Scientific Issues
Jan Długosz University
in Częstochowa
Mathematics XVII (2012)
69–76

MODULAR TECHNIQUE OF HIGH-SPEED PARALLEL COMPUTING ON THE SETS OF POLYNOMIALS

MIKHAIL SELYANINOV

Abstract

In this paper we present the modular computing structures (MCS) defined on the set of polynomials over finite rings of integers. This article is a continuation of research on the development of modular number systems (MNS) on arbitrary mathematical structures such as finite groups, rings and Galois fields [1-7].

1. Introduction

At the present time in the modern computer algebra, digital signal processing, coding theory, cryptography, many others fields of science and engineering the polynomial operations are of great importance. Therefore, studies on the development of modular technique of information processing in the direction of optimization the parallel computing structures defined on the polynomial ranges are of the utmost significance.

The developed technique of minimal redundant modular codification of ranges with vectorial structure is based on the introduction of minimal redundancy at a lower level (a level of real components) [1-3]. This universal and effective basis for synthesis of computer arithmetic procedures for the algebraic systems with polynomial carriers.

Mikhail Selyaninov — Jan Długosz University in Częstochowa.

The technique of interval-modular forms used for the real components of elements of coded ranges as well as the calculated relations for the interval-index characteristics of integer real numbers are the key elements of the proposed methodology [2, 3]. This allows us to create on the basis of the real minimal redundant modular systems the required variants of computer arithmetic for polynomial modular number systems under consideration.

2. Some theoretical foundations

Let us consider the set $\mathbf{Z}[x]$ of all polynomials of finite degree with coefficients in the ring $\mathbf{Z}$ of integers and the variable x. This set is a commutative ring with unity $e(x) = 1$ and zero $0(x)$.

Definition 1. *If the set of divisors of some element $f(x)$ of natural degree from the ring $\mathbf{Z}[x]$ is confined to polynomials of the form $Cd(x)$ such that $f(x) = Cd(x)$, where $C \in \mathbf{Z}$, then the polynomial $f(x)$ is called irreducible.*

Definition 2. *The common divisor $d(x)$ of polynomials $p_1(x), p_2(x), \ldots, p_n(x)$, $(n \geq 1)$, divisible by any other of their common divisor is called the least common divisor of polynomials and is denoted by*

$$d(x) = (p_1(x), p_2(x), \ldots, p_n(x)) .$$

In the case $d(x) = 1$, the polynomials $p_1(x), p_2(x), \ldots, p_n(x)$ are called pairwise coprime.

Definition 3. *The polynomial from $\mathbf{Z}[x]$ with unitary coefficient at the high-order degree of x is called the normalized polynomial.*

Following the offered technique of constructing a MNS [3] in this case first of all requires the creation of the complete set of residues (CSR) for the factor ring $\mathbf{Z}[x]/(p_l(x))$ $(l = 1, 2, \cdots, n;\ n \geq 2)$ with respect to selected pairwise relatively prime polynomial modules $p_1(x)$, $p_2(x)$, $\ldots$, $p_n(x)$ generating in $\mathbf{Z}[x]$ principal ideals $(p_1(x))$, $(p_2(x))$, $\ldots$, $(p_n(x))$. At the same time the governing equivalence relation is actually given by Euclidean lemma [1, 9] formulated as follows.

Lemma 1. *For any polynomial $f(x)$ in $\mathbf{Z}[x]$ and polynomial modules $p(x)$ when $\deg p(x) \geq 1$ there are unique elements $q(x)$ and $r(x)$ such that*

$$f(x) = q(x) \cdot p(x) + r(x) \quad (\deg r(x) < \deg p(x)). \tag{1}$$

3. Polynomial modular number system

As in computer applications the finite mathematical structures are used, then for the construction of polynomial MNS (PMNS) instead of the ring $\mathbf{Z}[x]$ the ranges of the form

$$\mathbf{Z}_m^s[x] = \left\{ A(x) = \sum_{j=0}^{s} a_j x^j \mid (a_0, a_1, \dots, a_{s-1}) \in (\mathbf{Z}_m \times \mathbf{Z}_m \times \dots \times \mathbf{Z}_m), \right\},$$

are used, where m and s are the fixed positive integers; $m \geq 2$. The cardinality of the set $\mathbf{Z}_m^s[x]$ is equal to $N = |\mathbf{Z}_m^s[x]| = m^s$.

Let $\mathbf{Z}_m$ be the set of all polynomials over the ring $\mathbf{Z}$, and $p(x)$ be any element of sth degree from $\mathbf{Z}_m$. Then according to Euclidean lemma (which is valid also for the ring $\mathbf{Z}_m$) the set $\mathbf{Z}_m^s[x]$ coincides with the set of all residual $r(x)$ of division of $f(x)$ by $p(x)$ (see (1)), while $f(x)$ represents every element from the set $\mathbf{Z}_m$. Thus, the ring $\mathbf{Z}_m^s[x]$ is a CSR modulo $p(x)$. For the CSR of this type a notation $\langle\cdot\rangle_{p(x)}$ is used. The operation modulo $p(x)$ over the polynomial $f(x)$, is designated as $\langle f(x)\rangle_{p(x)}$. It is also quite clear that any two rings $\langle\cdot\rangle_{p(x)}$ and $\langle\cdot\rangle_{g(x)}$ modulo $p(x)$ and $g(x)$ of the same degree $(p(x), g(x) \in \mathbf{Z}_m^s[x])$, $\deg p(x) = \deg g(x)$, respectively, are automorphic (i.e. are isomorphic and have the same carrier).

On this basis, in the general case the PMNS with pairwise relatively prime polynomial modules $(p_1(x), p_2(x), \dots, p_n(x))$ is defined as an algebraic system

$$S_{PMNS} =$$

$$= \left\langle \mathbf{Z}_m,\ \langle\cdot\rangle_{P(x)}, \langle\cdot\rangle_{p_1(x)}, \langle\cdot\rangle_{p_2(x)} \cdots\ \langle\cdot\rangle_{p_n(x)};\ (+, +, \dots, +),\ (\cdot, \cdot, \dots, \cdot) \right\rangle, \quad (2)$$

where $P(x) = \prod_{l=1}^{n} p_l(x)$.

The isomorphism $\phi : P(x) \to p_1(x) \times p_2(x) \times \dots \times p_n(x)$ defining the PMNS establishes a one-to-one correspondence between the polynomial $A(x)$ from the range $P(x)$ and the polynomial modular code

$$(a_1(x), a_2(x), \dots, a_n(x))$$

where the l-th component is the residual $a_l(x) = \langle A(x)\rangle_{p_l(x)}$ of division of $A(x)$ by a module $p_l(x)$ $(l = 1, 2, \dots, n)$. The ring operations in the PMNS over any two polynomials

$$A(x) = (a_1(x), a_2(x), \ldots, a_n(x)) \quad \text{and} \quad B(x) = (b_1(x), b_2(x), \ldots, b_n(x))$$

are naturally executed independently on each of residues, i.e. according to the rule

$$\langle A(x) \circ B(x) \rangle =$$

$$= \left(\langle a_1(x) \circ b_1(x) \rangle_{p_1(x)}, \langle a_2(x) \circ b_2(x) \rangle_{p_2(x)}, \ldots, \langle a_n(x) \circ b_n(x) \rangle_{p_n(x)} \right), \qquad (3)$$

where $\circ \in \{+, \ \cdot\}$.

As long as in the PMNS all operations (both modular and non-modular) are performed in the ring $\mathbf{Z}_m$, and this ring is included in the conditional notation (2). This ring is called the scalar range or the numeric range of the PMNS. It follows from formula (3) that the efficiency level of the PMNS arithmetic depends significantly on the degrees $\deg p_l(x)$ of modules $p_l(x)$, and its analytical form, on the one hand, and on the number system in which calculation over polynomial residuals in the ring $\mathbf{Z}_m$ are performed, on the other hand. Due to the modular structure of these calculations it is quite natural to use the real MNS with the modules $m_1, m_2, \ldots, m_k$ for encoding and processing of elements from the scalar range $\mathbf{Z}_m$ [2, 3]. With such an approach the parameter m is equal to $M_k = \prod_{i=1}^{k} m_i$, i.e. the ring

$$\mathbf{Z}_{M_k} = \{0, 1, \ldots, M_k - 1\}$$

is used as a numeric range of the PMNS.

Definition 4. *The PMNS with modular coding of elements of scalar range is called the polynomial-numerical or polynomial-scalar MNS with the modules* $(p_1(x), p_2(x), \ldots, p_n(x)), m_1, m_2, \ldots, m_k$ *and is denoted by the symbolic notation* $\langle \langle \cdot \rangle_{P(x)}; \ | \cdot |_{M_k} \rangle$.

As for the problem of a choice of polynomial modules

$$(p_1(x), p_2(x), \ldots, p_n(x))$$

it is clear that the normalized polynomials of the first degree $p_l(x) = x - r_l$, ($r_l \in \mathbf{Z}_{M_k}$ $l = 1, 2, \ldots, n$) are the most appropriate. At the same time for practical applications, for example, in the digital signal processing, digital communications or coding theory the polynomial modules for which

$$P(x) = \prod_{l=1}^{n} p_l(x)$$

is of the form $x^n \pm 1$ are of particular interest. It was shown in several studies that the indicated restrictions to the choice of modules PMNS are compatible. In the rings $\mathbf{Z}_{M_k}$ the polynomials $x^n \pm 1$ admit a factorization of the form $x^n \pm 1 = \prod\limits_{l=1}^{n}(x - r_l)$.

4. Minimal redundant polynomial modular number system

The principle of minimal redundant modular coding assumes that the set

$$\mathbf{Z}_{2M}^{-} = |\cdot|_{2M}^{-} = \{-M, -M+1, \ldots, M-1\}$$

($M = \prod\limits_{i=0}^{k-1} m_i$, m_0 is the auxiliary natural module) is used as a scalar range of the PMNS [2, 3].

Definition 5. *The PMNS with minimal redundant modular coding of the elements of a scalar range is called the minimal redundant polynomial-numerical or polynomial-scalar MNS with the modules*

$$(p_1(x), p_2(x), \ldots, p_n(x)), m_1, m_2, \ldots, m_k$$

and is denoted by the symbolic notation $\left\langle \langle\cdot\rangle_{P(x)};\ |\cdot|_{2M}^{-} \right\rangle$.

Let us consider the minimal redundant polynomial-scalar MNS (PSMNS) with modules m_1, m_2, …, m_k and $p_l(x) = x - r_l$ ($r_l \in \mathbf{Z}_{2M}^{-}$) such that $P(x) = x^n - 1$ or $P(x) = x^n + 1$. In accordance with the stated above, an arbitrary polynomial $A(x) \in \langle\cdot\rangle_{P(x)}$ in minimal redundant PSMNS is encoded by a set of residues

$$(A_{1,1},\ A_{1,2}, \ldots,\ A_{1,k};\ A_{2,1},\ A_{2,2}, \ldots,\ A_{2,k}; \ldots;\ A_{n,1},\ A_{n,2}, \ldots,\ A_{n,k}), \quad (4)$$

where $A_{l,i} = |A_l|_{m_i}$; $A_l = \langle A(x)\rangle_{p_l(x)}$ is a residue of division $A(x)$ by a module $p_l(x) = x - r_l$ which taking into account the Bezout theorem [8], is calculated by the formula $A_l = |A(r_l)|_{M_k}$; $l = 1, 2, \ldots, n$; $i = 1, 2, \ldots, k$.

Decoding mapping for minimal redundant PSMNS $\langle\langle\cdot\rangle_{P(x)};\ |\cdot|^{-}_{2M}\rangle$ assigning to each code of the form (4) a polynomial $A(x)=\sum\limits_{\nu=0}^{n-1} a_\nu x^\nu$ from the range $\langle\cdot\rangle_{P(x)}$ is implemented by means of the following theorem.

Theorem 1. *If $p_l(x) = x - r_l$ $(r_l \in \mathbf{Z}_{M_k})$, $P(x) = \prod\limits_{l=1}^{n} p_l(x) = x^n \pm 1$ and $(n, M_k) = 1$, then the coefficients of the polynomial $A(x) = \sum\limits_{\nu=0}^{n-1} a_\nu x^\nu \in \langle\cdot\rangle_{P(x)}$ corresponding to a minimal redundant position-scalar modular code* (4) *are defined by the following relations*

$$a_\nu = \sum_{i=1}^{k-1} M_{i,k-1}|M^{-1}_{i,k-1}|a_\nu|_{m_i}|_{m_i} + I(a_\nu)M_{k-1}, \tag{5}$$

$$|a_\nu|_{m_i} = \left| n^{-1}\sum_{l=1}^{n} A_{l,i}\, r_l^{-\nu} \right|_{m_i}, \tag{6}$$

where $I(a_\nu)$ is an interval index of the number a_ν calculated in accordance with the relations given in the article [2].

The validity of the use of interval-modular form (5) to restore the values of the polynomial coefficients a_ν on the basis of their modular code

$$(|a_\nu|_{m_1},\ |a_\nu|_{m_2},\ \ldots,\ |a_\nu|_{m_k})$$

is guaranteed by the minimum redundancy of the encoding elements of a scalar range $\mathbf{Z}^{-}_{2M}$. As for the formula (6), it follows from the Chinese reminder theorem [1, 9] which for the PMNS with modules $p_1(x),\ p_2(x),\ \ldots,\ p_n(x)$ gives

$$A(x) = \left\langle \sum_{l=1}^{n} P_l(x)\left\langle P_l(x)^{-1} A(x)\right\rangle_{p_l(x)} \right\rangle_{P(x)} =$$
$$= \sum_{l=1}^{n} P_l(x)\left\langle P_l(x)^{-1} A_l\right\rangle_{p_l(x)}, \tag{7}$$

where $P_l(x) = P(x)/p_l(x) = (x^n \pm 1)/(x - r_l)$.

The ring operations in the PSMNS are performed component-wise. In accordance with (3), the operation $\circ \in \{+,\ \cdot\}$ over any two polynomials $A(x)$ and $B(x)$ is executed by the rule

$$
\begin{aligned}
&(A_{1,1},\ A_{1,2},\ldots,\ A_{1,k};\ A_{2,1},\ A_{2,2},\ldots,\ A_{2,k};\ldots;\ A_{n,1},\ A_{n,2},\ldots,\ A_{n,k})\circ\\
&\circ(B1,1,\ B_{1,2},\ldots,\ B_{1,k};\ B_{2,1},\ B_{2,2},\ldots,\ B_{2,k};\ldots;\ B_{n,1},\ B_{n,2},\ldots,\ B_{n,k}) =\\
&= (\,|A_{1,1}\circ B_{1,1}|_{m_1},\ |A_{1,2}\circ B_{1,2}|_{m_2},\ \ldots,\ |A_{1,k}\circ B_{1,k}|_{m_k};\\
&|A_{2,1}\circ B_{2,1}|_{m_1},\ |A_{2,2}\circ B_{2,2}|_{m_2},\ \ldots,\ |A_{2,k}\circ B_{2,k}|_{m_k};\ \ldots\\
&|A_{n,1}\circ B_{n,1}|_{m_1},\ |A_{n,2}\circ B_{n,2}|_{m_2},\ \ldots,\ |A_{n,k}\circ B_{n,k}|_{m_k}\,), \qquad (8)
\end{aligned}
$$

where $A_{l,i} = |A(r_l)|_{m_i}$ and $B_{l,i} = |B(r_l)|_{m_i}$ are the digits of polynomial-scalar modular codes of the operands $A(x)$ and $B(x)$, respectively (see (4)).

The unique possibility to calculate the sum, difference and especially the product of two polynomials in accordance with (8) in one clock tick is one of the main advantages of the PSMNS. Thus, in this system both the addition and the multiplication of any two polynomials modulo $P(x) = x^n \pm 1$ for their implementation require n real additions and multiplications, respectively, which can also execute in parallel. In contrast, in the case of traditional arithmetic the computational complexity of the two polynomials multiplication in the ring $\langle\cdot\rangle_{P(x)}$ amounts to $n(n-1)$ real additions and n^2 real multiplications.

The minimal redundant PMNS have all advantages of the classical PMNS. In addition, these algebraic systems are characterized by more simple computer arithmetic. The use of minimal redundant coding on the lower level allows us to increase the efficiency of computer arithmetic due to optimization of the non-modular procedures [1]. Moreover, it should be noted that on the basis of technique for constructing the MNS [2, 3] the minimal redundant PSMNS with a range of complex scalars can be defined. In this case the efficiency gain is even more impressive than in the case of real PSMNS.

References

[1] 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).

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

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

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

[5] M. Selianinau, *High-speed modular structures for parallel computing in the space of orthogonal projections*, Scientific Issues, Jan Długosz University in Częstochowa, Ser. Technikal and IT Education, **V**, (2010), 87-96.

[6] M. Selyaninov, *Arithmetic of quadratic minimal redundant modular number systems* Scientific Issues, Jan Długosz University in Częstochowa, Mathematics, **XVI**, (2011), 129-134.

[7] M. Selianinau, *Modular principles of high-speed adaptive filtration of discrete signals*, Scientific Issues, Jan Długosz University in Częstochowa, Ser. Technical and IT education, **V**, (2011), 75-84.

[8] G. Korn, T. Korn, *Mathematical Handbook for Scientists and Engineers*, Nauka, Moscow 1974. (In Russian).

[9] I. M. Vinogradov, *Elements of Number Theory*, Nauka, Moscow 1981. (In Russian).

Mikhail Selyaninov
Jan Długosz University,
Institute of Technical Education and Safety,
42-200 Częstochowa, Al. Armii Krajowej 13/15, Poland
E-mail address: m.selianinov@ajd.czest.pl