TILBURG UNIVERSITY
KATHOLIEKE UNIVERSITEIT BRABANT

POSTBOX 90153
5000 LE TILBURG
THE NETHERLANDS

[redacted]

DEPARTMENT OF ECONOMICS

RESEARCH MEMORANDUM

AN ALGORITHM ON ADDITION CHAINS WITH RESTRICTED MEMORY

M.J. Coster

FEW 603

Communicated by Prof.dr. M.H.C. Paardekooper

An Algorithm on Addition Chains with Restricted Memory

M.J. Coster

June 1, 1993

Abstract

This paper considers addition chains, addition sequences and vector addition chains, introducing a new constraint —namely restricted memory— which is important in all of the applications on computers. We consider an algorithm for calculating addition chains, addition sequences and vector addition chains —namely a Generalized Continued Fraction Algorithm— which uses just a restricted number of memory locations on the computer. The average length of addition chains/sequences constructed by this algorithm will be calculated using a number theoretical tools (from Ergodic Theory and Special Function Theory). Finally, this algorithm will be compared to some other known algorithms.

Keywords & Phrases: Addition Chain, Addition Sequence, Vector Addition Chain, Algorithm, Fast Exponentiation, RSA, Space- and Time- Complexity, Ergodic Theory.

1985 AMS Mathematics Subject Classification: 65V05, 68M20; Computing Reviews code: F21: Number theoretic computation; G4: Algorithm analysis and efficiency.

1 Introduction

Much research has been concerned with speeding up RSA calculations, with the aim of increasing the speed of multiplications. More recently, further improvements have been achieved by applying so-called addition chains. In RSA applications, an exponentiation is done by some modular multiplications using addition chains. For each element in the addition chain, a multiplication is done. Hence RSA becomes faster if the addition chain is shorter.

For instance, new RSA-applications (cf. [21] and [15]) can take advantage of a generalization called vector addition chains. Use of these shorter addition chains significantly speeds up the RSA application. Olivos gave in [27] a description of how such vector addition chains can be constructed. This construction was implemented by Bos in [8]. Addition chains also have applications in exponentiations of discrete log-based systems [19], exponentiations in GF(2^n) (cf. [1]) and factoring algorithms (cf. [25, 39]). In fact, addition chains and addition sequences can be used for any abelian group with large sizes. This paper will often use X, X^n, $Y \cdot Z$, as if we were doing an RSA-calculation. The reader may substitute an addition or another group operation.

Many algorithms on addition chains and addition sequences are known: the Binary Algorithm, the Window Algorithm (cf. [23]), the Generalized Window Algorithm (cf. [40, 33]), the Continued Fraction Algorithm (cf. [4, 3]), the Generalized Continued Fraction Algorithm (cf. [8]) and the Batch-RSA Algorithm (cf. [21]). For a good overview, see [16]. But in applications on the computer, not all these algorithms are equal. It is clear that the length of the chains and sequences constructed by those algorithms is important (time complexity). But also the number of memory location used by the computer when the algorithms are applied is important (space complexity). For example, the Generalized Window Algorithm is rather fast, but it uses a large number of memory locations (cf. [16]). We are interested in algorithms which are both fast and use only a small number of memory locations. The Generalized Continued Fraction Algorithm is such an algorithm. It is based on the Multi-Continued Fraction Algorithm of Brun, (cf. [10, 12, 30]). Thus we will call it the Brun Algorithm. The two-dimensional case was described in [4]. This paper will show that the Brun Algorithm uses a small number of memory locations, and we will predict the time complexity, insofar as that is possible.

This paper consists of 5 sections. Section 2 defines the notation used in this paper and Section 3 gives a brief review of the literature, explains the space complexity, defines the average number of steps and explains the Brun Algorithm.

Section 4 provides a proof that the number of memory locations used by the Brun–algorithm is equal to the width of the sequence (or vector addition chain). From there the average number of steps can be calculated. This is far from trivial. We need deep Ergodic Theory, partly known theory, partly new theory. Comparable theory was used in order to calculate the number of steps in Euclid's Algorithm. We find an expression in terms of n-dimensional integrals, which can be solved for small dimensions. Unfortunately, since in this paper we were unable to calculate these integrals, we conjecture that the average lengths of chains and sequences, constructed by the Brun Algorithm, are of the order $O(n \log(\max(a_1, \ldots, a_n))/\log(n))$, where $a_1, \ldots, a_n$ are the numbers for which an addition sequence/vector addition chain has to be found.

The last section discusses the results, mentioning some open problems and suggesting topics for further research.

Results that are related to vector addition chains will be omitted. In fact, all results proved in this paper hold also for vector addition chains. For a good survey on vector addition chains [8, 16, 23, 27].

2 Definitions and notation.

The following notation will be used:

$\mathbf{a}$	a vector
$\lfloor x \rfloor$	largest integer which does not exceed x
$\nu(n)$	the number of ones that occur in the binary representation of n
$\log_2 n$	2–based logarithm
$\lambda(n)$	$\lfloor \log_2 n \rfloor$

$\ln n$	$\log_e n$
μ_n	root of the equation $x^n - x^{n-1} - 1 = 0$, with $\mu_n > 1$
E_n	Unit cube in n dimensions $= \{\mathbf{x} \mid 0 \leq x_i \leq 1 \text{ for } 1 \leq i \leq n\}$
$E_{n,k}$	$= \{\mathbf{x} \mid 0 \leq x_i \leq \frac{1}{k} \text{ for } 1 \leq i \leq n\}$
$\Delta_{n,k}$	$E_{n,k} \setminus E_{n,k+1}$
$M(L)$	Number of memory locations used by Algorithm L
$T(a_1, \ldots, a_n)$	an integral map related to the Brun–algorithm, see Section 4.1
$t(x_1, \ldots, x_n)$	a real map on E_n related to the Brun–algorithm, see Section 4.1
$\Psi_n(\mathbf{x})$	$\dfrac{1}{(1+x_1)\cdots(1+x_1+\cdots+x_n)}$
X_n	$\int\int_{E_n}\int \Psi_n(\mathbf{x})\,\mathrm{d}\mathbf{x}$
Y_n	$-\int\int_{E_n}\int \ln(\max(x_1, \cdots, x_n)) \cdot \Psi_n(\mathbf{x})\,\mathrm{d}\mathbf{x}$
$Z_{n,k}$	$\int\int_{E_{n,k}}\int \Psi_n(\mathbf{x})\,\mathrm{d}\mathbf{x}$

An *addition chain* for a positive integer a is the set of positive integers $\{b_0, \ldots, b_l\}$ with the following properties:

(i) $b_0 = 1$,

(ii) for all $1 \leq k \leq l$ there exist i, j such that $b_k = b_i + b_j$, for $0 \leq i, j < k$,

(iii) $b_l = a$.

We call the index l the length of the addition chain. We denote an addition chain by $L(a)$ and its length by $l(a)$.

An addition sequence for a set of positive integers $\{a_1, \ldots, a_n\}$ is a set of positive integers $\{b_0, \ldots, b_l\}$ with the following properties:

(i) $b_0 = 1$,

(ii) for all $1 \leq k \leq l$ there exist i, j such that $b_k = b_i + b_j$, for $0 \leq i, j < k$,

(iii) for $1 \leq m \leq n$: $a_m \in \{b_0, \ldots, b_l\}$.

We call n the *width* of the addition sequence and l the length. It will be assumeed in the rest of the text that an addition sequence will be constructed for $a_1, \ldots, a_n$. The set $\{b_0, \ldots, b_l\}$ will be denoted by $L(a_1, \ldots, a_n)$. An addition chain is an addition sequence of width 1.

We use also the following definitions and functions:

$L^{(k)}(a_1, \ldots, a_n)$	an addition sequence containing $a_1, \ldots, a_n$ using only k memory locations ($k \geq n$)
$l(a_1, \ldots, a_n)$	length of an addition sequence containing $a_1, \ldots, a_n$

$\rho(a_1,\ldots,a_n)$	$l(a_1,\ldots,a_n)/\log_2 a_n$
$\overline{\rho}(\alpha,n)$	average value of $\rho(a_1,\ldots,a_n)$ such that $\lambda(a_n)=a$. We abbreviate this notation to $\overline{\rho}$
$L_1(a)$	the addition chain for a constructed by the binary algorithm
$L_n(a_1,\ldots,a_n)$	the addition sequence containing $a_1,\ldots,a_n$ constructed by the Brun–algorithm (cf. [16, 8])
$l_n(a_1,\ldots,a_n)$	length of the addition sequence containing $a_1,\ldots,a_n$, constructed by the Brun–algorithm
$\rho_n(a_1,\ldots,a_n)$	$l_n(a_1,\ldots,a_n)/\log_2 a_n$
$\overline{\rho_n}$	average value of $\rho_n(a_1,\ldots,a_n)$

3 A brief review of the literature

Much is known about bounds for addition chains. For instance, it is known that

$$\log_2 a + \log_2 \nu(a) - 2.13 \leq l(a). \tag{1}$$

This bound is from [29]. In [9] Brauer gives an upper bound of

$$l(a) \leq \log_2 a + \log_2 a/\log_2\log_2 a + o(\log a/\log\log a). \tag{2}$$

This bound is theoretical. In practise we can't get this bound for larger numbers. The k–window–method (k–ary–method) described in [23] gives a worse upper bound:

$$l(a) \leq \log_2 a + \tfrac{1}{k}\log_2 a + 2^{k-1} - k - 1, \tag{3}$$

which is optimal if $k^2 \cdot 2^k \approx 2 \cdot \log_2 a/\ln 2$. Less is known about addition sequences and vector addition chains. Straus gives in [33] an upper bound for vector addition chains:

$$l(a_1,\ldots,a_n) \leq \log_2 a_n + \tfrac{1}{k}\log_2 a_n + 2^{nk} - n - 1, \tag{4}$$

which is optimal if $k^2 \cdot 2^{nk} \approx \log_2 a_n/(n \cdot \ln 2)$. In [40], Yao gives an upper bound for addition sequences:

$$l(a_1,\ldots,a_n) \leq \log_2 a_n + \tfrac{n}{k}\log_2 a_n + n \cdot 2^k - k - 1, \tag{5}$$

which is optimal if $k^2 \cdot 2^k \approx \log_2 a_n/\ln 2$. Here a_n is the largest number in the sequence.

3.1 Space complexity

In the practice of RSA it is possible to calculate X^{23} by X, X^2, X^4, X^5, X^{10}, X^{11}, X^{22}, X^{23} or by X, X^2, X^4, X^8, X^{16}, X^{17}, X^{19}, X^{23}; the length of the chains in both cases are equal (7). The difference is that in the second case, 3 memory locations are needed for storing X, X^2, and X^4, in order to calculate X^{17}, X^{19}, and X^{23} respectively, while in the first case only X has to be stored for later use. Therefore we introduce a new constraint, namely addition chains and sequences with a restricted number of memory locations. The definition of the number of memory locations seems to be arbitrary, but it corresponds to the practical situation (see [16, 8]).

Definition. Let $L(a) = \{a_0, a_1, \ldots, a_l\}$, where $a_0 = 1$, $a_l = a$ be an addition chain for a. We define by m_i the number of memory locations which are in use after the calculation of X^{a_i}. More precisely: $m_i = \#\{a_j, 0 \leq j \leq i \mid \exists a_k, i+1 \leq k \leq l, \text{ with } a_k = a_{k-1} + a_j \text{ and } k - j > 1\}$. (In this definition we assume star-step chains, but the definition can easily be generalized.) We define $M(L) = \max m_i$ the total number of memory locations used for constructing $L(a)$. The definitions for the memory restrictions on addition sequences and vector addition chains are comparable.

Example. $L(23) = 1, 2, 3, 5, 10, 20, 23$. Now $a_2 = 3$ and $m_2 = 2$, since X^2 is stored for calculating X^5 and X^3 is stored for calculating X^{23}.

We define by $L^{(n)}(a)$ an addition chain which uses at most n memory locations. The binary algorithm can be executed as an $L^{(1)}$ algorithm, (namely by storing X and multiplying by X for each bit "1" in the binary representation of a. Nevertheless there exists a faster $L(1)$ algorithm than the binary algorithm (cf. [16]).

Less is known about $L^{(n)}$ algorithms for $n > 1$. The Generalized Window Algorithm of Yao is an $L^{(n(2^k-1))}$ algorithm, here is n the width and k the size of the windows. The algorithm of Straus is an $L^{(2^{kn}-1)}$ algorithm. Both algorithms are therefore of no use in the RSA practice for larger n.

3.2 Brun's algorithm

This algorithm is a generalization of the continued fraction algorithm described in [4]. In that paper only sequences of width 2 were obtained. The Brun Algorithm is its generalization. We distinguish two algorithms. The first algorithm is an addition sequence algorithm. The second algorithm is the vector addition chain algorithm, which was considered in [8]. The description of this algorithm will not be given in this paper. The basis for both algorithms is Brun's multi continued fraction algorithm. Suppose that $a_1 \leq \cdots \leq a_n$. Let $r = \left\lfloor \frac{a_n}{a_{n-1}} \right\rfloor$. Let $T : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ be a map with $T(a_1, \ldots, a_n) = (a_1, \cdots, a_i, b, a_{i+1}, \cdots, a_{n-1})$, where $b = a_n - r a_{n-1}$ and $a_i \leq b \leq a_{i+1}$. Suppose that the addition sequence for $T(a_1, \ldots, a_n)$ is known. The addition sequence for $a_1, \ldots, a_n$ can then be constructed by adding to $L_n(T(a_1, \ldots, a_n))$ the elements $r_i a_{n-1}$ for $1 \leq i \leq l$ and a_n, where $L_1(r) = \{r_0, r_1, \cdots, r_l\}$ is the binary addition chain for r.

This algorithm is an $L^{(n)}$ algorithm. Hence, using the Brun Algorithm we need only n memory locations. This will be proved in the following theorem.

Theorem 3.1 *The Brun Algorithm for width n is an $L^{(n)}$ algorithm.*

Proof. This will be proved by induction to n and $a = \max\{a_1, \ldots, a_n\}$. For $n = 1$ we consider the binary algorithm, which needs only 1 memory location. Suppose we proved the theorem up to $n - 1$ and for n-tuples with $a_n < a$. Now we consider $L_n(a_1, \ldots, a_n)$, with $a_n = a$. Hence we proved that we can construct $L_n(T(a_1, \ldots, a_n))$ with at most n

memory locations. We may assume that after constructing $L_n(T(a_1, \ldots, a_n))$ the memory locations are filled by X^c, where c runs through the elements of $T(a_1, \ldots, a_n)$. Since the binary algorithm is an $L(1)$ algorithm, we can construct $X^{a_{n-1}}$, $X^{2a_{n-1}}$, $\ldots$, $X^{ra_{n-1}}$ without any extra memory location. Then we calculate $X^b \cdot X^{ra_{n-1}}$, where $b = a_n - ra_{n-1}$ and place the result in the memory location where X^b was stored. □

In case of the Brun Algorithm for vector addition chains of width n, it can be proved that this is an $L^{(n)}$ algorithm too. For examination of the proof, see [16]. For a detailed description of the algorithm, see [8].

4 Average value of the Brun algorithm

Suppose that the computer needs t operations on average for a multiplication $Y \cdot Z$ or Y^2. (This paper makes no distinction between multiplying different multiplicands and squaring; there are differences, however, if we consider, eg., GF(2^n) (cf. [1]).) The number of operations in order to calculate $L(a_1, \ldots, a_n)$ is $t \cdot l(a_1, \ldots, a_n)$. We introduce the number $\rho(a_1, \ldots, a_n) = l(a_1, \ldots, a_n)/\log_2 a_n$. Now the number of operations can be expressed in terms of $\log_2 a_n$. If $\rho(a_1, \ldots, a_n)$ were independent of the choice of $a_1, \ldots, a_n$, then we could easily calculate the number of operations. Unfortunately this is not the case. However we can approximate $\rho(a_1, \ldots, a_n)$ by $\overline{\rho}(\alpha, n)$. We define $\overline{\rho}(\alpha, n)$ by

$$\overline{\rho}(\alpha, n) = \frac{1}{\Sigma} \cdot \sum_{(a_1, \ldots, a_n)} \frac{l_n(a_1, \ldots, a_n)}{\log_2 a_n}, \tag{6}$$

where the sum is taken over all n-tuples $(a_1, \ldots, a_n)$ with $\lambda(a_n) = \alpha$ and Σ is the number of those n-tuples $(a_1, \ldots, a_n)$. We call $\overline{\rho}(\alpha, n)$ the average value of sequences/chains of width n. We will abbreviate this notation to $\overline{\rho}$. Notice that for Algorithm L_1 we have $\overline{\rho}(\alpha, 1) = \frac{3}{2}$. We will now study approximations of the form

$$l(a_1, \ldots, a_n) \approx \overline{\rho} \log_2 a_n$$

in the case of the Brun Algorithm. In the case of the Brun Algorithm, we will denote the average value of ρ by $\overline{\rho_n}$, where the index n indicates the width.

Theorem 4.1 *Let X_n, Y_n, and $Z_{n,k}$ be the integrals, which were defined in Section 2.*

Then $\overline{\rho_n} = \frac{\sigma_n}{\tau_n}$, *where* $\tau_n = \frac{Y_{n-1}}{\ln 2 \cdot X_{n-1}}$ *and* $\sigma_n = 1 + \sum_{k=1}^{\infty} \frac{Z_{n-1,k}}{X_{n-1}} \cdot (l_1(k) - l_1(k-1))$.

Without proof, the following corollary will be given in this paper. The proof of (*i*) can be found in [16], while the proof of (*ii*) is still unpublished. In fact, the proofs consist of a numerical evaluation of Theorem 4.1. It can be verified that these results correspond very well with the results in Table II of the Appendix.

Corollary 4.2 *We have*

(*i*) $\overline{\rho}_2 = 1,6080967\ldots$,

(*ii*) $\overline{\rho}_3 = 1,7768807\ldots$.

The following conjecture indicates the behavior of $\overline{\rho_n}$.

Conjecture 4.3 $\overline{\rho_n} = O\left(\frac{1}{\log_2 \mu_n}\right)$, *where* μ_n *is the root of the equation* $x^n - x^{n-1} = 1$, *with* $\mu_n > 1$.

We were unable to find a proof for this conjecture. We used two approaches. One approach was trying to find an upperbound for $\frac{Y_{n-1}}{X_{n-1}}$, the other approach is sketched in the motivation of this conjecture. A consequence of this conjecture is

Conjecture 4.4 $\overline{\rho_n} = O\left(\frac{n}{\log_2 n}\right)$.

4.1 Ergodic theoretical background

Before proving Theorem 4.1 and sketching Conjecture 4.3, we will give a brief overview of results from Ergodic Theory which will be used. Let E_n be the n-dimensional unit-cube. We consider on E_n the map $t : E_n \to E_n$ defined by $t(x_1, \ldots, x_n) = \left(\frac{1}{x_i} - \left\lfloor\frac{1}{x_i}\right\rfloor, \frac{x_1}{x_i}, \ldots, \frac{x_n}{x_i}\right)$, if $\max(x_1, \ldots, x_n) = x_i$. (All coordinates except of the largest one is divided by the largest coordinate, while the largest coordinate is replaced by a function of it.) Notice that $x_1, \cdots, x_n$ are not necessarily ordered. This map t is due to Brun. In fact we consider the so called *Transposed Brun Algorithm*, while Brun's map is slightly different. For a good survey, see [35].

Ergodic Theory is interested in the behavior of $x_1, \ldots, x_n$ after several steps. Questions like "how often is $\left\lfloor\frac{1}{x_i}\right\rfloor = 1$?", "how large is $\max(x_1, \ldots, x_n)$ in average?" and "how often is $\frac{1}{x_i} - \left\lfloor\frac{1}{x_i}\right\rfloor$ smaller than the other coordinates?" can be answered using this theory.

Let $f : E_n \to \mathbb{R}$ be an integrable function. Suppose we want to know the average value $\frac{1}{m}\sum_{k=0}^{m-1} f(t^k(x_1, \ldots, x_n))$, if m tends to infinity. Then Ergodic Theory tells us that

$$\lim_{m\to\infty} \frac{1}{m}\sum_{k=0}^{m-1} f(t^k(\mathbf{x})) = \frac{1}{X_n}\int\int_{E_n}\int f(\mathbf{x})\cdot\Psi_n(\mathbf{x})\,\mathrm{d}\mathbf{x}, \tag{7}$$

where $\mathbf{x} = (x_1, \ldots, x_n)$ and $X_n = \int\int_{E_n}\int \Psi_n(\mathbf{x})\,\mathrm{d}\mathbf{x}$ as defined in Section 2. Here $\Psi_n(\mathbf{x}) = \frac{1}{(1+x_1)\cdots(1+x_1+\cdots+x_n)}$ is called the *invariant measure*. For the case $n = 1$, this can be found in [6]. The case in which $n > 1$ is rather new. Schweiger found in [30] another invariant measure. He uses another map t and instead of the unit cube E_n, he uses the area B_n, which is defined by $B_n = \{\mathbf{x} | 0 \le x_1 \le \cdots \le x_n \le 1\}$. (In fact he folded the unit cube E_n $n!$ times and got B_n). His invariant measure seems to be different, but the two invariant measures are in fact identical ([32]).

4.2 Proofs

Proof of Theorem 4.1. Our proof can be compared with the calculation of the average number of steps in Euclid's Algorithm (cf. [23]). In fact, using this proof one can generalize the result to an algorithm for calculating $\gcd(a_1, \ldots, a_n)$ using Brun's Algorithm. Unfortunately this yields worse results than $\gcd(gcd(a_1, a_2), a_3)$, etc.

Let $(a_1, \ldots, a_n)$ be an arbitrary n-tuple (hence not necessarily ordered). Let $u_k = \max(T^k(a_1, \ldots, a_n))$. Then $\rho_n(a_1, \ldots, a_n) = l_n(a_1, \ldots, a_n)/\log_2 u_0$. First we consider the denominator. Notice that $u_0 = \frac{u_0}{u_1} \cdot \frac{u_1}{u_2} \cdot \cdots \cdot \frac{u_{m-1}}{u_m}$, (we assume that $u_m = 1$). And therefore we have that $\log_2(u_0) = \frac{1}{\ln 2} \sum_{k=0}^{m-1} \ln\left(\frac{u_k}{u_{k+1}}\right)$. Now we consider the numerator. $l_n(a_1, \ldots, a_n) = l_n(T(a_1, \ldots, a_n)) + l_1(r) + 1$, where $r = \left\lfloor \frac{u_0}{u_1} \right\rfloor$. Therefore $l_n(a_1, \ldots, a_n) = \sum_{k=0}^{m-1}(l_1\left(\left\lfloor \frac{u_k}{u_{k+1}} \right\rfloor\right) + 1)$. Instead of the map $T(a_1, \ldots, a_n)$ we will consider $t\left(\frac{a_1}{a_i}, \ldots, \frac{a_n}{a_i}\right)$, in which the i th coordinate is removed (hence we consider a map on E_{n-1}). Let $v_k = \max(t^k\left(\frac{a_1}{a_i}, \ldots, \frac{a_n}{a_i}\right))$. Then we have $v_k = \frac{u_{k+1}}{u_k}$. Now $\rho_n(a_1, \ldots, a_n)$ can be expressed as

$$\rho_n(a_1, \ldots, a_n) = \frac{\frac{1}{m}\sum_{k=0}^{m-1}(l_1\left(\left\lfloor \frac{1}{v_k} \right\rfloor\right) + 1)}{\frac{-1}{m \cdot \ln 2}\sum_{k=0}^{m-1}\ln(v_k)}. \tag{8}$$

In order to consider $\overline{\rho_n}$ we may assume that m tends to infinity. Notice that both the numerator and denominator of Formula 8 are finite. A small step is made from rational numbers v_k to real numbers. This is allowed, (see [6]). (For a more precise approach, see [23]). We apply Ergodic Theory on the numerator and denominator as was described in the previous section. It will be shown that

$$\lim_{m\to\infty} \frac{1}{m} \sum_{k=0}^{m-1}(l_1\left(\left\lfloor \frac{1}{v_k} \right\rfloor\right) + 1) = \sigma_n$$

and

$$\lim_{m\to\infty} \frac{-1}{m \cdot \ln 2} \sum_{k=0}^{m-1} \ln(v_k) = \tau_n.$$

The calculation for the denominator is easy. We have

$$\begin{aligned}
\tau_n &= \lim_{m\to\infty} \frac{-1}{m \cdot \ln 2} \sum_{k=0}^{m-1} \ln(v_k) \\
&= \frac{-1}{\ln 2} \frac{1}{X_{n-1}} \int\int_{E_{n-1}} \int \ln(\max(x_1, \cdots, x_n)) \cdot \Psi_{n-1}(\mathbf{x})\, d\,\mathbf{x} \\
&= \frac{Y_{n-1}}{\ln 2 \cdot X_{n-1}}.
\end{aligned}$$

For the numerator we have

$$
\begin{aligned}
\sigma_n &= \lim_{m\to\infty} \tfrac{1}{m} \sum_{k=0}^{m-1} (l_1\left(\left\lfloor \frac{1}{v_k} \right\rfloor\right) + 1) \\
&= \frac{1}{X_{n-1}} \int\int_{E_{n-1}} \int (l_1(\max(x_1, \cdots, x_n)) + 1) \cdot \Psi_{n-1}(\mathbf{x})\, \mathrm{d}\,\mathbf{x} \\
&= 1 + \frac{1}{X_{n-1}} \sum_{k=1}^{\infty} \int\int_{\Delta_{n-1,k}} \int l_1(k) \cdot \Psi_{n-1}(\mathbf{x})\, \mathrm{d}\,\mathbf{x} \\
&= 1 + \frac{1}{X_{n-1}} \sum_{k=1}^{\infty} l_1(k) \cdot (Z_{n-1,k} - Z_{n-1,k+1}).
\end{aligned}
$$

This proves Theorem 4.1. □

Motivation of Conjecture 4.3. Let $a_1 < a_2 < \cdots < a_n$ and $T(a_1, \ldots, a_n) = (a_1, \cdots, a_i, b, a_{i+1}, \cdots, a_n)$ where $b = a_n - r a_{n-1}$ and $r = \left\lfloor \frac{a_n}{a_{n-1}} \right\rfloor$. It is simple to prove that $\lim_{n\to\infty} \sigma_n = 1$. This can be verified in Table I of the Appendix. It corresponds to the fact that if n tends to infinity then r tends to 1.

In order to approximate the behavior of τ_n if n tends to infinity, we have to approximate $\dfrac{max\{a_1, \ldots, a_n\}}{max\{T(a_1, \ldots, a_n)\}}$. Suppose $b = x_n - x_{n-1} < a_1$ and

$$\frac{a_n}{a_{n-1}} = \frac{a_{n-1}}{a_{n-2}} = \ldots = \frac{a_1}{b}. \tag{9}$$

Denote $\mu_n = \frac{a_{i+1}}{a_i}$. Then $a_k = \mu_n^k \cdot b$. Hence $b = a_n - a_{n-1} = (\mu_n^n - \mu_n^{n-1})b$. Under these conditions we have

$$\overline{\rho_n} \approx \frac{max\{a_1, \ldots, a_n\}}{max\{T(a_1, \ldots, a_n)\}} \approx \frac{\log_{\mu_n} a_n}{\log_2 a_n} = \frac{\ln 2}{\ln \mu_n}, \tag{10}$$

using Formula 6. The main open question is how much do $a_1, \ldots, a_n$ differ from the situation sketched in 9 and what are the consequences?

Motivation of Conjecture 4.4. An approximation of the largest root of $x^n - x^{n-1} = 1$ is $\mu \approx 1 + \frac{\ln n}{n}$, since $(1 + \frac{\ln n}{n})^n \approx e^{n \ln(1+\frac{\ln n}{n})} \approx e^{\ln n} = n$ and $(1 + \frac{\ln n}{n})^{n-1} \approx n - 1$.

5 Remarks, conclusions and open problems

The tables. Appendix A presents two tables. Table I shows some numerical approximations of the integrals X_n, Y_n and $Z_{n,2}$. Notice that $\overline{\rho_n} \approx \dfrac{1}{\tau_n} \approx \dfrac{X_{n-1}}{\ln(2) \cdot Y_{n-1}}$. Table II contains the results of 100 experiments for each width. Each experiment started by choosing randomly n 512-bit numbers. First we applied $2n$ steps of the Brun Algorithm without paying attention to the results. Then we considered 100 steps of which the results have been tabulated.

There are many multi-continued fraction algorithms (cf. [10]). Another algorithm, which is related to the Jacobi-Perron Algorithm, can be defined on E_n by

$$t(x_1,\ldots,x_n) = \left(\frac{y}{x_i},\frac{x_1}{x_i},\ldots,\frac{x_n}{x_i}\right), \text{ where } y = \frac{1}{x_i} - \left\lfloor\frac{1}{x_i}\right\rfloor \text{ and } x_i = \max(x_1,\ldots,x_n).$$

This algorithm was considered by Veugen in [37]. He found worse results compared to the results of the Brun Algorithm. Besides this experimental fact, there is another problem. Even though it has been proved that Ergodic Theory can be applied on this algorithm, the invariant measure is still unknown (cf. [30]).

Some open problems. Let $L_{\mathrm{OPT}}(a)$ denote a smallest addition chain for a, and let $l_{\mathrm{OPT}}(a)$ be its length. Let $m_{\mathrm{OPT}}(a) = M(L_{OPT}(a))$. Let d_n be the smallest number such that $m_{\mathrm{OPT}}(d_n) = n$. Which are the numbers d_n? We found $d_1 = 1$ and $d_2 = 15$. A comparable problem can be posed for addition sequences and vector addition chains.

Let $L(a_1,\ldots,a_n)$ be a minimal addition sequence which needs k memory locations. How many memory locations are needed for the corresponding minimal vector addition chain? (In [23, 27, 8] one can read how vector addition chains are related to addition sequences.)

We are interested in a precise evaluation of the integrals X_n, Y_n and $Z_{n,k}$ for $n > 2$. We were able to express X_2, Y_2 and $Z_{2,k}$ in terms of the poly-logarithm by applying [26]. Especially interesting is a precise evaluation of $\frac{Y_{n-1}}{X_{n-1}}$, since this fraction approximates $\overline{\rho_n}$.

Acknowledgement. I gratefully thank Cor Kraaikamp and Prof. H. Jager for their ideas concerning Ergodic theory and Leonard Flatto for his comments regarding my use of Ergodic theory. I profitted greatly from discussions with Prof. M.H.C. Paardekooper and Jurjen Bos and I am grateful to David Chaum, Eugène van Heyst and John Tromp for reading some parts of the manuscript. Furthermore I want to thank Herman te Riele and Lambert Meertens for the work they invested in this report.

References

[1] Agnew G.B., R.C. Mullin and S.A. Vanstone: "Arithmetic Operations in GF(2^n)", to appear in *J. of Cryptology*.

[2] Bellman R.: " Advanced problem 5125", *Amer. Math. Monthly* **70**, (1963), 765.

[3] Bergeron F., J. Berstel and S. Brlek: "A unifying approach to the generalisation of addition chains", in preparation, 1989.

[4] Bergeron F., J. Berstel, S. Brlek, C. Duboc: "Addition Chains Using Continued Fractions", *Journal of Algorithms* **10**, (1989), 403–412.

[5] Bergeron F., J. Olivos: "Vectorial addition chains using Euclid's algorithm", Prel. version, Univ. Québec à Montréal, 1989.

[6] Billingsley P.: "Ergodic theory and information", Wiley, New York, **1965**, pp. 40–50.

[7] Bos J.N.E. and M.J. Coster: "Addition chain heuristics", *Lecture Notes in Comp. Sc. 435*, Proceedings Crypto '89, Springer–Verlag, **1990**, pp. 400–407.

[8] Bos J.N.E. , "Practical Security", Desertation, Eindhoven, the Netherlands, **1992**, pp. 55–87.

[9] Brauer, "On addition chains", *Bull. Am. Math. Soc.* **45** (1939), pp 736–739.

[10] Brentjes A.J.: "Multi–dimensional continued fraction algorithms", *Mathematical Centre Tract 145*, Amsterdam, **1981**.

[11] Brlek S. and P. Castéran: "The addition chain control structure", in preparation, 1989.

[12] Brun V.: "Algorithmes euclidiens pour trois et quatres nombres", 13ième Congr. Scand., (1957) pp. 45–64.

[13] Chaum D.: "Online Cash Checks", Eurocrypt '89, *Lecture Notes in Computer Science*, pp. 288–293.

[14] Chaum D., and others: "Efficient cash checks", to appear, 1993.

[15] Chaum D., H. den Boer, E. van Heyst, S. Mjøolsnes and A. Steenbeek: "Efficient offline electronic checks", Eurocrypt '89, *Lecture Notes in Computer Science*, pp.294–301.

[16] Coster M.J., "Some algorithms on addition chains and their complexity", *Report CS-R9024*, C.W.I., Amsterdam, 1990.

[17] Dobkin D. and R. J. Lipton: "Addition chain methods for the evaluation of specific polynomials", *Siam J. Comput.* **9** (1980), 121–125.

[18] Downey P., B. Leony and R. Sethi: "Computing sequences with addition chains", *Siam Journ. Comput.* **3** (1981), 638–696.

[19] ElGamal T.: "A Public Key Cryptosystem and a Signature Scheme Based on Discrete logarithms", *IEEE Trans. Inf. Th.* **31** (1985).

[20] Erdös P.: "Remarks on number theory III, on addition chains", *Acta Arith.* **6**, (1960), 77–81.

[21] Fiat A.: "Batch RSA", *Lecture Notes in Comp. Sc. 435*, Proceedings Crypto '89, Springer–Verlag, 1990, pp. 175–185.

[22] Jager H.: "Metrical results for the nearest integer continued fraction", *Indag. Math.* **47** (1985), 417–427.

[23] Knuth D.E.: "The art of computer programming", Vol. **2**, Seminumerical algorithms, Addison–Wesley, Reading, Mass., (1969), second edition **1981**, pp. 339–364 and pp. 441–466.

[24] Kraaikamp C.: "Metric and arithmetic results for continued fraction expansions", Thesis, Amsterdam, **1990**.

[25] Lenstra H.W., jr.: "Factoring integers with elliptic curves", *Report 86-18*, Universiteit van Amsterdam, 1986.

[26] Lewin L.: "Dilogarithms and associated functions", Macdonald & Co, London, **1958**.

[27] Olivos J.: "On Vectorial Addition Chains", *J. of Algorithms* **2**, (1981), 13–21.

[28] Perron O., "Die Lehre von den Kettenbrüchen", Chelsea, New York 1929.

[29] Schönhage A.: "A lower bound on the length of addition chains", *Theoret. Comput. Sci.* **1**, (1975), 1–12.

[30] Schweiger F.: "Invariant measures and ergodic proporties of numbertheoretical endomorphisms", *Dyn. Systems and Ergodic Theory*, Banach Center Publ. **23** (1989), 283–295.

[31] Schweiger F.: "Ergodic properties of Multidimensional Subtractive Algorithms", to appear in *New trends in Probab. & Statistics*, Vol. **II**.

[32] Schweiger F.: "Personal communication", 1992.

[33] Straus E.G.: "Addition chains of vectors", *Amer. Math. Monthly* **71** (1964), 806–808 (problem 5125).

[34] Tsai Y.H. and Y. H. Chin: "A study of some addition chain problems", *Intern. J. Comp. Math.* **22**, (1987), 117–134.

[35] Toussaint H.-J.: "Der Algorithmus von Viggo Brun und verwandte Kettenbruchentwicklungen", Thesis, Techn. Univ. München, 1986.

[36] Vegh E.: "A note on addition chains", *J. Comb. Th. (A)* **19**, (1975), 117–118.

[37] Veugen Th.: "Some Mathematical and Computational Aspects of Electronic Cash", Master Thesis, Eindhoven, 1991.

[38] Veldhorst M. and H. Zantema: "Average length of addition chains", personal communication, **1989**.

[39] Williams H.C., "A $p+1$ method of factoring", *Math. Comp.* **39**, (1982), 225–234.

[40] Yao A., " On the evaluation of powers", *Siam J. Comput.* **5**, (1976), 100–103.

[41] Zantema H.: "Minimizing sums of addition chains", Univ. of Utrecht, *Report RUU-CS-89-15*, **1989**.

A Some Tables.

Table I	Numerical approximation of X_n, Y_n and $Z_{n,2}$.				
n	X_{n-1}	Y_{n-1}	$\tau_n = X_{n-1}/\ln(2)\cdot Y_{n-1}$	$Z_{n-1,2}$	$Z_{n-1,2}/X_{n-1}$
2	0.693147	0.8225	0.5841	0.4055	0.5850
3	0.374053	0.2504	1.035	0.1394	0.3726
4	0.166879	0.082	1.41	0.0418	0.2505
5	0.063856	0.025	1.75	0.0112	0.1748
6	0.021484	0.007	2.1	0.0027	0.1254

Table II	Approximations of $\overline{\rho_n}$ by experiments.					
n	$\sigma_n - 1$	$1/\tau_n$	$\overline{\rho_n}$	$\overline{\frac{1}{\tau_n}}$	$\overline{\frac{1}{\log_2(\mu_n)}}$	$\overline{\rho_n}\log_2(\mu_n)$
2	1.7977	1.7396	1.6083	0.5747	1.4404	1.1166
3	0.7247	0.9694	1.7791	1.0315	1.8134	0.9811
4	0.3913	0.7079	1.9654	1.4126	2.1507	0.9138
5	0.2470	0.5727	2.1775	1.7462	2.4650	0.8837
6	0.1596	0.4847	2.3923	2.0631	2.7625	0.8660
7	0.1124	0.4286	2.5954	2.3331	3.0472	0.8517
8	0.0730	0.3808	2.8175	2.6259	3.3215	0.8483
9	0.0555	0.3483	3.0302	2.8709	3.5873	0.8447
10	0.0462	0.3228	3.2414	3.0983	3.8459	0.8393
11	0.0332	0.3004	3.4395	3.3290	4.0983	0.8420
12	0.0257	0.2803	3.6586	3.5670	4.3451	0.8388
13	0.0206	0.2652	3.8477	3.7701	4.5872	0.8347
14	0.0161	0.2523	4.0271	3.9633	4.8249	0.8399
15	0.0124	0.2383	4.2488	4.1968	5.0586	0.8432
16	0.0097	0.2264	4.4594	4.4165	5.2889	0.8404
17	0.0075	0.2173	4.6356	4.6011	5.5158	0.8438
18	0.0044	0.2074	4.8433	4.8221	5.7398	0.8492
19	0.0059	0.1987	5.0618	5.0321	5.9610	0.8475
20	0.0037	0.1916	5.2374	5.2181	6.1796	0.8443
21	0.0031	0.1857	5.4003	5.3836	6.3959	0.8503
22	0.0022	0.1783	5.6206	5.6084	6.6098	0.8528
23	0.0017	0.1722	5.8179	5.8081	6.8217	0.8535
24	0.0016	0.1669	6.0015	5.9919	7.0316	0.8516
25	0.0008	0.1623	6.1650	6.1600	7.2397	0.8484
30	0.0005	0.1418	7.0543	7.0508	8.0550	0.8585
40	0.0002	0.1134	8.8177	8.8159	10.1877	0.8655
50	0.0000	0.0951	10.5200	10.5200	12.0248	0.8749

For the explanation of the experiments, see Section 5.

IN 1992 REEDS VERSCHENEN

532 F.G. van den Heuvel en M.R.M. Turlings
Privatisering van arbeidsongeschiktheidsregelingen
Refereed by Prof.Dr. H. Verbon

533 J.C. Engwerda, L.G. van Willigenburg
LQ-control of sampled continuous-time systems
Refereed by Prof.dr. J.M. Schumacher

534 J.C. Engwerda, A.C.M. Ran & A.L. Rijkeboer
Necessary and sufficient conditions for the existence of a positive definite solution of the matrix equation $X + A^{*}X^{-1}A = Q$.
Refereed by Prof.dr. J.M. Schumacher

535 Jacob C. Engwerda
The indefinite LQ-problem: the finite planning horizon case
Refereed by Prof.dr. J.M. Schumacher

536 Gert-Jan Otten, Peter Borm, Ton Storcken, Stef Tijs
Effectivity functions and associated claim game correspondences
Refereed by Prof.dr. P.H.M. Ruys

537 Jack P.C. Kleijnen, Gustav A. Alink
Validation of simulation models: mine-hunting case-study
Refereed by Prof.dr.ir. C.A.T. Takkenberg

538 V. Feltkamp and A. van den Nouweland
Controlled Communication Networks
Refereed by Prof.dr. S.H. Tijs

539 A. van Schaik
Productivity, Labour Force Participation and the Solow Growth Model
Refereed by Prof.dr. Th.C.M.J. van de Klundert

540 J.J.G. Lemmen and S.C.W. Eijffinger
The Degree of Financial Integration in the European Community
Refereed by Prof.dr. A.B.T.M. van Schaik

541 J. Bell, P.K. Jagersma
Internationale Joint Ventures
Refereed by Prof.dr. H.G. Barkema

542 Jack P.C. Kleijnen
Verification and validation of simulation models
Refereed by Prof.dr.ir. C.A.T. Takkenberg

543 Gert Nieuwenhuis
Uniform Approximations of the Stationary and Palm Distributions of Marked Point Processes
Refereed by Prof.dr. B.B. van der Genugten

544 R. Heuts, P. Nederstigt, W. Roebroek, W. Selen
Multi-Product Cycling with Packaging in the Process Industry
Refereed by Prof.dr. F.A. van der Duyn Schouten

545 J.C. Engwerda
Calculation of an approximate solution of the infinite time-varying LQ-problem
Refereed by Prof.dr. J.M. Schumacher

546 Raymond H.J.M. Gradus and Peter M. Kort
On time-inconsistency and pollution control: a macroeconomic approach
Refereed by Prof.dr. A.J. de Zeeuw

547 Drs. Dolph Cantrijn en Dr. Rezaul Kabir
De Invloed van de Invoering van Preferente Beschermingsaandelen op Aandelenkoersen van Nederlandse Beursgenoteerde Ondernemingen
Refereed by Prof.dr. P.W. Moerland

548 Sylvester Eijffinger and Eric Schaling
Central bank independence: criteria and indices
Refereed by Prof.dr. J.J. Sijben

549 Drs. A. Schmeits
Geïntegreerde investerings- en financieringsbeslissingen; Implicaties voor Capital Budgeting
Refereed by Prof.dr. P.W. Moerland

550 Peter M. Kort
Standards versus standards: the effects of different pollution restrictions on the firm's dynamic investment policy
Refereed by Prof.dr. F.A. van der Duyn Schouten

551 Niels G. Noorderhaven, Bart Nooteboom and Johannes Berger
Temporal, cognitive and behavioral dimensions of transaction costs; to an understanding of hybrid vertical inter-firm relations
Refereed by Prof.dr. S.W. Douma

552 Ton Storcken and Harrie de Swart
Towards an axiomatization of orderings
Refereed by Prof.dr. P.H.M. Ruys

553 J.H.J. Roemen
The derivation of a long term milk supply model from an optimization model
Refereed by Prof.dr. F.A. van der Duyn Schouten

554 Geert J. Almekinders and Sylvester C.W. Eijffinger
Daily Bundesbank and Federal Reserve Intervention and the Conditional Variance Tale in DM/$-Returns
Refereed by Prof.dr. A.B.T.M. van Schaik

555 Dr. M. Hetebrij, Drs. B.F.L. Jonker, Prof.dr. W.H.J. de Freytas
"Tussen achterstand en voorsprong" de scholings- en personeelsvoorzieningsproblematiek van bedrijven in de procesindustrie
Refereed by Prof.dr. Th.M.M. Verhallen

556 Ton Geerts
Regularity and singularity in linear-quadratic control subject to implicit continuous-time systems
Communicated by Prof.dr. J. Schumacher

557 Ton Geerts
Invariant subspaces and invertibility properties for singular systems: the general case
Communicated by Prof.dr. J. Schumacher

558 Ton Geerts
Solvability conditions, consistency and weak consistency for linear differential-algebraic equations and time-invariant singular systems: the general case
Communicated by Prof.dr. J. Schumacher

559 C. Fricker and M.R. Jaïbi
Monotonicity and stability of periodic polling models
Communicated by Prof.dr.ir. O.J. Boxma

560 Ton Geerts
Free end-point linear-quadratic control subject to implicit continuous-time systems: necessary and sufficient conditions for solvability
Communicated by Prof.dr. J. Schumacher

561 Paul G.H. Mulder and Anton L. Hempenius
Expected Utility of Life Time in the Presence of a Chronic Noncommunicable Disease State
Communicated by Prof.dr. B.B. van der Genugten

562 Jan van der Leeuw
The covariance matrix of ARMA-errors in closed form
Communicated by Dr. H.H. Tigelaar

563 J.P.C. Blanc and R.D. van der Mei
Optimization of polling systems with Bernoulli schedules
Communicated by Prof.dr.ir. O.J. Boxma

564 B.B. van der Genugten
Density of the least squares estimator in the multivariate linear model with arbitrarily normal variables
Communicated by Prof.dr. M.H.C. Paardekooper

565 René van den Brink, Robert P. Gilles
Measuring Domination in Directed Graphs
Communicated by Prof.dr. P.H.M. Ruys

566 Harry G. Barkema
The significance of work incentives from bonuses: some new evidence
Communicated by Dr. Th.E. Nijman

579 J. Ashayeri, W.H.L. van Esch, R.M.J. Heuts
Amendment of Heuts-Selen's Lotsizing and Sequencing Heuristic for Single Stage Process Manufacturing Systems
Communicated by Prof.dr. F.A. van der Duyn Schouten

580 H.G. Barkema
The Impact of Top Management Compensation Structure on Strategy
Communicated by Prof.dr. S.W. Douma

581 Jos Benders en Freek Aertsen
Aan de lijn of aan het lijntje: wordt slank produceren de mode?
Communicated by Prof.dr. S.W. Douma

582 Willem Haemers
Distance Regularity and the Spectrum of Graphs
Communicated by Prof.dr. M.H.C. Paardekooper

583 Jalal Ashayeri, Behnam Pourbabai, Luk van Wassenhove
Strategic Marketing, Production, and Distribution Planning of an Integrated Manufacturing System
Communicated by Prof.dr. F.A. van der Duyn Schouten

584 J. Ashayeri, F.H.P. Driessen
Integration of Demand Management and Production Planning in a Batch Process Manufacturing System: Case Study
Communicated by Prof.dr. F.A. van der Duyn Schouten

585 J. Ashayeri, A.G.M. van Eijs, P. Nederstigt
Blending Modelling in a Process Manufacturing System
Communicated by Prof.dr. F.A. van der Duyn Schouten

586 J. Ashayeri, A.J. Westerhof, P.H.E.L. van Alst
Application of Mixed Integer Programming to A Large Scale Logistics Problem
Communicated by Prof.dr. F.A. van der Duyn Schouten

587 P. Jean-Jacques Herings
On the Structure of Constrained Equilibria
Communicated by Prof.dr. A.J.J. Talman

IN 1993 REEDS VERSCHENEN

588 Rob de Groof and Martin van Tuijl
The Twin-Debt Problem in an Interdependent World
Communicated by Prof.dr. Th. van de Klundert

589 Harry H. Tigelaar
A useful fourth moment matrix of a random vector
Communicated by Prof.dr. B.B. van der Genugten

590 Niels G. Noorderhaven
Trust and transactions; transaction cost analysis with a differential behavioral assumption
Communicated by Prof.dr. S.W. Douma

591 Henk Roest and Kitty Koelemeijer
Framing perceived service quality and related constructs
A multilevel approach
Communicated by Prof.dr. Th.M.M. Verhallen

592 Jacob C. Engwerda
The Square Indefinite LQ-Problem: Existence of a Unique Solution
Communicated by Prof.dr. J. Schumacher

593 Jacob C. Engwerda
Output Deadbeat Control of Discrete-Time Multivariable Systems
Communicated by Prof.dr. J. Schumacher

594 Chris Veld and Adri Verboven
An Empirical Analysis of Warrant Prices versus Long Term Call Option Prices
Communicated by Prof.dr. P.W. Moerland

595 A.A. Jeunink en M.R. Kabir
De relatie tussen aandeelhoudersstructuur en beschermingsconstructies
Communicated by Prof.dr. P.W. Moerland

596 M.J. Coster and W.H. Haemers
Quasi-symmetric designs related to the triangular graph
Communicated by Prof.dr. M.H.C. Paardekooper

597 Noud Gruijters
De liberalisering van het internationale kapitaalverkeer in historisch-institutioneel perspectief
Communicated by Dr. H.G. van Gemert

598 John Görtzen en Remco Zwetheul
Weekend-effect en dag-van-de-week-effect op de Amsterdamse effectenbeurs?
Communicated by Prof.dr. P.W. Moerland

599 Philip Hans Franses and H. Peter Boswijk
Temporal aggregration in a periodically integrated autoregressive process
Communicated by Prof.dr. Th.E. Nijman