



*A Flexible Modulus
Residue Number System
for Complex Digital
Signal Processing*

N.M. Wigley , G. A. Jullien

U N I V E R S I T Y O F

WINDSOR

V L S I R e s e a r c h G r o u p

A Flexible Modulus Residue Number System for Complex Digital Signal Processing

N.M. Wigley , G. A. Jullien

VLSI Research Group
University of Windsor
Ontario, Canada N9B 3P4

Introduction

Many digital processing algorithms require the manipulation of streams of complex numbers. Using conventional arithmetic implementations (fixed or floating point binary) multiplication represents a considerable hardware overhead. Possibly the more serious problem, however, is the required interaction between the real and imaginary streams of data. For high density circuitry on a single chip, this will increase the testing overhead and may also increase the overhead in on-line fault detection techniques.

A method of handling complex data, so that the two channels are completely independent, is the Quadratic Residue Number System (QRNS) [1]. The real and imaginary data are mapped to two channels that compute over finite fields; the algebraic properties of the ring structure represented by these two channels is such that the channels can proceed in an independent fashion for all addition and multiplication operations on the data. The results of the computations are fitted together using an inverse map, together with the Chinese Remainder Theorem, to give the final answer.

The QRNS method requires the use of moduli which have a special property: each prime divisor of the modulus must be of the form $4k + 1$. This requirement imposes a rather harsh limitation on the supply of eligible moduli.

In this letter we shall give an alternative to the QRNS method (the FMRNS) which allows the use of any odd integer (> 1) as modulus. Since a given implementation may use a modulus whose factors are all numbers of a given bit-size, say five bits, this flexibility will enable the choice of factors at the top end of the scale, which will in turn increase the dynamic range of the implementation.

The QRNS Method

The Quadratic Residue Number System (QRNS) method consists of converting complex additions and multiplications to related computations performed inside various finite rings of the form $R(m) \times R(m)$. Here $R(m)$ represents the usual set of residue classes of the integers modulo m , and the symbol \times means all ordered pairs of such residue classes (i.e. the cross-product ring). Within each ring, $R(m)$, the computation proceeds independently of all other computations in all of the other rings. A modulus M is chosen large enough to afford the necessary dynamic range. This modulus factors into smaller factors m_k , so that $M = \prod_{k=0}^K m_k$.

It will be helpful to produce a formal algebraic construction of the QRNS method as follows: Let X denote an indeterminate, and let a complex number, $c(k) = c^r(k) + jc^i(k)$, be written

$$c(k) = c^r(k) + Xc^i(k) \tag{1}$$

where the indeterminate, X , replaces the complex unit j . We then consider $c(k)$ to be a polynomial in the variable X over the ring $R(M)$.

In the QRNS approach we then view $R(M)$ itself as a direct product of the rings $R(m_1)$, $R(m_2)$, ..., and $R(m_K)$ (Chinese Remainder Theorem). Thus, viewed in this light, $c(k)$ can be represented as a polynomial in X over each of the rings $R(m_k)$. In each of these polynomial rings, we take the algebraic quotient modulo the ideal generated by the polynomial $X^2 + 1$; or, equivalently, we reduce the powers of X according to the rule $X^2 = -1$ (which is, of course, the defining equation of the imaginary unit). Since this polynomial has degree two, it means that the polynomial quotient ring can be written, under an isomorphism, as a direct product of the ring $R(m_k)$ with itself. The existence of the isomorphism is guaranteed by the requirement that each modulus m_k have only prime divisors of the form $4k + 1$.

This isomorphism is given by the map $A^\circ = a^r + ja^i$, $A^* = a^r - ja^i$; it is equivalent to the map given by evaluating the polynomial $a^r + Xa^i$ at the two roots $X = j$ and $X = -j$.

The FMRNS Method

The FMRNS method is constructed in a manner similar to the QRNS, but with the difference that the polynomial used to generate the ideal in the quotient ring is not the "sensible" one, namely $X^2 + 1$, but rather one that is merely convenient.

We let $g(X)$ denote the polynomial $g(X) = X(X^2 - 1)$. This polynomial has roots $0, \pm 1$. We define $FMR(m_k)$ by the mapping $A^\circ = a^r$, $A^* = a^r + a^i$, and $A^+ = a^r - a^i$, with $A^\circ, A^*, A^+ \in R(m_k)$. This is evaluation of the polynomial $a^r + Xa^i$ at the *three* roots $0,$

+1 and -1 of $g(X)$. (Note that the QRNS map is based on evaluation of $a^r + Xa^i$ at the *two* roots $\pm j$ of $X^2 + 1$). This evaluation map sets up an isomorphism between the quotient ring of polynomials modulo the ideal generated by $g(X)$, and the cross-product of the ring $R(m_k)$ with itself *three* times. Multiplications and additions are performed component-wise in these rings, just as in the other cases.

The QRNS method requires that there be a root in $R(m_k)$ of the polynomial $X^2 + 1$. This can be shown to be equivalent to the requirement that each odd prime divisor, p_i , of m_k be of the form $4k + 1$. The quotient map is given by identifying the power X^2 with the constant -1 ; this is the same equation as satisfied by the complex unit.

The FMRNS method uses the polynomial $g(X) = X(X^2 - 1)$, but other polynomials could be used. In order to effect the isomorphism between the quotient ring and the direct product ring we require that each difference of two roots of $g(X)$ be an invertible element of the ring $R(m_k)$ for each k [4].

The degree of $g(X)$ is dictated by the inner product; as the sum of products of linear polynomials, it will be a polynomial of degree two, and thus cannot belong to the ideal generated by $g(X)$ unless all of its coefficients are zero in the ring $R(M)$. It is true that the equation $X^3 - X = 0$ causes identification of X^3 with X ; but this has no meaning in the present situation because we never deal with polynomials of degree three or higher. Thus $g(X)$ has been selected for convenience; it is chosen to have degree three because the only possible polynomial of degree less than three would lead to the QRNS method, and the roots 0 and ± 1 are chosen because these roots are guaranteed to exist for any value of m_k (except, of course, for $m_k = 2$, for which they would not be distinct). We should also note that these roots provide forward mapping computational requirements

that are lower than that required for the QRNS method (here we count the multiplication by j in the QRNS method as a non-trivial operation).

Thus the FMRNS imposes no requirements on the prime divisors of m_k other than that they be odd.

Example

Let us give an example by means of the single complex multiplication $(2 - 3j)(1 + 2j) = 8 + j$. The data indicate that the modulus 21 will afford the requisite dynamic range. We write the multipliers as the polynomials $2 - 3X$ and $1 + 2X$. Ultimately we shall set $X = j$, but first we perform the required multiplication by means of the following steps:

- a) Reduce these polynomials (mod 3) and (mod 7).
- b) Perform the forward mapping by setting, respectively, $X = 0, +1$ and -1 .
- c) Perform the desired multiplication by multiplying components together.
- d) Invert the polynomial maps of step b) above.
- e) Invert the maps of a) above by means of the CRT.
- f) Finally, set $X = j$ to obtain the final answer.

Step a) above yields the polynomials -1 and $1 - X$ for the case of the modulus 3, and $2 - 3X$ and $1 + 2X$ for the modulus 7.

For step b), the forward map must first be defined for all polynomials of degree two or less. The polynomial $A + BX + CX^2$ will map to the triple $(A, A + B + C, A - B + C)$, which is then reduced by the appropriate modulus. The matrices of this transformation

and its inverse are given by

$$\Phi = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \end{bmatrix} \text{ and } \Phi^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ -1 & \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

where the fractions denote inverses in the respective rings $R(3)$ and $R(7)$.

First assume we are dealing with the ring $R(3)$. Then the input polynomials -1 and $1 - X$ map to the triples $(-1, -1, -1)$ and $(1, 0, -1)$. The multiplication of the inputs (step c)) is performed by multiplying these triples together componentwise, yielding $(-1, 0, 1)$. Applying the inverse map, for step d), we use the matrix $\Phi^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ -1 & -1 & -1 \end{bmatrix}$, and

obtain the polynomial $-1 + X$.

Within the ring $R(7)$ the input polynomials map to the triples $(2, -1, -2)$ and $(1, 3, -1)$. The multiplication (step c)) then yields the triple $(2, -3, 2)$. Applying the inverse map, which is now given by the matrix $\Phi^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & 3 \\ -1 & -3 & -3 \end{bmatrix}$, we obtain the polynomial $2 + X + X^2$.

Thus our final answer will come from the polynomial $A + BX + CX^2$ over the ring $R(21)$ for which $A + BX + CX^2 \equiv -1 + X \pmod{3}$, and $A + BX + CX^2 \equiv 2 + X + X^2 \pmod{7}$. By the Chinese Remainder Theorem (step e)) we easily get $2 + X - 6X^2$.

Finally (step f)) we evaluate this polynomial by setting $X = j$, and the result is $2 + j - 6j^2 = 8 + j$.

Comparison of the Methods.

In either the QRNS or FMRNS methods several moduli are chosen to effect an adequate dynamic range. With the QRNS there is a considerable restriction that all prime divisors of the moduli must be of the form $4k + 1$.

Let us consider an example. Suppose it has been decided to generate as large as possible computational dynamic range using moduli no greater than five-bits (this turns out to be an efficient size for certain high performance VLSI implementations [2]). For the QRNS method the only eligible divisors of M are 29, 25, 17, and 13, a total of four moduli for a dynamic range of 17.29 bits. For the FMRNS we can select all odd numbers from 31 down. The maximum dynamic range selection is 31, 29, 27, 25, 23, 19, 17, 13, 11 and 7 for a dynamic range of 42.04 bits. If we wish a 4-modulus system (the same number of moduli as the *best* QRNS system) we obtain a dynamic range of 19.21 bits. These extra 2 bits will provide a four-fold increase in the number of inner product terms that can be computed within the computational dynamic range. In terms of hardware implementation using look-up tables, our FMRNS moduli more efficiently use the binary dynamic range than do the QRNS moduli (here we define 100% efficiency as that achieved by using a ring modulus of 32). The desirable QRNS property of channel independent computations is retained in the FMRNS with no extra overhead in forward mapping; other techniques that use three channels do not preserve this property [3]. The overhead related to three channels for the FMRNS versus two for the QRNS, is compensated by the increased supply of available moduli within a defined bit size. In terms of scaling, there is no more difficulty with the FMRNS than with the QRNS for the same number of moduli; indeed, the FMRNS results will be preliminarily written as polynomials of degree two in X ; but immediately we can

identify X^2 with -1 , and scaling proceeds alike with both methods.

As a final note, there is nothing to prevent us from mixing the QRNS and FMRNS methods together. We can use QRNS for $4k + 1$ prime divisor moduli, and mix in other moduli that support the FMRNS. As an example, for four 6-bit moduli we can select a dynamic range of 23.52 bits using moduli 63, 61, 59, and 53. Two of the moduli (61, 53) support the QRNS and the other two (63, 59) support the FMRNS. Our computational overhead is now only 25% (10 channels versus 8) with more than a doubling of the dynamic range over that provided by the best four 6-bit QRNS moduli, 37, 41, 53 and 61 (22.23 bits).

References

1. Jenkins, W. K. and J. J. Krogmier. Error Detection and Correction in Quadratic Residue Number Systems. 26th Midwest Symposium on Circuits and Systems. 408-411, 1983.
2. Jullien, G. A., P. D. Bird, J. T. Carr, M. Taheri and W. C. Miller. "An Efficient Bit-Level Systolic Cell Design for Finite Ring Digital Signal Processing Applications." *J. VLSI Sig. Proc.* I, pp. 193-211, 1989.
3. Krishnan, R., G. A. Jullien and W. C. Miller. "The Modified Quadratic Residue Number System (QRNS) for Complex High Speed Signal Processing." *IEEE Transactions on Circuits & Systems*. Vol. CAS-33, pp. 325-327, 1986.
4. Wigley, N. M. and G. A. Jullien. "On Moduli Replication for Residue Arithmetic Computations of Complex Inner Products." *IEEE Trans. Comp.* 1990.

Acknowledgements:

The authors acknowledge support from the Natural Science and Engineering Research Council of Canada for funding this work.

Key Words :

Quadratic Residue Systems; Complex Arithmetic; Finite Rings; Digital Signal Processing; VLSI Implementations.

Author Affiliation

N.M. Wigley , G. A. Jullien
VLSI Research Group, University of Windsor
Windsor, Ontario, Canada N9B 3P4