An algorithm on addition chains with restricted memory
Coster, M.J.

Document version:
Publisher's PDF, also known as Version of record

Publication date:
1993

Link to publication

Citation for published version (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright, please contact us providing details, and we will remove access to the work immediately and investigate your claim.
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 · 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:

- $a$: 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
- $\lambda(n) = \lfloor \log_2 n \rfloor$
In the log equation \( x^n - x^{n-1} - 1 = 0 \), with \( \mu_n > 1 \)

- \( E_n \) is the unit cube in \( n \) dimensions, \( \{x | 0 \leq x_i \leq 1 \text{ for } 1 \leq i \leq n\} \)
- \( E_{n,k} \) is \( \{x | 0 \leq x_i \leq \frac{1}{k} \text{ for } 1 \leq i \leq n\} \)
- \( \Delta_{n,k} = E_{n,k} \setminus E_{n,k+1} \)
- \( M(L) \) is the number of memory locations used by Algorithm \( L \)
- \( T(a_1, \ldots, a_n) \) is an integral map related to the Brun-algorithm, see Section 4.1
- \( t(x_1, \ldots, x_n) \) is a real map on \( E_n \) related to the Brun-algorithm, see Section 4.1

\[
\Psi_n(x) = \frac{1}{(1 + x_1) \cdots (1 + x_1 + \cdots + x_n)}
\]

\[
X_n = \int \int_{E_n} \int \Psi_n(x) \, dx
\]

\[
Y_n = -\int \int_{E_n} \int \ln(\max(x_1, \ldots, x_n)) \cdot \Psi_n(x) \, dx
\]

\[
Z_{n,k} = \int \int_{E_{n,k}} \int \Psi_n(x) \, dx
\]

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

1. \( b_0 = 1 \),
2. for all \( 1 \leq k \leq l \) there exist \( i, j \) such that \( b_k = b_i + b_j \), for \( 0 \leq i, j < k \),
3. \( b_l = a \).

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:

1. \( b_0 = 1 \),
2. for all \( 1 \leq k \leq l \) there exist \( i, j \) such that \( b_k = b_i + b_j \), for \( 0 \leq i, j < k \),
3. \( b_l = a_m \in \{b_0, \ldots, b_l\} \).

We call \( n \) the width of the addition sequence and \( l \) the length. It will be assumed 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:

- \( L(k)(a_1, \ldots, a_n) \) is an addition sequence containing \( a_1, \ldots, a_n \) using only \( k \) memory locations \( (k \geq n) \)
- \( l(a_1, \ldots, a_n) \) is the length of an addition sequence containing \( a_1, \ldots, a_n \)
\[ \rho(a_1, \ldots, a_n) \quad \nu(a_1, \ldots, a_n)/\log_2 a_n \]
\[ \overline{\rho}(\alpha, n) \quad \text{average value of } \rho(a_1, \ldots, a_n) \text{ such that } \lambda(a_n) = \alpha. \text{ We abbreviate this notation to } \overline{\rho} \]

- \( L_1(a) \) 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

\[ \log_2 a + \log_2 \nu(a) - 2.13 \leq \nu(a). \] (1)

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

\[ \nu(a) \leq \log_2 a + \log_2 a/\log_2 \log_2 a + o(\log a/\log \log a). \] (2)

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

\[ \nu(a) \leq \log_2 a + \frac{1}{k} \log_2 a + 2^{k-1} - k - 1, \] (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:

\[ \nu(a_1, \ldots, a_n) \leq \log_2 a_n + \frac{1}{k} \log_2 a_n + 2^{nk} - n - 1, \] (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:

\[ \nu(a_1, \ldots, a_n) \leq \log_2 a_n + \frac{n}{k} \log_2 a_n + n \cdot 2^k - k - 1, \] (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 multi-
plying 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 $L^{(n)2^{k-1}}$ 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 se-
quence 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 pa-
per. The basis for both algorithms is Brun’s multi continued fraction algorithm. Sup-
pose that $a_1 \leq \cdots \leq a_n$. Let $r = \left\lfloor \frac{a_n}{a_{n-1}} \right\rfloor$. Let $T : \mathbb{Z}^n \to \mathbb{Z}^n$ be a map with
$T(a_1, \ldots, a_n) = (a_1, \ldots, a_{i}, b, a_{i+1}, \ldots, a_{n-1})$, where $b = a_n - ra_{n-1}$ 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 $r_ia_{n-1}$
for $1 \leq i \leq l$ and $a_n$, where $L_1(r) = \{r_0, r_1, \ldots, r_l\}$ 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 \( X^n \), 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 \( \bar{\rho}(\alpha, n) \). We define \( \bar{\rho}(\alpha, n) \) by

\[
\bar{\rho}(\alpha, n) = \frac{1}{\Sigma} \sum_{(a_1, \ldots, a_n)} \frac{l_n(a_1, \ldots, a_n)}{\log_2 a_n},
\]

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

\[
l(a_1, \ldots, a_n) \approx \bar{\rho} \log_2 a_n
\]

in the case of the Brun Algorithm. In the case of the Brun Algorithm, we will denote the average value of \( \rho \) by \( \bar{\rho}_n \), 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 \( \bar{\rho}_n = \frac{\sigma_n}{\tau_n} \), 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) \( \bar{\rho}_2 = 1.6080967 \ldots \),

(ii) \( \bar{\rho}_3 = 1.7768807 \ldots \).
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 $\mu_n$ 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 $t(x_1, \ldots, x_n) = \left( \frac{1}{x_i} - \left\lfloor \frac{1}{x_i} \right\rfloor, x_1, \ldots, x_n \right)$, 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 $x_1, \ldots, x_n$ are not necessarily ordered. This map $t$ is due to Brun. In fact we consider the so called *Trantasposed 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 $|\frac{1}{x_i} - \left\lfloor \frac{1}{x_i} \right\rfloor| = 1$?”, “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

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

where $x = (x_1, \ldots, x_n)$ and $X_n = \int \int_{E_n} \Psi_n(x) \, dx$ as defined in Section 2. Here

$$
\Psi_n(x) = \frac{1}{(1 + x_1) \cdots (1 + x_1 + \cdots + x_n)}
$$

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 $B_n = \{x|0 \leq x_1 \leq \cdots \leq x_n \leq 1\}$. (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 \( u_0 = \frac{u_1}{u_1} \cdot \frac{u_2}{u_2} \cdots \frac{u_m-1}{u_m} \), (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.

\[
l_n(a_1, \ldots, a_n) = l_n(T(a_1, \ldots, a_n)) + l_1(r) + 1, \quad \text{where } r = \left\lfloor \frac{u_0}{u_1} \right\rfloor.
\]

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 \( v_k = u_{k+1} \). Now \( \rho_n(a_1, \ldots, a_n) \) can be expressed as

\[
\rho_n(a_1, \ldots, a_n) = \frac{1}{m} \sum_{k=0}^{m-1} \left( l_1 \left( \left\lfloor \frac{1}{v_k} \right\rfloor \right) + 1 \right).
\]

(8)

In order to consider \( \bar{\rho}_n \) 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

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

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

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

\[
= \frac{1}{\ln 2} \int \int_{E_{n-1}} \int \ln(\max(x_1, \ldots, x_n)) \cdot \Psi_{n-1}(x) \, d\mathbf{x}
\]

\[
= \frac{Y_{n-1}}{\ln 2 \cdot X_{n-1}}.
\]
For the numerator we have

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

\[
= \frac{1}{X_{n-1}} \int \int \int_{E_{n-1}} \left( l_i(\max(x_1, \ldots, x_n)) + 1 \right) \cdot \Psi_{n-1}(x) \, dx
\]

\[
= 1 + \frac{1}{X_{n-1}} \sum_{k=1}^{\infty} \int \int_{\Delta_{n-1,k}} \int l_i(k) \cdot \Psi_{n-1}(x) \, dx
\]

\[
= 1 + \frac{1}{X_{n-1}} \sum_{k=1}^{\infty} l_i(k) \cdot (Z_{n-1,k} - Z_{n-1,k+1}).
\]

This proves Theorem 4.1.

**Motivation of Conjecture 4.3.** Let \( a_1 < a_2 < \cdots < a_n \) and \( T(a_1, \ldots, a_n) = (a_1, \ldots, a_i, b, a_{i+1}, \ldots, a_n) \) where \( b = a_n - r a_{n-1} \) and \( r = \left| \frac{a_n}{a_{n-1}} \right| \). It is simple to prove that \( \lim \sigma_n = 1 \). 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 \( \tau_n \) if \( n \) tends to infinity, we have to approximate \( \frac{\max\{a_1, \ldots, a_n\}}{\max\{T(a_1, \ldots, a_n)\}} \). Suppose \( b = x_n - x_{n-1} < a_1 \) and

\[
\frac{a_n}{a_{n-1}} = \frac{a_{n-1}}{a_{n-2}} = \cdots = \frac{a_1}{b}.
\]

(9)

Denote \( \mu_n = \frac{a_{n+1}}{a_n} \). 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

\[
\bar{\rho}_n \approx \frac{\max\{a_1, \ldots, a_n\}}{\max\{T(a_1, \ldots, a_n)\}} \approx \frac{\log_\mu_n a_n}{\log_2 a_n} = \frac{\ln 2}{\ln \mu_n},
\]

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 \( \bar{\rho}_n \approx \frac{1}{\tau_n} \approx \frac{X_{n-1}}{\ln(2) \cdot Y_{n-1}} \). 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

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

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 $L_{OPT}(a)$ denote a smallest addition chain for $a$, and let $l_{OPT}(a)$ be its length. Let $m_{OPT}(a) = M(L_{OPT}(a))$. Let $d_n$ be the smallest number such that $m_{OPT}(d_n) = n$. 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**


**A  Some Tables.**

<table>
<thead>
<tr>
<th>Table I</th>
<th>Numerical approximation of $X_n$, $Y_n$ and $Z_{n,2}$.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
<td>$X_{n-1}$</td>
</tr>
<tr>
<td>--</td>
<td>---------</td>
</tr>
<tr>
<td>2</td>
<td>0.693147</td>
</tr>
<tr>
<td>3</td>
<td>0.374053</td>
</tr>
<tr>
<td>4</td>
<td>0.166879</td>
</tr>
<tr>
<td>5</td>
<td>0.063856</td>
</tr>
<tr>
<td>6</td>
<td>0.021484</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table II</th>
<th>Approximations of $\overline{p}_n$ by experiments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
<td>$\sigma_n - 1$</td>
</tr>
<tr>
<td>--</td>
<td>-----------------</td>
</tr>
<tr>
<td>2</td>
<td>1.7977</td>
</tr>
<tr>
<td>3</td>
<td>0.7247</td>
</tr>
<tr>
<td>4</td>
<td>0.3913</td>
</tr>
<tr>
<td>5</td>
<td>0.2470</td>
</tr>
<tr>
<td>6</td>
<td>0.1596</td>
</tr>
<tr>
<td>7</td>
<td>0.1124</td>
</tr>
<tr>
<td>8</td>
<td>0.0730</td>
</tr>
<tr>
<td>9</td>
<td>0.0555</td>
</tr>
<tr>
<td>10</td>
<td>0.0462</td>
</tr>
<tr>
<td>11</td>
<td>0.0332</td>
</tr>
<tr>
<td>12</td>
<td>0.0257</td>
</tr>
<tr>
<td>13</td>
<td>0.0206</td>
</tr>
<tr>
<td>14</td>
<td>0.0161</td>
</tr>
<tr>
<td>15</td>
<td>0.0124</td>
</tr>
<tr>
<td>16</td>
<td>0.0097</td>
</tr>
<tr>
<td>17</td>
<td>0.0075</td>
</tr>
<tr>
<td>18</td>
<td>0.0044</td>
</tr>
<tr>
<td>19</td>
<td>0.0059</td>
</tr>
<tr>
<td>20</td>
<td>0.0037</td>
</tr>
<tr>
<td>21</td>
<td>0.0031</td>
</tr>
<tr>
<td>22</td>
<td>0.0022</td>
</tr>
<tr>
<td>23</td>
<td>0.0017</td>
</tr>
<tr>
<td>24</td>
<td>0.0016</td>
</tr>
<tr>
<td>25</td>
<td>0.0008</td>
</tr>
<tr>
<td>30</td>
<td>0.0005</td>
</tr>
<tr>
<td>40</td>
<td>0.0002</td>
</tr>
<tr>
<td>50</td>
<td>0.0000</td>
</tr>
</tbody>
</table>

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 personeelsvoor-
zieningsproblematiek van bedrijven in de procesindustrie
Refereed by Prof.dr. Th.M.M. Verhallen
Regularity and singularity in linear-quadratic control subject to implicit continuous-time systems
Communicated by Prof.dr. J. Schumacher

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

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

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

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

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

The covariance matrix of ARMA-errors in closed form
Communicated by Dr. H.H. Tigelaar

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

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

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

Harry G. Barkema
The significance of work incentives from bonuses: some new evidence
Communicated by Dr. Th.E. Nijman
567 Rob de Groof and Martin van Tuijl
Commercial integration and fiscal policy in interdependent, financially integrated two-sector economies with real and nominal wage rigidity.
Communicated by Prof.dr. A.L. Bovenberg

568 F.A. van der Duyn Schouten, M.J.G. van Eijs, R.M.J. Heuts
The value of information in a fixed order quantity inventory system
Communicated by Prof.dr. A.J.J. Talman

569 E.N. Kertzman
Begrotingsnormering en EMU
Communicated by Prof.dr. J.W. van der Dussen

570 A. van den Elzen, D. Talman
Finding a Nash-equilibrium in noncooperative N-person games by solving a sequence of linear stationary point problems
Communicated by Prof.dr. S.H. Tijs

571 Jack P.C. Kleijnen
Verification and validation of models
Communicated by Prof.dr. F.A. van der Duyn Schouten

572 Jack P.C. Kleijnen and Willem van Groenendaal
Two-stage versus sequential sample-size determination in regression analysis of simulation experiments

573 Pieter K. Jagersma
Het management van multinationale ondernemingen: de concernstructuur

574 A.L. Hempenius
Explaining Changes in External Funds. Part One: Theory
Communicated by Prof.Dr.Ir. A. Kapteyn

575 J.P.C. Blanc, R.D. van der Mei
Optimization of Polling Systems by Means of Gradient Methods and the Power-Series Algorithm
Communicated by Prof.dr.ir. O.J. Boxma

576 Herbert Hamers
A silent duel over a cake
Communicated by Prof.dr. S.H. Tijs

577 Gerard van der Laan, Dolf Talman, Hans Kremers
On the existence and computation of an equilibrium in an economy with constant returns to scale production
Communicated by Prof.dr. P.H.M. Ruys

578 R.Th.A. Wagemakers, J.J.A. Moors, M.J.B.T. Janssens
Characterizing distributions by quantile measures
Communicated by Dr. R.M.J. Heuts
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 aggregation in a periodically integrated autoregressive process
Communicated by Prof.dr. Th.E. Nijman
600 René Peeters
On the p-ranks of Latin Square Graphs
Communicated by Prof. dr. M.H.C. Paardekooper

601 Peter E.M. Borm, Ricardo Cao, Ignacio García-Jurado
Maximum Likelihood Equilibria of Random Games
Communicated by Prof. dr. B.B. van der Genugten

602 Prof. dr. Robert Bannink
Size and timing of profits for insurance companies. Cost assignment for products with multiple deliveries.
Communicated by Prof. dr. W. van Hulst