On Converting Numbers to the Double-Base Number System

Valerie Berthe, Laurent Imbert

On Converting Numbers to the Double-Base Number System

Valérie Berthé[a], and Laurent Imbert[a,b]

[a] LIRMM, CNRS UMR 5506
161 rue Ada, 34392 Montpellier cedex 5, France

[b] ATIPS, CISaC, University of Calgary
2500 University drive N.W, Calgary, T2N 1C2, Canada

ABSTRACT

This paper is an attempt to bring some theory on the top of some previously unproved experimental statements about the double-base number system (DBNS). We use results from diophantine approximation to address the problem of converting integers into DBNS. Although the material presented in this article is mainly theoretical, the proposed algorithm could lead to very efficient implementations.

Keywords: Double base number system, Ostrowski's numeration, continued fractions, diophantine approximations

1. INTRODUCTION

The Double-Base number system (DBNS), introduced by V. Dimitrov and G. A. Jullien[1] has advantages in many applications, like cryptography[2] and digital signal processing.[3] Recently, in his Ph.D. dissertation,[4] R. Muscedere proposed hardware-based solutions for the difficult operations in the Multi-Dimensional Logarithmic Number System (MDLNS), which can be seen as a generalization of the DBNS. He addresses the problems of addition, subtraction, and conversion from binary. Efficient methods have been proposed – using lookup-tables with specific addressing scheme – for digital signal processing applications, where the dynamic range of the numbers do not usually exceed 16-to-32 bits. However, such table-based solutions become unrealistic to implement as the numbers grow, as with cryptographic applications for example, and seem also quite difficult to generalize.

The main objective of this paper is to find one of the probably many theoretical approaches to the problem of converting a number from binary to DBNS. We tackle the problem using continued fractions, Ostrowski's number systems, and diophantine approximations.

In the Double-Base number system, we represent integers in the form

$$x = \sum_{i,j} d_{i,j}\, 2^i\, 3^j, \tag{1}$$

where $d_{i,j} \in \{0, 1\}$ and i, j are non-negative, independent integers. In the rest of the paper, we shall refer to numbers of the form $2^a 3^b$ as 2-*integers*.

Clearly, this representation is highly redundant. For every integer x, the representations with the minimum number of 2-integers (less than, or equal to x) are called the *canonic double-base number representations*. For example, 127 has 783 different representations, amongst which 3 are canonic (with only three 2-integers).

$$127 = 2^2 3^3 + 2^1 3^2 + 2^0 3^0 = 2^2 3^3 + 2^4 3^0 + 2^0 3^1 = 2^5 3^1 + 2^0 3^3 + 2^2 3^0.$$

Further author information:
E-mail: `Berthe@lirmm.fr`
E-mail: `Laurent.Imbert@lirmm.fr`
LIRMM: Laboratoire d'Informatique, Robotique et Microélectronique de Montpellier.
ATIPS: Advanced Technology Information Processing Systems, Dept. of Electrical and Computer Engineering.
CISaC: Center for Information Security and Cryptography, Dept. of Mathematics.

Finding the canonic DBNS representation of an integer from its binary representation is a difficult problem. A greedy algorithm was proposed[5] which gives the so-called *near-canonic double-base number representation*. Given x, it finds the largest 2-integer s less than or equal to x, and continues with $x - s$ until reaching zero. It is proved that the greedy algorithm terminates in $O\left(\frac{\log x}{\log\log x}\right)$ iterations.

In this paper we investigate the problem of finding the largest 2-integer less than or equal to x. Although this is not a difficult problem, we shall see that our solution is much more efficient than the straightforward approach performing the exhaustive search.

More precisely, we try to find two non-negative integers a, b such that $2^a 3^b \leq x$, and amongst the solutions to this problem, $2^a\,3^b$ is the largest possible value, i.e.

$$2^a 3^b = \max\left\{2^c 3^d,\ \text{such that } (c,d) \in \mathbb{N}^2,\ \text{and } 2^c 3^d \leq x\right\}. \tag{2}$$

If we let $a, b \in \mathbb{N}$ be such that $2^a 3^b \leq x$, our problem can be reformulated as finding non-negative integers a and b such that

$$a\,\log 2 + b\,\log 3 \leq \log x, \tag{3}$$

and such that, no other integers $c, d \geq 0$ give a better left approximation to $\log x$.

Let us define $\alpha = \log_3 2$ and $\beta = \{\log_3 x\} = \log_3 x - \lfloor \log_3 x \rfloor$ (β is the fractional part of $\log_3 x$). Then we try to find the best left approximation to $\log_3 x$ with non-negative integers. If a, b are solutions to this problem, then, for all $c, d \in \mathbb{N}^2$, with $c \neq a, d \neq b$, we have

$$c\,\alpha + d < a\,\alpha + b \leq \beta + \lfloor \log_3 x \rfloor. \tag{4}$$

A graphical interpretation to this problem is to consider the line Δ of equation $y = -\alpha\,x + \log_3 x$. The solutions are the points with integer coordinates, located in the area defined by the line Δ and the axes (in grey on Fig. 1). The best solution is the point which best approximate $\log_3 x$.

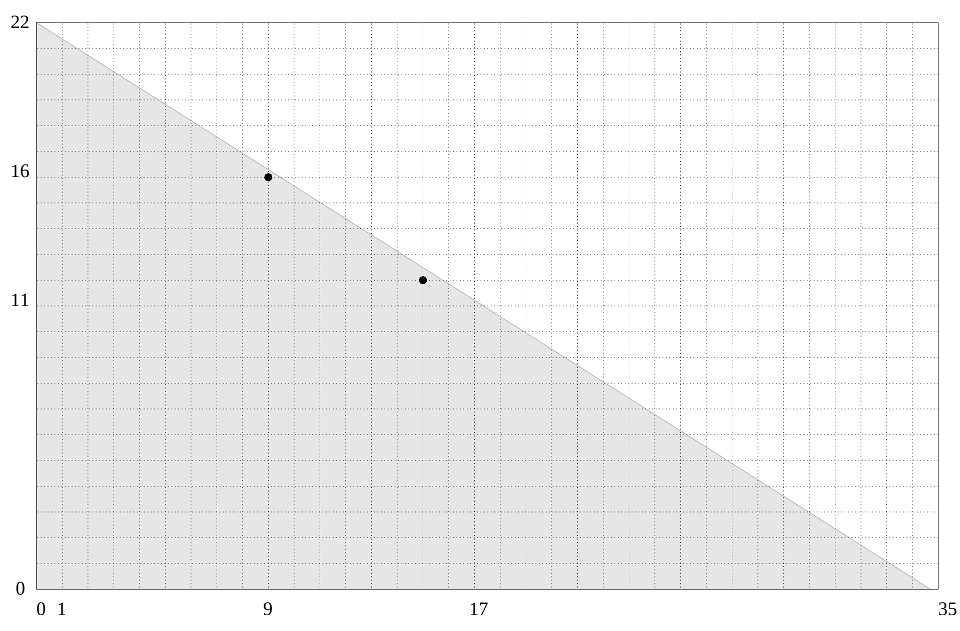

Figure 1. Graphical interpretation to the problem of finding the largest 2-integer less than x.

To solve this problem, we use results from the theory of continued fractions and diophantine approximations. We introduce the necessary mathematical background in the next section.

2. CONTINUED FRACTIONS AND OSTROWSKI'S NUMBER SYSTEM

A *simple continued fraction* is an expression of the form

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}},$$

where the *partial quotients* a_i are ≥ 1. A continued fraction is represented by the sequence $(a_n)_{n\in\mathbb{N}}$ which can either be *finite* or *infinite*.

An important result is that every irrational real number α can be expressed uniquely as an infinite simple continued fraction, written is a compact abbreviated notation as $\alpha = [a_0, a_1, a_2, a_3, \ldots]$. Similarly, every rational number can be expressed uniquely as a finite simple continued fraction. For example, the infinite continued fraction expansions of the irrationals π and e are

$$\begin{aligned} \pi &= [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, \ldots] \\ e &= [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]. \end{aligned}$$

The quantity obtained by restricting the continued fraction to its first $n+1$ partial quotients

$$\frac{p_n}{q_n} = [a_0, a_1, a_2, \ldots, a_n]$$

is called the *nth convergent*. The series $(p_n)_{n\in\mathbb{N}}$ and $(q_n)_{n\in\mathbb{N}}$ are computed inductively, starting with $p_{-1} = 1, q_{-1} = 0, p_0 = 0, q_0 = 1$, and for all $n \in \mathbb{N}$

$$p_{n+1} = a_{n+1}\, p_n + p_{n-1}, \qquad q_{n+1} = a_{n+1}\, q_n + q_{n-1}. \tag{5}$$

The sequence of the convergents of a infinite continued fraction gives a series of rational approximations of an irrational number. For example, the first convergents of π are listed in table 1.

Partial quotients	Convergents	Value
$[3]$	3	3.000000000
$[3, 7]$	$\frac{22}{7}$	3.142857143
$[3, 7, 15]$	$\frac{333}{106}$	3.141509434
$[3, 7, 15, 1]$	$\frac{355}{113}$	3.141592920
$[3, 7, 15, 1, 292]$	$\frac{103993}{33102}$	3.141592653

Table 1. The first partial quotients and convergents of π.

Ostrowski's number system[6] is associated with the series $(q_n)_{n\in\mathbb{N}}$ of the denominators of the convergents of the continued fraction expansion of an irrational number $0 < \alpha < 1$. The following proposition holds.

Proposition 1. *Every integer N can be written uniquely on the form*

$$N = \sum_{k=1}^{m} d_k\, q_{k-1}, \tag{6}$$

where

$$\begin{cases} 0 \leq d_1 \leq a_1 - 1, \ \textit{and}\ 0 \leq d_k \leq a_k \ \textit{for}\ k > 1, \\ d_k = 0 \ \textit{if}\ d_{k+1} = a_{k+1}. \end{cases}$$

For example, if $\alpha = \frac{1+\sqrt{5}}{2} = [1, 1, 1, 1, \dots]$ is the golden section, we obtain the well known Fibonacci number system, and the condition $d_k = 0$ if $d_{k+1} = a_{k+1}$ correspond to the fact that we do not have two consecutive ones. This representation is called the Zeckendorf representation.[7]

Ostrowski's representation of integers can be extended to real numbers.[8] The base is given by the sequence $(\theta_n)_{n\in N}$, where $\theta_n = (q_n\alpha - p_n)$. We have the following proposition.

Proposition 2. *Every real number β such that $-\alpha \le \beta < 1 - \alpha$ can be written uniquely on the form*

$$\beta = \sum_{k=1}^{+\infty} b_k\, \theta_{k-1}, \tag{7}$$

where

$$\begin{cases} 0 \le b_1 \le a_1 - 1, \ \textit{and}\ 0 \le b_k \le a_k \ \textit{for}\ k > 1, \\ b_k = 0 \ \textit{if}\ b_{k+1} = a_{k+1}. \end{cases}$$

Prop. 2 can be used to approximate β modulo 1 (i.e. by only considering the fractional part) by numbers of the form $N\alpha$. If we represent β using (7), the best approximations are given by the integers

$$N_n = \sum_{k=1}^{n} b_k\, q_{k-1}. \tag{8}$$

In some circumstances, it might be interesting to define the best left approximations of β. In this case, we represent β according to the base $(|\theta_n|)_{n\in\mathbb{N}}$. The following proposition holds.

Proposition 3. *Every real number β such that $0 \le \beta < 1$, can be written uniquely on the form*

$$\beta = \sum_{k=1}^{+\infty} c_k |\theta_{k-1}|, \tag{9}$$

where

$$\begin{cases} 0 \le c_k \le a_k \ \textit{for}\ k > 1, \\ c_{k+1} = 0 \ \textit{if}\ c_k = a_k. \end{cases}$$

In this case, the sequence of best left approximations is more difficult to define due to the alternate signs of $(\theta_n)_{n\in\mathbb{N}}$. In the next section, we present an algorithm[9] which solves this problem.

3. DEFINITION OF THE SEQUENCE OF NON-HOMOGENEOUS BEST APPROXIMATIONS OF β

Let $0 < \alpha < 1$ such that $\alpha = [0, a_1, a_2, \dots]$, and $0 < \beta \le 1$ be given. Non-homogeneous left approximations of β are numbers of the form $k\alpha + l$ less than or equal to β, where k, l are integers. It is clear that there are infinitely many such approximations. We are trying to define two increasing sequences of integers $(k_n)_{n\in\mathbb{N}}$ and $(l_n)_{n\in\mathbb{N}}$, such that for all $n \in \mathbb{N}$

$$0 < k_n\alpha - l_n < k_{n+1}\alpha - l_{n+1} < \beta,$$

and, furthermore, for all n, for all $k < k_{n+1}$, $k \ne k_n$, and for all $l \in \mathbb{Z}$ such that $0 \le k\alpha - l \le \beta$, then

$$0 < k\alpha - l < k_n\alpha - l_n < \beta.$$

For simplicity, we define $f_n = |\theta_n|$. We have $f_{-1} = 1$, $f_0 = \alpha$, $f_1 = 1 - a_1\alpha$, and for all $n > 1$

$$f_{n+1} = f_{n-1} - a_{n+1} f_n. \tag{10}$$

The sequence $(f_n+f_{n+1})_{n\in\mathbb{N}}$ is decreasing, and since $0<\beta\le 1$, there exists a unique non-negative integer n such that $f_n+f_{n+1}<\beta\le f_n+f_{n-1}$. Before we give the algorithm to define the series of best left non-homogeneous approximations of β, we prove the two following lemmas.

Lemma 1. *Let $0<\beta\le 1$ and $(f_n)_{n\in\mathbb{N}}$ defined as above. Then, there exists a unique non-negative integer n, a unique non-negative integer c, and a unique real number e such that*

$$\beta = cf_n + f_{n+1} + e, \tag{11}$$

with $0<e\le f_n$, $1\le c\le a_{n+1}$ if $n\ge 1$; and $1\le c\le a_1-1$, if $n=0$.

Proof. In $n\ge 1$, then with $f_n+f_{n+1}<\beta\le f_n+f_{n-1}$, and (10), we have $f_n<\beta-f_{n+1}\le f_{n-1}+f_n-f_{n+1}=(a_{n+1}+1)f_n$. If $n=0$, then $f_0+f_1<\beta\le 1=f_{-1}=a_1f_0+f_1$. Remark that $a_1\ge 2$ in this case. □

Lemma 2. *Let $\alpha=[0,a_1,a_2,\dots]$, and $(p_n)_{n\in\mathbb{N}}$, $(q_n)_{n\in\mathbb{N}}$ be the sequences of the numerators and denominators of the convergents of α. We define the integers k,l by setting $k=q_n$, $l=p_n$ if n is even; and $k=-cq_n+q_{n+1}$, $l=-cp_n+p_{n+1}$ is n is odd. Then we have $0<\beta-(k\alpha-l)<\beta$.*

Proof. Assume first that n is even. We have $\beta-(k\alpha-l)=\beta-f_n$, and thus $0<\beta-(k\alpha-l)<\beta$. Now, if n is odd, $\beta-(k\alpha-l)=\beta-[-c(q_n\alpha-p_n)+(q_{n+1}\alpha-p_{n+1})]=\beta-cf_n+f_{n+1}=e$, and hence $0<\beta-(k\alpha-l)\le f_n<\beta$. This concludes the proof. □

We can now propose an algorithm which computes the two sequences of non-negative integers $(k_n)_{n\in\mathbb{N}}$, and $(l_n)_{n\in\mathbb{N}}$ such that $(k_n\alpha-l_n)_{n\in\mathbb{N}}$ is the sequence of non-homogeneous best left approximations to β. With $(f_n)_{n\in\mathbb{N}}$ defined as above, we start with $k_0=0$, $l_0=0$, and we inductively define, the n_i, c_i, e_i, k_i, and l_i as follows: If

$$\beta-(k_i\alpha-l_i)=c_if_{n_i}+f_{n_i+1}+e_i,$$

with $0<e_i\le f_{n_i}$, $1\le c_i\le a_{n_i+1}$, if $n_i>0$; and $1\le c_i\le a_1-1$, if $n_i=0$; then we set

$$\begin{array}{lll} k_{i+1}=k_i+q_{n_i}, & l_{i+1}=l_i+p_{n_i}, & \text{if } n_i \text{ is even,}\\ k_{i+1}=k_i-c_iq_{n_i}+q_{n_i+1}, & l_{i+1}=l_i-c_ip_{n_i}+p_{n_i+1}, & \text{if } n_i \text{ is odd.}\end{array}$$

This algorithm is inspired by[10] where it is proved that it gives the best left approximations of β by numbers of the form $k\alpha$. For a similar algorithm, see.[11–13] Note that $\beta-k_{i+1}\alpha$ is equal to e_i if n_i is odd, and to $(c-1)f_{n_i}+f_{n_i+1}+e_i$, if n_i is even. Hence, we may have $n_{i+1}=n_i$. This happens if and only if n_i is even and $c_i>1$; this will then happen (c_i-1) times, and after the sequence n_i continues to grow, if β is not a positive multiple of α, so $n_i\to+\infty$. Next we prove that this algorithm does actually provide the best left approximations to β. The following proposition holds.

Proposition 4. *Let $0<\alpha<1$ such that $\alpha=[0,a_1,a_2,\dots]$, and $0<\beta\le 1$ be given. Let $(p_n/q_n)_{n\in\mathbb{N}}$ be the sequence of the convergents of α. Then, the increasing sequences of integers $(k_i)_{i\in\mathbb{N}}$ and $(l_i)_{i\in\mathbb{N}}$ given by the previous algorithm satisfy, for all $i\in\mathbb{N}$,*

$$0<k_i\alpha-l_i<k_{i+1}\alpha-l_{i+1}<\beta, \tag{12}$$

and furthermore, for all i, for all $k<k_{i+1}$, $k\ne k_i$, and for all $l\in\mathbb{Z}$ such that $0\le k\alpha-l\le\beta$, then

$$0<k\alpha-l<k_i\alpha-l_i<\beta. \tag{13}$$

Proof. From Lemma 2, we have for all i, $0<k_i\alpha-l_i<\beta$. We first prove (12) by considering the cases n_i even and n_i odd. If n_i is even, then $\beta>k_{i+1}-l_{i+1}=(k_i\alpha-l_i)+q_{n_1}\alpha-p_{n_i}=(k_i\alpha-l_i)+f_{n_i}>(k_i\alpha-l_i)>0$. We prove the case n_i odd in a similar way. If n_i is odd, then $\beta > k_{i+1} - l_{i+1} = (k_i\alpha - l_i) - c_i(q_{n_i}\alpha - p_{n_i}) + q_{n_i+1}\alpha - p_{n_i+1} = (k_i\alpha - l_i) + c_i f_{n_i} + f_{n_i+1} > k_i\alpha - l_i > 0$.

Let us now consider $k_i < k < k_{i+1}$, and $l \in \mathbb{Z}$ such that $0 < k\alpha - l < \beta$, and let us try to prove (13). By rewriting $\beta - (k\alpha - l)$, we have

$$0 < \beta - (k\alpha - l) = \beta - (k_i\alpha - l_i) + (k_i\alpha - l_i - k_{i+1}\alpha + l_{i+1}) + (k_{i+1}\alpha - l_{i+1} - k\alpha + l) < \beta$$

We consider two cases depending on the parity of n_i.

- Let us first assume that n_i is even. We have

  $$\beta - (k\alpha - l) = \beta - (k_{i+1}\alpha - l_{i+1}) - f_{n_i} + (k_{i+1}\alpha - l_{i+1} - k\alpha + l).$$

  Thus, what remains to be proved is that the last term $(k_{i+1}\alpha - l_{i+1} - k\alpha + l)$ is greater than f_{n_i}. It is well known that since $|k_{i+1} - k| < |k_{i+1} - k_i| = q_{n_i}$, we have $|(k_{i+1}\alpha - l_{i+1} - k\alpha + l)| > f_{n_i}$; but this only gives a partial result. However, it is easy to see that $(k_{i+1}\alpha - l_{i+1} - k\alpha + l)$ cannot be negative. Indeed, from Lemma 2, we have $-f_{n_i} < \beta - (k_i\alpha - l_i) - f_{n_i}$. Since k, l are such that $0 < \beta - (k\alpha - l) < \beta$, we have $f_{n_i} < (k_{i+1}\alpha - l_{i+1} - k\alpha + l)$. This concludes the case n_i even.

- If we now assume that n_i is odd, we have

  $$\beta - (k\alpha - l) = \beta - (k_i\alpha - l_i) - c_i f_{n_i} - f_{n_i+1} + (k_{i+1}\alpha - l_{i+1} - k\alpha + l).$$

  From Lemma 2, we have $-cif_{n_i} - f_{n_i+1} < \beta - (k_i\alpha - l_i) - c_i f_{n_i} - f_{n_i+1} < \beta - c_i f_{n_i} - f_{n_i+1}$. Since k, l are such that $0 < \beta - (k\alpha - l) < \beta$, we have $c_i f_{n_i} + f_{n_i+1} < (k_{i+1}\alpha - l_{i+1} - k\alpha + l)$. Hence the result.

Thus, we have proved $\beta - (k\alpha - l) > \beta - (k_i\alpha - l_i)$. □

4. EXPLICIT SOLUTION OF THE NON-HOMOGENEOUS APPROXIMATION PROBLEM

As briefly stated in the introduction, finding for the largest 2-integer less than or equal to x is equivalent to finding the two non-negative integers a, b such that $2^a 3^b \le x$ and amongst the many solutions to this problem $2^a 3^b$ takes the largest possible value, i.e.

$$2^a 3^b = \max\left\{2^c 3^d, \text{ such that } (c, d) \in \mathbb{N}^2, \text{ and } 2^c 3^d \le x\right\}.$$

Let $a, b \in \mathbb{N}$ be one of the solutions to the approximation problem, that is, such that $2^a 3^b \le x$. Clearly, we have

$$a \log 2 + b \log 3 \le \log x.$$

If $\alpha = \log_3(2)$ (note that α is irrational and $0 < \alpha < 1$), and $\beta = \{\log_3(x)\}$, is the fractional part of $\log_3(x)$ such that $\beta = \log_3(x) - \lfloor \log_3(x) \rfloor$, then the problem reduces to finding the two non-negative integers a, b such that

$$a\,\alpha + b \le \beta + \lfloor \log_3(x) \rfloor.$$

We note that $a \le \lfloor \log_2(x) \rfloor$ and $b \le \lfloor \log_3(x) \rfloor$.

We are thus looking for $(p, q) \in \mathbb{N}^2$ such that

$$\begin{cases} p\alpha - q \le \beta \\ p\alpha - q = \max\left\{r\alpha - s \text{ such that } (r, s) \in \mathbb{N}^2, \text{ and } 0 \le r\alpha - s \le \beta,\ r \le \lfloor \log_2(x) \rfloor,\ s \le \lfloor \log_3(x) \rfloor\right\} \end{cases}$$

Proposition 5. *Let $x \in \mathbb{N}$ be given. Let $\alpha = \log_3(2)$, ($0 < \alpha < 1$ and $\alpha \notin \mathbb{Q}$), $\beta = \{\log_3(x)\}$. Let n be such that $k_n \le \lfloor \log_2(x) \rfloor < k_{n+1}$. Let $q = k_n$, $p = l_n$. Then*

$$\max\left\{r\alpha - s,\ \textit{such that } (r, s) \in \mathbb{N}^2,\ \textit{and } 0 \le r\alpha - s \le \beta,\ r \le \lfloor \log_2(x) \rfloor,\ s \le \lfloor \log_3(x) \rfloor\right\} = p\alpha - q.$$

This means that by setting $a = p$, and $b = \lfloor \log_3(x) \rfloor - q$, we get the expected result

$$2^a3^b = \max\left\{2^c3^d,\ \textit{such that } (c,d) \in \mathbb{N}^2,\ \textit{and } 2^c3^d \le x\right\}.$$

Proof. The proof comes directly from the proof of Prop. 4 in section 3. $\square$

Example 1. Let $x = 23832098195$. We try to find the two non-negative integers a, b such that 2^a3^b is the largest 2-integer less than or equal to x. Let $\alpha = \log_3(2) = 0.6309$. We have $\beta = \{\log_3(x)\} = \{21.7495\} = 0.7495$. ($\lfloor \log_3(x) \rfloor = 21$). We set $k_0 = 0$, $l_0 = 0$. The partial quotients in the continued fraction expansion of α, and the corresponding convergents are given in table 2.

i	a_i	p_i	q_i	$f_i = \lvert q_i\alpha - p_i\rvert$
0	0	0	1	0.630930
1	1	1	1	0.369070
2	1	1	2	0.261860
3	1	2	3	0.107211
4	2	5	8	0.047438
5	2	12	19	0.012335
6	3	41	65	0.010434
7	1	53	84	0.001901

Table 2. Partial quotients of the continued fraction expansion of $\alpha = \log_3(2)$, and the corresponding sequences $(p_i)_{i\ge0}$, $(q_i)_{i\ge0}$, and $(\lvert q_i\alpha - p_i\rvert)_{i\ge0}$.

Table 3 gives the first best non-homogeneous left approximations to β.

i	e_i	n_i	c_i	k_{i+1}	l_{i+1}	$k_{i+1}\alpha - l_{i+1}$
0	0.7495	1	1	1	0	0.1186
1	0.1186	4	2	9	5	0.0712
2	0.0712	4	1	17	10	0.0237
3	0.0237	5	1	63	39	−0.999

Table 3. Best left approximations of $\beta = 0.7495$ with numbers of the form $k\log_3(2) - l$.

We get $a = 17$ and $b = 21 - 10 = 11$. Note that we stop at this stage because the next best left approximation would lead a negative exponent for the second base ($21 - 39 = -18$). In order to find the DBNS representation of x, we apply the same algorithm with the value $x - 2^{17}3^{11} = 613086611$. For completeness, the DBNS representation of x provided by the greedy algorithm is

$$x = 2^{17}3^{11} + 2^73^{14} + 2^73^8 + 2^23^8 + 2^93^0 + 2^23^1 + 2^03^1.$$

5. DISCUSSIONS

A straightforward approach to the problem of finding the largest 2-integer less than or equal to x consists in computing the distance between the line Δ of equation $y = -\alpha x + \beta$ for all integer x from 0 to $\lfloor \log_2(x) \rfloor$, and to keep the values (x, y) which lead to the smallest distance, i.e the smallest fractional part of $\beta - \alpha x$ for all integer $0 \leq x \leq \lfloor \log_2(n) \rfloor$. More efficiently, we can consider the line $\Delta' : y' = -\log_2(3)x + \log_2(x)$, and keep the minimum distance amongst all integers $0 \leq x' \leq \lfloor \log_3(x) \rfloor$, simply because the function $\log_3(t)$ grows faster than $\log_2(t)$.

In Fig. 1 we have plotted the line $\Delta = -0.6309x + 0.7495$ which corresponds to the previous example, together with the points we have to scan in the straightforward approach, and those we deduce from the proposed algorithm. We clearly remark that the algorithm based on continued fractions and Ostrowski's number system we have introduced in the previous sections only scans four possible solutions, whereas the straightforward algorithm must scan all the points on a discrete line under Δ.

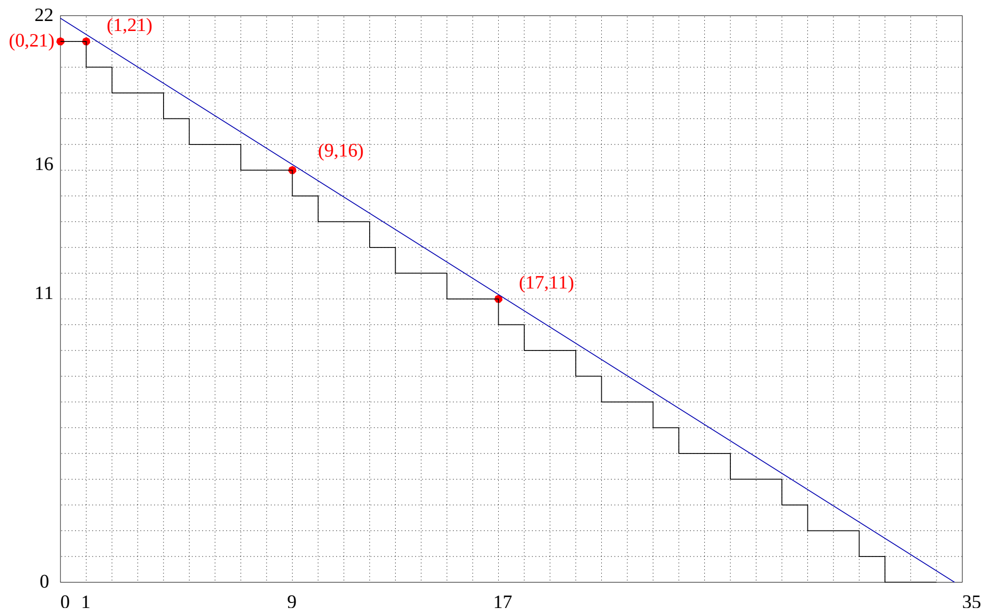

Figure 2. Graphical interpretation of the problem of finding the largest 2-integer less than (or equal) to $x = 23832098195$ and the points scanned using both the straightforward approach and the proposed algorithm.

For large values of x, the proposed algorithm is much faster than the classical approach. We have implemented the two solutions in Maple for integers of various size (see Table 4). Although the timings themselves are not very relevant because of non-optimized Maple interpreted code, the ratios clearly show the efficiency of the proposed algorithm.

Size of x (in bits)	163	241	337	459	595
Time with straightforward algo.	0.47	1.14	2.02	1.23	5.65
Time with new algo.	0.21	0.41	0.71	3.43	1.96
Time ratio	45%	39%	35%	36%	35%

Table 4. CPU time for binary to DBNS conversion using the greedy algorithm for numbers of various sizes. The largest 2-integer is computed at each step using the straightforward approach (line 2) and new proposed algorithm (line 3).

6. CONCLUSION

We proposed an algorithm to find the largest 2-integer less than or equal to an integer x. This operation is required at each iteration of the greedy algorithm used to convert numbers into DBNS. This very preliminary study will be pursue to answer some more difficult questions related to the double-base number system and its generalization, the multi-dimensional logarithmic number system.

ACKNOWLEDGMENTS

This work has been done during Laurent Imbert leave of absence at the university of Calgary with the ATIPS (Advanced Technology Information Processing Systems) and CISaC (Centre for Information Security and Cryptography) laboratories.

REFERENCES

1. V. S. Dimitrov, G. A. Jullien, and W. C. Miller, "Theory and applications of the double-base number system," *IEEE Transactions on Computers* **48**, pp. 1098–1106, October 1999.
2. V. S. Dimitrov and T. V. Cooklev, "Two algorithms for modular exponentiation based on nonstandard arithmetics," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science* **E78-A**, pp. 82–87, January 1995. Special issue on cryptography and information security.
3. V. S. Dimitrov, J. Eskritt, L. Imbert, G. A. Jullien, and W. C. Miller, "The use of the multi-dimensional logarithmic number system in DSP applications," in *15th IEEE symposium on Computer Arithmetic*, pp. 247–254, (Vail, CO, USA), June 2001.
4. R. Muscedere, *Difficult Operations in the Multi-Dimensional Logarithmic Number System*. PhD thesis, University of Windsor, Windsor, ON, Canada, 2003.
5. V. S. Dimitrov, G. A. Jullien, and W. C. Miller, "An algorithm for modular exponentitation," *Information Processing Letters* **66**, pp. 155–159, May 1998.
6. J.-P. Allouche and J. Shallit, *Automatic Sequences*, Cambridge University Press, 2003.
7. E. Zeckendorf, "Représentation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas," *Fibonacci Quarterly* **10**, pp. 179–182, 1972.
8. V. Berthé, "Autour du système de numération d'Ostrowski," *Bulletin of the Belgian Mathematical Society* **8**, pp. 209–239, 2001.
9. V. Berthé, N. Chekhova, and S. Ferenczi, "Covering numbers: Arithmetics and dynamics for rotations and internal exchanges," *Journal d'Analyse Mathématique* **79**, pp. 1–31, 1999.
10. N. B. Slater, "Gaps and steps for the sequence $n\theta \bmod 1$," *Mathematical Proceedings of the Cambridge Philosophical Society* **63**, pp. 1115–1123, 1967.
11. V. T. Sós, "On the theory of diophantine approximations. I," *Acta Mathematica Hungarica* **8**, pp. 461–472, 1957.
12. V. T. Sós, "On the theory of diophantine approximations. II," *Acta Mathematica Hungarica* **9**, pp. 229–241, 1958.
13. V. T. Sós, "On a problem of Hartman about normal forms," *Colloquium Mathematicum* **7**, pp. 155–160, 1960.