Optimal Addition-Subtraction Chains

Nathan Mihm

Submitted under the supervision of Professor Victor Reiner to the University Honors Program at the University of Minnesota–Twin Cities in partial fulfilment of the requirements for the degree of Bachelor of Science summa cum laude in Mathematics.

Abstract

This paper explores the formalizations of addition-subtraction chains as an extension to the well-researched addition chains. An addition chain for a positive integer n is a sequence $1 = a_0, a_1, a_2, \ldots, a_\ell = n$ in which each $a_k = a_i + a_j$ for some $i, j < k$; an addition-subtraction chain allows $a_k = a_i \pm a_j$. This paper explores a graph-theoretic method to compute $\bar{\ell}(n)$, the length of a shortest addition-subtraction chain for n, similar to the methods known for addition chains. We present an algorithm for computing such chains in an efficient manner, along with some preliminary computation results. This research may prove practical in applications where this arithmetic represents computationally intensive tasks such as with elliptic curves.

Contents

Acknowledgments

I would like to thank my advisor Victor Reiner for his guidance and careful proofreading of my work, as well as his countless ideas for improvements. I also thank Anna Weigandt and Peter Webb for agreeing to be readers of this thesis and for their support. Finally, I would like to thank my family and the mathematics department for supporting my undergraduate education.

1 Introduction

Additions chains arises in various optimizations problems, and have a sizable amount of research behind them. For instance, [1, 3], along with famous authors such as Paul Erdös [2] and Donald Knuth [6]. An addition chain simply is a finite sequence of numbers in which each new element is the sum of two prior elements, starting from one.

Definition 1.1. An *addition chain* is a finite sequence of integers $a_0, a_1, \cdots, a_m$ such that for all $1 \leq k \leq m$, $a_k = a_i + a_j$ for some $0 \leq i, j < k$.

In other words, we are creating a list of integers by adding two existing numbers together at each step. For instance, say you wanted to obtain three, starting from one. Let $a_0 = 1$, then we can extend $a_1 = a_0 + a_0 = 1+1 = 2$, and finally $a_2 = a_0 + a_1 = 1+2 = 3$. This gives the sequence

$$1, 2, 3 \tag{1}$$

Typically we are interested in finding the shortest such chains. Determining the shortest chain to produce an arbitrary integer starting with $a_0 = 1$ is a profound question that has no known trivial solution.

Definition 1.2. The *optimal addition chain* length for an integer n, denoted $\ell(n)$, is the smallest positive integer m such that there exists an addition chain $a_0, \cdots, a_m$ with $a_0 = 1$ and $a_m = n$. For the purposes of this paper, unless otherwise noted, n will be positive.

For a longer example, an addition chain that reaches 31 in eight steps can be given by

$$1, 2, 4, 8, 16, 24, 28, 30, 31 \tag{2}$$

This is created using the "naïve approach" to repeatedly double each new element until we reach $2^{\lfloor \log_2 n \rfloor}$, in this case 16. Next, combine all the necessary powers of two in the binary expansion of n. While this does provide a simple upper bound, it becomes clear that this is not always the optimal method. An optimal chain for 31 is in fact

$$1, 2, 3, 6, 12, 15, 30, 31 \tag{3}$$

which implies $\ell(31) = 7$ steps. However, this would be difficult to verify by hand, and in general computing optimal chains is nontrivial. In this paper, we will focus on the lesser researched variant of addition chains where subtraction is also allowed.

Definition 1.3. An *addition-subtraction chain* is a finite sequence $a_0, a_1, \cdots, a_m$ such that for all $1 \leq k \leq m$, either $a_k = a_i + a_j$ or $a_k = a_i - a_j$ for some $0 \leq i, j < k$.

In the exact same manner, one defines the following.

Definition 1.4. The *optimal addition-subtraction chain* length for an integer n, denoted $\bar{\ell}(n)$, is the smallest positive integer m such that there exists an addition-subtraction chain $a_0, \cdots, a_m$ with $a_0 = 1$ and $a_m = n$. For the purposes of this paper, unless otherwise noted, n will be positive.

As an example, the chain given in (3) for 31 is no longer the optimal. Instead, we can simply double our way up until 32 and then use a subtraction to obtain $32 - 1 = 31$:

$$1, 2, 4, 8, 16, 32, 31 \tag{4}$$

Which now only takes $\bar{\ell}(31) = 6$ steps. In fact, 31 is the smallest integer n such that $\ell(n) \neq \bar{\ell}(n)$, which is shown in the Online Encyclopedia of Integer Sequences (OEIS) at A229624 [9].

This paper seeks to explore these computational methods on both types of chains. As a simple heuristic of the computational difficulty, we can compute an upper bound on the number of chains of a given length.

Proposition 1.5. *An upper bound on the number of addition chains length m is given by $(m!)^2$ and an upper bound on the number addition-subtraction chains is $2^m(m!)^2$.*

Proof. In an addition chain of length k, while selecting the next element there are k^2 choices. This is given by k possibilities on the first and k on the second. Therefore, given m total steps we obtain $(m!)^2$ total possibilities. Likewise, for addition subtraction, there is also an additional binary choice per step based on if we want to add or subtract. This multiplies the original bound by 2^m. □

Note that in either case, these are vast overestimates as elements in the chain often can be obtained in multiple different ways. So while there are $(m!)^2$ different possible steps, not every one leads to a distinct chain.

Using these and other properties, we can vastly reduce the search space looking for optimal chains. Just 20 steps already presents over 10^{24} addition-subtraction chains in the upper bound, which is difficult to search through even with modern hardware. For the simpler variant with only addition, prior research using graph theoretic approaches has allowed the computation of $\ell(n)$ up until $n = 2^{39}$. [1,3] We will discuss some of these optimizations in the following section.

Addition chains have numerous possible applications, such as optimal matrix multiplications to reach a power [4,6]. While less knowledge exists on optimal addition-subtraction chains, there have been some potential applications found. Its primary use would be when addition and subtraction represent computationally intense tasks. This requires addition and subtraction to be of roughly equal computational cost. A known example of this involves elliptic curve arithmetic [8]. In matrix exponentiation of an invertible matrix, subtraction is represented as matrix division or the solution of a linear system. This has the same classical time complexity as multiplication, $O(n^3)$.[1] However, due to implementation details, this may not be useful unless $\bar{\ell}(n) \ll \ell(n)$.

While some previous research has computed optimal chains for small Hamming-weight numbers (≤ 4), no algorithms have been developed and implemented to compute provably optimal chains for arbitrary integers under any sizable upper bound [7, 12]. Here the Hamming weight refers to the number of twos in binary form. In some cases this applies to "negative" Hamming weight $\bar{h}$ as well, which for integer n is the minimal $|E|$ such that

$$E \subset \mathbb{Z}^+, \quad n = \sum_{e_i \in E} w(e_i) 2^{e_i}, \quad w : \mathbb{Z}^+ \to \{-1, 1\} \tag{5}$$

which is given in OIES A007302, and is also unbounded as

$$\bar{h}\left(\frac{2^{2n-1}+1}{3}\right) = n \tag{6}$$

as given in A007583. The lack of general computation is in contrast to the optimal addition chain known up to the moderately large $n = 2^{39}$. This is still relatively small, about 500 billion, but the largest computation available for addition subtraction chains is only up to $n = 87$, given in OEIS A128998 [9]. Compared to addition chains, the search space is slightly larger as described in Proposition 1.5. Many of the optimization techniques used on addition chains will adapt to addition subtraction chains, so there are significant computational improvements to be made.

[1] Yes, matrix multiplication can be done with lower time complexity such as the Strassen Algorithm.

2 Basic properties

First, we lay some foundations on addition-subtraction chains. Addition chains represent a simpler structure: starting from one, all elements must be positive given that each element is greater than its addends. They can also they always can be written in increasing order.[2] However, in principle an addition subtraction chain could contain nonpositive elements, as indicated by the chain

$$1, \quad 1+1=2, \quad 1-2=-1, \quad 1+(-1)=0. \tag{7}$$

However, given an optimal chain length for a positive number, a chain exists that is entirely positive by rearrangement. In other words, no optimal chain relies on the use of a nonpositive number. First, present the following extension

Definition 2.1. A *generalized addition-subtraction* chain is one that allows new elements to be the negated sum of two prior elements alongside addition or subtraction. That is, finite given sequence $a_0, a_1, \cdots, a_m$ for all $1 \le k \le m$ there exists $0 \le i, j < k$ such that

$$a_k \in \{a_i + a_j, a_i - a_j, -a_i + a_j, -a_i - a_j\} \tag{8}$$

Note that all addition-subtraction chains are also generalized chains, but the chain

$$1, \quad -1-1=-2, \quad -(-2)-(-2)=4 \tag{9}$$

is not.

Proposition 2.2. *Any optimal addition subtraction chain can be formed without using negative numbers.*

Proof. First show this property holds for generalized chains. Let $a_0, \cdots, a_m$ be an generalized addition-subtraction chain where $a_k < 0$ is the first negative value. Then, for some $0 \le i, j < k$, we have

$$a_k \in \{a_i + a_j, a_i - a_j, -a_i + a_j, -a_i - a_j\}. \tag{10}$$

Note that $-a_k$ is also in this set as it consists of two pairs with equal magnitude, opposite sign. Therefore, we can replace a_k with $-a_k$ in the chain.

Next, to show all subsequent values are still obtainable, let a_s be formed from a_k and a_r. Here,

$$a_s \in \{a_k + a_r, a_k - a_r, -a_k + a_r, -a_k - a_r\} \tag{11}$$

Label the modified sequence as a' with $a'_k = -a_k$. Then

$$a_s = a'_s \in \{-a'_k + a'_r, -a'_k - a'_r, a'_k + a'_r, a'_k - a'_r\} \tag{12}$$

If $a_s = a_r + a_k$, then $a'_s = a'_r - a'_k$. Likewise, if $a_s = a_r - a_k$ then $a'_s = a'_r + a'_k$. However, if $a_s = a_k - a_r$ we cannot directly obtain $a'_s = -a'_k - a'_r$. A similar argument holds in the case $r = k$. In the end, we have a chain a' that is exactly the same except a_k is positive.

Repeat this process to remove the next negative value. By carrying out this transformation along the entire sum, we end with a chain of only positive values.

To show this holds for just addition-subtraction chains, we simply need to show that a negated sum operation will not be used in the final conversion. If it was ever used, say on a_k, then

$$a_k = -a_i - a_j \le 0 \tag{13}$$

which contradicts the fact that all elements are nonnegative. In the case $a_k = 0$, both $a_i = a_j = 0$, so this chain cannot be optimal as it contains repeated elements. □

[2] Assume otherwise, there would exist $a_i > a_{i+1}$. Then a_{i+1} cannot be formed using a_i and we could swap their places.

To illustrate this proposition, consider the chain given by

$$1, \quad 1+1=2, \quad 2+2=4, \quad 1-4=-3, \quad 4-(-3)=7 \tag{14}$$

is an optimal chain for seven with four steps. However, it can simply be rewritten as

$$1, \quad 1+1=2, \quad 2+2=4, \quad 4-1=3, \quad 3+4=7 \tag{15}$$

with the same number of steps. There is an easy corollary of this.

Corollary 2.3. *Any optimal addition subtraction chain can be formed with only positive numbers, that is, avoiding zeroes.*

Proof. We simply need to show an optimal chain can be constructed without zero. Let $a_k = 0$ be the first zero value. Simply delete a_k and a shorter chain will be constructed: $a_i \pm 0$ will not create a repeat value, and $0 - a_i$ will create a negative number, or zero again.

Note that we are focusing on optimal chains that reach positive numbers. Zero could always be reached in a single step with $1-1=0$. □

3 Graphical representation

Computation of optimal additional chains has been done to the greatest extent by computer scientist Neill Clift. [1] Instead of a basic, brute force approach to determine the shortest such chains, they use a graph theoretic approach. By analyzing necessary patterns in optimal chains, they are are able to significantly reduce the search space.

Many, but not all of the optimizations used by Clift also apply to the generalized case where subtraction is also allowed. The key difference here is that subtraction allows multiple results from two input elements. Therefore, to allow this, we will use weighted graphs instead of standard graphs. Similar to before, these graphs are still multigraphs and directed.

Definition 3.1. The weighted, directed multigraph associated with an addition-subtraction chain $a_0, \cdots, a_m$ has $m+1$ vertices labeled by each element in the sequence. Other than the starting vertex 1, every vertex has two directed edges coming in, representing the elements it was formed by. All edges have a weight of ±1. This can be represented as an ordered quadruple (V, E, α, ω):

- V is the set of vertices.
- E is the set of edges.
- $\alpha : E \to V$ is a map that determines the source vertex for a particular edge.
- $\omega : E \to V$ is a map that determines the target vertex for a particular edge.

together with two functions, $p : V \to \mathbb{Z}$ determines the value at a vertex, and $w : E \to \{-1, 1\}$ determines the weight of a particular edge. From our construction, the following holds

$$p(v) = \sum_{e \in E | \omega(e) = v} w(e) \cdot p(\alpha(e)) \tag{16}$$

for all vertices except the starting vertex v_0.

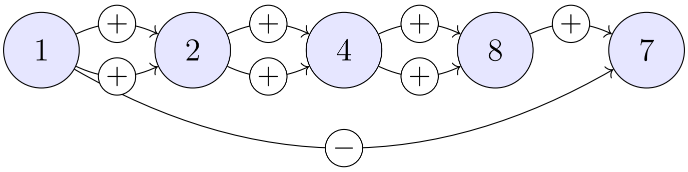

Figure 1: Graph constructed on an optimal chain for 7. Edges labeled + and − represent weights of +1 and −1 respectively to simplify the diagram.

For example, an optimal chain for seven can be given by 1,2,4,8,7. Seven is the smallest integer that has an optimal addition subtraction chain that contains a subtraction. We represent this as the graph shown in Figure 1. The summation in (16) is represented by the arrows pointing toward a given node.

Not every graph of this type is a valid addition subtraction chain. For instance one cannot have two -1 weights entering a node.

Definition 3.2. The *in-degree* of a vertex v, $\operatorname{indeg}(v)$, is given by the cardinality of the set $\{e \in E \mid \omega(e) = v\}$. The *out-degree* $\operatorname{outdeg}(v)$ is the cardinality of the set $\{e \in E \mid \alpha(e) = v\}$.

In our current construction, other than the starting node, every vertex must have an in-degree of exactly 2. There is no bound on the out-degree. However, we should certainly expect every node to have nonzero out-degree except the last one if we desire an optimal chain. This would mean an element remains unused.

3.1 Graph reduction

While these graphs are helpful for visualizing, more importantly they allow us to characterize an optimal chain and drastically reduce the search space. One of the best ways to do this is by graph reduction. This reduction can take place whenever a vertex has an out degree of 1.

Definition 3.3. A graph can be *reduced* whenever the out-degree of a vertex v_i is equal to 1. This can be done by removing the vertex and forwarding all edges that point into the vertex. Adjust the weights as necessary. In symbols, if $\operatorname{outdeg}(v_i) = 1$, then there exists unique $f \in E$ such that $\alpha(f) = v_i$. We create a new graph $(V', E', \alpha', \omega')$ with $V' = V \setminus \{v_i\}$ and $E' = E \setminus \{f\}$. For edge $e \in E$, if $\omega(e) = v_i$ then $\omega'(e') = \omega(f)$ and $w(e') = w(f) \cdot w(e)$. For all other edges, α and ω remain unchanged.

For example, the we can reduce the graph of the graph for seven in Figure 1. Remove the vertex for eight and forward the two edges that point to it to the vertex for seven. This is shown in Figure 2.

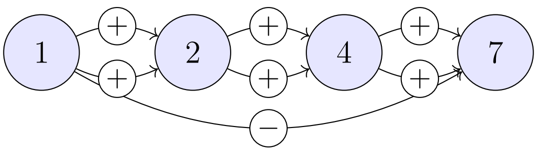

Figure 2: Fully reduced graph representing an optimal chain for 7.

A downside of this reduction is that the number of vertices no longer prescribes the length of the chain. However, there is an easy way to compute $\bar{\ell}(n)$ from an optimal graph which is described in Proposition 3.7.

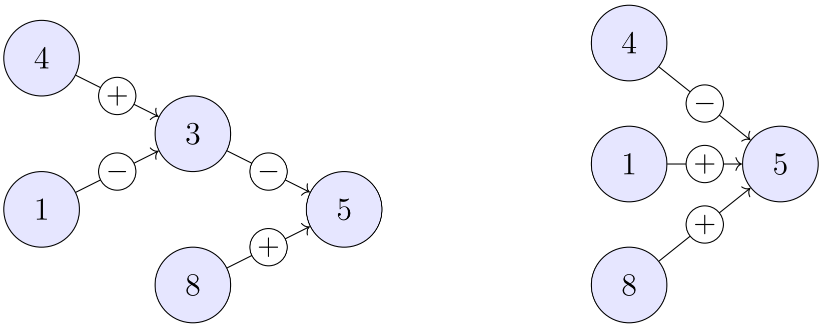

Figure 3: A reduction where the removed edge has negative weight. The forwarded edges have negated weights, which ensures the vertex equation still holds, $5 = -4 + 1 + 8$.

A more general example is shown in Figure 3, which demonstrates the case when the deleted edge represents a subtraction.

Proposition 3.4. *The vertex equation given in* (16) *still holds after reduction.*

Proof. Let $v_j = \omega(f)$, that is, the destination vertex of the edge removed during the reduction. The edges going into every other vertex remain unchanged, so therefore we only need to check the equation still holds for v_j. Split the summation into the original and forwarded parts.

$$\begin{aligned}
p(v_j) &= \sum_{\substack{e' \in E': \\ \omega(e')=v_j}} w(e') \cdot p(\alpha(e')) \\
&= \sum_{\substack{e \in E: \\ \omega(e)=v_i}} w(f) \cdot w(e) \cdot p(\alpha(f)) + \sum_{\substack{e \in E \setminus \{f\}: \\ \omega(e)=v_j}} w(e) \cdot p(\alpha(e)) \\
&= w(f) \left(\sum_{\substack{e \in E: \\ \omega(e)=v_i}} w(e) \cdot p(\alpha(f)) \right) + \sum_{\substack{e \in E \setminus \{f\}: \\ \omega(e)=v_j}} w(e) \cdot p(\alpha(e)) \\
&= w(f) \cdot p(v_i) + \sum_{\substack{e \in E \setminus \{f\}: \\ \omega(e)=v_j}} w(e) \cdot p(\alpha(e)) \\
&= \sum_{\substack{e \in E: \\ \omega(e)=v_j}} w(e) \cdot p(\alpha(e)) \qquad (17)
\end{aligned}$$

as desired. Note that the equality (17) used the fact that, by our construction, $v_i = \alpha(f)$. □

Searching for reduced graphs requires a method to expand back into the original graph in order to produce an addition-subtraction chain.

Definition 3.5. Whenever a vertex has in degree greater than 2, we can *expand* the graph to reverse reduction. Let v be a vertex such that $\text{indeg}(v) > 2$ and select two of the edges e and f with $\omega(e) = \omega(f) = v$. Create a new graph (V', E') with new vertex u such that $V' = V \cup \{u\}$ and $E' = (E \cup \{e', f', g\}) \setminus \{e, f\}$. Here the additional edges have $\alpha(e') = \alpha(e)$, $\alpha(f') = \alpha(f)$, $\alpha(g) = u$ and $\omega(e') = \omega(f') = u$ and $\omega(g) = v$. The weights of the edges are prescribed as $w(g) = 1$, $w(e') = w(e)$, and $w(f') = w(f)$.

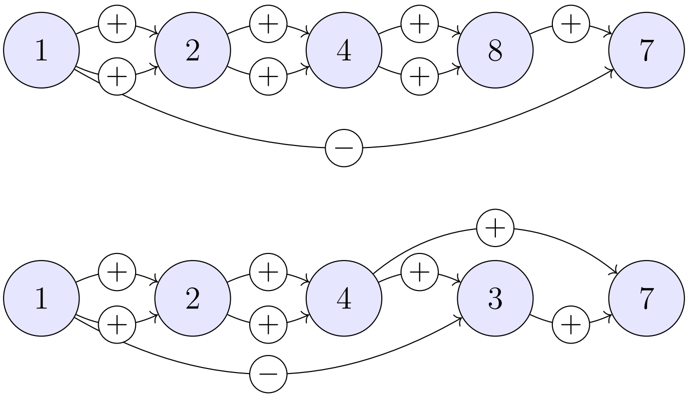

Figure 4: Two possible expansions of the reduced graph for 7. The represent the chains $1, 2, 4, 8, 7$ and $1, 2, 4, 3, 7$ respectively.

This process is not necessarily unique, but will result in two chains of the same length. By selecting a different pair of edges in the reduction process, two possible expansions exist for the graph in Figure 2, which are drawn in Figure 4.

Definition 3.6. A graph is called *reduced* or *fully reduced* when no further reductions can be made, i.e., no vertex has out degree of 1. Furthermore, we require that when expanded into an addition-subtraction chain it starts with one and contains no unused elements.

Note that an element is considered unused in an addition subtraction chain when it is not the last element and is not used in the creation of any subsequent elements. This means the chain cannot be optimal as we could simply remove this element.

The decreased size of E and V helps for optimization. However, this means the number of vertices no longer indicates the length of a chain. There is a quick alternative method to determine the length of the chain when expanded.

Proposition 3.7. *A reduced graph represents a chain containing* $|E| - |V| + 1$ *steps if it were to be fully expanded.*

Proof. In the original, fully expanded graph, we start with vertex v_1 and all subsequent vertices are a step, therefore, it contains $|V| - 1$ steps. Each step adds two edges so a separate representation is $|E|/2$ steps. Thus, if s represents the number of steps

$$s = |V| - 1 = |E|/2 \quad \Longrightarrow \quad s = 2(|E|/2) - (|V| - 1) = |E| - |V| + 1 \tag{18}$$

Each reduction step removes one edge and one vertex. Therefore, $|V'| = |V| - 1$ and $|E'| = |E| - 1$, which implies

$$|E'| - |V'| + 1 = (|E| - 1) - (|V| - 1) + 1 = |E| - |V| + 1 = s \tag{19}$$

as desired. Repeat by induction to show this property still holds with an arbitrary number of reductions. □

There is a simple alternative formulation to this

Corollary 3.8. *A reduced graph represents a chain containing*

$$1 + \sum_{v \in V} (\text{indeg}(v) - 1) \tag{20}$$

steps if it were to be fully expanded.

Proof. This can be expanded into

$$\begin{aligned} 1 + \sum_{v \in V} (\operatorname{indeg}(v) - 1) &= \sum_{v \in V} \operatorname{indeg}(v) - \sum_{v \in V} 1 \\ &= 1 + |E| - |V| \end{aligned}$$

which follows from Proposition 3.7. □

An alternative equation restricts the summand to the vertices other than the start, which would then exclude the +1 outside.

Of course, not every directed multigraph can properly represent an addition subtraction chain.

To simplify the following classification, we will use the generalized addition-subtraction chain moving forward. As shown in Proposition 2.2, no positive chain can use this.

Proposition 3.9. *A graph is reduced if and only if all of the following hold*

(1) It has no directed cycles.

(2) Contains a starting vertex v_0 with zero in degree and $p(v_0) = 1$.

(3) Contains an ending vertex v_n with zero out degree.

(4) All other in and out degrees are at least two.

(5) The equation in (16) *holds for all vertices except v_0.*

Proof. First, show the forward direction. The expanded graph formed from a chain must have a *topological order* derived from the original order of the chain elements. That is, we need to assign the vertices $v_0, v_1, \cdots, v_n$ such for any directed edge going from v_i to v_j, we must have $i < j$. This means the expanded graph cannot have cycles.[3] Any cycles in the reduced graph would remain after expansion as we simply add vertices in between existing paths, implying (1).

By simply taking the first and last elements from the chain, we find a vertex with zero in degree and zero out degree respectively. Note that reduction will not effect or create any vertices with zero in or out degree, which shows (2) and (3).

Assuming the graph is reduced, we cannot have more than one vertex with out degree zero. One such vertex would not be the final element in the chain, leading to it being unused. No vertex can have out degree 1 or it is not reduced by Definition 3.6. Likewise, every element in an addition-subtraction chain other than 1 is formed by two elements, so in the expanded graph they all have in degree 2. Reduction can only increase this. Together, these show (4) holds.

By Proposition 3.4 and by our initial construction, any reduced graph must adhere to the vertex equation aside from the starting vertex, showing (5).

Next, we show the converse. To do this, we create an addition subtraction chain from a graph with these five properties. First, expand on any vertex that has in degree greater than two. By repeating this process, we will create a graph where every vertex except v_0 has in degree 2 using (2) and (4). This process cannot create cycles, so using (1) we can

[3] If a graph with directed cycle $v_{i_1} \to v_{i_2} \to \cdots v_{i_k} \to v_{i_1}$ were to be topologically ordered, then by transitivity on the first $k-1$ edges, $i_1 < i_k$. But this would contradict the last edge.

assign a topological ordering to the resulting graph.[4] Then, simply starting from the first vertex, create the addition subtraction chain adhering to this order. The vertex equation from (5) can be used to determine whether each operation is addition, subtraction, or negated addition.

Finally, the chain will not have any unused elements. In our ordering, v_n must represent the last element as all other vertices have nonzero out degree by (3) and (4). Thus, if an element is not last in the chain it must be used later on. □

This proposition will become very important once we attempt to search for addition-subtraction chains. There are no restrictions on the edge weights. An example is demonstrated in Figure 5, creating the chain

$$1,\ 1+1=2,\ 1+2=3,\ 3+3=6,\ 6-2=4 \tag{21}$$

which is clearly not optimal as 4 can be contsructed with 2 steps.

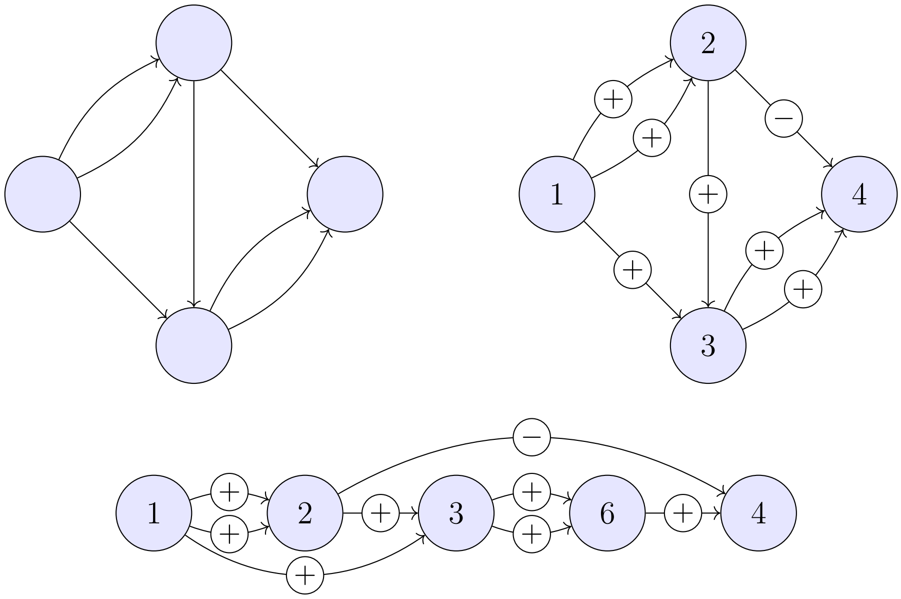

Figure 5: Creation of an addition-subtraction chain from a directed acyclic graph. First, ensure degree criteria are met. Then, assign weights to each of the edges and induce a topological order. Labeling the starting vertex 1, and follow the order to assign weights to each vertex according to the vertex equation (in this case, it is the same as the order). Finally, perform any expansions (in this case, on 4) and write out as a chain: 1,2,3,6,4.

This classification appears to be somewhat symmetric, which will give rise to the opposite graphs considered in Section 4. Some basic additional definitions are as follows.

Definition 3.10. The *target value* of a reduced graph is the value of the last vertex, $p(v_n)$.

Definition 3.11. An *optimal* graph is a reduced graph that when expanded produces an optimal addition-subtraction chain.

There is a simple alternative way to view this.

[4] One way for finite graphs is via Kahn's Algorithm [5]. All such directed acyclic graphs must have a node with zero indegree. Otherwise, starting from an arbitrary vertex, we could always move backwards to a new vertex, eventually exhausting all of the finite vertices and creating a cycle. Label this vertex 0, remove, and recurse on the remaining (acyclic) vertices. This also holds in the infinite case using the axiom of choice, see Szpilrajn extension theorem.

Proposition 3.12. *A reduced graph is optimal if and only if $|E| - |V| + 1$ is minimized over all reduced graphs with the same target value.*

Proof. If a reduced graph is optimal, then the number of steps when expanded is $|E| - |V| + 1$ by Proposition 3.7. This must be minimized, otherwise a graph with a smaller value could be expanded to produce an addition-subtraction chain with fewer steps. Likewise, as every chain can be represented as an reduced graph, if $|E| - |V| + 1$ is minimized the graph must represent an optimal addition-subtraction chain. □

4 Opposite graphs

Once a graph is reduced, we can actually reverse the edges to produce a separate graph that represents the same target value. In this manner, we can create a completely different addition-subtraction chain, as demonstrated in Figure 6. Other sources refer to this as a dual graph, [1] however, we will use the term opposite graph to prevent confusion with other concepts such as the planar dual.[5]

Definition 4.1. The *opposite* graph associated with a reduced graph can be formed by reversing all the edges, that is, create the new graph (V, E') with $\alpha(e') = \omega(e)$, $\omega(e') = \alpha(e)$, and $w(e') = w(e)$. Assign the last vertex value 1, $p(v_n) = 1$, and assign subsequent vertices using the vertex equation given in (16).

We will keep the vertices labeled according to their original order. An example is shown in Figure 6. This demonstrates the target value remains the same, which is proven in Theorem 4.6. Note the intermediate vertex are not necessarily preserved.

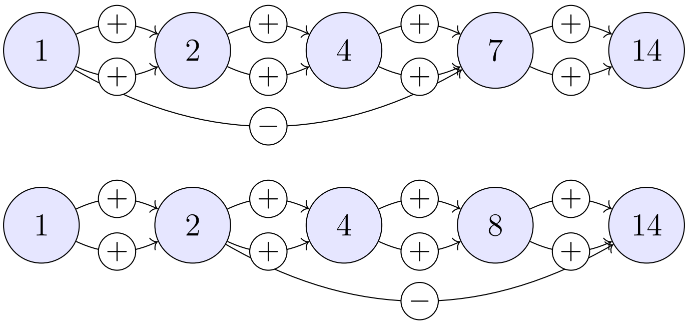

Figure 6: Opposite graph for a reduced graph with target value 14. Note the intermediate vales are different, and they create two separate addition-subtraction chains when expanded: 1,2,4,8,7,14 and 1,2,4,8,16,14 respectively. These are both optimal and additional variation exists when expanding the graphs.

Two important but trivial results are now shown.

Proposition 4.2. *The opposite of a reduced graph is still reduced.*

Proof. We will rely on the criterion described in Proposition 3.9. By contrapositive, if the opposite graph had a directed cycle, when we reduce the edges we would still have a

[5] As an interesting side note, there does exist nonplanar reduced graphs. For instance, take the complete graph K_5 (undirected) and arbitrarily assign a topological ordering. Then direct each edge according to this ordering, adding two additional parallel edges to ensure degree requirements are met. This produces an addition chain for 18 with a nonoptimal $12 - 5 + 1 = 8$ steps. (The optimal number is 5 steps)

cycle by simply going in the other direction. This means the original graph could not be reduced.

Upon switching the vertices, the in and out degrees of a vertex will switch. Therefore, v_n becomes the starting vertex and v_0 becomes the ending vertex. All other in and out degrees will remain no less than two. Simply by our definition, the vertex equation (16) will still hold aside from v_n.

□

By our construction, it follows trivially that the opposite of an opposite graph returns us to the original graph. Perhaps a more interesting result is that an opposite graph forms a potentially distinct chain with the same final element. To show this, we first need to present an alternative method for determining the target value.

Definition 4.3. A *target path* is a path from the starting vertex v_0 to the ending vertex v_n. This can be thought as a sequence of edges $e_1, \cdots, e_k$ such that $\alpha(e_1) = v_0$, $\omega(e_i) = \alpha(e_{i+1})$, and $\omega(e_k) = v_n$

Definition 4.4. The *weight* of a target path is the product of the ± 1 weights of all of the edges in the sequence.

In this case, weight are 1 and -1 corresponding to $+$ and $-$ on the figures. Additional weights are considered later in Section 8. Note we may have a trivial graph with just v_0. In this case, there is one target path which is empty and by convention will empty product of weights is 1.

Lemma 4.5. *The target value of a reduced graph is equal to the sum of the weights of all possible distinct target paths:*

$$p(v_n) = \sum_{(e_i)\in P} \left(\prod_i w(e_i) \right) \tag{22}$$

where P represents the set of all target path sequences.

Proof. Label the vertices $v_0, v_1, \cdots, v_n$ consistent with the topological order of a graph prescribed in Proposition 3.9. Consider the subgraph formed by just the vertices $v_0, v_1, \cdots, v_k$ and proceed by induction. Note this subgraph may not be reduced as the strict out degree requirements may not be met until more vertices are added. In any case, it still holds that $p(v_k)$ is equal to the weight sum of all target paths.

In the base step with a single vertex v_0, there is only the empty path which is consistent with $p(v_0) = 1$.

Now assume it holds up until v_k and show for v_{k+1} No path to v_i can contain v_j if $j > i$ by our ordering. Therefore, using strong induction $p(v_i)$ is equal to the weight sum of all paths from v_0 to v_i. The paths to v_{k+1} must consist of a path to a previous vertex and an inbound edge. Let $P(v_i)$ represent the collection of all paths from v_0 to v_i. Then

$$p(v_{k+1}) = \sum_{\substack{e\in E: \\ \omega(e)=v_{k+1}}} w(e) \cdot p(\alpha(e)) \tag{23}$$

$$= \sum_{\substack{e\in E: \\ \omega(e)=v_{k+1}}} w(e) \cdot \left(\sum_{(f_i)\in P(\alpha(e))} \left(\prod_i w(f_i) \right) \right) \tag{24}$$

$$= \sum_{\substack{e \in E: \\ \omega(e) = v_{k+1}}} \left(\sum_{(f_i) \in P(\alpha(e))} \left(w(e) \cdot \prod_i w(f_i) \right) \right) \tag{25}$$

$$= \sum_{(f_i) \in P(v_{k+1})} \left(\prod_i w(f_i) \right) \tag{26}$$

which completes the induction. □

Theorem 4.6. *The target value of a reduced graph remains unchanged in the opposite graph.*

Proof. Consider a path from v_n to v_0 in the opposite graph. Once all the edges are flipped, reverse this path to go from v_0 to v_n. This works in both directions, so a target path in the original graph has a clear bijective correspondence to target paths in the opposite graph.

$$p'(v_0) = \sum_{(e'_i) \in P'} \left(\prod_i w(e'_i) \right) = \sum_{(e_i) \in P} \left(\prod_i w(e_i) \right) = p(v_n) \tag{27}$$

The edge order is simply reversed, but the weights remain the same. □

This fact was presented without proof for addition chains in [1], and the included references don't appear to provide proof either. In that case, simply the number of paths may be used as all edges have weight 1.

Corollary 4.7. *The opposite graph corresponds to an addition subtraction chains with the same number of elements and final value as the original chain.*

Proof. By Proposition 3.7, the number of steps is $|E| - |V| + 1$. As we simply flip the edges, the number of vertices and edges will not change and therefore the number of steps. Using the prior theorem, this gives rise to two separate addition-subtraction chains with the same final element. □

Note that variation is also possible when expanding a reduced graph. Combined with the opposite, potentially an entire class of distinct optimal chains can be derived from just one.

5 Impossible structures

Some reduced graph constructions can easily be recognized as non optimal constructions, or can easily be arranged into alternative forms of the same length.

Proposition 5.1. *In any collection of parallel edges, all edges must have positive weight.*

Proof. If such an optimal reduced graph with parallel edges of differing sign existed, then we could choose to expand along these edges first. In the expansion, this would create a parallel edge pair consisting of a positive and negative edge. By the vertex equation given in (16), the value at the ending vertex would be zero. After converting this into a chain, this would violate (2.3).

Furthermore, if a parallel edge consisted of only negative signs, any expansion would require the existence of a double negative step. This represents negated addition, which isn't strictly allowed, and even if it were, it would violate the positivity condition as shown in (2.2).

The only remaining possibility is that a parallel edge consists of only positive weighted edges. □

Examples are shown in Figure 8. Attempts to expand on such parallel edges would result in nonpositive chain values.

The following is already known for addition chains, [1] and using proposition 5.1, this result should come naturally. However, the proof is rather simple.

Proposition 5.2. *No collection of parallel edges can have more than 3 edges.*

Proof. As shown in proposition 5.1, it follows that any vertices u, v connected with more than 3 edges must all be positive. Select 4 of these input edges and remove them. Add another vertex x and place two edges from u to x and two from x to v, all positive. Using the vertex equation, $p(x) = 2p(u)$ which contributes $4p(u)$ to v, the same as in the original construction.

This version has one more vertex while still obtaining all the same values, meaning $|E| - |V| + 1$ was not minimized. By proposition 3.7, this cannot represent an optimal chain. This proof is shown visually in Figure 7. □

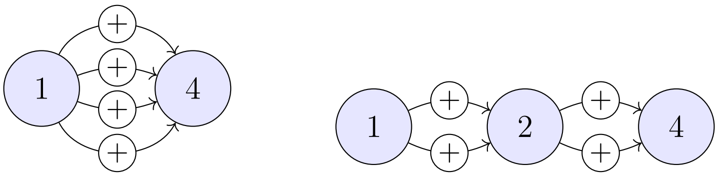

Figure 7: The left graph represents a chain with 3 steps: 1,2,2,4 when expanded, whereas the right graph represents a chain with just 2 steps: 1,2,4.

Examples of impossible parallel edge combinations are shown in Figure 8.

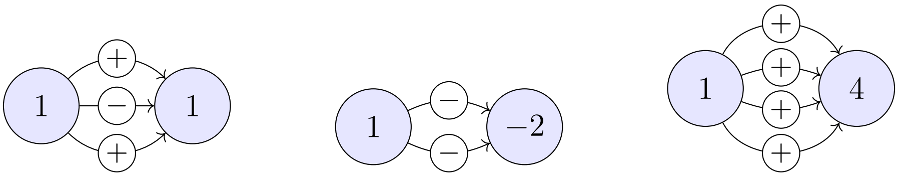

Figure 8: Impossible parallel edge combinations.

We will introduce a simple notation to assist with upcoming propositions.

Definition 5.3. Let the *multiplicity* between vertices a and b, denoted $m(a, b)$, be the number of distinct edges from a to b, regardless of weight. In symbols,

$$m(a, b) = |\{e \in E \mid \alpha(e) = a \text{ and } \omega(e) = b\}| \tag{28}$$

The following is another proposition already known for addition chains, which prevents the existence of multiple groups of parallel edges stemming from the same vertex [1]. As parallel edges are positive, the proof is more or less the same.

Proposition 5.4. *Given three distinct vertices $a, b, c \in V$, we must have $m(a, b) < 2$ or $m(a, c) < 2$.*

Proof. Assume the contrary, $m(a, b) \geq 2$ and $m(a, c) \geq 2$. By proposition 5.1, it follows that all involved edges are positive. Create an additional vertex d with only two incoming positive edges from a. Select 4 edges leaving a: two to b and two to c. Replace these with an edge d to b and d to c. Note that $p(d) = 2p(a)$, so via the vertex equation $p(b)$ and $p(c)$ will remain unchanged.

The total number of edges remains the same, however, we have added one vertex. This means $|E| - |V| + 1$ was not minimized. By proposition 3.12, this cannot represent an optimal chain. □

This can be extended using the opposite graph.

Corollary 5.5. *Given three distinct vertices $a, b, c \in V$, we must have $m(b, a) < 2$ or $m(c, a) < 2$.*

Proof. If $m(b, a) > 1$ and $m(c, a) > 1$, consider the opposite graph. When all edges are reversed, $m(a, b) > 1$ and $m(a, b) > 1$. By the prior proposition, this graph cannot be optimal. Construct a shorter chain from this graph, and by Corollary 4.7, the original chain cannot be optimal. □

An example of such impossible graphs are shown in Figure 9. These are viewed as subsets of a larger reduced graph. The right example speaks to the importance of opposite graphs, as there is no clear rearrangement to provide a more optimal chain.

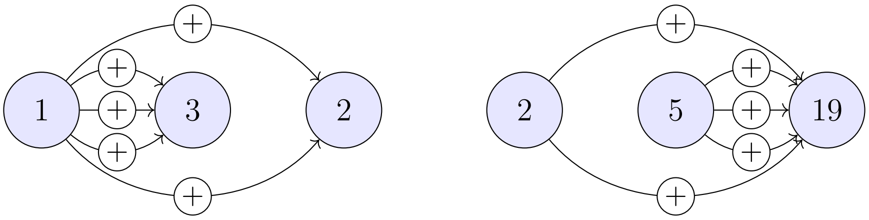

Figure 9: Impossible parallel edge combinations. In particular, the left represents Proposition 5.4 with values $1, 3, 2$ for vertices a, b, c respectively. The right represents Corollary 5 with values $2, 5, 19$ for c, b, a respectively.

6 Structure requirements

Rather than considering properties which immediately lead to nonoptimal addition-subtraction chains, we will now look at structures that must exist within the set of all optimal graphs for a given target value. First, we can adapt Theorem C from [1].

Proposition 6.1. *If the target value in an addition-subtraction chain is not a power of 2, then there must exist an optimal graph with* $\text{outdeg}(v_0) \geq 3$.

Proof. By Proposition 3.9, $\text{outdeg}(v_0) \geq 2$, so we consider the case when it is exactly 2. Let v_1 be the second vertex in our topological ordering. Again, $\text{indeg}(v_1) \geq 2$, but the edges can only come from prior vertices, in this case v_0. So if v_0 is to have out degree 2, they must both go to v_1. By Proposition 5.1 and the vertex equation 16, it follows that $p(v_1) = 2$. Furthermore, the vertex equation will also tell us $p(v_i)$ is even for all $i > 0$ as they cannot contain edges from v_0.

In this graph, we could simply move the doubling step to the end for an equivalent graph. Repeat this process inductively.

One of two things can happen: we eventually find a graph with $\text{outdeg}(v_0) \geq 3$, or $\text{outdeg}(v_i) = 2$ for all i. In the latter case, each added vertex v_{i+1} requires two input edges, but they can only come from v_i. By Proposition 5.1 and the vertex equation 16, it follows that $p(v_{i+1}) = 2p(v_i)$. This implies the target value is a power of two as $p(v_i) = 2^i$. □

Another, albeit more complex criterion can be implemented, analogous to [1, Thm. H].

Proposition 6.2. *Among all optimal reduced graphs for a particular target value, there exists a graph without this particular construction: a vertex with three or more input edges, with at least two parallel and the other stemming from a doubled vertex. A doubled vertex is one with only two input edges from the same source. This construction is depicted in Figure 10.*

Proof. Consider an optimal graph which contains this construction. For starters, both sets of parallel edges described must have all positive weights by Proposition 5.1. We use the vertex labeling as shown in Figure 10. From our construction, $p(b) = 2p(a)$. Rather than using b to form d, instead use an additional vertex e formed from a and c, and then double it into d.

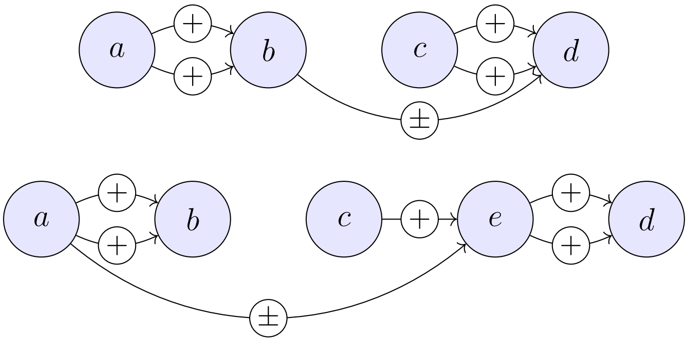

Figure 10: Rearrangement used in Proposition 6.2. With the exception of inward vertices on b, all other vertices may have additional inbound and outbound edges not shown to form a valid graph.

As shown in the figure, $p(e) = p(c) \pm p(a)$. The vertices shown contribute $2p(c) \pm 2p(b) = 2(p(c) \pm p(b)) = 2p(e)$ to vertex d. This is still the case under this rearrangement. Other inward edges to d remain unchanged, and therefore $p(d)$ does. All other inbound edges remain the same, and we do not delete any vertices so outbound edges can remain, showing this is a valid replacement. Importantly, this new graph also does not satisfy the construction, unless d has additional inbound edges from doubled vertices. In this case the process can be repeated.

Finally, this process adds one vertex and one edge, therefore the number of steps when expanded, $|E| - |V| + 1$, remains unchanged. By Proposition 3.12, this still represents an optimal chain. □

7 Algorithm

Using all the graph theoretic techniques discussed, we can now construct an algorithm to search for optimal reduced graphs, which can then be expanded back into optimal chains. To do this, start with a single vertex and add vertices recursively to increase the search space. We start by simply searching without any weights on the edges.

At each step, add all possible new vertices, however, we ensure they don't violate any of the aforementioned limitations on reduced graphs.

Once all graphs have been enumerated up to a certain length, then for each graph consider the possible weights of the non-parallel edges. In each case, recalculate the target value to determine if a new optimal graph is formed.

Some implementation work remains and additional work may be necessary to determine optimization parameters. For instance, in the addition chain case, limits were put on the in and out degrees based on the desired chain length. This algorithm would be capable of computing addition-subtraction chains to much higher values than previously obtained.

7.1 Preliminary results

I was able to compute optimal length chains and $\bar{\ell}(n)$ for all $n < 421$. This presents a list of 62 values where $\bar{\ell}(n) < \ell(n)$, a significant expansion on the existing OEIS A229624. I also present several values for which $\bar{\ell}(n) = \ell(n) - 2$, which are 127, 191, 254, 383. Note that $\ell(n) - \bar{\ell}(n)$ can be arbitrarily large, using the the bound

$$\log_2(n) + \log_2(h(n)) - 2.13 \leq \ell(n) \tag{29}$$

given in [11] with Hamming weight $h(n)$, the number of 1's in binary. It is rather straightforward to show that $\bar{\ell}(2^k - 1) = k + 1$ for $k > 2$, [7] therefore,

$$\begin{aligned} \ell(2^k - 1) - \bar{\ell}(2^k - 1) &\geq \log_2(2^k - 1) + \log_2(h(2^k - 1)) - 2.13 - k - 1 \qquad (30) \\ &\geq (k - 1) + \log_2(k) - 3 - k \\ &\geq \log_2(k) - 5 \qquad (31) \end{aligned}$$

which is unbounded. There are a significant amount of results and conjectures about addition chains that could be modified for addition-subtraction chains.

8 Complex generalizations

Much of what is devoted in this paper could apply to weights other than just -1 and 1.

Definition 8.1. A *weighted addition chain* is a sequence $a_0, a_1, \cdots a_m$ combined with a set of weights W such that for all $0 < k \leq m$, there exists $0 \leq i, j < k$ and $w_1, w_2 \in W$ with

$$a_k = w_1 a_i + w_2 a_j \tag{32}$$

We will primarily consider W to lie in $\mathbb{C}$, but it theory it could lie in any commutative ring with unity. In the reduction step from Definition 3.6, new edges are assigned the product of two existing weights. This means that our weight set should ideally be closed under multiplication. This limits or choices for a finite weight set.

Proposition 8.2. *If W is finite and closed under multiplication, then for all $w \in W$, the complex modulus $|w| \in \{0, 1\}$.*

Proof. Assume there exists a $|w| \notin \{0, 1\}$. If $|w| > 1$, then $w^n \in W$ and $|w^n| = |w|^n$ is unbounded for positive integer n. This means W cannot be finite. Likewise, if $0 < |w| < 1$, then $|w^n|^{-1} = |w|^{-n}$ is also unbounded and again W infinite. □

For now, consider $0 \notin W$. Over $\mathbb{R}$, the only such sets are

$$\{1\}, \qquad \{-1, 1\} \tag{33}$$

Proposition 8.3. *In $\mathbb{C}$, the possible finite weight sets are given with*

$$W \setminus \{0\} = \left\{ e^{2\pi i k/n} \mid k \in \mathbb{Z} \cap [0, n) \right\} \tag{34}$$

the complex roots of unity for $n \in Z_{\geq 0}$.

Proof. If $W \setminus \{0\}$ is empty, we obtain the trivial case $n = 0$. Otherwise, it must contain an element magnitude 1. Consider its argument divided by 2π. If this is irrational, we immediately get an infinite set. If it is rational, we obtain the roots of unity for the denominator in reduced form. Combining multiple rationals will yield the lowest common denominator. □

Definition 8.4. Denote the optimal weighted addition chain length for a given complex number z under a weight set W by $\ell_W(z)$. As before, this means $a_0 = 1$ and $a_m = z$ and m is minimized over all such chains. This remains undefined if z lies outside the possible values for such a chain.

Definition 8.5. Denote the n-th root of unity by

$$\zeta_n = e^{2\pi i/n} \tag{35}$$

These all have the following property.

Proposition 8.6. *Excluding z lying on the unit circle itself, $\ell_W(z)$ is n-fold rotational symmetric, where n corresponds to the root of unity used. That is, if $|z| \neq 1$ then*

$$\ell_W(z) = \ell_W(\zeta_n^k z). \tag{36}$$

for integer $0 \leq k < n$.

Proof. Let $1 = a_0, a_1, \cdots a_m = z$ be an optimal chain for z. Provided $|z| \neq 1$, we must have $m > 0$. This means $z = w_1 a_i + w_2 a_j$ for some $0 \leq i, j < k$ and $w_1, w_2 \in W$ by Definition 8.1. Given W is closed under multiplication, we could also choose the last step

$$\zeta_n^k z = w_1' a_i + w_2' a_j, \qquad w_1' = \zeta_n^k w_1,\ w_2' = \zeta_n^k w_2 \tag{37}$$

which yields a chain of the same length for ζ_n, implying $\ell_W(z) \geq \ell_W(\zeta_n^k z)$. Doing the same in reverse, $|\zeta_n^k z| = |z| \neq 1$, so let $\zeta_n^k z = w_1 b_i + w_2 b_j$ for some $0 \leq i, j < k$ and $w_1, w_2 \in W$

$$z = w_1' b_i + w_2' b_j, \qquad w_1' = \zeta_n^{n-k} w_1,\ w_2' = \zeta_n^{n-k} w_2 \tag{38}$$

showing $\ell_W(z) \leq \ell_W(\zeta_n^k z)$ and together $\ell_W(z) = \ell_W(\zeta_n^k z)$. □

This allows us to remove the ambiguity around $0 \in W$.

Proposition 8.7. *For $|z| > 1$ and $W \neq \{0\}$,*

$$\ell_{W \setminus \{0\}}(z) = \ell_W(z) \tag{39}$$

Proof. As $W \setminus \{0\}$ is a subset of W, every chain in the former is still a chain in the latter so

$$\ell_{W \setminus \{0\}}(z) \leq \ell_W(z) \tag{40}$$

If this inequality is strict, we would have a chain for z that requires use of a zero weight. Consider a step with $a_k = w_1 a_i + w_2 a_j$. If $w_2 = 0$, then this simply amounts to rotation of a_i. This step can then be removed by replacing all subsequent uses of a_k with $w_1 a_k$ and updating the weights.

If this is the final step, we know it is unnecessary by Proposition 8.6. Likewise, if both weights are zero then $a_k = 0$. This is only helpful when $z = 0$, otherwise any subsequent uses are also just rotations. Therefore, no chain necessitates the use of a zero weight and equality holds. □

Using this, it makes sense to consider W to be the only the roots of unity.

Definition 8.8. Let $\ell_n(z) = \ell_W(z)$ where

$$W = \left\{ e^{2\pi i k/n} \mid k \in \mathbb{Z} \cap [0, n) \right\} \tag{41}$$

Two cases we have already considered, $\ell_1(z) = \ell(z)$ is simply addition chains. Next, $\ell_2(z) = \bar{\ell}(z)$ for positive z as it amounts to addition-subtraction chains. It also allows for negated sums which means it is a generalized addition-subtraction chain. By Proposition 2.3, this is the same for positive z. Of course $\ell_1(z)$ has a domain of $\mathbb{Z}^+$ and $\ell_2(z)$ has domain $\mathbb{Z}$.

8.1 Gaussian integer case

A simple interesting example is $n = 4$ with

$$W = \{1, i, -1, -i\} \tag{42}$$

which can be thought as the simplest complex variant of addition chains. In this case, elements of the chain are Gaussian integers.

Proposition 8.9. *The domain of $\ell_4(z)$ is given by the Gaussian integers. That is, $z = a + bi$ for some $a, b \in \mathbb{Z}$.*

Proof. First, all Gaussian integers are obtainable through a chain. Using addition and subtraction, create subchains for integers a and b. Then, combine in a single step for $a + bi$.

Gaussian integers form a commutative ring, and therefore any new element $w_1 a_i + w_2 a_j$ will still be a Gaussian integer. This means no other complex numbers will be obtainable through a chain. □

We have not yet any counterexamples to $\ell_2(n) = \ell_4(n)$ over the real integers, although it is expected $\ell_4(n) < \ell_2(n)$ is a possibility. Given the very large search space, I was only able to compute 6 steps which yields no variation from $\ell_2(n)$, and only for all integers $n < 29$. Results for various nonreal values are depicted in Figure 11.

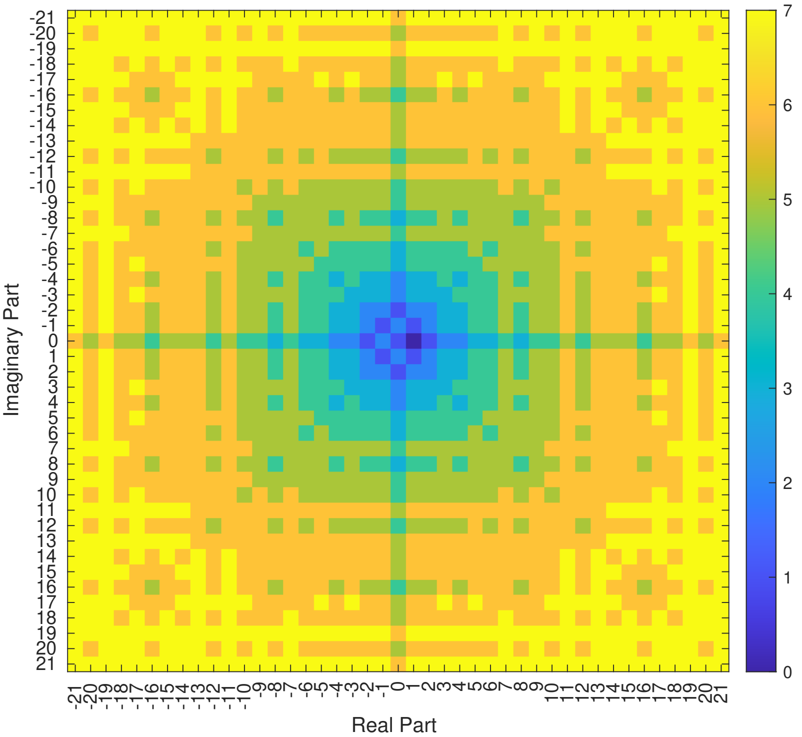

Figure 11: Optimal Gaussian integer weighted addition chain length depicted via coloring the complex plane. Zero weights were not allowed resulting in minor differences at the center (i takes 2 steps not 1).

It's likely any variation would require large n as no alternative optimal chains were found that used a complex number that wasn't either pure real or pure imaginary.

8.2 Eisenstein integers case

As mentioned earlier, other complex variants with a finite weight set must be complex roots of unity. Aside from the cases of 1 (addition), 2 (addition-subtraction), 4 (Gaussian integer), there are two other special cases worthy of consideration: 3 and 6. These both lie over the Eisenstein integers, which form a hexagonal lattice of the complex plane. All remaining cases have a dense domain in $\mathbb{C}$, as shown in Section 8.3.

Proposition 8.10. *The domains of $\ell_3(z)$ and $\ell_6(z)$ are the Eisenstein integers. That is,*

$$a + b\omega, \qquad \omega = e^{2\pi i/3} \tag{43}$$

for integers a, b.

Proof. First, note that all Eisenstein integers are obtainable through a chain. Using addition and subtraction on the integers, obtain a and b. When $n = 3$, -1 is not a weight but it can be quickly obtained with $\omega(1) + \omega^2(1) = -1$.

All six root of unity are Eisenstein, and as Eisenstein integers form a commutative ring (closed under multiplication and addition), then any new element in a chain will still be Eisenstein. This means no other complex numbers will be obtainable through a chain. □

An example when $n = 3$ gives the interesting pattern on the hexagonal lattice given in Figure 12. As expected, it has three-way radial symmetry with the shortest chains lying along the three roots of unity used as weights. I again was only able to compute 6 steps, but this was enough to find a peculiarity: 31 takes seven steps, aligned with $\ell_1(31)$ and not $\ell_2(31)$. While we can get a subtraction, it takes both nonreal weights together using an extra step.

While I haven't exhausted optimality, I'm conjecturing the first positive n such that $\ell_3(n) < \ell_1(n)$ is 127:

$$1, 2, 4, 8, 16, 32, 64, 128, 128 + \omega, (128 + \omega) + \omega^2 \cdot 1 = 127 \tag{44}$$

which takes 9 steps in contrast to $\ell_1(127) = 10$ and $\ell_2(127) = 8$.

8.3 Other cases

All the remaining possible finite weight sets create an interesting set of values that would be harder to examine computationally. This needs a basic Galois theory result:

Lemma 8.11. *For integer $n = 5$ or $n > 6$*

$$\cos\left(\frac{2\pi}{n}\right) \tag{45}$$

is irrational.

Proof. Let $\zeta_n = e^{2\pi i/n}$ and take automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Then,

$$\sigma\left(\cos\left(\frac{2\pi}{n}\right)\right) = \sigma\left(\frac{\zeta_n + \zeta_n^{-1}}{2}\right) = \frac{\zeta_n^j + \zeta_n^{-j}}{2} = \cos\left(\frac{2\pi j}{n}\right) \tag{46}$$

for some $0 \leq j < n$. By the definition of cosine, this can only occur with $j = 1, n-1$, and it can be fixed by at most two automorphisms. If it were rational, it would be fixed by every automorphism, meaning

$$|\,\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \varphi(n) \leq 2 \tag{47}$$

which by inspection is only satisfied by $1, 2, 3, 4, 6$. Note that $\varphi(n) \geq \sqrt{n/2}$ means it is not necessary to check values larger than 8. □

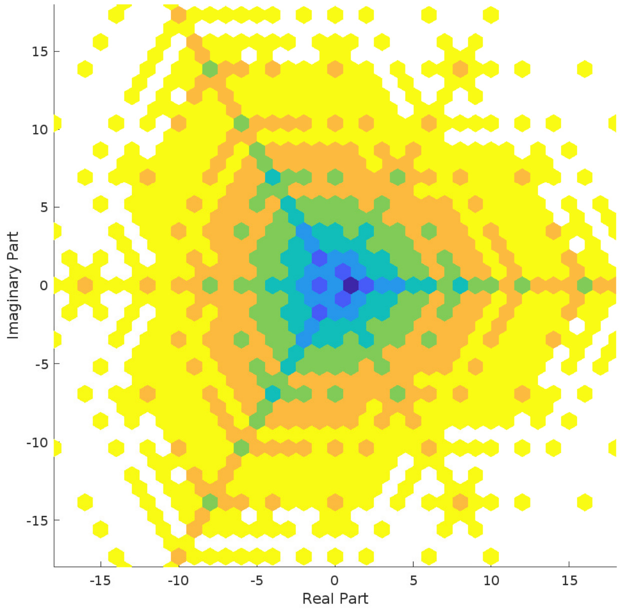

Figure 12: Optimal Eisenstein integer generalized addition chain length depicted via coloring the complex plane. Only the three weights $1, \omega, \omega^2$ were used to simplify the search space compared to all 6. This also yields an interesting triangular symmetry, and is the only case that is not symmetric around the imaginary axis other than $n = 1$.

This proof was based on [10].

Proposition 8.12. *The domains of $\ell_5(z)$ and $\ell_n(z)$ for $n > 6$ are dense in $\mathbb{C}$.*

Proof. Label $\zeta_n = e^{2\pi i/n}$. First, create the element -1, assuming $n > 1$. If n is even, this is given by $\zeta_n^{n/2}$. Otherwise, the sum of all roots of unity is zero, meaning we can sum all roots other than 1. This can be done iteratively in the chain

$$(\zeta_n \cdot 1 + \zeta_n^2 \cdot 1) \cdot 1 + \zeta_n^3 \cdots \tag{48}$$

to obtain -1. From this, we can easily expand to all integers through repeated addition. Next, consider

$$\zeta_n \cdot 1 + \zeta_n^{n-1} \cdot 1 = \zeta_n + \overline{\zeta_n} = 2\cos\left(\frac{2\pi}{n}\right) = \alpha, \tag{49}$$

which is irrational for $n = 5$ and $n > 6$ using Lemma 8.11. Using the Dirichlet approximation theorem, there exist p, q integers such that $|q\alpha - p|$ is arbitrarily small. We can obtain $q\alpha$ by repeated addition if positive. If negative, multiply by all roots of unity and sum to obtain $-\alpha$ and use repeated addition again.

Given that α is irrational, $|q\alpha - p|$ can never be zero. This allows us to approximate any value in $\mathbb{R}$ to arbitary precision. If $0 < |q\alpha - p| < \varepsilon$, repeated summation will get us within ε of any $r \in \mathbb{R}$.

Finally, as ζ_n and 1 are linearly independent, for all $z \in \mathbb{C}$ there exists $r, s \in \mathbb{R}$ such that $z = r\zeta_n + s$. By approximating r and s arbitrarily close in this manner, we can approximate z arbitrarily close.

Despite the fact these chains may be obscenely long, this shows the possible values are dense in $\mathbb{C}$. □

These can still create more optimal chains than addition alone. When n is odd, combining the roots to subtract may become faster than addition on $2^k - 1$ for sufficiently large k.

References

[1] N. M. Clift. Calculating optimal addition chains. *Springer Computing*, 91:265–284, 2011.

[2] P. Erdős. Remarks on number theory. iii: On addition chains. *Acta Arithmetica*, 6(1):77–81, 1960.

[3] A. Flammenkamp. Shortest addition chains. `https://wwwhomes.uni-bielefeld.de/achim/addition_chain.html`, 2024. Accessed: 2024-10-25.

[4] D. M. Gordon. A survey of fast exponentiation methods. *Journal of Algorithms*, 27(1):129–146, 1998.

[5] A. B. Kahn. Topological sorting of large networks. *Commun. ACM*, 5:558–562, 1962.

[6] D. E. Knuth. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*. Addison-Wesley, 1st edition, 1969.

[7] D. Moody and A. Tall. On addition-subtraction chains of numbers with low hamming weight. *Notes on Number Theory and Discrete Mathematics*, 25(2):155–168, 2019.

[8] F. Morain and J. Olivos. Speeding up the computations on an elliptic curve using addition-subtraction chains. *Informatique théorique et applications*, 24(6):531–543, 1990.

[9] OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences, 2024. Published electronically at `http://oeis.org`.

[10] W. Ong. When is cos(2*pi/n) rational? `https://wilsonong.wordpress.com/2010/06/25/when-is-cos2pin-irrational/`, 2024. Accessed: 2024-12-12.

[11] A. Schönhage. A lower bound for the length of addition chains. *Theoretical Computer Science*, 1(1):1–12, 1975.

[12] H. Volger. Some results on addition/subtraction chains. *Information Processing Letters*, 20(3):155–160, 1985.