Doctopic: Algorithms, automata, complexity and games ARTICLE IN PRESS TCS:11405

Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Internal structure of addition chains: Well-ordering

Harry Altman

ARTICLE INFO

Article history:
Received 7 May 2017
Received in revised form 28 September 2017
Accepted 5 December 2017
Available online xxxx
Communicated by L.M. Kirousis

Keywords:
Addition chains
Well-ordering

ABSTRACT

An *addition chain* for n is defined to be a sequence $(a_0, a_1, \dots, a_r)$ such that $a_0 = 1$, $a_r = n$, and, for any $1 \le k \le r$, there exist $0 \le i, j < k$ such that $a_k = a_i + a_j$; the number r is called the length of the addition chain. The shortest length among addition chains for n, called the addition chain length of n, is denoted $\ell(n)$. The number $\ell(n)$ is always at least $\log_2 n$; in this paper we consider the difference $\delta^\ell(n) := \ell(n) - \log_2 n$, which we call the addition chain defect. First we use this notion to show that for any n, there exists K such that for any $k \ge K$, we have $\ell(2^k n) = \ell(2^K n) + (k - K)$. The main result is that the set of values of δ^ℓ is a well-ordered subset of $[0, \infty)$, with order type ω^ω. The results obtained here are analogous to the results for integer complexity obtained in [1] and [3]. We also prove similar well-ordering results for restricted forms of addition chain length, such as star chain length and Hansen chain length.

1. Introduction

An *addition chain* for n is defined to be a sequence $(a_0, a_1, \dots, a_r)$ such that $a_0 = 1$, $a_r = n$, and, for any $1 \le k \le r$, there exist $0 \le i, j < k$ such that $a_k = a_i + a_j$; the number r is called the length of the addition chain. The shortest length among addition chains for n, called the *addition chain length* of n, is denoted $\ell(n)$. Addition chains were introduced in 1894 by H. Dellac [14] and reintroduced in 1937 by A. Scholz [21], who raised a series of questions about them. They have been much studied in the context of computation of powers, since an addition chain for n of length r allows one to compute x^n from x using r multiplications. Extensive surveys on the topic can be found in Knuth [18, Section 4.6.3] and Subbarao [26].

Addition chain length is approximately logarithmic; it satisfies the bounds

$$\log_2 n \le \ell(n) \le \lfloor \log_2 n \rfloor + \nu_2(n) - 1,$$

in which $\nu_2(n)$ counts the number of 1's in the binary expansion of n. A. Brauer [6] proved in 1939 that $\ell(n) \sim \log_2 n$.

The addition chain length function $\ell(n)$ seems complicated and hard to compute. An outstanding open problem about it is the *Scholz–Brauer conjecture* [21, Question 3], which asserts that

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

To investigate it Brauer [6] introduced a restricted type of addition chain called a *star chain*, and later authors introduced other restricted types of addition chains, such as *Hansen chains*, discussed in Section 1.3. Later Knuth [18] introduced the quantity $s(n) := \ell(n) - \lfloor \log_2 n \rfloor$, which he called the number of *small steps* of n. This notion was subsequently used by other authors [15,23,25] investigating the general behavior of $\ell(n)$ and the Scholz–Brauer conjecture. The Scholz–Brauer conjecture has been verified to hold for $n < 5784689$, by computations of Clift [9].

E-mail address: haltman@umich.edu.

https://doi.org/10.1016/j.tcs.2017.12.002
0304-3975/

Please cite this article in press as: H. Altman, Internal structure of addition chains: Well-ordering, Theoret. Comput. Sci. (2018), https://doi.org/10.1016/j.tcs.2017.12.002

In this paper we introduce and study a function of addition chain length related to small steps, where instead of rounding we subtract off the exact logarithm $\log_2 n$.

Definition 1.1. The *addition chain defect* $\delta^\ell(n)$ of n is

$$\delta^\ell(n) := \ell(n) - \log_2 n.$$

This quantity is related to the number of small steps of n by the equation

$$s(n) = \lceil \delta^\ell(n) \rceil.$$

The lower bound result above shows that

$$\delta^\ell(n) \geq 0,$$

with equality holding for $n = 2^k$ for $k \geq 0$. In a sense, $\delta^\ell(n)$ encodes the "hard part" of computing $\ell(n)$; $\log_2 n$ is an easy-to-compute approximation to $\ell(n)$, and $\delta^\ell(n)$ is the extra little bit that is not so easy to compute. The object of this paper is to show that the addition chain defect encodes a subtle structural regularity of the addition chain length function.

1.1. Main results

The main results of the paper concern the structure of the set of all addition chain defect values.

Definition 1.2. We define $\mathscr{D}^\ell$ to be the set of all addition chain defect values:

$$\mathscr{D}^\ell = \{\delta^\ell(n) : n \in \mathbb{N}\}.$$

The main result of this paper is the following well-ordering theorem.

Theorem 1.3. (ℓ-defect well-ordering theorem) *The set $\mathscr{D}^\ell$ is a well-ordered subset of $\mathbb{R}$, of order type ω^ω.*

This theorem may at first appear to come out of nowhere, but we will discuss why it is true in Section 1.2.

A second result is related to the determination of the set of integers having a given value α of the addition chain defect. We will show that If $\delta^\ell(n_1) = \delta^\ell(n_2) = \alpha$ with $n_1 \neq n_2$ then it is necessary (but not always sufficient) that $n_1 = 2^k n_2$ for some (positive or negative) integer k.

It is always the case that $\ell(2n) \leq \ell(n) + 1$, and the equality $\ell(2n) = \ell(n) + 1$ corresponds to $\delta^\ell(2n) = \delta^\ell(n)$. One might hope that this equality always holds, but this is not the case; the smallest counterexample is $n = 191$, with $\ell(382) = 11 = \ell(191)$. In fact, a theorem of Thurber provides infinitely many such examples [25]. So in fact for infinitely many n it occurs that $\delta^\ell(2n) < \delta^\ell(n)$. However we'll see here that infinitely many n do satisfy $\delta^\ell(2n) = \delta^\ell(n)$, which is part of a more general stabilization phenomenon.

Definition 1.4. A number m is called *ℓ-stable* if

$$\ell(2^k m) = \ell(m) + k, \quad \text{for all} \quad k \geq 0.$$

Otherwise it is called *ℓ-unstable*.

Using the defect, we will prove:

Theorem 1.5. (ℓ-stability theorem) *We have:*

(1) *If α is a value of δ^ℓ, and*

$$S(\alpha) := \{m : \ \delta^\ell(m) = \alpha\}$$

then there is a unique integer n such that $S(\alpha)$ has either the form $\{n \cdot 2^k : 0 \leq k \leq K\}$ for some finite K or else the form $\{n \cdot 2^k : k \geq 0\}$. The integer n will be called the leader *of* $S(\alpha)$.

(2) *The set $S(\alpha)$ is infinite if and only if α is the smallest defect occurring among all defects $\delta^\ell(2^k n)$ for $k \geq 0$, where n is the leader of $S(\alpha)$.*

(3) *For a fixed odd integer n, the sequence $\{\delta^\ell(n \cdot 2^k) : k \geq 0\}$ is non-increasing. This sequence takes on finitely many values, all differing by integers, culminating in a smallest value α such that if $\delta^\ell(m) = \alpha$ and $k \geq 0$, then*

$$\ell(m \cdot 2^k) = \ell(m) + k.$$

Please cite this article in press as: H. Altman, Internal structure of addition chains: Well-ordering, Theoret. Comput. Sci. (2018), https://doi.org/10.1016/j.tcs.2017.12.002