Jan Długosz University in Częstochowa
Scientific Issues, Mathematics XVI, Częstochowa 2011

ARITHMETIC OF QUADRATIC MINIMAL REDUNDANT MODULAR NUMBER SYSTEMS

Mikhail Selyaninov

Institute of Technical Education and Safety
Jan Długosz University in Częstochowa
al. Armii Krajowej 13/15, 42-200 Częstochowa, Poland
e-mail: m.selianinov@ajd.czest.pl

Abstract. In this paper, research in the field of modular computing structures defined on sets of Gaussians are presented. The basis of the qualitatively new technique for the organization of high-speed parallel computations in a complex plane is presented by quadratic minimum redundant modular number systems (QMRMNS).

1. Introduction

For the organization of high speed parallel information processing, the quadratic modular number systems (QMNS) are the most adjusted and convenient among number systems with complex ranges. In such systems all the modules $m_1, m_2, \ldots, m_k$ can be represented as products of pairs of the complex-conjugate multipliers [1]. Using quadratic minimal redundant modular coding, the essentially higher optimality of computer procedures can be reached in comparison with the use of standard complex modular coding. This is caused by a property of arithmetical closing of the quadratic minimal redundant modular codes, i.e. by the possibility of performance of all arithmetical operations (including not modular) without transition to real components of complex ranges. Our study is aimed at implementation of this distinctive feature of QMNS.

2. Quadratic modular number system

Let us consider QMNS defined by means of the set of pairwise prime natural modules $m_1, m_2, \ldots, m_k$ such that all of them are representing as products of two conjugated integer complex numbers (ICN): $m_l = p_l\,\bar{p}_l$, where

$p_l = p_l^{'} + ip_l^{''}$, $\bar{p}_l = p_l^{'} - i\,p_l^{''}$; $p_l^{'}$, $p_l^{''} \in \mathbf{Z}$; $p_l^{'} > 0$, $p_l^{''} > 0$ and $(p_l^{'}, p_l^{''}) = 1$; $l = 1, 2, \ldots, k$.

According to the theorem 3 from [1] for modules of type $m = p\,\bar{p}$, the Cartesian product $\langle\cdot|_p \times \langle\cdot|_{\bar{p}}$ is isomorphic to the set

$$|\cdot|_{\|p\|} \times |\cdot|_{\|\bar{p}\|} = |\cdot|_m \times |\cdot|_m,$$

which in one's part is isomorphic to the complete set of residues $\langle\cdot|_m$. Therefore, in the QMNS with modules $m_1, m_2, \ldots, m_k$ every ICN $X = X^{'} + i\,X^{''}$ from a range $\langle\cdot|_{M_k} = |\cdot|_{M_k} \times |\cdot|_{M_k}$ can be uniquely presented by the complex modular code (MC)

$$((\mathrm{X}_1^{'};\ \mathrm{X}_1^{''}), (\mathrm{X}_2^{'};\ \mathrm{X}_2^{''}), \ldots, (\mathrm{X}_k^{'};\ \mathrm{X}_k^{''})), \tag{1}$$

where

$$(\mathrm{X}_l^{'};\ \mathrm{X}_l^{''}) = (R_{p_l}(X); R_{\bar{p}_l}(X)), \tag{2}$$

$$R_{p_l}(X) = R_{p_l}(X^{'}, X^{''}) = |X^{'} + J_l X^{''}|_{\|p_l\|},$$

$$R_{\bar{p}_l}(X) = R_{\bar{p}_l}(X^{'}, X^{''}) = |X^{'} - J_l X^{''}|_{\|\bar{p}_l\|},$$

$$J_l = \left|\frac{p_l^{''}}{p_l^{'}}\right|_{\|p_l\|}, \quad l = 1, 2, \ldots, k. \tag{3}$$

The main advantage which is reached with the use of complex-conjugate modules consists in simplicity of performance of multiplication operations modulo $p_l^{'}$ and $p_l^{''}$. The given operations require only two real multiplications modulo m_l in contrast to standard complex multiplication modulo m_l which demands four real multiplications and two real additions [1]. At the same time the addition operations with respect to the pair of complex modules $(p_l^{'}, p_l^{''})$ and real module m_l are identical with respect to complexity.

3. Quadratic minimal redundant modular number system

Efficiency of QMNS arithmetic essentially rises by use of minimal redundant modular coding which, as it is known, leads to simplification of not modular procedures [2]. According to [2, 3], in order that the MC (1) should be the minimal redundant it is enough that the real and imaginary parts of the coded ICN, $X = X^{'} + i\,X^{''}$, should be elements of the range $\mathbf{D} = \mathbf{Z}_{2M}^{-}$ $= \{-M, -M+1, \ldots, M-1\}$, where $M = \prod_{l=0}^{k-1} m_i$, m_0 is the auxiliary natural module satisfying the condition $m_k >= 2m_0 + \rho$.

Decoding mapping in quadratic minimal redundant modular number system (QMRMNS) is realized by the relations

$$X^{'} = \sum_{l=1}^{k-1} M_{l,k-1}|M_{l,k-1}^{-1}\,\chi_l^{'}|_{m_l} \; + \; I(X^{'})M_{k-1}, \tag{4}$$

$$X^{''} = \sum_{l=1}^{k-1} M_{l,k-1}|M_{l,k-1}^{-1}\,\chi_l^{''}|_{m_l} \; + \; I(X^{''})M_{k-1}, \tag{5}$$

where $\chi_l^{'} = |X^{'}|_{m_l}$, $\chi_l^{''} = |X^{''}|_{m_l}$, $l = 1, 2, \dots, k$; $I(X^{'})$ and $I(X^{''})$ are the interval indexes of the ICN $X^{'}$ and $X^{''}$, respectively [2–4].

Due to the simplicity of realization of the interval-modular forms (IMF) (4) and (5), application of QMRMNS for parallel information processing in the complex plane provides exclusively high efficiency not only on modular segments of computing processes but also on the segments containing not modular operations.

As follows from [1], in the considered QMRMNS the operations of modular addition, subtraction and multiplication for any ICN $A = A^{'} + i\,A^{''}$ and $B = B^{'} + i\,B^{''}$ $(A^{'}, A^{''}, B^{'}, B^{''} \in \mathbf{D})$ are realized by the same general rule:

$$\begin{aligned}((\mathrm{A}_1^{'};\ \mathrm{A}_1^{''}), (\mathrm{A}_2^{'};\ \mathrm{A}_2^{''}), \dots, (\mathrm{A}_k^{'};\ \mathrm{A}_k^{''})) \circ ((\mathrm{B}_1^{'};\ \mathrm{B}_1^{''}), (\mathrm{B}_2^{'};\ \mathrm{B}_2^{''}), \dots, (\mathrm{B}_k^{'};\ \mathrm{B}_k^{''})) = \\ = ((|\mathrm{A}_1^{'} \circ \mathrm{B}_1^{'}|_{m_1};\ |\mathrm{A}_1^{''} \circ \mathrm{B}_1^{''}|_{m_1}),\ (|\mathrm{A}_2^{'} \circ \mathrm{B}_2^{'}|_{m_2};\ |\mathrm{A}_2^{''} \circ \mathrm{B}_2^{''}|_{m_2}), \dots \\ \dots,\ (|\mathrm{A}_k^{'} \circ \mathrm{B}_k^{'}|_{m_k};\ |\mathrm{A}_k^{''} \circ \mathrm{B}_k^{''}|_{m_k})),\end{aligned} \tag{6}$$

where $\mathrm{A}_l^{'}$, $\mathrm{A}_l^{''}$ and $\mathrm{B}_l^{'}$, $\mathrm{B}_l^{''}$ are the digits of quadratic MC of the numbers A and B modulo m_l, accordingly (see (1)–(3)), $l = 1, 2, \dots, k$; $\circ \in \{+, -, \cdot\}$.

As for the problem of performing not-modular operations in the QMRMNS, the IMF (3) and (4) for the real and imaginary parts of elements $X = X^{'} + i\,X^{''}$ $(X^{'}, X^{''} \in \mathbf{D})$ are of importance for its solution.

Theorem. In the QMRMNS with pairwise prime odd modules $m_1, m_2, \dots, m_{k-1}, m_k$; $m_k >= 2m_0 + \rho$ $(m_0 >= \rho)$, the IMF of the real and imaginary components of arbitrary ICN $X = X^{'} + i\,X^{''} = ((\mathrm{X}_1^{'};\ \mathrm{X}_1^{''}), (\mathrm{X}_2^{'};\ \mathrm{X}_2^{''}), \dots, (\mathrm{X}_k^{'};\ \mathrm{X}_k^{''}))$ (see (1)–(3)) such that $(X^{'}; X^{''}) \in \mathbf{D} \times \mathbf{D}$ are defined as follows:

$$X^{'} = \sum_{l=1}^{k-1} M_{l,k-1} \left| \frac{\mathrm{X}_l^{'} + \mathrm{X}_l^{''}}{2M_{l,k-1}} \right|_{m_l} \; + \; I(X^{'})M_{k-1}, \tag{7}$$

$$X^{''} = \sum_{l=1}^{k-1} M_{l,k-1} \left| \frac{\mathrm{X}_l^{'} - \mathrm{X}_l^{''}}{2\,J_l\,M_{l,k-1}} \right|_{m_l} \; + \; I(X^{''})M_{k-1}, \tag{8}$$

where interval indexes $I(X^{'})$ and $I(X^{''})$ of ICN $X^{'}$ and $X^{''}$, respectively, are calculated in accordance with expressions (15)–(17) from [2], when

$$\chi_l = \chi_l^{'} = |X^{'}|_{m_l} = \left|\frac{\mathrm{X}_l^{'} + \mathrm{X}_l^{''}}{2}\right|_{m_l} \quad (l = 1, 2, \ldots, k), \tag{9}$$

$$\chi_l = \chi_l^{''} = |X^{''}|_{m_l} = \left|\frac{\mathrm{X}_l^{'} - \mathrm{X}_l^{''}}{2\, J_l}\right|_{m_l} \quad (J_l = \left|\frac{p_l^{''}}{p_l^{'}}\right|_{m_l}; \quad l = 1, 2, \ldots, k). \tag{10}$$

Proof. For the proof of formulated theorem it is sufficiently to evaluate the digits $\chi_l^{'}$ and $\chi_l^{''}$ by analogous digits $\mathrm{X}_l^{'}$ and $\mathrm{X}_l^{''}$ of the given number X for all $l = 1, 2, \cdots, k$. Then the received expressions should be substituted into formulas (4), (5) as well as into the calculated relations for the interval indexes $I(X^{'})$ and $I(X^{''})$.

As follows from (2) and (3), the pairs of residues $(\chi_l^{'};\, \chi_l^{''})$ and $(\mathrm{X}_l^{'}; \mathrm{X}_l^{''})$ are connected with each other by the set of equations

$$\begin{cases} |\chi_l^{'} + J_l\, \chi_l^{''}|_{m_l} = \mathrm{X}_l^{'}, \\ |\chi_l^{'} - J_l\, \chi_l^{''}|_{m_l} = \mathrm{X}_l^{''}. \end{cases} \tag{11}$$

Addition and subtraction of the equalities modulo m_l in (11) gives

$$\begin{cases} |2\, \chi_l^{'}|_{m_l} = |\mathrm{X}_l^{'} + \mathrm{X}_l^{''}|_{m_l}, \\ |2\, J_l\, \chi_l^{''}|_{m_l} = |\mathrm{X}_l^{'} - \mathrm{X}_l^{''}|_{m_l}. \end{cases} \tag{12}$$

As the real and imaginary parts of multiplicative components $p_l = p_l^{'} + i p_l^{''}$ and $\bar{p}_l = p_l^{'} - i\, p_l^{''}$ of modules $m_l = p_l\, \bar{p}_l$ satisfy the condition $(p_l^{'},\ p_l^{''}) = 1$, then on the basis of equality $(p_l^{'})^2 + (p_l^{''})^2 = m_l$, by the rule of contraries, it is easy to prove that $(m_l,\, p_l^{'}) = 1$ and $(m_l,\, p_l^{''}) = 1$. This provides an existence of the element $J_l = \left|\frac{p_l^{''}}{p_l^{'}}\right|_{m_l}$ and its multiplicative inverse $\left|\frac{1}{J_l}\right|_{m_l} = \left|\frac{p_l^{'}}{p_l^{''}}\right|_{m_l}$ in the ring $\mathbf{Z}_{m_l} = \{0, 1, \cdots, m_l - 1\}$. Furthermore, in view of the fact that all the modules $m_1, m_2, \ldots, m_k$ are odd, then in the ring $\mathbf{Z}_{m_l}$ there are also the residues $\left|\frac{1}{2}\right|_{m_l}$ and $\left|\frac{1}{2 J_l}\right|_{m_l}$ for all $l = 1, 2, \ldots, k$. Hence, from (12) it follows that

$$(\chi_l^{'}\,;\, \chi_l^{''}) = \left(\left|\frac{\mathrm{X}_l^{'} + \mathrm{X}_l^{''}}{2}\right|_{m_l};\ \left|\frac{\mathrm{X}_l^{'} - \mathrm{X}_l^{''}}{2\, J_l}\right|_{m_l}\right).$$

Therefore substitution of (9) and (10) into (4) and (5), accordingly, gives the desired IMF (7) and (8) for numbers $X^{'}$ and $X^{''}$, correspondingly.

Due to the theorem, the methods of performance of not modular operations in the real MRMNS [3] are propagated in the trivial way to QMRMNS.

Let us consider, for example, the procedure of transformation with scaling of positional code of the ICN $X = X^{'} + i\,X^{''}$ into quadratic minimal redundant MC (QMRMC). In contrast to a case of complex MRMNS [1, 3], in which the required transformation is reduced to corresponding transformations of the positional codes of the real and imaginary parts of the given number X, for forming the resulting quadratic MC both numbers $X^{'}$ and $X^{''}$ should be used jointly (see (1), (2)).

Let for the ICN $X = X^{'} + i\,X^{''}$ be necessary to generate the QMRMC of the approximate value $\hat{X} = \hat{X}^{'} + i\,\hat{X}^{''} = X/S = (X^{'} + i\,X^{''})/S$, where S is some natural scale, for example $S = 2h$, h is a natural number. According to the method of approximation described in [3, p. 240], the value $\hat{X}$ is defined by the equality

$$\hat{X} = \sum_{j=0}^{n-1} (F_j(X_j^{'},\, h) + i\,F_j(X_j^{''},\, h)),$$

where $F_j(X_j^{'},\, h) = \rfloor F_j(X_j^{'})\,2^{-h}\lfloor,\ F_j(X_j^{''},\, h) = \rfloor F_j(X_j^{''})\,2^{-h}\lfloor$; the symbol $\rfloor x \lfloor$ designates the rounding of a real number x; $X_j^{'}$ and $X_j^{''}$ are the additive components of positional codes of the integer real numbers $X^{'}$ and $X^{''}$, n is the number of such components.

Therefore, according to (1)–(3), for digits of QMRMC the following formulas are true:

$$R_{p_l}(\hat{X}) = |\hat{X}^{'} + J_l \hat{X}^{''}|_{m_l} = \left| \sum_{j=0}^{n-1} R_l^{'}(X_j^{'},\, X_j^{''},\, j) \right|_{m_l}, \tag{13}$$

$$R_{\bar{p}_l}(\hat{X}) = |\hat{X}^{'} - J_l \hat{X}^{''}|_{m_l} = \left| \sum_{j=0}^{n-1} R_l^{''}(X_j^{'},\, X_j^{''},\, j) \right|_{m_l}, \tag{14}$$

where

$$R_l^{'}(X_j^{'},\, X_j^{''},\, j) = \Big|(F_j(X_j^{'},\, h) + J_l\,F_j(X_j^{''},\, h))\Big|_{m_l}, \tag{15}$$

$$R_l^{''}(X_j^{'},\, X_j^{''},\, j) = \Big|(F_j(X_j^{'},\, h) - J_l\,F_j(X_j^{''},\, h))\Big|_{m_l}. \tag{16}$$

It is supposed that bit capacity of numbers $X_j{}'$, $X_j{}''$ and j allow the generation of residues (15) and (16) by means of table method. In this case expressions (13) and (14) can be implemented within $\lfloor \log l \rfloor + 1$ modular clock intervals, where $\lfloor x \rfloor$ designates the integer part of a real number x.

References

[1] M. Selyaninov. Modular number systems in the complex plane. *Scientific Issues, Jan Długosz University of Częstochowa, Mathematics,* **XV**, 131–138, 2010.

[2] M. Selyaninov. Modular technique of parallel information processing. *Scientific Issues, Jan Długosz University of Częstochowa, Mathematics,* **XIII**, 43–52, 2008.

[3] A.F. Chernyavsky, V.V. Danilevich, A.A. Kolyada, M.Y. Selyaninov. *High-speed Methods and Systems of Digital Information Processing.* Belgosuniversitet, Minsk 1996. (In Russian).

[4] M. Selyaninov. Construction of modular number systems with arbitrary finite ranges. *Scientific Issues, Jan Długosz University of Częstochowa, Mathematics,* **XIV**, 105–115, 2009.