INDIRECT MEASUREMENTS IN FINITE FIELDS

P. A. Arutyunov
UDC 621.382

It is demonstrated that application of the arithmetic of residual classes possesses a number of interesting and useful properties for construction of measurement algorithms and indirect measurement procedures. This warrants attention since certain measurement problems of digital processing can be solved on a qualitatively new level, especially in connection with the general tendency of development of powerful parallel systems.

Digital methods and algorithms of processing measuring information are widely used at present for design of information measuring systems and radio electronic equipment. These methods have substantially changed the principles of designing the instrumentation and its elementary base and, of course, the measuring procedures themselves. "Calculation of a property" became a new concept in measuring procedures. Measuring procedures have been converted into measuring-computational ones. This transition to the new model of computation required a change in mathematical methods to organize the computational process in the so-called finite fields (Galois fields). As early as in the 1950s, the idea has arisen to utilize for representation of integers the so-called residual classes (unimodular and multimodular arithmetics). Nowadays – due to successes in microelectronics – we witness the second birth of digital methods of processing measurement information in residual class systems (RCS) in connection with the development of powerful parallel systems. It has been shown in a number of papers that application of the RCS arithmetic possesses a number of interesting and useful properties for construction of algorithms of error-free calculations [1–13].

In [3–5], problems of representing the basic measurement equation in the form of a digital equivalent (for direct observations) in unimodular arithmetic and representation of the same equation in multimodular arithmetic by representing an integer in a number system with a mixed base were considered. These two problems are now being extended to indirect measurements where the required value of a quantity is determined based on the results of direct measurements of other physical quantities connected with the required one by means of a known functional relationship. Indirect measurements are multichannel and measurement-computational ones. As a rule, their results are represented by a rational fraction which expresses either certain lawlike relationship or a physical coefficient.

One of the main advantages of algorithms in RCS is the feature that in measurement-computational algorithms modified definitions of addition and multiplication are used which satisfy the conditions of closure and exact equality. This prevents the overflow effect and renders the measurement-computational process to become error-free, i.e., absolutely exact.

Digital Equivalents of Measurement Equations in Unimodular Arithmetic for Rational Numbers. Indirect measurements are usually represented by a rational fraction which expresses either certain lawlike relationship or a physical coefficient. The basic idea in the case of error-free processing of an indirect measurement in the mathematical language is a mapping of rational operands into the set of integers \( \mathbb{Q} \), execution of arithmetic operations in the ring \( (\mathbb{Q}, +, \cdot) \) and then mapping the integer-valued results into corresponding rational numbers. In this case, it is convenient to select a measure in the form \( [G] = p^r \) where \( p \) is a prime and \( r \) is a positive integer. The rational numbers \( G_1/G_2 \) for which \( (G_2, p) = 1 \) are mapped into \( \mathbb{Q} \). It is assumed here that the inverse element \( G_2^{-1}[G] \) exists if and only if \( (G_2, p) = 1 \). This is a case of the so-called \( p \)-adic numbers. If \( r = 1 \), then \( [G] \) coincides with the prime \( p \).

Example 1. When measuring velocity \( v = l/t \), the result of a measurement is obtained in the form of fractions \( l_1/t_1, l_2/t_2, \ldots \), i.e., a rational fraction is obtained. Or, for example, measuring the velocity of a target in a pulse RLS \( c\Delta f_1/2f_1, c\Delta f_2/2f_2, \ldots \). In these two examples, the numerator and denominator can be represented by two measurement equations in two mathematically equivalent forms:

---

Translated from Izmeritel'naya Tekhnika, No. 4, pp. 11–16, April, 1999.

\[ G_1 = [G_1][G] + G_{R1}, \]
\[ G_2 = [G_2][G] + G_{R2}. \]  

or

\[ G_1 \equiv G_{R1}(\text{mod } [G]), \]
\[ G_2 \equiv G_{R2}(\text{mod } [G]). \]  

where 0 \leq G_{R1} \leq [G] and 0 \leq G_{R2} \leq [G].

Equations (1) read: "the quantity \( G \) is comparable with the residual \( G_R \) modulo \([G]\)." In the ideal case, \( G = 0 \) (mod \([G]\)). It should be noted that a ratio of integers in unimodular arithmetic of residuals – provided it exists – is always an integer, even in those cases when \( G \) is not divisible by \([G]\). It is easy to see that the mapping mod \([G]\) in the form (1) defines a subdivision on \([G]\) of nonintersecting equivalence classes (residual classes). Equations (1) and (2) can be processed without an error by means of algorithms for processing integers [1, 3, 5]. As a result, we obtain a numerical fraction \( G_1/G_2 \). To transform a rational fraction into an integer, it is necessary to fulfill the homomorphism condition relative to addition and multiplication operations.

It is proven in the number theory [4, 11, 14] that firstly, there is a connection between the rings \( \tilde{\mathbb{R}}a, +, - \) and \( \mathbb{R}a, +, - \) where \( \mathbb{R}a \) is the set of rational numbers \( \mathbb{R}a \in \mathbb{R}e; \tilde{\mathbb{R}}a \) is the set of rational numbers which admit a mapping into \( \mathbb{R}a \). Indeed, by definition

\[ \tilde{\mathbb{R}}a = \{G_1/G_2 : (G_2, p) = 1\} \]

and every integer \( k \in \mathbb{R}a \) is an image of an infinite set of elements in \( \mathbb{R}a \) to be denoted \( \mathbb{R}a_k \), where \( k = 0, 1, ..., p - 1 \), i.e.,

\[ \mathbb{R}a_k = \{G_1/G_2 \in \tilde{\mathbb{R}}a : |G_1/G_2| \equiv k\}, \]

whence

\[ \tilde{\mathbb{R}}a = \bigcup_{k=0}^{p-1} \mathbb{R}a_k. \]

Here \( \mathbb{R}a_k \) are the nonintersecting subsets or generalized residual classes mod \([G]\) since they include the usual residual classes as proper subsets \( \mathbb{R}a_k \subset \mathbb{R}a_k \), \( k = 0, 1, ..., p - 1 \).

Secondly, the mapping

\[ \tilde{\mathbb{R}}a \rightarrow \mathbb{R}a \]  

defines a homomorphism relative to the operations of addition and multiplication and it is not one-to-one since every integer \( k \in \mathbb{R}a \) is an image of an infinite subset of \( \mathbb{R}a_k \) of rational numbers. Consequently, the mapping (3) does not possess an inverse.

Thirdly, we shall utilize the order-\( N \) Farey fractions

\[ F_N = \{G_1/G_2 \in \tilde{\mathbb{R}}a : (G_1, G_2) = 1\} \]

and the conditions

\[ 0 \leq |G_1| \leq N, 0 \leq |G_2| \leq N, \]

where \( N \) is an integer. Let \( N \) be the maximal integer for which the inequality