JOURNAL OF FORMALIZED MATHEMATICS
Volume 11, Released 1999, Published 2003
Inst. of Computer Science, Univ. of Białystok

Definitions of Radix-2^k Signed-Digit Number and its Adder Algorithm

Yoshinori Fujisawa
Shinshu University
Nagano

Yasushi Fuwa
Shinshu University
Nagano

Summary. In this article, a radix-2^k signed-digit number (Radix-2^k SD number) is defined and based on it a high-speed adder algorithm is discussed.

The processes of coding and encoding for public-key cryptograms require a great deal of addition operations of natural number of many figures. This results in a long time for the encoding and decoding processes. It is possible to reduce the processing time using the high-speed adder algorithm.

In the first section of this article, we prepared some useful theorems for natural numbers and integers. In the second section, we defined the concept of radix-2^k, a set named k-SD and proved some properties about them. In the third section, we provide some important functions for generating Radix-2^k SD numbers from natural numbers and natural numbers from Radix-2^k SD numbers. In the fourth section, we defined the carry and data components of addition with Radix-2^k SD numbers and some properties about them. In the fifth section, we defined a theorem for checking whether or not a natural number can be expressed as n digits Radix-2^k SD number.

In the last section, a high-speed adder algorithm on Radix-2^k SD numbers is proposed and we provided some properties. In this algorithm, the carry of each digit has an effect on only the next digit. Properties of the relationships of the results of this algorithm to the operations of natural numbers are also given.

MML Identifier: RADIX_1.

WWW: http://mizar.org/JFM/Vol11/radix_1.html

The articles [8], [11], [9], [1], [4], [7], [3], [10], [6], [2], and [5] provide the notation and terminology for this paper.

1. Some Useful Theorems

We follow the rules: i, k, m, n, x, y are natural numbers, i_1, i_2, i_3 are integers, and e is a set.

We now state several propositions:

(2)[1] If $n \bmod k = k-1$, then $(n+1) \bmod k = 0$.

(3) If $k \neq 0$ and $n \bmod k < k-1$, then $(n+1) \bmod k = (n \bmod k)+1$.

(4) If $m \neq 0$, then $k \bmod m \cdot n \bmod n = k \bmod n$.

(5) If $k \neq 0$, then $(n+1) \bmod k = 0$ or $(n+1) \bmod k = (n \bmod k)+1$.

[1] The proposition (1) has been removed.

(6) If $i \neq 0$ and $k \neq 0$, then $(n \bmod i^k) \div i^{k-'1} < i$.

(7) If $k \leq n$, then $m^k \mid m^n$.

(8) If $i_2 > 0$ and $i_3 \geq 0$, then $i_1 \bmod i_2 \cdot i_3 \bmod i_3 = i_1 \bmod i_3$.

2. Definition for Radix-2^k, k-SD

Let us consider n. The functor $\mathrm{Radix}\, n$ yields a natural number and is defined as follows:

(Def. 1) $\mathrm{Radix}\, n = 2^n$.

Let us consider k. The functor $k-\mathrm{SD}$ yields a set and is defined as follows:

(Def. 2) $k-\mathrm{SD} = \{e; e$ ranges over elements of $\mathbb{Z}$: $e \leq \mathrm{Radix}\, k - 1 \ \wedge \ e \geq -\mathrm{Radix}\, k + 1\}$.

One can prove the following propositions:

(9) $\mathrm{Radix}\, n \neq 0$.

(10) For every e holds $e \in 0-\mathrm{SD}$ iff $e = 0$.

(11) $0-\mathrm{SD} = \{0\}$.

(12) $k-\mathrm{SD} \subseteq (k+1)-\mathrm{SD}$.

(13) If $e \in k-\mathrm{SD}$, then e is an integer.

(14) $k-\mathrm{SD} \subseteq \mathbb{Z}$.

(15) If $i_1 \in k-\mathrm{SD}$, then $i_1 \leq \mathrm{Radix}\, k - 1$ and $i_1 \geq -\mathrm{Radix}\, k + 1$.

(16) $0 \in k-\mathrm{SD}$.

Let us consider k. One can verify that $k-\mathrm{SD}$ is non empty.
Let us consider k. Then $k-\mathrm{SD}$ is a non empty subset of $\mathbb{Z}$.

3. Functions for Generating Radix-2^k SD Numbers from Natural Numbers and Natural Numbers from Radix-2^k SD Numbers

In the sequel a is a n-tuple of $k-\mathrm{SD}$.
Next we state the proposition

(18)[2] If $i \in \mathrm{Seg}\, n$, then $a(i)$ is an element of $k-\mathrm{SD}$.

Let i, k, n be natural numbers and let x be a n-tuple of $k-\mathrm{SD}$. The functor $\mathrm{DigA}(x,i)$ yields an integer and is defined by:

(Def. 3)(i) $\mathrm{DigA}(x,i) = x(i)$ if $i \in \mathrm{Seg}\, n$,

(ii) $\mathrm{DigA}(x,i) = 0$ if $i = 0$.

Let i, k, n be natural numbers and let x be a n-tuple of $k-\mathrm{SD}$. The functor $\mathrm{DigB}(x,i)$ yields an element of $\mathbb{Z}$ and is defined as follows:

(Def. 4) $\mathrm{DigB}(x,i) = \mathrm{DigA}(x,i)$.

Next we state two propositions:

(19) If $i \in \mathrm{Seg}\, n$, then $\mathrm{DigA}(a,i)$ is an element of $k-\mathrm{SD}$.

(20) For every 1-tuple x of $\mathbb{Z}$ such that $x_1 = m$ holds $x = \langle m \rangle$.

[2] The proposition (17) has been removed.

Let i, k, n be natural numbers and let x be a n-tuple of $k-\mathrm{SD}$. The functor $\mathrm{SubDigit}(x,i,k)$ yielding an element of $\mathbb{Z}$ is defined by:

(Def. 5) $\mathrm{SubDigit}(x,i,k) = (\mathrm{Radix}\,k)^{i-'1} \cdot \mathrm{DigB}(x,i)$.

Let n, k be natural numbers and let x be a n-tuple of $k-\mathrm{SD}$. The functor $\mathrm{DigitSD}\,x$ yielding a n-tuple of $\mathbb{Z}$ is defined by:

(Def. 6) For every natural number i such that $i \in \mathrm{Seg}\,n$ holds $(\mathrm{DigitSD}\,x)_i = \mathrm{SubDigit}(x,i,k)$.

Let n, k be natural numbers and let x be a n-tuple of $k-\mathrm{SD}$. The functor $\mathrm{SDDec}\,x$ yielding an integer is defined by:

(Def. 7) $\mathrm{SDDec}\,x = \sum \mathrm{DigitSD}\,x$.

Let i, k, x be natural numbers. The functor $\mathrm{DigitDC}(x,i,k)$ yields an element of $k-\mathrm{SD}$ and is defined by:

(Def. 8) $\mathrm{DigitDC}(x,i,k) = (x \bmod (\mathrm{Radix}\,k)^i) \div (\mathrm{Radix}\,k)^{i-'1}$.

Let k, n, x be natural numbers. The functor $\mathrm{DecSD}(x,n,k)$ yields a n-tuple of $k-\mathrm{SD}$ and is defined by:

(Def. 9) For every natural number i such that $i \in \mathrm{Seg}\,n$ holds $\mathrm{DigA}(\mathrm{DecSD}(x,n,k),i) = \mathrm{DigitDC}(x,i,k)$.

4. Definition for Carry and Data Components of Addition

Let x be an integer. The functor $\mathrm{SD\_Add\_Carry}\,x$ yielding an integer is defined as follows:

(Def. 10) $\mathrm{SD\_Add\_Carry}\,x = \begin{cases} \text{(i)} \quad 1, \text{ if } x > 2, \\ \text{(ii)} \quad -1, \text{ if } x < -2, \\ \quad 0, \text{ otherwise.} \end{cases}$

Next we state the proposition

(21) $\mathrm{SD\_Add\_Carry}\,0 = 0$.

Let x be an integer and let k be a natural number. The functor $\mathrm{SD\_Add\_Data}(x,k)$ yields an integer and is defined by:

(Def. 11) $\mathrm{SD\_Add\_Data}(x,k) = x - \mathrm{SD\_Add\_Carry}\,x \cdot \mathrm{Radix}\,k$.

Next we state two propositions:

(22) $\mathrm{SD\_Add\_Data}(0,k) = 0$.

(23) If $k \geq 2$ and $i_1 \in k-\mathrm{SD}$ and $i_2 \in k-\mathrm{SD}$, then $-\mathrm{Radix}\,k+2 \leq \mathrm{SD\_Add\_Data}(i_1+i_2,k)$ and $\mathrm{SD\_Add\_Data}(i_1+i_2,k) \leq \mathrm{Radix}\,k-2$.

5. Definition for Checking whether or not a Natural Number can be Expressed as n Digits Radix-2^k SD Number

Let n, x, k be natural numbers. We say that x is represented by n, k if and only if:

(Def. 12) $x < (\mathrm{Radix}\,k)^n$.

One can prove the following propositions:

(24) If m is represented by 1, k, then $\mathrm{DigA}(\mathrm{DecSD}(m,1,k),1) = m$.

(25) For every n such that $n \geq 1$ and for every m such that m is represented by n, k holds $m = \mathrm{SDDec}\,\mathrm{DecSD}(m,n,k)$.

(26) If $k \geq 2$ and m is represented by 1, k and n is represented by 1, k, then $\mathrm{SD\_Add\_Carry}\,\mathrm{DigA}(\mathrm{DecSD}(m,1,k),1) + \mathrm{DigA}(\mathrm{DecSD}(n,1,k),1) = \mathrm{SD\_Add\_Carry}\,m+n$.

(27) If m is represented by $n+1$, k, then $\mathrm{DigA}(\mathrm{DecSD}(m,n+1,k),n+1) = m \div (\mathrm{Radix}\,k)^n$.

6. Definition for Addition Operation for a High-Speed Adder Algorithm on Radix-2^k SD Number

Let k, i, n be natural numbers and let x, y be n-tuples of $k-\mathrm{SD}$. Let us assume that $i \in \mathrm{Seg}\, n$ and $k \geq 2$. The functor $\mathrm{Add}(x,y,i,k)$ yielding an element of $k-\mathrm{SD}$ is defined by:

(Def. 13) $\mathrm{Add}(x,y,i,k) = \mathrm{SD\_Add\_Data}(\mathrm{DigA}(x,i) + \mathrm{DigA}(y,i),k) + \mathrm{SD\_Add\_Carry}\,\mathrm{DigA}(x,i -' 1) + \mathrm{DigA}(y,i -' 1)$.

Let n, k be natural numbers and let x, y be n-tuples of $k-\mathrm{SD}$. The functor $x' +' y$ yields a n-tuple of $k-\mathrm{SD}$ and is defined by:

(Def. 14) For every i such that $i \in \mathrm{Seg}\, n$ holds $\mathrm{DigA}(x' +' y, i) = \mathrm{Add}(x,y,i,k)$.

The following propositions are true:

(28) If $k \geq 2$ and m is represented by 1, k and n is represented by 1, k, then $\mathrm{SDDec}\,\mathrm{DecSD}(m,1,k)' +' \mathrm{DecSD}(n,1,k) = \mathrm{SD\_Add\_Data}(m+n,k)$.

(29) Let given n. Suppose $n \geq 1$. Let given k, x, y. Suppose $k \geq 2$ and x is represented by n, k and y is represented by n, k. Then $x + y = \mathrm{SDDec}\,\mathrm{DecSD}(x,n,k)' +' \mathrm{DecSD}(y,n,k) + (\mathrm{Radix}\,k)^n \cdot \mathrm{SD\_Add\_Carry}\,\mathrm{DigA}(\mathrm{DecSD}(x,n,k),n) + \mathrm{DigA}(\mathrm{DecSD}(y,n,k),n)$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/nat_1.html`.

[2] Grzegorz Bancerek. Joining of decorated trees. *Journal of Formalized Mathematics*, 5, 1993. `http://mizar.org/JFM/Vol5/trees_4.html`.

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finseq_1.html`.

[4] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/funct_1.html`.

[5] Andrzej Kondracki. The Chinese Remainder Theorem. *Journal of Formalized Mathematics*, 9, 1997. `http://mizar.org/JFM/Vol9/wsierp_1.html`.

[6] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Journal of Formalized Mathematics*, 5, 1993. `http://mizar.org/JFM/Vol5/binarith.html`.

[7] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/power.html`.

[8] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. `http://mizar.org/JFM/Axiomatics/tarski.html`.

[9] Michał J. Trybulec. Integers. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/int_1.html`.

[10] Wojciech A. Trybulec. Pigeon hole principle. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finseq_4.html`.

[11] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/subset_1.html`.

Received September 7, 1999

Published January 2, 2004