Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 271 – 277

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

AN EFFICIENT VLSI ARCHITECTURE FOR MATRIX BASED RNS BACKWARD CONVERTER

Bhavana Rayapudi [a,*], I.B.K Raju[a], Gneneshwara Chary[a], Pranay Deekonda[a], Prashanth Ummadisetti[a]

[a]*B.V Raju Institute of Technology, Narsapur, Medak-502 313, Telangana, India*

Abstract

Residue Number System (RNS) is the important research area from last five decades. Forward & backward conversion process is the bottle neck which limits the use of RNS for computing needs.. In this paper, we proposed an efficient VLSI architecture for Matrix based RNS backward converter. We analysed the performance of proposed architecture for different modulo sets of size up to ten . Implemented using TSMC standard cell 180 nm CMOS technology libraries and result analysis indicated that, the performance of proposed converter achieved about 59% area reduction and 30% efficient with respective to Time-Delay Product when compared to the state of art Backward converters.

Peer-review under responsibility of the Organizing Committee of CMS 2016

Keywords: Residue Number System; Chinese remainder theorem(CRT); Backward Convertor; Computer Arithmetic

1. Introduction

In weighted number system, the main disadvantage is carry chain propagation because of this, there is performance degradation in computing hardware. So carry chain propagation is the main challenging problem. For reduction and elimination of carry chain there are many conventional number system approaches like carry look ahead, parallel prefix Adders, ELM adder. With all these approaches we can propagate the carry but not eliminating the carry totally. Whenever integer arithmetic for large numbers is needed this conventional number system will not

* Corresponding author. Rayapudi Bhavana.
*E-mail address:*bhavana.rayapudi@gmail.com

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.233

be a better choice. So, there is few unconventional approach like Residue number system [1] which restrict the carry chain propagation within the residue digits by which parallel execution can be achieved .This property makes it suitable for fast computer arithmetic's. It has many advantages like parallelism, fault tolerance, modularity, carry free nature etc.., with all these features it is well suited for digital signal processors (DSP) applications [5] such as digital filtering, convolutions, correlation, fast Fourier transforms, computer security (cryptography) [6], fault tolerance, fault detection, error correction, communication engineering[7] and image processing [8].

RNS processors have three components [2] forward Convertor, Modulo Arithmetic Unit and Backward Convertor. Among all these steps backward conversion is cost overhead. To overcome this problem there are different backward conversion algorithms like CRT [1], Mixed Radix Conversion (MRC) [1], Matrix Method (MATR) [3], CRT-I and CRT-II [4]. CRT is desirable because of its parallelism but the drawback is large modulo-M addition operation during the last stage. In MRC algorithm only Mixed Radix Digits are added in the last stage but is sequential in nature. The main disadvantage with CRT-l and CRT-ll is they restricted to specific class of module sets. MATR is the backward conversion algorithm proposed is [3] sequential in nature but needs less computations steps when compared with MRC. There are no VLSI architectures are existing. In this paper, we proposed VLSI architecture for MATR

The paper we briefly present the necessary background in Section 2. Section 3 describes the proposed VLSI architecture for Matrix Method for efficient residue to decimal conversion. We evaluate the performance of our proposal in Section 4. Finally section 5 gives conclusion.

2. Background

RNS is an unconventional number system that is defined in terms of relatively prime moduli set $\{m_1, m_2, m_3 \ldots\ldots, m_n\}$ that is gcd(m$_i$,m$_j$) for i≠j . A weighted number can be represented as $X = (x_1, x_2, \ldots\ldots, x_n)$ where

$$x_i = X\ mod\ m_i = X|x_i, 0 \le x_i < m_i \tag{1}$$

RNS has unique representation for any integer in the range$[0\ to\ M-1]$, where M is the dynamic range of the moduli set $\{m_1, m_{2,\ldots\ldots}, m_n\}$, which is equal to the product of m_i terms.

In this paper we are evaluating the performance of CRT (Chinese Remainder Theorem), MRC (Mixed Radix Conversion) and MATR (Matrix Method). CRT defined for a set of pair-wise relatively-prime moduli, $\{m_1, m_{2,\ldots\ldots}, m_n\}$ and a residue representation $(x_1, x_2, \ldots., x_n)$ in that system of some number X, i.e. $x_i = |X|_{m_i}$, that number and its residues are related by the equation

$$|X|_M = \left| \sum_{i=1}^{N} x_i |M_i^{-1}|_{m_i} M_i \right|_M \tag{2}$$

The ROM based reverse converter architecture for Chinese remainder theorem is given below. The main drawback of CRT is large modulo-M operation.

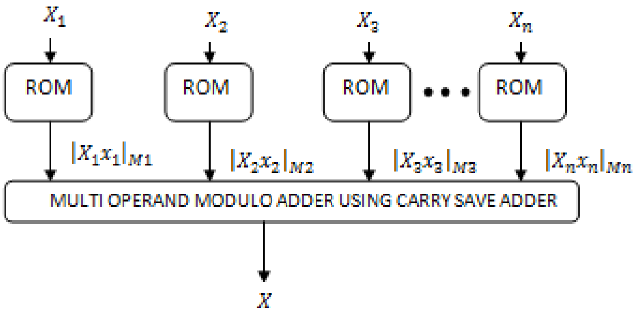

Fig 1: ROM based CRT Architecture

MRC approach is inherently a sequential approach. It is defined as assume that there is set of residues $(x_1, x_2, \ldots., x_n)$ with the moduli set $\{m_1, m_{2,\ldots\ldots}, m_n\}$ and the corresponding mixed radix digits are $Z_1, Z_2, \ldots\ldots, Z_N$, then the equation for converting residue to decimal conversion X is as follow.