A New Interpretation of "Polynomial Residue Number System"

Ming-Chwen Yang and Ja-Ling Wu

***Abstract*—In this correspondence, we will show that the polynomial residue number system can be interpreted in terms of the Chinese remainder theorem for polynomials (CRTP) over a finite ring.**

I. The Polynomial Residue Number Systems

The polynomial residue number system of order N (PRNS(N)) [1] examines the problem of multiplying two $(N-1)$th degree polynomials mod $(x^N \pm 1)$ over some modular ring $Z_m = \{0, 1, \ldots, m-1\}$ and is a generalization of the quadratic residue number system. The most attractive property of PRNS is that it performs the aforecited polynomial product with only N multiplications in parallel instead of N^2. Thus it provides a useful tool for computing multiplication-intensive digital signal processing operations, such as convolutions and correlations.

Consider two polynomials in x, $A(x) = \sum_{i=0}^{N-1} a_i x^i$ and $B(x) = \sum_{i=0}^{N-1} b_i x^i$ also denoted as $A = (a_0, a_1, \ldots, a_{N-1})$ and $B = (b_0, b_1, \ldots, b_{N-1})$ and consider that $\langle c \rangle_m$ denotes the operation c mod m for integers, while $\langle C(x) \rangle_{Q(x)}$ denotes the operation $C(x)$ mod $Q(x)$ for polynomials. It was shown in [1] that if the polynomials $(x^N \pm 1)$ can be factorized in Z_m as

$$x^N \pm 1 = (x - r_0)(x - r_1) \cdots (x - r_{N-1}), \quad r_i \in Z_m, \quad i = 0, 1, \ldots, N-1 \tag{1}$$

then there exists an isomorphic mapping between $P(m)$ and Z_m^N, where $P(m) = \{\sum_{i=0}^{N-1} p_i x^i, p_i \in Z_m\}$, a finite structure containing the $(N-1)$th order polynomials with coefficients in Z_m, and $Z_m^N = \bigoplus_{i=1}^{N} Z_m$, the Nth degree direct sum of Z_m, respectively. The above statement can be written in a more tracible form as

$$\langle A(x)B(x) \rangle_{x^N \pm 1} \overset{f_N}{\longleftrightarrow} f_N^{-1}(\langle a_0^* b_0^* \rangle_m, \langle a_1^* b_1^* \rangle_m, \ldots, \langle a_{N-1}^* b_{N-1}^* \rangle_m) \tag{2}$$

where the forward mapping is

$$f_N : A = (a_0, a_1, \ldots, a_{N-1}) \rightarrow A^* = (a_0^*, a_1^*, \ldots, a_{N-1}^*) \tag{3}$$

with

$$a_i^* = \langle a_0 + a_1 r_i + a_2 r_i^2 + \cdots + a_{N-1} r_i^{N-1} \rangle_m \tag{4}$$

and the inverse mapping is

$$f_N^{-1} : A^* = (a_0^*, a_1^*, \ldots, a_{N-1}^*) \rightarrow A = (a_0, a_1, \ldots, a_{N-1}) \tag{5}$$

with

$$a_i = \langle N^{-1}(a_0^* r_0^{-i} + a_1^* r_1^{-i} + a_2^* r_2^{-i} + \cdots + a_{N-1}^* r_{N-1}^{-i}) \rangle_m, \quad i = 0, 1, \ldots, N-1 \tag{6}$$

where N^{-1} and r_j^{-i} are the multiplicative inverses of N and r_j^i in Z_m. Equations (4) and (6) can be written in a more compact form, respectively, as:

$$a_i^* = \langle \langle A(x) \rangle_{(x-r_i)} \rangle_m = \langle A(r_i) \rangle_m, i = 0, 1, \ldots, N-1 \tag{7}$$

and

$$A(x) = \sum_{i=0}^{N-1} a_i^* Q_i(x) \tag{8}$$

where

$$Q_i(x) = N^{-1}(1 + r_i^{-1} x + r_i^{-2} x^2 + \cdots + r_i^{-(N-1)} x^{N-1}). \tag{9}$$

Moreover, the necessary and sufficient condition for the existence of the factorization in (1) is [1]

$$\begin{cases} N \mid (p_i - 1)/2), & \text{for } x^N + 1 \\ N \mid (P_i - 1), & \text{for } x^N - 1 \end{cases} \tag{10}$$

where $a \mid b$ means 'a divides b' and $m = p_1^{e_1} p_2^{e_2} \cdots p_L^{e_L}$ with p_i:distinct prime numbers and $N < p_i$.

II. The Chinese Remainder Theorem and the PRNS

It is well-known that [2] if $m_1(x), m_2(x), \ldots, m_L(x)$ are polynomials which are relatively prime in pairs, then the system of congruences $R(x) = r_i(x) \bmod m_i(x)$, for $i = 1, 2, \ldots, L$, has a unique solution $R(x)$ given by

$$R(x) = \sum_{i=1}^{L} r_i(x) M_i(x) N_i(x) \bmod M(x) \tag{11}$$

where

$$M(x) = \prod_{i=1}^{L} m_i(x) = m_i(x) M_i(x) \tag{12}$$

and $N_i(x)$ uniquely satisfies the congruence

$$M_i(x) N_i(x) = 1 \bmod m_i(x). \tag{13}$$

Now consider the following congruence equation:

$$C(x) = \langle A(x) \cdot B(x) \rangle_{x^N \pm 1} \tag{14}$$

and let Z_m be chosen such that the condition (10) is satisfied. Then, based on the CRTP and (1), (14) can be decomposed into the following N congruence equations:

$$c_i^* = \langle a_i^* \cdot b_i^* \rangle_m, i = 0, 1, \ldots, N-1 \tag{15}$$

where $a_i^* = \langle \langle A(x) \rangle_{(x-r_i)} \rangle_m$ and $b_i^* = \langle \langle B(x) \rangle_{(x-r_i)} \rangle_m$. The polynomial $C(x)$ can be reconstructed by using the CRTP, that is

$$M_i(x) = \prod_{j=0, j \neq i}^{N-1} (x - r_j) i = 0, 1, \ldots, N-1 \tag{16}$$

$$= (x^N \pm 1)/(x - r_i) = x^{N-1} + r_i x^{N-2} + r_i^2 x^{N-3} + \cdots + r_i^{N-2} x + r_i^{N-1}. \tag{17}$$

As a result

$$\langle M_i(x) \rangle_{(x-r_i)} = M_i(r_i) = N r_i^{N-1}. \tag{18}$$

Thus

$$N_i(r_i) = (M_i(r_i))^{-1} = N^{-1} r_i^{-(N-1)} \bmod m. \tag{19}$$

Manuscript received August 3, 1993; revised February 7, 1994. The associate editor coordinating the review of this paper and approving it for publication was Prof. Henrik V. Sorenson.

The authors are with the Department of Computer Science and Information Engineering, National Taiwan University, Taipei 10764, Taiwan, Republic Of China.

IEEE Log Number 9401927

1053–587X/94$04.00 © 1994 IEEE

Authorized licensed use limited to: National Taiwan University. Downloaded on March 19, 2009 at 23:55 from IEEE Xplore. Restrictions apply.

It is easy to verify that

$$\langle N_i(r_i)\rangle_m \cdot M_i(x) = N^{-1} r_i^{-(N-1)}(x^{N-1} + r_i x^{N-2} + \cdots + r_i^{N-2}x + r_i^{N-1}). \quad (20)$$

Compare (9) with (20), it follows that $\langle N_i(r_i)\rangle_m \cdot M_i(x) = Q_i(x)$. It is easy to check $\langle Q_i(x)\rangle_{(x-r_i)} = 1$ and $\langle Q_i(x)\rangle_{(x-r_j)} = 0$, for $i \neq j$. By CRTP, $C(x)$ can be obtained as

$$C(x) = \sum_{i=0}^{N-1} c_i^* \langle N_i(r_i)\rangle_m \cdot M_i(x) = \sum_{i=0}^{N-1} c_i^* Q_i(x) \quad (21)$$

III. Conclusion

From the derivations given in Section II, the polynomial residue number system can be interpreted by the terminology of Chinese remainder theorem for polynomials over a finite ring, which is more familiar for the computer and signal processing societies.

References

[1] A. Skavantzos and F. J. Taylor, "On the polynomial residue number system," *IEEE Trans. Signal Processing*, vol 39, no. 2, pp. 376–382, Feb. 1991.

[2] J. H. McClellan and C. M. Rader, *Number Theory in Digital Signal Processing*. Englewood Cliffs, NJ: Prentice-Hall, 1979.

Wavelet Coefficient Computation with Optimal Prefiltering

Xiang-Gen Xia, C.-C. Jay Kuo, and Zhen Zhang

***Abstract*—Discrete wavelet transform (DWT) is often used to approximate wavelet series transform (WST) and continuous wavelet transform (CWT), since it can be computed numerically. In this research, we first study the accuracy of the computed DWT coefficients obtained from the Shensa algorithm as an approximate of the WST coefficients. Based on the accuracy analysis, we then propose a procedure to design optimal FIR prefilters used in the Shensa algorithm to reduce the approximation error. Finally, numerical examples are presented to demonstrate the performance of the optimal FIR prefilters.**

Manuscript received September 15, 1992; revised November 28, 1993. This work was supported by National Science Foundation Grant NCR-9205265, National Science Foundation Young Investigator (NYI) Award ASC-9258396 and the Presidential Faculty Fellow (PFF) Award ASC-9350309. The associate editor coordinating the review of this paper and approving it for publication was Prof. James Cooley.

X.-G. Xia is with the Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson AFB, OH 45433-7765 USA.

C.-C. J. Kuo is with the Signal and Image Processing Institute, Department of Electrical Engineering-Systems, University of Southern California, Los Angeles, CA 9089–2564 USA.

Z. Zhang is with the Communication Science Institute, Department of Electrical Engineering-Systems, University of Southern California. Los Angeles, CA 9089–2565 USA.

IEEE Log Number 9401921.

I. Introduction

Wavelet transforms have recently been recognized as useful tools for various applications such as signal and image processing, numerical analysis and physics. There are three types of wavelet transforms discussed in the literature, namely, continuous wavelet transform (CWT) [4], wavelet series transform (WST) [3], and discrete wavelet transform (DWT) [6], [8]. These transforms using biorthogonal wavelet bases are briefly summarized below. We use the notation

$$f_{jk}(t) \triangleq 2^{j/2} f(2^j t - k), \quad j,k \in \mathbf{Z},$$

and

$$f_{a,b}(t) = |a|^{-1/2} f\left(\frac{t-b}{a}\right), \quad a \neq 0, b \in \mathbf{R}.$$

Let $\psi(t)$ and $\tilde{\psi}(t)$ be, respectively, a real wavelet function and its dual such that $\{\psi_{jk}(t)\}_{j,k}$ and $\{\tilde{\psi}_{jk}(t)\}_{j,k}$ form a biorthogonal wavelet basis in $L^2(\mathbf{R})$. Then, for $f(t) \in L^2(\mathbf{R})$, its CWT with respect to the wavelet $\psi(t)$ is defined as

$$\mathrm{CWT}\{f(t); a, b\} \triangleq \int_{-\infty}^{\infty} f(t)\psi_{a,b}(t)dt$$

where a and b are called the scale and time parameters, respectively. The WST of $f(t)$ is obtained by sampling its CWT in the scale-time plane (a, b) with the so-called "dyadic" grid, i.e.

$$\mathrm{WST}\{f(t); j, k\} = \mathrm{CWT}\{f(t); a = 2^{-j}, b = k2^{-j}\}, j, k \in \mathbf{Z}.$$

Thus, the WST coefficients, also denoted by $b_{j,k}$, can be determined by

$$b_{j,k} \triangleq \mathrm{WST}\{f(t); j, k\} = \int_{-\infty}^{\infty} f(t)\psi_{jk}(t)dt, \quad j,k \in \mathbf{Z}. \quad (1)$$

Moreover, $f(t)$ can be reconstructed via

$$f(t) = \sum_j \sum_k b_{j,k}\tilde{\psi}_{jk}(t).$$

The orthogonal wavelet is a special case of the biorthogonal one by requiring $\psi(t) = \tilde{\psi}(t)$. If the t as well as parameters (a, b) all take discrete values, which are recognized as a natural wavelet transform for the discrete-time signal $f(m\Delta t)$ with $m \in \mathbf{Z}$, the resulting transform is called the DWT of $f(t)$. It is clear that only the DWT coefficients can be computed numerically, and the CWT and WST coefficients have to be approximated by the DWT coefficients in practice.

Several numerical algorithms have been proposed to compute the DWT coefficients such as the Mallat algorithm [6], the "à trous" algorithm of Holschneider *et al.* [5], and the Shensa algorithm [8] as a unified approach for the former two. Efficient implementations and detailed computational complexity analysis for these algorithms were discussed by Rioul and Duhamel [7]. However, an important issue which has not yet been addressed is the numerical accuracy of the computed DWT coefficients $b'_{j,k}$ with respect to the true WST coefficients $b_{j,k}$ as defined in (1). This was considered as an open problem in the work by Rioul and Duhamel [7] and Shensa [8]. In this research, after a brief review of some results from wavelet theory in Section II, we derive formulas to characterize the error between the computed and true wavelet coeficients in Section III. With such an error analysis, we develop a procedure to design the optimal FIR prefilter $q[n]$ to reduce the error as much as possible in Section

1053–587X/94$04.00 © 1994 IEEE

Authorized licensed use limited to: National Taiwan University. Downloaded on March 19, 2009 at 23:55 from IEEE Xplore. Restrictions apply.