JOURNAL OF FORMALIZED MATHEMATICS
Volume 15, Released 2003, Published 2003
Inst. of Computer Science, Univ. of Białystok

Magnitude Relation Properties of Radix-2^k SD Number

Masaaki Niimura
Shinshu University
Nagano

Yasushi Fuwa
Shinshu University
Nagano

Summary. In this article, magnitude relation properties of Radix-2^k SD number are discussed.

Until now, the Radix-2^k SD Number is proposed for the high-speed calculations for RSA Cryptograms. In RSA Cryptograms, many modulo calculations are used, and modulo calculations need a comparison between two numbers.

In this article, we discussed about a magnitude relation of Radix-2^k SD Number. In the first section, we prepared some useful theorems for operations of Radix-2^k SD Number. In the second section, we proved some properties about the primary numbers expressed by Radix-2^k SD Number such as 0, 1, and Radix(k). In the third section, we proved primary magnitude relations between two Radix-2^k SD Numbers. In the fourth section, we defined Max/Min numbers in some cases. And in the last section, we proved some relations about the addition of Max/Min numbers.

MML Identifier: RADIX_5.

WWW: http://mizar.org/JFM/Vol15/radix_5.html

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

1. Some Useful Theorems

One can prove the following propositions:

(1) For every natural number k such that $k \geq 2$ holds $\mathrm{Radix}\, k - 1 \in k - \mathrm{SD}$.

(2) For all natural numbers i, n such that $i > 1$ and $i \in \mathrm{Seg}\, n$ holds $i -' 1 \in \mathrm{Seg}\, n$.

(3) For every natural number k such that $2 \leq k$ holds $4 \leq \mathrm{Radix}\, k$.

(4) For every natural number k and for every 1-tuple t_1 of $k - \mathrm{SD}$ holds $\mathrm{SDDec}\, t_1 = \mathrm{DigA}(t_1, 1)$.

2. Properties of Primary Radix-2^k SD Number

We now state several propositions:

(5) For all natural numbers i, k, n such that $i \in \mathrm{Seg}\, n$ holds $\mathrm{DigA}(\mathrm{DecSD}(0, n, k), i) = 0$.

(6) For all natural numbers n, k such that $n \geq 1$ holds $\mathrm{SDDec}\, \mathrm{DecSD}(0, n, k) = 0$.

(7) For all natural numbers k, n such that $1 \in \operatorname{Seg} n$ and $k \geq 2$ holds $\operatorname{DigA}(\operatorname{DecSD}(1,n,k),1) = 1$.

(8) For all natural numbers i, k, n such that $i \in \operatorname{Seg} n$ and $i > 1$ and $k \geq 2$ holds $\operatorname{DigA}(\operatorname{DecSD}(1,n,k),i) = 0$.

(9) For all natural numbers n, k such that $n \geq 1$ and $k \geq 2$ holds $\operatorname{SDDec} \operatorname{DecSD}(1,n,k) = 1$.

(10) For every natural number k such that $k \geq 2$ holds $\operatorname{SD\_Add\_Carry} \operatorname{Radix} k = 1$.

(11) For every natural number k such that $k \geq 2$ holds $\operatorname{SD\_Add\_Data}(\operatorname{Radix} k, k) = 0$.

3. Primary Magnitude Relation of Radix-2^k SD Number

The following propositions are true:

(12) Let n be a natural number. Suppose $n \geq 1$. Let k be a natural number and t_1, t_2 be n-tuples of $k-\mathrm{SD}$. If for every natural number i such that $i \in \operatorname{Seg} n$ holds $\operatorname{DigA}(t_1,i) = \operatorname{DigA}(t_2,i)$, then $\operatorname{SDDec} t_1 = \operatorname{SDDec} t_2$.

(13) Let n be a natural number. Suppose $n \geq 1$. Let k be a natural number and t_1, t_2 be n-tuples of $k-\mathrm{SD}$. If for every natural number i such that $i \in \operatorname{Seg} n$ holds $\operatorname{DigA}(t_1,i) \geq \operatorname{DigA}(t_2,i)$, then $\operatorname{SDDec} t_1 \geq \operatorname{SDDec} t_2$.

(14) Let n be a natural number. Suppose $n \geq 1$. Let k be a natural number. Suppose $k \geq 2$. Let t_1, t_2, t_3, t_4 be n-tuples of $k-\mathrm{SD}$. Suppose that for every natural number i such that $i \in \operatorname{Seg} n$ holds $\operatorname{DigA}(t_1,i) = \operatorname{DigA}(t_3,i)$ and $\operatorname{DigA}(t_2,i) = \operatorname{DigA}(t_4,i)$ or $\operatorname{DigA}(t_2,i) = \operatorname{DigA}(t_3,i)$ and $\operatorname{DigA}(t_1,i) = \operatorname{DigA}(t_4,i)$. Then $\operatorname{SDDec} t_3 + \operatorname{SDDec} t_4 = \operatorname{SDDec} t_1 + \operatorname{SDDec} t_2$.

(15) Let n, k be natural numbers. Suppose $n \geq 1$ and $k \geq 2$. Let t_1, t_2, t_3 be n-tuples of $k-\mathrm{SD}$. Suppose that for every natural number i such that $i \in \operatorname{Seg} n$ holds $\operatorname{DigA}(t_1,i) = \operatorname{DigA}(t_3,i)$ and $\operatorname{DigA}(t_2,i) = 0$ or $\operatorname{DigA}(t_2,i) = \operatorname{DigA}(t_3,i)$ and $\operatorname{DigA}(t_1,i) = 0$. Then $\operatorname{SDDec} t_3 + \operatorname{SDDec} \operatorname{DecSD}(0,n,k) = \operatorname{SDDec} t_1 + \operatorname{SDDec} t_2$.

4. Definition of Max/Min Radix-2^k SD Numbers in Some Digits

Let i, m, k be natural numbers. Let us assume that $k \geq 2$. The functor $\operatorname{SDMinDigit}(m,k,i)$ yielding an element of $k-\mathrm{SD}$ is defined by:

(Def. 1) $$\operatorname{SDMinDigit}(m,k,i) = \begin{cases} -\operatorname{Radix} k + 1, & \text{if } 1 \leq i \text{ and } i < m, \\ 0, & \text{otherwise.} \end{cases}$$

Let n, m, k be natural numbers. The functor $\operatorname{SDMin}(n,m,k)$ yielding a n-tuple of $k-\mathrm{SD}$ is defined as follows:

(Def. 2) For every natural number i such that $i \in \operatorname{Seg} n$ holds $\operatorname{DigA}(\operatorname{SDMin}(n,m,k),i) = \operatorname{SDMinDigit}(m,k,i)$.

Let i, m, k be natural numbers. Let us assume that $k \geq 2$. The functor $\operatorname{SDMaxDigit}(m,k,i)$ yielding an element of $k-\mathrm{SD}$ is defined by:

(Def. 3) $$\operatorname{SDMaxDigit}(m,k,i) = \begin{cases} \operatorname{Radix} k - 1, & \text{if } 1 \leq i \text{ and } i < m, \\ 0, & \text{otherwise.} \end{cases}$$

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

(Def. 4) For every natural number i such that $i \in \operatorname{Seg} n$ holds $\operatorname{DigA}(\operatorname{SDMax}(n,m,k),i) = \operatorname{SDMaxDigit}(m,k,i)$.

Let i, m, k be natural numbers. Let us assume that $k \geq 2$. The functor $\operatorname{FminDigit}(m,k,i)$ yields an element of $k-\mathrm{SD}$ and is defined as follows:

(Def. 5) $\text{FminDigit}(m,k,i) = \begin{cases} 1, & \text{if } i = m, \\ 0, & \text{otherwise.} \end{cases}$

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

(Def. 6) For every natural number i such that $i \in \text{Seg}\, n$ holds $\text{DigA}(\text{Fmin}(n,m,k),i) = \text{FminDigit}(m,k,i)$.

Let i, m, k be natural numbers. Let us assume that $k \geq 2$. The functor $\text{FmaxDigit}(m,k,i)$ yields an element of $k-\text{SD}$ and is defined as follows:

(Def. 7) $\text{FmaxDigit}(m,k,i) = \begin{cases} \text{Radix}\, k - 1, & \text{if } i = m, \\ 0, & \text{otherwise.} \end{cases}$

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

(Def. 8) For every natural number i such that $i \in \text{Seg}\, n$ holds $\text{DigA}(\text{Fmax}(n,m,k),i) = \text{FmaxDigit}(m,k,i)$.

5. Properties of Max/Min Radix-2^k SD Numbers

The following four propositions are true:

(16) Let n, m, k be natural numbers. Suppose $n \geq 1$ and $k \geq 2$ and $m \in \text{Seg}\, n$. Let i be a natural number. If $i \in \text{Seg}\, n$, then $\text{DigA}(\text{SDMax}(n,m,k),i) + \text{DigA}(\text{SDMin}(n,m,k),i) = 0$.

(17) Let n be a natural number. Suppose $n \geq 1$. Let m, k be natural numbers. If $m \in \text{Seg}\, n$ and $k \geq 2$, then $\text{SDDec}\, \text{SDMax}(n,m,k) + \text{SDDec}\, \text{SDMin}(n,m,k) = \text{SDDec}\, \text{DecSD}(0,n,k)$.

(18) Let n be a natural number. Suppose $n \geq 1$. Let m, k be natural numbers. If $m \in \text{Seg}\, n$ and $k \geq 2$, then $\text{SDDec}\, \text{Fmin}(n,m,k) = \text{SDDec}\, \text{SDMax}(n,m,k) + \text{SDDec}\, \text{DecSD}(1,n,k)$.

(19) For all natural numbers n, m, k such that $m \in \text{Seg}\, n$ and $k \geq 2$ holds $\text{SDDec}\, \text{Fmin}(n+1,m+1,k) = \text{SDDec}\, \text{Fmin}(n+1,m,k) + \text{SDDec}\, \text{Fmax}(n+1,m,k)$.

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

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

[4] Yoshinori Fujisawa and Yasushi Fuwa. Definitions of radix-2^k signed-digit number and its adder algorithm. *Journal of Formalized Mathematics*, 11, 1999. `http://mizar.org/JFM/Vol11/radix_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] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. `http://mizar.org/JFM/Axiomatics/tarski.html`.

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

Received November 7, 2003

Published January 2, 2004