Jan Długosz University of Częstochowa
Scientific Issues, Mathematics XIII, Częstochowa 2008

MODULAR TECHNIQUE OF PARALLEL INFORMATION PROCESSING

Mikhail Selyaninov

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

Abstract
In the present paper, modular number systems (MNS) named also as residue number systems are investigated. In such systems, digits of output computation of arithmetical operations over two and more numbers are formed only by analogous digits of these numbers that is in parallel. Because of internal parallelism and short bit capacity of modular data encoding, specified property of MNS enables real possibility of creation on their basis of high-speed specialized data processors.

1. Introduction

In modern computer applications of data processing (digital signal processing, coding theory, numerical methods, theoretical mechanics, physics and other sciences) high-speed computational procedures on data having complicated multidimensional structure are of fundamental importance. Therefore, the researches aimed at creation of untraditional, fundamentally new methods concerning effectiveness, algorithmic and hardware structures of a fast and reliability parallel data processing are currently central.

At the present time, one of the most promising directions of research is a direction which is oriented on application of the parallel-pipelined

architectures of modular type and also on the extension of their functionality and optimization [1–5]. Basic criteria of optimization of high-speed modular computing structures are minimal redundancy of data encoding, minimization of execution times of computational procedures, maximization of carrying capacity of arithmetical units.

2. Modular number systems

Arithmetical properties of either number system first of all are defined by character of interbit links during execution of operations on codewords. It is well known that arithmetical operations in real computers are executed on the numbers presented in positional number system (PNS). In the given number system, digits of output computation are calculated sequentially starting with low-oder positions.

During execution of dyadic arithmetical operations in PNS, there can occur bitwise overflows which should be taken into account in superior number position with respect to the considered one. In other words, PNS has strictly sequential structure. This makes greatly difficult the construction of high-speed specialized computers on the basis of PNS, especially at high bit capacity of processed data. It is reasonable that number systems with parallel structure are the most convenient for the organisation of parallel computations. Exactly MNS is a number system in which interbit links during arithmetical operations are absent [1–3].

In an MNS, an integer X is represented by a set of residuals $\chi_1 = |X|_{m_1},\ \chi_2 = |X|_{m_2}, \dots, \chi_k = |X|_{m_k}$ which are results of division of X by natural modules (radix numbers) $m_1,\ m_2, \dots, m_k$. It can be noted conditionally as $X = (\chi_1,\ \chi_2, \dots, \chi_k)$.

It follows from the given definition that a set of integers satisfying simultaneous congruences [6]

$$\begin{cases} X \equiv \chi_1 \pmod{m_1} \\ X \equiv \chi_2 \pmod{m_2} \\ \quad \dots \\ X \equiv \chi_k \pmod{m_k} \end{cases} \tag{1}$$

corresponds to a modular code (MC) of integer X.

In the case when modules $m_1,\ m_2, \dots, m_k$ are pairwise prime, the solution of this simultaneous congruences (1) is the residue class modulo

$M_k = \prod_{i=1}^{k} m_i$ defined by the relation

$$X = \sum_{i=1}^{k} M_{i,k}\mu_{i,k}\chi_i \pmod{M_k}, \tag{2}$$

where $M_{i,k} = M_k/m_i,\ \mu_{i,k} = |M_{i,k-1}^{-1}|_{m_i}\ \chi_i = |X|_{m_i}\ (i = 1,\ 2, \ldots, k)$.

Formula (2) given above is the essence of the so-called Chinese remainder theorem (CRT).

In an MNS with modules $m_1,\ m_2, \ldots, m_k$ for the sum, difference and product of integers A and B, accordingly, defined by their MC: $A = (\alpha_1,\ \ , \alpha_2, \ldots, \alpha_k)$ and $B = (\beta_1,\ \beta_2, \ldots, \beta_k)$ $(\alpha_i = |A|_{m_i}$, $\beta_i = |B|_{m_i},\ i = 1,\ 2, \ldots, k)$, the following relations are true [1, 2]:

$$|A + B|_{M_k} = (|\alpha_1 + \beta_1|_{m_1},\ |\alpha_2 + \beta_2|_{m_2}, \ldots, |\alpha_k + \beta_k|_{m_k}); \tag{3}$$

$$|A - B|_{M_k} = (|\alpha_1 - \beta_1|_{m_1},\ |\alpha_2 - \beta_2|_{m_2}, \ldots, |\alpha_k - \beta_k|_{m_k};) \tag{4}$$

$$|AB|_{M_k} = (|\alpha_1\beta_1|_{m_1},\ |\alpha_2\beta_2|_{m_2}, \ldots, |\alpha_k\beta_k|_{m_k}). \tag{5}$$

Moreover, if A is divided by B without remainder and, in addition, the least common divisor is such that $(\beta_i, m_i) = 1$ for all $i = 1,\ 2, \ldots, k$, then

$$|A/B|_{M_k} = (|\alpha_1/\beta_1|_{m_1},\ |\alpha_2/\beta_2|_{m_2}, \ldots, |\alpha_k/\beta_k|_{m_k}). \tag{6}$$

Thus, arithmetical operations in MNS are performed independently modulo $m_i, i = 1,\ 2, \ldots, k$, which indicates the parallelism of a given system. Lack of interbit links during realization of operations (3)-(6) is one of fundamental and most attractive characteristic property of modular arithmetic (MA). The operations which have property of independence of digits are called modular.

Each modular operation is realized in a definite time equal to time of its execution at the greatest module. In the case of small bit capacity of modules, all modular operations can be realized by means of look-up tables in equal time. If operations of addition, subtraction, multiplication and division by integer are carred out in accordance with rules (3)-(6) without possible overrunning of results of operation over range of MNS, then they are called formal.

There are a lot of important computer applications for which a principle of formal data processing in a MNS is applied successfully. It is

possible, for example, when modules $m_1,\ m_2, \ldots,\ m_k$ are selected so that a range of MNS always contains the results of realized computational process. At the same time, subproducts of computations are able to overstep the limits of data range. However, the overflow check during arithmetical operations is required in the most of computer applications. In an MNS, the given operations such as sign detection, round-off, scaling and others have different structure in contrast to modular operations and are more complicated and time-consumimg. This is caused because an MC does not contain the evident information about a number value as distinct from positional codes.

Operations of MA for which the resulting digits depend not only on the analogous but also on other digits of operands are called not modular. For their realization, it is nessesary to use various integral characteristics. Their choice and methods of their calculation are defined by complexity and singularities of realization of algorithms in MA.

3. Integral characteristics of a modular code

Synthesis of not modular procedures is based on using of various integral characteristics of MC (ICMC). Among them, coefficients of polyadic forms, rank, kernel, interval index are generally used. The given characteristics allow us to obtain the required information about number value from its MC [1, 2].

Often, as an ICMC, the digits of positional number representations are applied. In this case, a key element of all not modular procedures is the conversion of an MC to a corresponding PC. In the generalized PNS (GPNS), which is also called as a polyadic or mixed radix number system, the integer $X \in |\bullet|_{M_k} = \{0, 1, \ldots, M_k - 1\}$ is represented as

$$X = x_1 + x_2 M_1 + x_3 M_2 + \ldots + x_k M_{k-1}, \tag{7}$$

where $x_i \in |\bullet|_{m_i} = \{0, 1, \ldots, m_i - 1\}$; $M_i = \prod_{j=1}^{i} m_j$; m_i is the ith radix $(i = 1,\ 2,\ \ldots, k)$.

The conversional algorithm of an MC of an integer $X = (\chi_1,\ \chi_2, \ldots, \chi_k)$ to a code of a GPNS is one of approaches to constructing not modular procedures with high modularity. Using formula (7), it is easy to obtain the following calculated relations for the polyadic code digits $x_1,\ x_2, \ldots, x_k$ of the number X

$$x_i = |X^{(i)}|_{m_i}, \quad i = 1,\ 2, \ldots, k, \tag{8}$$

where

$$X^{(i)} = \begin{cases} X \ \text{ if } i = 1, \\ (1/m_{i-1})(X_{i-1} - x_i) \ \text{ if } \ i = 2,\ 3, \ldots, k, \end{cases} \tag{9}$$

modules $m_1,\ m_2, \ldots, m_k$ are pairwise prime.

Digits $x_1,\ x_2, \ldots, x_k$ of polyadic code obtained using relations (8) and (9) are represented in an ICMC which are widely used in algorithmic constructions of MA. As is obvious from formula (9), in the conversional algorithm only two modular operations are used: subtraction and multiplication by inverse multiplicative value of some module. However, even though high modularity, this algorithm, which is also called the chain algorithm, cannot be effectively used for construction of parallel computing procedures since it possesses strictly sequential character.

From the point of view of parallelism, the CRT provides greater capabilities for obtaining of number value from its MC. In order to convert a number from an MNS to a PNS, it is possible to apply the CRT formulated in the form of the relation (2). However, high-speed realizations of the relation (2) by means of positional summators modulo M_k demand rather considerable hardware environment and in the case of great values of M_k become practically unacceptable. In addition, the positional structure of such realizations essentially limits a code conversion speed.

Much greater efficiency is ensured with parallel procedures for the computation of ICMC which have high modularity, i.e. mainly include modular operations. According to formula (2) for arbitrary $X \in |X|_{M_k}$, there exists a unique integer $\rho_k(X)$ which is called a rank of number X in a MNS with modules $m_1,\ m_2, \ldots, m_k$ such that [1]

$$X = \sum_{i=1}^{k} M_{i,k}\chi_{i,k} \ - \ \rho_k(X)M_k, \tag{10}$$

where $\chi_{i,k} = |M_{i,k-1}^{-1}\chi_i|_{m_i}$.

Expression (10) is called the rank form of integer X. With its help, all not modular operations can be realised. In this connection, calculation of rank $\rho_k(X)$ is the basic auxiliary operation. As computational algorithm according to formula (10) is easily exposed to parallelizing, then the considered approach to construction of not modular procedures allows us to reach high processing speed.

Others ICMC, which ensure high level of parallelism of not modular procedures and have greater modularity in comparison with rank $\rho_k(X)$, are the so-called kernel characteristics: kernel $h(X) = \sum_{i=1}^{k} \tau_i \lfloor X/m_i \rfloor$ and normalized kernel $\eta(X) = \sum_{i=1}^{k} \lfloor \tau_i X/m_i \rfloor$ of number X, where $\tau_1,\ \tau_2, \ldots, \tau_k$ are specially selected integer weights, the value $\lfloor x \rfloor$ is designated to the integer part of a real number x [1].

At a choice of the base ICMC for construction and implementation of not modular operations along with modularity, it is also necessary to consider the value of used characteristics. From the point of view of a modularity principle, the kernel characteristics $h(X)$ and $\eta(X)$ are equivalent but sets of their values differ essentially from each other. In comparison with a kernel $h(X)$, the range of a normalized kernels $\eta(X)$ is narrower. Therefore, its application as the base ICMC is more preferable.

If values $\tau_1,\ \tau_2, \ldots, \tau_k$ are selected so that $\eta(M_k) = m_k$, then expression for $\eta(X)$ looks like [1]:

$$\eta(X) = M_{i,k-1}^{-1} \left(X - \sum_{i=1}^{k} M_{i,k-1} \chi_{i,k-1} \right), \tag{11}$$

where $M_{k-1} = \prod_{i=1}^{k-1} m_i,\ \chi_{i,k-1} = |M_{i,k-1}^{-1} \chi_i|_{m_i}\ M_{i,k-1} = M_{k-1}/m_i$.

Let us note that existence and uniqueness of integer-valued number $\eta(X)$ for any $X \in |\bullet|_{M_k}$ follow directly from CRT. The characteristic of the form (11) which represents the best variant of kernel ICMC is called an interval index (II) and for it the special notation $I(X)$ was introduced in [1, 2].

As will be shown further, thanks to application of insignificant redundancy, the computation of II $I(X)$ represents extremely simple operation of summation of residues modulo m_k. Therefore, due to high modularity and parallelism of computational procedure an II $I(X)$ has a priority among ICMC.

4. Minimal redundant modular number systems

For the purpose of improving properties of MNS and raising efficiency of MA, redundancy of encoding of the numerical information is introduced. Redundant modular encoding allows us to simplify not modular operations essentially, first of all, full multiplication, scaling (multiplication or division by constants) and code conversion [1, 2].

The known techniques realising the specified approach to optimization of modular computatational structures require application of the greater redundancy. More often, the size of a code word increases approximately twice so that the result of product of any two numbers is uniquely represented in an MNS. At the same time, arithmetical properties of MNS can be improved essentially using minimal redundancy.

For optimization of modular computational structures, another variant of redundant coding is most reasonable, when a certain subset $D \in |X|_{M_k}$ is used as a range of MNS. As a subset D, we will use $|\bullet|_M = \{-M, -M+1, \ \dots, M-1\}$, where $M = \prod_{i=0}^{k-1} m_i$, m_0 is the auxiliary natural module. The resultant redundant MNS is naturally a restriction of basic MNS and possesses all its properties [1–4].

The main aim of using the less cardinality of a set D consists in construction of an MNS which with a minimum of code redundancy provides more simple base relation for decoding transformation. Let an integer $X \in D$, $X = (\chi_1, \ \chi_2, \dots, \chi_k)$. Then according to the CRT by analogy to formula (2), we have

$$|X|_{M_{k-1}} = \left| \sum_{i=1}^{k} M_{i,k-1} |M_{i,k-1}^{-1} \chi_i|_{m_i} \right|_{M_{k-1}}. \tag{12}$$

This means that there is some value $I(X)$ such that the interval-modular form of a number X is specified by a relation

$$X = \sum_{i=1}^{k-1} M_{i,k-1} \chi_{i,k-1} \ + \ I(X) M_{k-1}. \tag{13}$$

As it is obvious from (2), expression (13) does not contain modulo M_k operations. Therefore, decoding procedures synthesised on the base of II $I(X)$ are more effective than procedures realising direct implementations of the CRT [1–3].

The basic content of the principle of minimum redundant modular coding consists in the following theorem.

Theorem.

In order that in a MNS with pairwise prime modules $m_1,\ m_2, \dots, m_k$ $(k > 1)$ an II $I(X)$ of number $X \in D = |\bullet|_M$ is completely defined by a residue $\hat{I}_k(X) = |I(X)|_{m_k}$, the kth module m_k must satisfy the necessary and sufficiently condition $m_k > 2m_0 + \rho$, where $\rho = \max\{\rho_{k-1}(X)\}$, $\rho_{k-1}(X)$ is a rank defined by equality

$$|X|_{M_{k-1}} = \sum_{i=1}^{k-1} M_{i,k-1}\chi_{i,k-1} \ - \ \rho_{k-1}(X)M_{k-1}; \tag{14}$$

in addition, for II $I(X)$ the following calculating expressions are valid:

$$I(X) = \begin{cases} \hat{I}_k(X) \ \text{ if } \ \hat{I}_k(X) < m_0; \\ \hat{I}_k(X) - m_k \ \text{ if } \ \hat{I}_k(X) > m_k - m_0 - \rho; \end{cases} \tag{15}$$

$$\hat{I}_k(X) = \left| \sum_{i=1}^{k} R_{i,k}(\chi_i) \right|_{m_k}; \tag{16}$$

$$R_{i,k}(\chi_i) = \left| \frac{\chi_{i,k-1}}{M_{k-1}} \right|_{m_k}; \quad R_{k,k}(\chi_k) = \left| \frac{\chi_k}{M_{k-1}} \right|_{m_k}. \tag{17}$$

Proof.

From interval-modular form of a number X (13) it follows that

$$I(X) = \sum_{i=1}^{k-1} \frac{\chi_{i,k-1}}{m_i} + \frac{X}{M_{k-1}}. \tag{18}$$

Therefore, in order to obtain relation (16), it is sufficient to apply a residue modulo m_k operation in formula (18) taking into account designation (17).

Let $I_{\min} = \min\limits_{X \in D}\{I(X)\}$ and $I_{\max} = \max\limits_{X \in D}\{I(X)\}$. Then the necessary and sufficient condition of reciprocal single-valued correspondence between values of II $I(X)$ and residue $\hat{I}_k(X)$ is realization of inequality

$$m_k > I_{\max} - I_{\min} + 1. \tag{19}$$

In addition, for $I(X)$ the following formula is true

$$I(X) = \begin{cases} \hat{I}_k(X) \ \text{ if } \ \hat{I}_k(X) < I_{\max}; \\ \hat{I}_k(X) - m_k \ \text{ if } \ \hat{I}_k(X) > m_k + I_{\min}. \end{cases} \tag{20}$$

Subtracting and adding $\rho_{k-1}(X)M_{k-1}$ in the right part of expression (13) and applying then formula (14), we obtain

$$X = \sum_{i=1}^{k-1} M_{i,k-1}\chi_{i,k-1} - \rho_{k-1}(X)M_{k-1} + \rho_{k-1}(X)M_{k-1} + I(X)M_{k-1} =$$

$$= |X|_{M_{k-1}} \ + \rho_{k-1}(X)M_{k-1} + I(X)M_{k-1}.$$

It follows that according to a Euclidean lemma from the theory of divisibility [6], we have

$$\rho_{k-1}(X) + I(X) = \left\lfloor \frac{X}{M_{k-1}} \right\rfloor. \tag{21}$$

Taking into account that $\lfloor X/M_{k-1} \rfloor$ for any $X \in [-M;\ -M + M_{k-1})$ has a minimum and in an interval $[-M;\ -M + M_{k-1})$ there is a number $-M+X_0$ for which $\rho(-M+X_0) = \rho_{k-1}(|-M+X_0|_{M_{k-1}}) = \rho_{k-1}(X_0) = \rho$, it follows from formula (21) that

$$I_{\min} = \min_{X \in D} \left\{ \left\lfloor \frac{X}{M_{k-1}} \right\rfloor - \rho_{k-1}(X) \right\} =$$

$$= \left\lfloor \frac{-M + X_0}{M_{k-1}} \right\rfloor - \rho_{k-1}(-M + X_0) = -m_0 - \rho.$$

Analogously, as $\lfloor X/M_{k-1} \rfloor$ for any $X \in [M - M_{k-1};\ M - 1)$ reaches a maximum and $\rho(M - M_{k-1}) = \rho_{k-1}(|-M + M_{k-1}|_{M_{k-1}}) = \rho_{k-1}(0) = 0$, on the basis of formula (21) it follows that

$$I_{\max} = \max_{X \in D} \left\{ \left\lfloor \frac{X}{M_{k-1}} \right\rfloor - \rho_{k-1}(X) \right\} =$$

$$= \left\lfloor \frac{M - M_{k-1}}{M_{k-1}} \right\rfloor - \rho_{k-1}(M - M_{k-1}) = m_0 - 1.$$

Now for concluding the proof of the theorem, it is sufficient to substitute the obtained lower $I_{\min}$ and upper $I_{\max}$ boundaries of variation of $I(X)$ into relations (19) and (20).

It is obvious that an MNS with modules $m_1, m_2..., m_k$ and effective range $D = |\bullet|_M$ which are selected according to the theorem has the minimum redundancy if the equation $m_k - 2m_0 - \rho = |m_k - \rho|_2$ is carried out. Just in this case an MNS is called the minimal redundant MNS.

Though the fact that introduced redundancy is small enough, thanks to this computation of II $I(X)$ in minimum redundant MNS becomes trivial operation. Eventually, it also ensures simplicity of not modular procedures synthesized on the basis of interval-modular form (13), first of all code conversion and scaling [1–3].

References

[1] A.A. Kolyada, I.T. Pak. *Modular Structures of Pipeline Processing of the Digital Information.* Universitetskoe, Minsk 1992. (In Russian).

[2] 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).

[3] A.A. Kolyada, V.V. Revinsky, M.Y. Selyaninov *et al.* Elements of the theory and applications of modular technique of parallel information processing. *Modern Problems of Optics, Radiation Materials Science, Informatics, Radiophysics and Electronics. Proc. Sci. Research Inst. Appl. Phys. Probl.*, Belgosuniversitet, Minsk, vol. 2, pp. 1–51, 1996. (In Russian).

[4] M.Y. Selyaninov. Theoretical bases of modular codification of algebraic systems. *Proc. Nat. Acad. Sci. Belarus,* No. 1, 114–119, 2002. (In Russian).

[5] M.Y. Selyaninov. Application of numerically-analytical modular computing techniques for performance of additive and multiplicative operations over signals in spaces of orthogonal projections. *Rep. Nat. Acad. Sci. Belarus,* **46**, No. 2, 62–66, 2002. (In Russian).

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