Journal of Computer Science 2 (12): 875-878, 2006
ISSN 1549-3636

An Algorithm for Accelerated Acquirement of Minimal Representation of Super-large Numbers

Mohammed Al-Maitah
Computer Science Department, Jordan-Jerash Private University, Jordan

Abstract: An algorithm for accelerated acquirement of minimal representation of super-large numbers was presented. The algorithm considers a new form of arithmetic, which was called arithmetic of *q*-representation of large range integers; which was based on the numbers of the generalized sequence of Fibonacci. The estimations of the complexity of the offered algorithms are presented.

Key words: M-representation, integer number, fibonacci p-number, fibonacci p-codes

INTRODUCTION

Storage of large volume of information and their protection against an unauthorized access are considered as one of the most important problems facing the designers of modern computer systems. Often in solving such problems, quite different approaches are applied. The results that have been found by many researchers[1-6] are based only on the application of the original method of super-large integer numbers representation (1024 binary digits and more) along with the arithmetic of such numbers. In this case, for compression of information, the block of digital data of any length will be considered as super-large integer positive number, which is presented as a set of *p*+2 small numbers[3]. In this kind of representation of numbers, which is called linear form, is the basis of efficient algorithms, for performing computations over super-large numbers[2,4] required for the solution of problems dealing with cryptographic protection of information.

Super-large numbers representation is based on the optimizing properties of Fibonacci *p*-numbers. Anisimov *et al.*[1] presented an algorithm for obtaining Fibonacci linear form for particular case *p*=1. However, Luzhetsky and Al-Maitah[3] described an algorithm for determining any positive integer *p*. The shortcomings of these algorithms are the huge volume of computations, in addition to the necessity of the multiplication of super-large numbers.

The proposed algorithm, in the current work, makes less complexity of computations because of its dependence on of the addition and subtraction operations only. The proposed algorithm depends on the linear form representation.

Linear form representation: In order to represent integer numbers in linear form, let us consider the integer number *z* as one of the integer number elements series $\{w_{p,l}\}$, which is generated by the recurrent relationship as follows:

$w_{p,l} = w_{p,l-1} + w_{p,l-p-1}$, $p \geq 1$ and $l \geq 0$

For determining the values of the initial elements: $w_{p,0}, w_{p,1}, \ldots, w_{p,p}$.

It has been proved by[3] that for the given integer numbers $w_{p,0}, w_{p,1}, \ldots, w_{p,p}$ the following relationship can be used as follows:

$$w_{p,l+2p} = w_{p,p}\varphi_p(l+p) + \sum_{i=0}^{p-1} w_{p,i}\varphi_p(l+p-i-1),$$

Where $\varphi_p(n)$ is the n th Fibonacci *p*-number.

Fibonacci *p*-numbers for positive *n* are calculated on the basis of the recurrent relationship

$$\varphi_p(n+p+1) = \varphi_p(n+p) + \varphi_p(n) \qquad (1)$$

Here $\varphi_p(0) = 0, \varphi_p(1) = \cdots = \varphi_p(p) = 1$.

By noting that the Fibonacci series *p*-number has the following property:

$$\lim_{n\to\infty} \frac{\varphi_p(n)}{\varphi_p(n-1)} = \alpha_p,$$

Where α_p is golden ratio.

Then, the task of integer number representation *z* mainly includes the determination of the integer values of the initial series elements $\{w_{p,l}\}$ sequence and the number of elements, which is equal to *z*.

Proceeding from this assumption, any integer number *z* is represented in the following form:

$$z = \sum_{i=1}^{p+1} q_i \varphi_p(j+i-p) \qquad (2)$$

Where q_i is an integer number (representing the coordinates).

J is a positive integer number (representing an index).

It follows from equation (Eq.2), that *z* is determined by *p*+2 integer numbers, i.e. $z = f(q_1, q_2, \ldots, q_{p+1}, j)$. Such representation of the integer number *z* is called *q*-representation.

Among the set of values implied by (Eq.2), there is a single *minimal representation* called (M-representation), possessing the property $\{min|q_i|;\ i=1,2,\ldots,p+1\}$.

The following steps should be considered to obtain M-representation of positive integer positive number, *z,* Calculate the products:

$q_i^* = \left[z\alpha_p^{-i}\right]$, $i=1,2,\ldots,p$,

Rounded off to the nearest integer number using α_p, the word length of which is equal to the word length of the number *z*.

Taking the calculated products as initial elements of the series:

$w_0=z,\ w_1=q_1^*,\ w_2=q_2^*,\ldots,\ w_p=q_p^*$,

Perform calculations

$w_h = w_{h-p-1} - w_{h-1}, \quad h=p+1,p+2,\ldots$

until $w_h > 0.$

If computations are performed *j* times, then M-presentation index will become *j*. In this case, the coordinate's representation (Eq.2) will be as follows:

$q_1 = w_{j+2};\ q_2 = w_{j+3};\ \cdots q_p = w_{j+p+1};\ q_{p+1} = w_{j+1}.$

Addition of M-representations: Addition of the numbers, z_1 given by $z_1 = \sum_{i=1}^{p+1} q_i(z_1)\varphi_p(j_1+i-p)$ and z_2 given by $z_2 = \sum_{i=1}^{p+1} q_i(z_2)\varphi_p(j_2+i-p)$.

are performed in four stages[4]:

* Comparison of indexes
* Addition of the similar coordinates
* Minimization of coordinates sum
* Increase of sum index.

At the stage of index comparison, the difference $\Delta j = j_1 - j_2$ is determined.

If $\Delta j = 0$, then the transition to the next stage is realized. If $\Delta j > 0,$ then the following transformation is carried out

$$q_{p+1}^* = q_{p+1} + q_p;\ q_1^* = q_{p+1}; \qquad (3)$$
$$q_2^* = q_1;\ q_3^* = q_2;\cdots;\ q_p^* = q_{p-1},$$

where q_i^*, $q_i -$ new and initial values of coordinate respectively.

The, Δj times for coordinate of the number Z_1 and if $\Delta j < 0,$ then the transformation in carried out $|\Delta j|$ times the coordinates of the number Z_2.

Addition of the similar coordinates may lead to the case, that the sums of coordinates will not possess the properties of minimally. In this case, the coordinates must be minimized by performing a certain number of the following transformations:

$$q_p^* = q_{p+1} - q_1;\ q_{p+1}^* = q_1; \qquad (4)$$
$$q_1^* = q_2;\ q_2^* = q_3;\cdots\ q_{p-1}^* = q_p.$$

Each transformation leads to the increase of index by a unit. The sequence of transformations is finished if $q_p^* < 0$.

At the stage of increase of sum index, j_2 is increased if $\Delta j > 0,$ and j_1 is increased also when $\Delta j < 0$ by the number of transformations (Eq.4).

Algorithms of accelerated achievement M-representation: It is known[5] that any integer positive number *z* can be represented in the form:

$$z = \sum_{l=1}^{n} a_l \varphi_p(l), \qquad (5)$$

where $a_l = \{0;1\}$.

The following algorithm is used to determine the values of a_l.

Algorithm 1: [Traditional]

Step 1: Determine the element in Fibonacci *p*-numbers series; which satisfies the condition $z = \varphi_p(l) + r,$ where *r* - remainder, $0 \le r < \varphi_p(l-1)$.

Step 2: $a_l = 1.$

Step 3: Take remainder *r* as an initial number and pass to step 1.

Steps 1-3 are to be executed until remainder *r* equals zero.

The non-unity values of a_l have zero-values.

The set $a_n a_{n-1}\ldots a_2 a_1$ is called Fibonacci *p*-code of the number *z*[5].

M-representation corresponds to number $\varphi_p(l)$; *p* coordinate of which equal to zero and one coordinate has the value 1, i.e.

$$\varphi_p(l) = f(0,0,\ldots 0,1,l-1). \qquad (6)$$

By substituting (Eq.6) into (Eq.5), the number, *z*, can be written as follows:

$$z = \sum_{l=1}^{n} a_l f(0,0,\ldots 0,1,l-1).$$

Subsequently, the process of obtaining M-representation of integer number, *z,* is performed by the addition of M-representations of Fibonacci *p*-numbers, which is controlled by numbers a_l of Fibonacci *p*-code, corresponding to integer number *z*. If $a_l = 1$, then

$f(0,0,\ldots 0,1,l-1)$ is added to the accumulated sum and in case if $a_l = 0$ then the addition is not performed.

Therefore, to obtain M-representation of integer positive number *z,* it is necessary to perform three procedures:

* Formation of Fibonacci *p*-numbers sequence;
* Determination of Fibonacci *p*-code a_l figures;

Accumulating addition of M-representation of Fibonacci *p*-numbers, corresponding to $a_l = 1$.

Stakhov and Luzhetsky[7] have shown that the formation of increasing series of Fibonacci *p*-numbers requires the storage of *p*+1 current element values of the series and computation by the formula (1). On the other hand, such formation of the series is not efficient for determination of a_l figures according to the algorithm 1. Since number *z*, being transformed and further remainder *r*, are compared with Fibonacci *p*-numbers, which have the greatest values, the storage of the whole *p*-numbers series will be required. Taking into consideration this fact, it is suggested to form diminishing series of Fibonacci *p*-numbers, using the recurrent relationship:

$$\varphi_p(l) = \varphi_p(l+p+1) - \varphi_p(l+p), \quad l = n, n-1, \ldots 1$$

for initial values of $\varphi_p(n+p+1), \varphi_p(n+p), \ldots \varphi_p(n+1)$.

In this case, in order to realize algorithm 1 it is sufficient to store only *p*+1 current value of $\varphi_p(l)$ elements and successively compare number *z* (remainder *r*) being transformed with Fibonacci *p*-numbers, using for this purpose the operation of subtraction.

Each accumulating addition of M-representations is not expedient to perform in four stages as it is mentioned early. It is sufficient to compare indices and realize addition of the similar coordinates and the stages of minimization of sum coordinates are performed after the execution of all additions, (i.e. intermediate sums will have *q*-representation and final sum — M-representation).

All these three procedures, therefore, necessary for obtaining M-representation of *z* number can be performed using the operations of addition and subtraction. In this case the initial data is integer positive number *z,* being transformed and the set of Fibonacci *p*-numbers $\varphi_p(n+p+1), \varphi_p(n+p), \ldots \varphi_p(n+1)$. If for the numbers being transformed maximal value is z_{max}, then $n = \lfloor log_{\alpha_p} z_{max} \rfloor$.

Taking into account the above-mentioned peculiarities of realization each of the procedures, the next algorithm of accelerated achievement of M-representation is proposed.

Algorithm 2: [Suggested]
Initialization:

$r = z;\ l = n;\ \varphi_p(n+p+1), \varphi_p(n+p), \ldots \varphi_p(n+1)$.

$S_{l+1} = f(0,0,\ldots 0,0,n);\ j = p$

Step 1: Perform transformation (Eq.3) for S_{l+1}.

Step 2: Calculate

$\varphi_p(l) = \varphi_p(l+p+1) - \varphi_p(l+p)$.

Step 3: Calculate, $\Delta = r - \varphi_p(l)$.

Step 4: If $\Delta < 0$ then go to step 7.

Step 5: Assign *r* value Δ.

Step 6: Perform addition of representations

$S_l = S_{l+1} + f(0,0,\ldots 0,1,l-1)$.

Step 7: Decrease by 1 value l.

Step 8: If $l > p+1$ then go to step 1.

Step 9: Perform transformation (Eq.4).

Step 10: If $q_p^* < 0$, then go to step 12.

Step 11: Increase by 1 value *j* and go to step 9.

Step 12: End.

The following example will illustrate operation of the algorithm for obtaining M-representation of number *z*=45.

Let *p*=1. Then

$r = 45;\ n = 9; l = 9;\ \varphi_1(11) = 89, \varphi_p(10) = 55;\ S_{l+1} = f(0,0,9);\ j = 1$.

$l = 9: (S_{10})_{tran.} = f(0,0,8)$; 89-55=34;

$\Delta = 45 - 34 = 11 > 0$, $r = 11$;

$S_9 = f(0,0,8) + f(0,1,8) = f(0,1,8)$.

$l = 8: (S_9)_{tran.} = f(1,1,7)$; 55-34=21;

$\Delta = 11 - 21 = -10 < 0$.

$l = 7: (S_8)_{tran..} = f(1,2,6)$; 34-21=13;

$\Delta = 11 - 13 = -2 < 0$.

$l = 6: (S_7)_{tran..} = f(2,3,5)$; 21-13=8;

$\Delta = 11 - 8 = 3 > 0$, $r = 3$;

$f(2,3,5) + f(0,1,5) = f(2,4,5)$.

$l = 5: (S_6)_{tran..} = f(4,6,4)$; 13-8=5;

$\Delta = 3 - 5 = -2 < 0$.

$l = 4: (S_5)_{tran..} = f(6,10,3)$; 8-5=3; $\Delta = 3 - 3 = 0$,

$r = 0$; $f(6,10,3) + f(0,1,3) = f(6,11,3)$.

$l = 3: (S_4)_{tran.} = f(11,17,2)$; 5-3=2;

$\Delta = 0 - 2 = -2 < 0$.

$l = 2: (S_3)_{tran..} = f(17,28,1)$; 3-2=1;

$\Delta = 0 - 1 = -1 < 0$.

q-representation $f(17,28,1)$ of the number 45 is obtained.

Minimization of q -representation:

28-17=11, j =2; 6-5=1, j =5;

17-11=6, j =3; 5-1=4, j =6;

11-6=5, j =4; 1-4=-3<0. End.

Thus M-representation of number 45 has the form $f(4,1,6)$.

In order to obtain a general evaluation of the considered algorithm, the complexity of each of its three procedures is to be evaluated. As a conventional unit of complexity will be used the operation of addition or subtraction of *m*-digit binary codes.

The word-length of binary codes, being processed while realization of the algorithm is determined proceeding from maximal value of Fibonacci *p*-numbers, $\varphi_p(n+p+1)$. In order to represent this number in binary code $n_{\text{Binary}} = (n+p+1)/R_p$ digits are necessary. The R_p represents the redundancy *p*-code Fibonacci.

Addition or subtraction of binary codes of n_{Binary} word length requires n_{Binary}/m addition or subtraction operations of *m*-digit codes. Taking into consideration this fact, the complexity of the procedures of Fibonacci *p*-number series formation S_{Form} and determination of figures a_l Fibonacci *p*-code $S_{\text{Deter.}}$ equals to:

$$S_{\text{Form}} = S_{\text{Deter.}} \approx \frac{n^2}{R_p m}.$$

Maximal quantity of units in Fibonacci *p*-code is equals to $n/(p+1)$. That is why maximal complexity of addition accumulation $S_{\text{Accum.}}$ procedure equals to:

$$S_{\text{Accum.}} \approx \frac{n(3p+4)}{p+1}.$$

From the given complexity evaluations of the algorithm for the separate procedures, the following general evaluation can be written:

$$S_{\text{suggested.}} = S_{\text{Form}} + S_{\text{Deter.}} + S_{\text{Accum.}} = \frac{2n^2}{R_p m} + \frac{n(3p+4)}{p+1}.$$

For the values $n \geq 1024$ and $m << n$ $S_{\text{suggested.}} \approx \frac{2n^2}{R_p m}$.

If in the known algorithm of obtaining M-representations, the multiplication of binary codes of n_{Binary} word-length will be performed only on the basis of addition, in this case its complexity will be equal to:

$$S_{\text{Known}} = \frac{n^2(p+1)}{R_p m}.$$

The proposed algorithm will be more efficient than the known one, if $\frac{S_{\text{Known}}}{S_{\text{suggested.}}} > 1$. Such relation is performed for all $p > 1$.

If in relationship $\frac{S_{\text{Known}}}{S_{\text{suggested.}}}$ by substituting $S_{\text{suggested.}} \approx \frac{2n^2}{R_p m}$ and $S_{\text{Known}} = \frac{n^2(p+1)}{R_p m}$, to obtain $\eta = \frac{S_{\text{Known}}}{S_{\text{suggested.}}} = \frac{p+1}{2}$. Table 1 illustrates given values η for difference *p*.

Table 1

p	1	2	3	4	5
η	1	1.5	2	2.5	3

For instance, if *p*=3 the complexity of suggested algorithm is two times less complicated than the complexity of the known algorithm.

CONCLUSION

The new algorithm of accelerated acquirement of minimal representation of super-large numbers is performed. The complexity of the given algorithm is less than the complexity of the known algorithm. Implementation of such an algorithm in practical aspects should have no shortcomings. The suggested algorithm is proven valid and it is expected to be used as a base of a new generation of arithmetic units.

REFERENCES

1. Anisimov, A.V., J.P. Rundin and S.E. Redko, 1982. Reverse transformation of Fibonacci. Cybernatics, 3: 9-11.
2. Anisimov, A.V., 1995. Fibonacci linear forms and parallel algorithms of the arithmetics. Cybernatics and System Analysis, 3: 106-115.
3. Luzhetsky, V. and Al-Maitah Mohammed, 1998. Way of representation of integers of a large range. MCTTP. 1: 156-162.
4. Luzhetsky, V. and Al-Maitah Mohammed, 1998. Arithmetics of integers of a large range. Measuring and Computing Engineering in Technological Processes, 2: 130-135.
5. Daykin, D.E., 1960. Representation of natural numbers as sums of generalized Fibonacci numbers. J. London Math. Soc., 34: 143–160.
6. Carlitz, L., 1968. Fibonacci Representation. The Fibonacci Quart., 6: 193–220.
7. Stakhov, A.P. and V.A. Luzhetsky, 1981. Machine arithmetic of digital computers in Fibonacci codes and golden proportion. M., Scientific Council of Academy of Science of the USSR on complex problem. Cybernetics: 64.