

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 $k \geq 2$ holds $\text{Radix } k - 1 \in k - \text{SD}$.
- (2) For all natural numbers i, n such that $i > 1$ and $i \in \text{Seg } n$ holds $i - 1 \in \text{Seg } n$.
- (3) For every natural number k such that $2 \leq k$ holds $4 \leq \text{Radix } k$.

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

2. PROPERTIES OF PRIMARY RADIX- 2^k SD NUMBER

Next we state several propositions:

- (5) For all natural numbers i, k, n such that $i \in \text{Seg } n$ holds $\text{DigA}(\text{DecSD}(0, n, k), i) = 0$.
- (6) For all natural numbers n, k such that $n \geq 1$ holds $\text{SDDec DecSD}(0, n, k) = 0$.
- (7) For all natural numbers k, n such that $1 \in \text{Seg } n$ and $k \geq 2$ holds $\text{DigA}(\text{DecSD}(1, n, k), 1) = 1$.
- (8) For all natural numbers i, k, n such that $i \in \text{Seg } n$ and $i > 1$ and $k \geq 2$ holds $\text{DigA}(\text{DecSD}(1, n, k), i) = 0$.
- (9) For all natural numbers n, k such that $n \geq 1$ and $k \geq 2$ holds $\text{SDDec DecSD}(1, n, k) = 1$.
- (10) For every natural number k such that $k \geq 2$ holds $\text{SD_Add_Carry Radix } k = 1$.
- (11) For every natural number k such that $k \geq 2$ holds $\text{SD_Add_Data}(\text{Radix } k, k) = 0$.

3. PRIMARY MAGNITUDE RELATION OF RADIX- 2^k SD NUMBER

Next we state four propositions:

- (12) Let n be a natural number. Suppose $n \geq 1$. 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 $i \in \text{Seg } n$ holds $\text{DigA}(t_1, i) = \text{DigA}(t_2, i)$, then $\text{SDDec } t_1 = \text{SDDec } t_2$.
- (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 -SD. If for every natural number i such that $i \in \text{Seg } n$ holds $\text{DigA}(t_1, i) \geq \text{DigA}(t_2, i)$, then $\text{SDDec } t_1 \geq \text{SDDec } t_2$.
- (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 -SD. Suppose that for every natural number i such that $i \in \text{Seg } n$ holds $\text{DigA}(t_1, i) = \text{DigA}(t_3, i)$ and $\text{DigA}(t_2, i) = \text{DigA}(t_4, i)$ or $\text{DigA}(t_2, i) = \text{DigA}(t_3, i)$ and $\text{DigA}(t_1, i) = \text{DigA}(t_4, i)$. Then $\text{SDDec } t_3 + \text{SDDec } t_4 = \text{SDDec } t_1 + \text{SDDec } t_2$.
- (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 -SD. Suppose that for every natural number i such that $i \in \text{Seg } n$ holds $\text{DigA}(t_1, i) = \text{DigA}(t_3, i)$ and $\text{DigA}(t_2, i) = 0$ or $\text{DigA}(t_2, i) =$

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

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 $\text{SDMinDigit}(m, k, i)$ yielding an element of k -SD is defined as follows:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. PROPERTIES OF MAX/MIN RADIX- 2^k SD NUMBERS

Next we state four propositions:

- (16) Let n, m, k be natural numbers. Suppose $n \geq 1$ 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 $\text{SDDec SDMax}(n, m, k) + \text{SDDec SDMin}(n, m, k) = \text{SDDec DecSD}(0, n, k)$.
- (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 $\text{SDDec Fmin}(n, m, k) = \text{SDDec SDMax}(n, m, k) + \text{SDDec DecSD}(1, n, k)$.
- (19) For all natural numbers n, m, k such that $m \in \text{Seg } n$ and $k \geq 2$ holds $\text{SDDec Fmin}(n+1, m+1, k) = \text{SDDec Fmin}(n+1, m, k) + \text{SDDec Fmax}(n+1, m, k)$.

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
