FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University 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 has been 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 discuss magnitude relation of Radix-2^k SD Number. In the first section, we present some useful theorems for operations of Radix-2^k SD Number. In the second section, we prove some properties of the primary numbers expressed by Radix-2^k SD Number such as 0, 1, and Radix(k). In the third section, we prove primary magnitude relations between two Radix-2^k SD Numbers. In the fourth section, we define Max/Min numbers in some cases. And in the last section, we prove some relations between the addition of Max/Min numbers.

MML Identifier: RADIX_5.

The terminology and notation used here are introduced in the following articles: [7], [8], [1], [6], [4], [2], [3], and [5].

1. Some Useful Theorems

The following propositions are true:

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

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

(3) For every natural number k such that $2 \leqslant k$ holds $4 \leqslant \operatorname{Radix} k$.

ISSN 1426–2630

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

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

Next we 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 $n \geqslant 1$ holds $\mathrm{SDDec}\, \mathrm{DecSD}(0, n, k) = 0$.

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

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

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

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

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

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

Next we state four propositions:

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

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

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

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

$\mathrm{DigA}(t_3, i)$ and $\mathrm{DigA}(t_1, i) = 0$. Then $\mathrm{SDDec}\, t_3 + \mathrm{SDDec}\, \mathrm{DecSD}(0, n, k) = \mathrm{SDDec}\, t_1 + \mathrm{SDDec}\, t_2$.

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

Let i, m, k be natural numbers. Let us assume that $k \geqslant 2$. The functor $\mathrm{SDMinDigit}(m, k, i)$ yielding an element of k −SD is defined as follows:

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

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

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

Let i, m, k be natural numbers. Let us assume that $k \geqslant 2$. The functor $\mathrm{SDMaxDigit}(m, k, i)$ yielding an element of k −SD is defined as follows:

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

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

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

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

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

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

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

Let i, m, k be natural numbers. Let us assume that $k \geqslant 2$. The functor $\mathrm{FmaxDigit}(m, k, i)$ yielding an element of k −SD is defined as follows:

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

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

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

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

Next we state four propositions:

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

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

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

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

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. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[4] Yoshinori Fujisawa and Yasushi Fuwa. Definitions of radix-2^k signed-digit number and its adder algorithm. *Formalized Mathematics*, 9(**1**):71–75, 2001.

[5] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.

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

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

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

Received November 7, 2003