Mixed Radix-2 and High-Radix RNS Bases for Low-Power Multiplication*

Ioannis Kouretas and Vassilis Paliouras

Electrical and Computer Engineering Dept.,
University of Patras, Greece

Abstract. This paper investigates the performance of a novel set of Residue Number System (RNS) bases, emphasizing on the minimization of the power×delay product. The proposed bases introduce moduli of the form 3^n, to the usual choice of moduli of the form 2^n, $2^n - 1$, or $2^n + 1$. It is found that for particular dynamic ranges, the introduction of high-radix modulo-3^n multipliers significantly improves the power×delay performance of residue multiplication, in comparison to conventional two's-complement implementations as well as to RNS architectures using bases composed of radix-2 moduli. Experimental results demonstrate reduction of the power×delay product by almost a factor of two, for some cases.

1 Introduction

The use of alternative number representations such as the Logarithmic Number System (LNS) and the Residue Number System (RNS), is a promising technique for the implementation of computationally-intensive special-purpose low-power systems [1][2].

RNS has been investigated as a possible choice for number representation in DSP applications [3][4][5], since it offers parallel multiplication or addition and error-correction properties [6]. Recently RNS has been proved to provide solutions in the field of wireless communications [7][8].

In RNS architectures, complexity reduction has been sought by resorting to the use of moduli that lead to simpler circuits. In particular, common choices are moduli of the form $2^n - 1$[9], 2^n, and $2^n + 1$ [9][10][11]. Moduli of the form $2^n - 1$ and $2^n + 1$ offer low-complexity circuits for arithmetic operations due to the end-around carry property, while moduli of the form 2^n lead to simple and regular architectures due to the carry-ignore property.

Furthermore, recent works [12][13] have demonstrated the low-power properties of RNS circuits in comparison to two's complement-based circuits, for the implementation of FIR digital filters. A different approach is given in [14], where it is reported that in case of RNS multiplication, the power supply voltage can be reduced for those moduli channels, that do not define the critical path of

* The support by the University of Patras through the "C. Caratheodory" project under contract No B-701 is gratefully acknowledged.

L. Svensson and J. Monteiro (Eds.): PATMOS 2008, LNCS 5349, pp. 93–102, 2009.

the RNS. Thus power can be reduced without affecting the performance of the overall RNS-based circuit, since only the delay of non-critical moduli channels increases.

This paper discusses the low-power aspects of architectures that perform arithmetic modulo $2^n - 1$ or 2^n, as well as 3^n. The modulo-3^n arithmetic circuits assume a radix-3 implementation [15][16]. The proposed bases comprise two or three moduli.

The benefits achieved by the proposed RNS-based approach come at the cost of a conversion overhead. This is common with alternative arithmetics, as circuits based on them are required to process data, usually available in a two's-complement format. It has been reported that since the conversion overhead cost remains fixed for important classes of applications, such as digital filtering, a sufficiently large number of multiplications can fully compensate this cost [12][13].

The remainder of the paper is organized as follows: Section 2 reviews the RNS basics. In section 3 the proposed RNS bases are presented and the corresponding performance is compared to a two's complement multiplier and a RNS multiplier using a base of radix-2. Finally conclusions are discussed in section 4.

2 Review of RNS Basics

The RNS maps an integer X to a N-tuple of *residues* x_i, as follows

$$X \xrightarrow{\text{RNS}} \{x_1, x_2, \ldots, x_N\}, \tag{1}$$

where $x_i = \langle X \rangle_{m_i}$, $\langle \cdot \rangle_{m_i}$ denotes the mod m_i operation, and m_i is a member of a set of pair-wise co-prime integers $\{m_1, m_2, \ldots, m_M\}$, called *base*. Co-prime integers have the property that $\gcd(m_i, m_j) = 1$, $i \neq j$. The modulo operation $\langle X \rangle_m$ returns the integer remainder of the integer division x div m, i.e., a number k such that $x = m \cdot l + k$, where l is an integer. Mapping (1) offers a unique representation of integer X, when $0 \leq X < \prod_{i=1}^{N} m_i$.

RNS is of interest because basic arithmetic operations can be performed in a carry-free manner. In particular the operation $Z = X \circ Y$, where $Y \xrightarrow{\text{RNS}} \{y_1, y_2, \ldots, y_N\}$, $Z \xrightarrow{\text{RNS}} \{z_1, z_2, \ldots, z_N\}$, and the symbol $\circ$ stands for addition, subtraction, or multiplication, can be implemented in RNS as $z_i = \langle x_i \circ y_i \rangle_{m_i}$, for $i = 1, 2, \ldots, M$. According to the above, each residue result z_i does not depend on any of the x_i, y_i, $j \neq i$, thus allowing fast data processing in N parallel independent residue channels. Inverse conversion is accomplished by means of the Chinese Remainder Theorem (CRT) or mixed-radix conversion [17].

3 Proposed Bases and Low-Power RNS Multiplication

This section proposes RNS bases of the form $\{2^{n_1}, 2^{n_2} - 1, 3^{n_4}\}$ and $\{2^{n_5}, 3^{n_6}\}$. RNS multipliers based on the proposed bases are compared to a two's complement (TC) structures as well as to RNS architectures using bases composed of radix-2 moduli, a common choice in the literature.