alpha>\beta\geq 0,\ \tau\geq 0,$$
$$\left(2^{2^{\alpha+1}}+2^{2^\alpha+2^\beta}\right)^{2^\tau},\alpha>\beta\geq 0,\ \tau\geq 0.$$

Now, we prove that $(2^x+2^y)^z \neq 2^t$, where $x>y>0$.

If $(2^x+2^y)^z = 2^t$, then $2^x+2^y = 2^{\frac{t}{z}}$, which is impossible. Therefore, $\ell_{AM}\left(2^{2^A+2^B+2^C}\right) \neq A+2$. Since the length of the chain

$$1,2,\ldots,2^{2^A},2^{2^A+2^B},2^{2^A+2^B+2^C}$$

is $A+3$, we get $\ell_{A.M}\left(2^{2^A+2^B+2^C}\right) = A+3$. □

Theorem 6.2. $\ell_{AM}\left(3^{2^A+2^B}\right) = A+3$, *where* $A>B\geq 0$.

Proof. If $B = A-1$, then

$$4^{2^A} < 3^{2^A+2^{A-1}} = \left(3\sqrt{3}\right)^{2^A} < 16^{2^A}.$$

Therefore, $\lambda_{AM}\left(3^{2^A+2^{A-1}}\right) = A+2$. Since $3^{2^A+2^{A-1}}$ is not a power of 2, then $\ell_{A.M}\left(3^{2^A+2^{A-1}}\right) > A+2$. Since $3^{2^A+2^{A-1}}$ is one of the cases of Theorem 1.2, we get that

$$\ell_{A.M}\left(3^{2^A+2^{A-1}}\right) = A+3.$$

If $B\leq A-2$, since

$$2^{2^A} < 3^{2^A+2^{A-2}} = \left(3\times 3^{2^{-2}}\right)^{2^A} < 4^{2^A} = 2^{2^{A+1}},$$

we get that $\lambda_{AM}\left(3^{2^A+2^B}\right) = A+1$, where $0\leq B\leq A-2$. Since $3^{2^A+2^B}$ is not a power of 2, where $0\leq B\leq A-2$, a shortest AM-chain for $3^{2^A+2^B}$ must contain at least one small step. If there exists a shortest AM-chain for $3^{2^A+2^B}$, with exactly one small step, then it must be one of the cases of Theorem 1.2. Since $3^{2^A+2^B}$ is an odd number, we have three possible cases:

$$3^{2^\alpha},\ \alpha\geq 0,$$
$$27^{2^{\alpha+\tau-1}},\ \alpha\geq 1,\ \tau\geq 1,$$
$$\left(2^{2^\alpha}+1\right)^{2^\tau},\ \alpha\geq 1,\ \tau\geq 0.$$

The first two cases are not equal to $3^{2^A+2^B}$, where $0\leq B\leq A-2$. If $3^{2^A+2^B} = \left(2^{2^\alpha}+1\right)^{2^\tau}$, we get

$$A+1 = \lambda_{AM}\left(3^{2^A+2^B}\right) = \lambda_{AM}\left(\left(2^{2^\alpha}+1\right)^{2^\tau}\right) = \alpha+\tau+1.$$

Therefore,

$$3^{2^A+2^B} = \left(2^{2^\alpha}+1\right)^{2^{A-\alpha}}.$$

Thus,

$$3^{2^\alpha+2^{B-\tau}} - 2^{2^\alpha} = 1,$$

which is impossible for $\alpha \geq 1$. Hence, a shortest AM-chain for $3^{2^A+2^B}$, where $0 \leq B \leq A-2$, must contain at least 2 small steps. The following chain shows that there is an AM-chain for $3^{2^A+2^B}$, where $0 \leq B \leq A-2$, with two small steps:

$$1,\ 2,\ 3, \ldots,\ 3^{2^A},\ 3^{2^A+2^B}.$$

Thus, $\ell_{A.M}\left(3^{2^A+2^B}\right) = A+3$, where $0 \leq B \leq A-2$. In general, we get that

$$\ell_{A.M}\left(3^{2^A+2^B}\right) = A+3, \text{ where } 0 \leq B \leq A-1.$$

□

Theorem 6.3. $\ell_{A.M}\left(5^{2^A+2^B}\right) = A+4$, *where* $A > B \geq 0$.

Proof. The proof is similar to the proof of Theorem 6.2. □

7. Conclusions and future work

Let $a_0, a_1, \ldots, a_l$ be an AM-chain with d squaring steps. We have found upper bounds for a_l and the number of non-squaring steps. We have also found all AM-chains with one small step. Finally, we have computed $\ell_{AM}(n)$ for some integers n.

There are still some interesting open problems related to this study, such as:

- Extend Theorem 1.1 to two small steps.
- Can the upper bounds given in Theorem 3.2 and Corollary 3.1 accelerate the generation of a shortest AM-chain [13]?
- Calculating the difference between the upper bounds of two consecutive elements in an AM-chain.

Author contributions

Conceptualization, S. T., M. A., H. B.; methodology, S. T., M. A.; formal analysis, S. T., M. A., H. B.; validation, S. T., M. A., H. B.; investigation, S. T., M. A., H. B.; writing—original draft, S. T., M. A.; writing—review and editing, S. T., M. A., H. B.; Funding acquisition H. B.. All authors have read and agreed to the published version of the manuscript.

Use of AI tools declaration

The authors declare that they have not used Artificial Intelligence (AI) tools in the creation of this article.

Funding

This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-DDRSP2602).

Conflict of interest

The authors declare that they have no conflict of interest.

References

1. D. E. Knuth, *The art of computer programming: Sorting and searching, Volume 3*, 1998.
2. A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, *Handbook of applied cryptography*, Boca Raton: CRC Press, 2018. https://doi.org/10.1201/9780429466335
3. P. J. Downey, B. L. Leong, R. Sethi, Computing sequences with addition chains, *SIAM J. Comput.*, **10** (1981), 638–646. https://doi.org/10.1137/0210047
4. D. M. Gordon, A survey of fast exponentiation methods, *J. Algorithms*, **27** (1998), 129–146. https://doi.org/10.1006/jagm.1997.0913
5. J. von zur Gathen, M. Nöcker, Computing special powers in finite fields, *Math. Comp.*, **73** (2004), 1499–1523. https://doi.org/10.1090/S0025-5718-03-01599-0
6. K. Järvinen, V. Dimitrov, R. Azarderakhsh, A generalization of addition chains and fast inversions in binary fields, *IEEE T. Comput.*, **64** (2014), 2421–2432. https://doi.org/10.1109/TC.2014.2375182
7. H. M. Bahig, H. M. Bahig, A new strategy for generating shortest addition sequences, *Computing*, **91** (2011), 285–306. https://doi.org/10.1007/s00607-010-0119-7
8. H. M. Bahig, M. Hazber, H. M. Bahig, An efficient simulated annealing algorithm for short addition sequences, *AIMS Math.*, **9** (2024), 11024–11038. https://doi.org/10.3934/math.2024540
9. R. J. Lipton, D. Dobkin, Complexity measures and hierarchies for the evaluation of integers and polynomials, *Theor. Comput. Sci.*, **3** (1976), 349–357. https://doi.org/10.1016/0304-3975(76)90051-7
10. F. Morain, J. Olivos, Speeding up the computations on an elliptic curve using addition–subtraction chains, *RAIRO Theor. Inf. Appl.*, **24** (1990), 531–543. https://doi.org/10.1051/ita/1990240605311
11. H. Volger, Some results on addition/subtraction chains, *Inform. Process. Lett.*, **20** (1985), 155–160. https://doi.org/10.1016/0020-0190(85)90085-7
12. H. M. Bahig, On a generalization of addition chains: Addition-multiplication chains, *Discrete Math.*, **308** (2008), 611–616. https://doi.org/10.1016/j.disc.2007.04.015
13. H. Bahig, A. Mahran, Efficient generation of shortest addition-multiplication chains, *J. Egypt. Math. Soc.*, **26** (2018), 3. https://doi.org/10.21608/joems.2018.2691.1052
14. H. M. Bahig, Star reduction among minimal length addition chains, *Computing*, **91** (2011), 335–352. https://doi.org/10.1007/s00607-010-0122-z

15. H. M. Bahig, Y. Kotb, An efficient multicore algorithm for minimal length addition chains, *Computers*, **8** (2019), 23. https://doi.org/10.3390/computers8010023

16. F. Bergeron, J. Berstel, S. Brlek, Efficient computation of addition chains, *J. Theor. Nombr. Bordx.*, **6** (1994), 21–38. https://doi.org/10.5802/jtnb.104

17. E. G. Thurber, N. M. Clift, Addition chains, vector chains, and efficient computation, *Discrete Math.*, **344** (2021), 112200. https://doi.org/10.1016/j.disc.2020.112200

18. E. G. Thurber, Efficient generation of minimal length addition chains, *SIAM J. Comput.*, **28** (1999), 1247–1263. https://doi.org/10.1137/S0097539795295663

19. F. Bergeron, J. Berstel, S. Brlek, C. Duboc, Addition chains using continued fractions, *J. Algorithms*, **10** (1989), 403–412. https://doi.org/10.1016/0196-6774(89)90036-9

20. H. M. Bahig, Y. Kotb, A multicore exact algorithm for addition sequence, *J. Comput.*, **14** (2019), 79–87. https://doi.org/10.17706/jcp.14.1.79-87

21. N. Nedjah, L. de Macedo Mourelle, Minimal addition chain for efficient modular exponentiation using genetic algorithms, In: *Developments in Applied Artificial Intelligence*, Berlin: Springer, 2002. https://doi.org/10.1007/3-540-48035-8_10

22. H. Altman, Internal structure of addition chains: Well-ordering, *Theor. Comput. Sci.*, **721** (2018), 54–69. https://doi.org/10.1016/j.tcs.2017.12.002 ,

AIMS Press