Theoretical Computer Science 1 (1975) 1–12.

A LOWER BOUND FOR THE LENGTH OF ADDITION CHAINS

Arnold SCHÖNHAGE

University Mathematics Institute, Tübingen, German Federal Republic

Communicated by M. Nivat
Received November 1973

Abstract. The length l of addition chains for z is shown to be bounded from below by $\log_2 z + \log_2 s(z) - 2.13$, where $s(z)$ denotes the sum of the digits in the binary expansion of z. The proof given here will also hold for addition-subtraction chains if $s(z)$ is replaced by an appropriate substitute. At first the proof is presented in a simplified version yielding the slightly weaker result $l \geqslant \log_2 z + \log_2 s(z) - O(\log\log s(z))$.

1. The problem of computing x^z from x by few multiplications gives rise to a consideration of so-called *addition chains*

$$\begin{cases} 1 = a_0, a_1, a_2, \ldots, a_l = z, \\ a_i = a_{m_i} + a_{p_i} \quad \text{with} \quad m_i, p_i < i \text{ for } 1 \leqslant i \leqslant l. \end{cases} \tag{1}$$

If for the evaluation of x^z divisions are also admitted, then we have more generally $a_i = \pm a_{m_i} \pm a_{p_i}$, the choice of the signs depending on i. Without restriction also in such *addition-subtraction chains* the a_i's are assumed to be positive and different from each other.

By induction on i the inequality $a_i \leqslant 2^i$ is obtained, which yields the lower bound

$$l \geqslant \log_2 z, \tag{2}$$

which can be attained for $z = 2^l$. Improvements, therefore, are possible only by exploitation of further properties of z. In this sense we consider the binary expansion

$$z = \sum_\nu \zeta_\nu 2^\nu \qquad (\zeta_\nu \in \{0, 1\})$$

and, with regard to addition chains especially, the *sum of the digits*

$$s(z) = \sum_\nu \zeta_\nu. \tag{3}$$

An improvement of (2) based upon $s(z)$ is obtained in the following way: In (1) we distinguish *large* and *small* steps, namely

$$G = \{i | m_i = p_i = i-1\}, \qquad K = \{i | m_i < i-1 \text{ or } p_i < i-1\} \tag{4}$$

with the cardinalities $g = |G|$, $k = |K|$, hence $l = g+k$. Since the large steps do not change the maximal sum of the digits reached so far, and each of the small steps, by reason of

$$s(x+y) \leqslant s(x)+s(y), \tag{5}$$

can at most double it, we have $k \geqslant \log_2 s(z)$.

If we recursively define $A_0 = 1$,

$$A_i = \begin{cases} 2A_{i-1} & \text{for } i \in G, \\ \gamma A_{i-1} & \text{for } i \in K, \end{cases} \tag{6}$$

where $\gamma = \frac{1}{2}(1+\sqrt{5})$ denotes the positive solution of $1+\gamma = \gamma^2$, then we can show by induction that $a_j \leqslant A_i$ for $j \leqslant i$. This implies

$$z = a_l \leqslant A_l = 2^g \gamma^k, \qquad g+k \log_2 \gamma \geqslant \log_2 z,$$

and, by means of $1-\log_2 \gamma = \log_2(\sqrt{5}-1) = 0.30\ldots$, finally

$$l = g+k \geqslant \log_2 z+0.3k \geqslant \log_2 z+0.3 \log_2 s(z). \tag{7}$$

This result will hold also for addition-subtraction chains if $s(z)$ is replaced by

$$\bar{s}(z) = \min\Big\{\sum_\nu |\bar{\zeta}_\nu| \,\Big|\, z = \sum_\nu \bar{\zeta}_\nu 2^\nu, \quad \bar{\zeta}_\nu \in \{-1, 0, 1\}\Big\}. \tag{8}$$

As a good approximation, the number of changes from $\zeta_\nu = 1$ to $\zeta_{\nu+1} = 0$ in the binary expansion of z lies between $\frac{1}{2}\bar{s}(z)$ and $\bar{s}(z)$. Special numbers $z = 2^{2^n}-1$ show how improvements of (7) are limited: we have $s(z) = 2^n$, and there are addition chains for z of length

$$l = 2^n+n-1 \approx \log_2 z+\log_2 s(z)-1,$$

e.g. 1, 2, 3, 5, 10, 15 ($n = 2$, $l = 5$).

Our main result is the lower bound

$$l \geqslant \log_2 z+\log_2 s(z)-2.13 \tag{9}$$

for the length of addition chains, which again remains true for addition-subtraction chains with $\bar{s}(z)$ instead of $s(z)$. The proof, however, is rather complicated. Therefore, after the explanation of some technical tools, we will first give a simplified presentation which, by modification of the proof of (7), will show the basic idea more clearly, yielding the slightly weaker estimate

$$l \geqslant \log_2 z+\log_2 s(z)-O(\log\log s(z)). \tag{10}$$

For reference, we mention Brauer's and Erdös's results [1, 2] and the extensive treatment of addition chains in Knuth's book [3], particularly Exercise 29. According to a private communication, A. Cotrell (Berkeley) has a proof of $l \geqslant \log_2 z+\log_3 s(z)-1$.

The author is indebted to V. Strassen for the first hints at taking the present subject and helpful discussions.

2. For binary numbers $x = \sum_\nu \xi_\nu 2^\nu$ and finite subsets $P \subseteq \mathbf{Z}$ we define

$$x \text{ in } P \Leftrightarrow \bigwedge_\nu (\xi_\nu = 1 \Rightarrow \nu \in P).$$

Maximal nonempty subsets $Q \subseteq P$ with the property

$$(u < v < w \wedge u, w \in Q) \Rightarrow v \in Q$$

are called *components* of P, and with regard to the partition into components $P = \dot{\bigcup}_j Q_j$ the *width* of P is $\beta(P) = \min_j |Q_j|$.

For $d \in \mathbf{N}$ we define *extensions* E_d by

$$E_d P = P \cup (P-1) \cup \ldots \cup (P-d), \quad \text{where } P+t = \{n+t \mid n \in P\}.$$

Lemma 1. *$\beta(P) \geqslant b$ implies that $\beta(E_d P) \geqslant b+d$ and*

$$\frac{|E_d P|}{b+d} \leqslant \frac{|P|}{b}. \tag{11}$$

Proof. The proof is based upon the partition into components $P = \dot{\bigcup}_j Q_j$. Because $E_d P = \dot{\bigcup}_j E_d Q_j$ each component of $E_d P$ contains an $E_d Q_j$, hence

$$\beta(E_d P) \geqslant \min_j |E_d Q_j| = \min_j (|Q_j|+d) = \beta(P)+d \geqslant b+d.$$

The inequality (11) follows from

$$|E_d P| \leqslant \sum_j |E_d Q_j| = \sum_j (|Q_j|+d)$$

$$= \sum_j |Q_j| \left(1 + \frac{d}{|Q_j|}\right) \leqslant \sum_j |Q_j| \left(1 + \frac{d}{b}\right) = |P| \frac{b+d}{b}.$$

In view of the addition of binary numbers we define an operation ∇ for finite subsets $P, R \subseteq \mathbf{Z}$ such that $P \nabla R$ shall denote the minimal set with the property

$$x \text{ in } P \wedge y \text{ in } R \Rightarrow x+y \text{ in } P \nabla R \quad \text{for arbitrary } x, y. \tag{12}$$

If $Q_1, Q_2, \ldots$ denote the components of $P \cup R$ and

$$Q_j' = \begin{cases} Q_j \cup (Q_j+1) & \text{if } Q_j \cap P \cap R \neq \emptyset, \\ Q_j & \text{otherwise,} \end{cases} \tag{13}$$

then we have $P \nabla R = \bigcup_j Q_j'$, i.e. extra bit positions for carries are necessary only where P and R overlap. From that we conclude

$$\beta(P \nabla R) \geqslant \beta(P), \beta(R), \tag{14}$$

$$|P \nabla R| \leqslant |P|+|R|. \tag{15}$$

For the discussion of addition-subtraction chains we shall use the modified definition

$$x \underline{\text{in}}\ P \Leftrightarrow \text{there exist } \bar{\xi}_\nu \in \{-1, 0, 1\} \text{ such that}$$
$$x = \sum_\nu \bar{\xi}_\nu 2^\nu \text{ and } \bigwedge_\nu (\bar{\xi}_\nu \neq 0 \Rightarrow \nu \in P),$$

and (12) can then be replaced by

$$x \underline{\text{ in }} P \wedge y \underline{\text{ in }} R \Rightarrow \pm x \pm y \underline{\text{ in }} P \nabla R. \tag{12'}$$

3. In this section we shall prove inequality (10) for addition chains. Possibly there may be some arbitrariness of succession in (1) which is eliminated by imposing the conditions

$$1 = a_0 < a_1 < a_2 < \ldots < a_l = z, \qquad m_i \leqslant p_i < i \qquad \text{for } 1 \leqslant i \leqslant l.$$

According to the distinction in (4), we recursively define *ranks*

$$r_0 = 0, \qquad r_i = \begin{cases} r_{i-1}+1 & \text{for } i \in G, \\ r_{i-1} & \text{for } i \in K, \end{cases} \tag{16}$$

which register the shifts of the binary expansion caused by doubling steps. From $r_{m_i} \leqslant r_{p_i}$ and

$$j < i \wedge \delta = r_i - r_j \Rightarrow a_j \leqslant 2^{-\delta} a_i \tag{17}$$

we obtain $r_{p_i} = r_{i-1}$. The difference $d_i = r_{i-1} - r_{m_i}$ approximately measures how far the binary expansion of a_{p_i} is shifted away from that of a_{m_i}.

With regard to a number $d \geqslant 1$ which will be chosen appropriately later on, we subdivide $K = K_1 \cup K_2$, where

$$K_1 = \{i \in K | d_i < d\}, \qquad K_2 = \{i \in K | d_i \geqslant d\}, \tag{18}$$

and recursively define numbers $b_0 \leqslant b_1 \leqslant \ldots \leqslant b_l$ and finite subsets $P_i \subseteq \mathbf{Z}$ such that the conditions

$$a_i \text{ in } P_i, \tag{19}$$

$$\beta(P_i) \geqslant b_i, \tag{20}$$

$$j \leqslant i \wedge \delta = r_i - r_j \Rightarrow P_j \subseteq E_\delta P_i \tag{21}$$

are preserved. The crucial point, thereby, will be that the P_i's do not become too large. Accordingly, we shall keep track of the growth of the quantities $|P_i|/b_i$ and b_i.

The recursion is initiated by $P_0 = \{0\}$, $b_0 = 1$. Three cases have then to be considered:

(i) for $i \in G$ put $P_i = P_{i-1}+1$, $b_i = b_{i-1}$.

(ii) for $i \in K_1$ put

$$P_i = E_{d_i+1}(P_{i-1}+1), \; b_i = b_{i-1}+1+d_i. \tag{22}$$

By reason of (21), the extension to the left by d_i many places assures a_{m_i} in P_i and a_{p_i} in P_i. The additional extension by one place to the right takes care of possible carries. Lemma 1 yields (20) and

$$\frac{|P_i|}{b_i} \leqslant \frac{|P_{i-1}|}{b_{i-1}}. \tag{23}$$

(iii) for $i \in K_2$, finally, $r_{p_i} = r_{i-1}$ is important; from (21) with $t = i-1$ we obtain a_{p_i} in $P_{p_i} \subseteq P_{i-1}$. In this case we define

$$P_i = P_{i-1} \nabla E_\tau P_{m_i}, \qquad b_i = b_{i-1}, \quad \text{where } \tau = b_{i-1} - b_{m_i}. \tag{24}$$

The insertion of E_τ and (14) guarantee (20), and (19) follows by means of (12). By Lemma 1 and (15) we have (in correspondence to (5))

$$\frac{|P_i|}{b_i} \leqslant \frac{|P_{i-1}|}{b_{i-1}} + \frac{|P_{m_i}|}{b_{m_i}}. \tag{25}$$

Now (22), (23), (25), and $z = a_l$ in P_l yield

$$s(z) \leqslant |P_l| = b_l \frac{|P_l|}{b_l} \leqslant \Big(1 + \sum_{i \in K_2} (1+d_i)\Big) 2^{k_2} \leqslant (1+k_1\, d)\, 2^{k_2}. \tag{26}$$

Instead of (6) we here use the inequalities

$$\begin{cases} a_i \leqslant 2a_{i-1} & \text{for } i \in G \cup K_1, \\ a_i \leqslant (1+2^{-d_i})\, a_{i-1} & \text{for } i \in K_2 \text{ (see (17))}, \end{cases}$$

hence

$$z \leqslant 2^{g+k_1} \prod_{i \in K_2} (1+2^{-d_i}) \leqslant 2^{g+k_1} (1+2^{-d})^{k_2}.$$

Combining this with (26) and taking logarithms gives

$$l = g + k_1 + k_2 \geqslant \log_2 z + \log_2 s(z) - k_2 \log_2 (1+2^{-d}) - \log_2 (1+k_1\, d). \tag{27}$$

In case of $k \geqslant \log_2 s(z)/0.3$, (10) is an immediate consequence of (7); otherwise we use (27) with $d = \lfloor \log_2 (k+2) \rfloor$.

4. The arrangement $a_0 < a_1 < \ldots < a_l$ may be inadequate for the proof of (9), just because, other reasons aside, all further considerations shall cover the case of addition-subtraction chains as well. In contrast to the definitions (4) and (16) of the sets G, K and the ranks r_i, which depend on the incidental numbering of the steps of the chain, we shall now introduce corresponding invariant quantities. At the same time we shall exhibit an especially suitable order of the steps.

The ranks r_i shall be constructed in such a way that the conditions

$$m_i = p_i \Rightarrow r_i = r_{p_i} + 1, \tag{28}$$

$$r_{m_i} = r_{p_i} = r_i - 1 \text{ or } r_{m_i} \leqslant r_{p_i} = r_i \tag{29}$$

are fulfilled ($r_{m_i} > r_{p_i}$ can be avoided by exchanging m_i and p_i). Then (29) leads to the classification

$$G = \{i | r_i = r_{p_i} + 1\}, \qquad K = \{i | r_i = r_{p_i}\} \tag{30}$$

of the steps $1 \leqslant i \leqslant l$, and by (28) $G_0 = \{i | m_i = p_i\}$ is a subset of G; in addition, let $G_{12} = G \setminus G_0$.

Again we write $d_i = r_{p_i} - r_{m_i}$ and subdivide K into

$$K_0 = \{i \in K | d_i = 0\}, \qquad K_{12} = \{i \in K | d_i \geqslant 1\}. \tag{31}$$

The definition of the r_i's and of the new order is accomplished by a recursive construction of the *levels* $L_\rho = \{i | r_i = \rho\}$.

Starting with $a_0 = 1$, $r_0 = 0$, and $L_0 = \{0\}$, assume that $L_0, L_1, \ldots, L_{\rho-1}$ are already fixed, together with the new order of the steps belonging to $I = L_0 \cup L_1 \cup \ldots \cup L_{\rho-1}$. Then at first all elements $i \in \{1, \ldots, l\} \setminus I$ with $m_i, p_i \in L_{\rho-1}$ are added (in an arbitrary order). We define $r_i = \rho$ for these elements; later on they will form the set $G \cap L_\rho$.

If $\gamma_\rho = |G \cap L_\rho| \geqslant 2$, then new i's with $m_i \neq p_i$ are successively added to L_ρ (i.e. $r_i = \rho$) as long as this is possible under the condition that r_{m_i} and r_{p_i} are already defined each time. These elements then form $K \cap L_\rho$, and L_ρ is complete.

If $\gamma_\rho = 1$, the first element thus added to L_ρ must be an $i \in K_{12}$ (if there is such an element at all), so we proceed as in the case $\gamma_\rho \geqslant 2$ only if the second step is also possible with some $i \in K_{12}$ (i.e. $r_{m_i} < \rho$). Otherwise L_ρ is complete after the first step.

Accordingly, the structure of L_ρ belongs to one of the following *types*:

$GG \ldots$	L_ρ begins with at least two G-steps; further G-steps, and after that, further K-steps can follow.
G	L_ρ consists of a single G-step.
$GK_{12}\,K_{12} \ldots$	L_ρ begins with a single G-step which is followed by at least two K_{12}-steps and possibly further K-steps.
GK_{12}	$L_\rho = \{\mu, \nu\}$ with $\mu \in G$, $\nu \in K_{12}$, and there is no $i \neq \nu$ with $p_i \in L_\rho$, $r_{m_i} < \rho$.

Our special strategy in the case $\gamma_\rho = 1$ serves to avoid $GK_{12}\,K_0$ at the beginning of L_ρ; instead of such a K_0-step there will follow a G_{12}-step in $L_{\rho+1}$. The inherent meaning of this particular design will become apparent later on.

In order to illustrate the construction of the levels L_ρ, we give an example: For the addition chain

$$(a_0, a_1, \ldots, a_{12}) = (1, 2, 4, 8, 9, 17, 19, 27, 34, 46, 51, 92, 126)$$

we obtain the sets

$$L_0 = \{0\}, \quad L_1 = \{1\}, \quad L_2 = \{2\}, \quad L_3 = \{3, 4\},$$
$$L_4 = \{5, 6, 7, 9\}, \quad L_5 = \{8, 11, 12, 10\},$$
$$G_0 = \{1, 2, 3, 8, 11\}, \quad G_{12} = \{5\}, \quad K_0 = \{9, 12\}, \quad K_{12} = \{4, 6, 7, 10\},$$

and the new order

$$1 \mid 2 \mid 4 \mid 8, 9 \mid 17, 19, 27, 46 \mid 34, 92, 126, 51.$$

As L_5 is of type $GG \ldots$, the elements 34, 92 and equally 126, 51 may be exchanged. Thus the new order is not always unique. From now on we restrict our discussion to those chains which are already in such a "new" order. In addition, we may assume that G_{12}-steps occur only at the beginning of the L_ρ's. Then $i \in G_{12}$ will imply (after

an eventual exchange of m_t, p_t)

$$m_t = i-2 \in G, \qquad p_t = i-1 \in K_{12}, \qquad L_{r_t-1} = \{i-2, i-1\}.$$

Writing $a_{t-2} = x$, $m_{t-1} = j$, and $a_j = y$ we have

$$r_j < r_{t-1} = r_t - 1, \qquad a_{t-1} = |x \pm y|, \qquad a_t = |2x \pm y| \tag{32}$$

with proper choice of the signs in the case of addition-subtraction chains. In this situation we can assume without restriction that L_{r_t} does not contain further G-steps apart from i, for a doubling of a_{t-1} can also be achieved by the K_{12}-step $|a_t \pm a_j|$, and if $2x$ is computed by doubling a_{t-2}, then the result $a_{t-2}+a_{t-1}$ of the G_{12}-step can be obtained in the form $|2x \pm a_j|$ by a K_{12}-step as well.

The further parts of the proof are based on a partition $K_{12} = K_1 \cup K_2$ similar to (18) which will be chosen suitably later on. By

$$G_\tau = \{i \in G_{12} | i-1 \in K_\tau\} \qquad (\tau \in \{1, 2\}) \tag{33}$$

it induces a corresponding partition $G_{12} = G_1 \cup G_2$. So we have

$$G = G_0 \cup G_1 \cup G_2, \; K = K_0 \cup K_1 \cup K_2, \text{ and } l = g+k_0+k_1+k_2. \tag{34}$$

5. As in Section 3, the next step of the proof is the construction of numbers $b_t \in \mathbf{N}$ and sets $P_t \subseteq \mathbf{Z}$ under the conditions (19), (20), and (21); again let $P_0 = \{0\}$, $b_0 = 1$.

(i) For $i \in G_0$ put

$$P_t = P_\mu + 1, \qquad b_t = b_\mu,$$

where $\mu = \max L_{r_t-1}$.

(ii) For $i \in G_1 \cup K_0 \cup K_1$ put

$$P_t = E_{d_t+1}(P_{t-1}+1), \qquad b_t = b_{t-1}+1+d_t$$

(see (22), (31)).

(iii) For $i \in K_2$ put

$$P_t = P_{t-1} \nabla E_\tau P_{m_t}, \qquad b_t = b_{t-1},$$

where $\tau = b_{t-1} - b_{m_t}$ (see (24)); here $r_{p_t} = r_{t-1}$ is guaranteed by $r_{p_t} = r_t$ and $p_t < i$.

(iv) For $i \in G_2$ we have $i-1 \in K_2$, hence

$$P_{t-1} = P_{t-2} \nabla E_\tau P_{m_{t-1}},$$

where $\tau = b_{t-2} - b_{m_{t-1}}$. In view of (32) we therefore put

$$P_t = (P_{t-2}+1) \nabla E_\tau P_{m_{t-1}}, \qquad b_t = b_{t-1}.$$

We may restrict the proof of (21) to the case $t = i \in G_2$ which, compared to Section 3, represents the essential innovation of the present proof. For $j \leqslant i-2$ (hence $\delta = r_t - r_j \geqslant 1$) we use (21) as induction hypothesis with $t = i-2$, and obtain

$$E_\delta P_i \supseteq E_\delta(P_{i-2}+1) \supseteq E_{\delta-1} P_{i-2} \supseteq P_j.$$

For $j = i-1$, the conclusion of (21) amounts to

$$P_{i-2} \nabla R \subseteq P_i \cup (P_i-1), \tag{35}$$

where $R = E_\tau P_{m_{i-1}}$. As $P_i = (P_{i-2}+1) \nabla R$ implies $P_i-1 = P_{i-2} \nabla (R-1)$, we obtain

$$x+\frac{y}{2} \text{ in } (P_i-1), \ \frac{y}{2} \text{ in } (P_i-1)$$

for arbitrary x in P_{i-2}, y in R, $\frac{y}{2}$ in $(R-1)$, hence

$$x+y \text{ in } (P_i-1) \cup P_i,$$

which implies (35) according to the definition of the operation ∇ (see (12)).

6. The recursive definition of the b_i's yields

$$b_i = 1+k_0+g_1+\sum_{i \in K_1}(1+d_i). \tag{36}$$

In order to estimate $|P_i|/b_i$ we use (23) for $i \in G_0 \cup G_1 \cup K_0 \cup K_1$, (25) for $i \in K_2$, and

$$\frac{|P_i|}{b_i} \leqslant \frac{|P_{i-2}|}{b_{i-2}} + \frac{|P_{m_{i-1}}|}{b_{m_{i-1}}} \quad \text{for } i \in G_2. \tag{37}$$

The latter inequality shows that $|P_i|/b_i \leqslant 2^{k_2+g_2}$ can be replaced by $|P_i|/b_i \leqslant 2^{k_2}$. A further improvement is possible if one of the levels contains several K_2-steps. We denote

$$\begin{aligned} &K_2' = \{i \in K_2 \mid i = \min(K_2 \cap L_{r_i})\}, \qquad K_2'' = K_2 \setminus K_2', \\ &k_2' = |K_2'|, \qquad k_2'' = |K_2''|, \qquad v_\rho = |K_2 \cap L_\rho|, \end{aligned} \tag{38}$$

hence

$$k_2'+k_2'' = k_2 = \sum_\rho v_\rho, \qquad \sum_\rho{}'(v_\rho-1) = k_2'',$$

where $\sum_\rho{}'$ denotes summation restricted to $\{\rho \mid v_\rho \geqslant 1\}$.

If we define $q_0 = 1$, $q_\rho = (1+v_\rho)\, q_{\rho-1}$ recursively, then by induction on ρ

$$\frac{|P_i|}{b_i} \leqslant q_\rho \quad \text{for } i \in L_0 \cup \ldots \cup L_\rho \cup (L_{\rho+1} \cap G), \tag{39}$$

because according to (25), the quantity $|P_i|/b_i$ can increase by at most $v_\rho\, q_{\rho-1}$ within the v_ρ many K_2-steps in L_ρ; for $i \in G_2 \cap L_{\rho+1}$ both quotients on the right-hand

side of (37) are bounded by $q_{\rho-1}$, and $q_\rho = 2q_{\rho-1}$ as $v_\rho = 1$ in this case. From (39) we obtain

$$\frac{|P_l|}{b_l} \leqslant \prod_\rho (1+v_\rho) = 2^{k_2'} \prod_\rho{}' (1+\tfrac{1}{2}(v_\rho - 1))$$

$$\leqslant 2^{k_2'} \prod_\rho{}' (1+\tfrac{1}{2})^{v_\rho - 1} = 2^{k_2} (\tfrac{3}{4})^{k_2''},$$

and finally, in view of $s(z) \leqslant |P_l|$, the inequality

$$k_2 \geqslant \log_2 s(z) + k_2'' \log_2 (\tfrac{4}{3}) - \log_2 b_l. \tag{40}$$

When dealing with addition-subtraction chains, we use $\bar{s}(z) \leqslant |P_l|$ instead (see (8)).

7. In this section we construct bounds $A_l \geqslant a_j$ for $j \leqslant i$, analogous to those in (6). For this we need a further subdivision of K_0 into

$$K_0'' = \{i \in K_0 | i-1 \in K_0\}, \quad K_0' = K_0 \setminus K_0'', \tag{41}$$

i.e. K_0' just contains the minimal elements of the components of K_0. We start with $A_0 = 1$ and define recursively

$$A_l = \begin{cases} 2A_\mu & \text{for } i \in G,\ \mu = \max L_{r_l - 1}, \\ 2A_{l-1} & \text{for } i \in K_0', \\ \gamma A_{l-1} & \text{for } i \in K_0'',\ \gamma = \frac{1}{2}(1+\sqrt{5}), \\ (1+2^{-d_l}) A_{l-1} & \text{for } i \in K_{12}. \end{cases} \tag{42}$$

Then the first line of (42) implies

$$j < i \wedge \delta = r_l - r_j \Rightarrow A_j \leqslant 2^{-\delta} A_l,$$

and for $i \in K_0''$ we have $i-1 \in K_0$, $A_{l-1} \geqslant \gamma A_{l-2}$. From these inequalities and (42) $a_j \leqslant A_l$ for $j \leqslant i$ is obtained by induction on i.

In (42) the G-steps cause $r_l = \max\{\rho | L_\rho \neq \emptyset\}$ doublings on the whole. $g' = g - r_l = \sum_\rho (\gamma_\rho - 1)$ counts those G-steps which appear on levels L_ρ of type $GG\ldots$ in the second position or in a subsequent one, i.e. $g' = |G'|$, where

$$G' = \{i \in G | r_l = r_{l-1}\}. \tag{43}$$

Writing $|K_0'| = k_0'$, $|K_0''| = k_0''$ we thus find that

$$z \leqslant A_l = 2^{r_l + k_0'} \gamma^{k_0''} \prod_{i \in K_{12}} (1+2^{-d_l})$$

and, after some computation, that

$$g + k_0 \geqslant \log_2 z + g' + 0.3 k_0'' - \sum_{i \in K_{12}} \log_2 (1+2^{-d_l}). \tag{44}$$

We supply the preceding estimations by

Lemma 2. *With reference to the foregoing notations we have that*

$$k_0'+g_1 \leqslant k_1+k_2''+2g'. \tag{45}$$

Proof. If $|L_\rho \cap K_0'| = c \geqslant 1$, then $L_\rho \cap K_0$ consists of c components, which must be separated from each other by K_{12}-steps. In case of type $GK_{12}\,K_{12}$ ... there are another two K_{12}-steps, hence $|K_{12} \cap L_\rho| \geqslant c+1$ and

$$|(K_1 \cup K_2'') \cap L_\rho| \geqslant c,$$

because $|K_2' \cap L_\rho| \leqslant 1$. If, however, L_ρ is of type GG ..., then we use $|G' \cap L_\rho| \geqslant 1$ and obtain

$$|(K_1 \cup K_2'') \cap L_\rho| + 2\,|G' \cap L_\rho| \geqslant c,$$

correspondingly. The assertion (45) now follows from these inequalities and the fact that according to the definition (33), there are at least g_1 additional L_ρ's of type GK_1. It is for this proof that the absence of levels of type GK_2K_0 is important.

8. By combining the inequalities derived in Sections 6 and 7 we now proceed to prove (9). By virtue of $k_0 = k_0'+k_0''$, Lemma 2 and (36) yield

$$b_l \leqslant B+k_0''+k_2''+2g',$$

where $B = 1+\sum_{l\in K_1}(2+d_l)$, and that in conjunction with (34), (40), (44) leads to

$$\begin{aligned} l \geqslant{}& \log_2 z+\log_2 s(z)+k_1-\sum_{l\in K_{12}}\log_2(1+2^{-d_l}) \\ &+0.3k_0''+k_2''\log_2\left(\tfrac{4}{3}\right)+g'-\log_2(B+k_0''+k_2''+2g'). \end{aligned} \tag{46}$$

As $0.5 \geqslant \log_2(\frac{4}{3}) \geqslant 0.3$ we now write $k_0''+k_2''+2g' = n$ and take advantage of the freedom to choose the partition $K_{12} = K_1 \cap K_2$ suitably. Then (9) is an immediate consequence of (46) and Lemma 3.

Lemma 3. *For every finite family of integers $d_l \geqslant 1$ $(l \in K_{12})$ there is a partition $K_{12} = K_1 \cup K_2$ such that with*

$$\begin{aligned} &k_1 = |K_1|, \qquad B = 1+\sum_{l\in K_1}(2+d_l), \\ &0.3n-\log_2(B+n)+k_1-\sum_{l\in K_{12}}\log_2(1+2^{-d_l}) \geqslant -2.13 \text{ for arbitrary } n\in\mathbb{N}. \end{aligned} \tag{47}$$

By the remarks at the end of Sections 2 and 6 it should be obvious that the entire proof of (9) is valid for addition-subtraction chains as well, if only $s(z)$ is replaced by $\bar{s}(z)$, and "in" by "$\underline{\text{in}}$", respectively.

9. In order to prove Lemma 3 we choose the partition $K_{12} = K_1 \cup K_2$ under the constraint $d_i \geqslant 2$ for $i \in K_2$ in such a way that $u = k_1 - \log_2 B - \delta_{B,1}$ becomes maximal. Then $2+d_i \geqslant B$ for $i \in K_2$, because otherwise $i \in K_1$ would yield a greater value of u, and clearly $2+d_i < B$ for $i \in K_1$. Therefore, $d = \max\{2, B-2\}$ separates the d_i's of the two kinds — just as in (18). In addition, with

$$n_t = \text{number of the } i\text{'s with } d_i = t,$$

the required maximality of u implies the conditions

$$\sum_{t=d}^{m} n_t + \delta_{B,1} \leqslant \log_2\left(1 + \frac{1}{B}\sum_{t=d}^{m}(2+t)\,n_t\right) \quad \text{for } m \geqslant d, \tag{48}$$

$$-\sum_{t=m}^{d-1} n_t \leqslant \log_2\left(1 - \frac{1}{B}\sum_{t=m}^{d-1}(2+t)\,n_t\right) \quad \text{for } 2 \leqslant m < d, \quad \text{if } \sum_{t<m} n_t \geqslant 1, \tag{49}$$

$$-\sum_{t=2}^{d-1} n_t \leqslant \log_2\left(\frac{2}{B}\right) \quad \text{if } n_1 < 1. \tag{49'}$$

With respect to (47) we consider the problem of minimizing

$$S_2 = -\sum_{t \geqslant d} n_t \log_2(1+2^{-t})$$

by variation of the numbers n_t (now infinitely many of them are allowed to be different from zero) for fixed $B \in \{1, 4, 5, 6, \ldots\}$ under the restriction (48). The solution, then, has the characteristic property that (48) does not hold with n_m+1 instead of n_m for any $m \geqslant d$. Thus we have $S_2 \geqslant S_2(B)$, where

$$S_2(B) = \begin{cases} -\log_2 \prod_{\nu=0}^{\infty}(1+2^{2-2^{\nu}B}) & \text{for } B \geqslant 4, \\ -2\log_2(\frac{5}{4}) + S_2(9) & \text{for } B = 1. \end{cases} \tag{50}$$

In a similar manner we deal with the problem of minimizing

$$S_1 = \sum_{t=1}^{d-1} n_t(1-\log_2(1+2^{-t}))$$

for fixed B under the conditions (49), (49'), and

$$1+\sum_{t<d}(2+t)\,n_t = B.$$

Here $n_2, \ldots, n_{d-1}$ are restricted to N, whereas for n_1 real values $\geqslant 0$ shall be admitted. We consider such values of $n_1, \ldots, n_{d-1}$ for which the minimum is attained, and form $h = \sum_{t=2}^{d-1} n_t$.

In the case where $h = 0$ we simply have $S_1 \geqslant \frac{1}{3}(B-1)\log_2(\frac{4}{3})$. For $h > 0$ we look at $f(t) = 1-\log_2(1+2^{-t})$ and notice the validity of

$$f(t-1)+f(t'+1) < f(t)+f(t') \quad \text{for } t \leqslant t'.$$

This convexity enables us to derive the characteristic property of the solution of the minimum problem that (49) does not hold with n_m+1 instead of n_m for any $m < d$ with $\sum_{t=2}^{m-1} n_t \geqslant 2$. By analyzing this property the following structure of the solution is obtained.

There are $t_1 > t_2 > \ldots > t_h \geqslant 2$ with $n_{t_j} = 1$, more precisely

$$t_j = \lfloor \tfrac{1}{2} \lceil B\, 2^{1-j} \rceil \rfloor - 2 \quad \text{for } 1 \leqslant j \leqslant h-1,$$

$$\lceil B\, 2^{1-h} \rceil = B - \sum_{j=1}^{h-1} (2+t_j) \geqslant 1+(2+t_h) \geqslant 5,$$

hence $B > 2^{1+h}$ and $n_1 \geqslant 1$, because otherwise (49') would lead to a contradiction. Thus (49) applies to all $m \geqslant 2$ and gives $t_h \leqslant \tfrac{1}{2} \lceil B\, 2^{1-h} \rceil - 2$, hence

$$2t_{j+1}+1 \leqslant t_j \quad \text{for } 1 \leqslant j \leqslant h-1,$$

and $1+3n_1 \geqslant B\, 2^{-h}$. Furthermore, only $t_h \geqslant 5$ is possible, for otherwise replacement of n_{t_h} by 0 and increase of n_1 by $\tfrac{1}{3}(2+t_h)$ would reduce S_1. In this way we obtain finally

$$S_1+S_2 \geqslant \tfrac{1}{3}(B\, 2^{-h}-1) \log_2 (\tfrac{4}{3}) + h - C \quad \text{for } h > 0, \tag{51}$$

where $C = \log_2 \prod_{\nu=0}^{\infty} (1+2^{-(6\cdot 2^\nu-1)}) \leqslant 0.0451$. Notice that C includes the bound $S_2(B)$ for every B.

Now we discuss the left-hand side of (47). For $B = 1$, it attains its minimum with $n = 4$, that is

$$1.2-\log_2 5+S_2(1) \geqslant -1.78.$$

If $B = 4$, then $n = 1$, $h = 0$, and $n_1 = 1$ yield the value

$$0.3+\log_2 (\tfrac{4}{3}) - \log_2 5 + S_2(4) \geqslant -1.96.$$

In the case where $B \geqslant 5$ and $n = 0$ we have

$$\tfrac{1}{3}(B-1) \log_2 (\tfrac{4}{3}) - \log_2 B + S_2(B) \geqslant -2.09 \quad \text{for } h = 0.$$

If $h > 0$, then (51) gives the bound (write $B\, 2^{-h} = x$)

$$\tfrac{1}{3}(x-1) \log_2 (\tfrac{4}{3}) - \log_2 x - 0.0451 \geqslant -2.13.$$

References

[1] A. Brauer, On addition chains, Bull. Am. Math. Soc. 45 (1939) 736–739.

[2] P. Erdös, Remarks on number theory III — On addition chains, Acta Arith. 6 (1960) 77–81.

[3] D. E. Knuth, The Art of Computer Programming, Vol. 2 (Addison-Wesley, New York, 1969) 398–422.