FORMALIZED MATHEMATICS
Volume 9, Number 1, 2001
University 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.

The notation and terminology used here are introduced in the following papers: [9], [6], [2], [3], [12], [4], [11], [1], [5], [7], [13], [10], and [8].

ISSN 1426–2630

1. Some Useful Theorems

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

The following propositions are true:

(1) If $n \neq 0$, then $m \div n = (m$ **qua** integer$) \div n$ **qua** integer and $m \bmod n = (m$ **qua** integer$) \bmod n$ **qua** integer.

(2) If $k \neq 0$ and $n \bmod k = k - 1$, 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 $m \neq 0$ and $n \neq 0$, then $k \bmod m \cdot n \bmod n = k \bmod n$.

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

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

(7) If $k \leqslant n$, then $m_{\mathbb{N}}^{k} \mid m_{\mathbb{N}}^{n}$.

(8) If $i_3 > 0$, 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 $\operatorname{Radix} n$ yields a natural number and is defined by:

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

Let us consider k. The functor k –SD yields a set and is defined by:

(Def. 2) $k\,\text{–SD} = \{e; e$ ranges over integers: $e \leqslant \operatorname{Radix} k - 1 \wedge e \geqslant -\operatorname{Radix} k + 1\}$.

The following propositions are true:

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

(10) For every e holds $e \in 0\,\text{–SD}$ iff $e = 0$.

(11) $0\,\text{–SD} = \{0\}$.

(12) $k\,\text{–SD} \subseteq k + 1\,\text{–SD}$.

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

(14) $k\,\text{–SD} \subseteq \mathbb{Z}$.

(15) If $i_1 \in k\,\text{–SD}$, then $i_1 \leqslant \operatorname{Radix} k - 1$ and $i_1 \geqslant -\operatorname{Radix} k + 1$.

(16) $0 \in k\,\text{–SD}$.

Let us consider k. Note that k –SD is non empty.

Let us consider k. Then k –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 denotes a tuple of n and k −SD.

We now state the proposition

(18)[1] If $i \in \mathrm{Seg}\, n$, then $a(i)$ is an element of k −SD.

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

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

One can prove the following propositions:

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

(20) For every tuple x of 1 and $\mathbb{Z}$ such that $\pi_1 x = m$ holds $x = \langle m \rangle$.

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

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

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

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

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

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

Let i, k, x be natural numbers. The functor $\mathrm{DigitDC}(x, i, k)$ yielding an element of k −SD is defined as follows:

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

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

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

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

4. Definition for Carry and Data Components of Addition

Let x be an integer. The functor SD_Add_Carry x yielding an integer is defined as follows:

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

One can prove the following proposition

(21) SD_Add_Carry $0 = 0$.

Let x be an integer and let k be a natural number.

The functor SD_Add_Data(x, k) yields an integer and is defined by:

(Def. 11) SD_Add_Data$(x, k) = x -$ SD_Add_Carry $x \cdot$ Radix k.

Next we state two propositions:

(22) SD_Add_Data$(0, k) = 0$.

(23) If $k \geqslant 2$ and $i_1 \in k$ −SD and $i_2 \in k$ −SD, then −Radix $k + 2 \leqslant$ SD_Add_Data$(i_1 + i_2, k)$ and SD_Add_Data$(i_1 + i_2, k) \leqslant$ 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) $x < (\text{Radix}\,k)^n_{\mathbb{N}}$.

Next we state four propositions:

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

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

(26) If $k \geqslant 2$ and m is represented by 1, k and n is represented by 1, k, then SD_Add_Carry DigA(DecSD$(m, 1, k), 1) +$ DigA(DecSD$(n, 1, k), 1) =$ SD_Add_Carry $m + n$.

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

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 tuples of n and k −SD. Let us assume that $i \in \mathrm{Seg}\, n$ and $k \geqslant 2$. The functor $\mathrm{Add}(x, y, i, k)$ yields an element of k −SD and is defined as follows:

(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 tuples of n and k −SD. The functor $x' +' y$ yielding a tuple of n and k −SD is defined by:

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

One can prove the following two propositions:

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

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[3] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[5] Marek Chmur. The lattice of natural numbers and the sublattice of it. The set of prime numbers. *Formalized Mathematics*, 2(**4**):453–459, 1991.

[6] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Euler's Theorem and small Fermat's Theorem. *Formalized Mathematics*, 7(**1**):123–126, 1998.

[7] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[8] Andrzej Kondracki. The chinese remainder theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.

[9] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

[10] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[11] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[12] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

[13] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received September 7, 1999