Interval Arithmetics over a Field $GF(p)$

L. V. Kupriyanova, D. V. Speransky, and V. G. Samoilov
Saratov State University, Russia
contact email KupriyanovaLV@info.sgu.ru

1 Introduction

Known methods of interval mathematics use, basically, arithmetic of intervals over a field of the real or complex numbers. In this work interval arithmetic over the finite fields $GF(p)$, where p is a prime number, is introduced, some properties of this arithmetic are proved and equations with interval coefficients are considered. Such arithmetic is necessary to develop methods of discrete systems theory. For example, it is possible to deduce the theory of linear sequential machines (LSM), which are defined over the finite fields $GF(p)$. LSM is a mathematical model of widely known actual discrete systems that carry out coding and decoding of information, signature analysis of output reactions of the device for its technical diagnosis, etc. From the physical point of view it is possible to measure levels of values of voltage for input and output values of signals, and also levels of state values of memory elements of electronic devices described by mathematical models LSM, in "quantum" units. As in specifications, the values of voltage have upper bounds, limiting value of this voltage (expressed in "quantum" units) just gives the characteristic p of a field $GF(p)$. From here there is a necessity to operate with quantum values of voltage in arithmetic modulo p. The levels of voltage are measured by devices with some error, and consequently instead of exact values of levels of signals there can be intervals, within the limits of which there are their valid values. To date, there has been no work on interval arithmetic over finite fields, and the present work can partly fill in this blank.

2 Notations and Basic Definitions

We denote the elements of $GF(p) = \{0, 1, \ldots, p-1\}$, where p is a prime number, by small Greek letters $\alpha, \beta, \ldots$, and also by Latin letters with feature from below or from above $\underline{a}, \overline{a}, \underline{b}, \overline{b}, \ldots$

Subset a of $GF(p)$ such, that $a = [\underline{a}, \overline{a}] = \{\alpha \mid \underline{a} \leq \alpha \leq \overline{a},\ \underline{a}, \overline{a} \in GF(p)\}$, we shall call as an *interior* closed interval, where $\underline{a}$ and $\overline{a}$ are its bottom and top bounds, respectively.

We shall interpret record of a form $b = [\underline{b}, \overline{b}]$, where $\underline{b} > \overline{b}$, as a set $GF(p) \setminus [\underline{b} + 1, \overline{b} - 1]$ and also to call this set as an *exterior* interval.

Interval of a form $[\underline{a}, \overline{a}]$, where $\underline{a} = \overline{a}$, we shall call a singular interval and to interpret it as an element of a field $GF(p)$.

Set of all intervals over $GF(p)$ we shall denote by $IGF(p)$, and the Latin letters we shall reserve behind notations of intervals.

Any exterior interval can be submitted as $[\underline{b}, \overline{b}] = [0, \overline{b}] \cup [\underline{b}, p - 1]$.

Let's introduce operations over elements of $IGF(p)$.

Let $* \in \{+, -, \cdot, \div\}$ be a binary arithmetic operation. If $a, b \in IGF(p)$, then

$$a * b := \{\xi = \alpha * \beta \mid \alpha \in a, \beta \in b\}$$

defines binary arithmetic operation over elements of $IGF(p)$. In case of division it is prospective, that $0 \notin b$.

As against real interval arithmetics, result of operation over an interval of $IGF(p)$ can appear set of points not being one interval, and representing association of several intervals scattered on a numerical axis. For example, for $p = 7$, $[1, 2] \cdot [2, 3] = [2, 4] \cup [6, 6]$. We shall name subset $A \in GF(p)$ such, that

$$A = \bigcup_{i \in I} a_i,$$

where $a_i \in IGF(p)$, I is a finite set of indexes and for $i \neq j$ $a_i \cap a_j = \emptyset$, as the *generalized* interval of a field $GF(p)$. The generalized interval we shall designate by a capital letter. The usual interval $IGF(p)$ is a special case of the generalized interval. Behind set of all generalized intervals we shall keep a designation $IGF(p)$. Now let's introduce arithmetic operations over the generalized intervals.

Let $A = \bigcup\limits_{i \in I} a_i$, $B = \bigcup\limits_{j \in J} b_j$, where a_i, b_j is usual interval of a field $GF(p)$, then

$$A * B = (\bigcup_{i \in I} a_i) * (\bigcup_{j \in J} b_j) = \bigcup_{i \in I, j \in J} a_i * b_j.$$

Let's introduce unary operation over a usual interval $-x = [-\overline{x}, -\underline{x}]$, where $'-\xi'$ is an element of $GF(p)$, opposite to ξ on addition, then the appropriate operation over the generalized interval is

$$-X = (\bigcup_{i \in I} (-x_i).$$

Let's denote also $1/X = (\bigcup\limits_{\xi \in X} (1/\xi)$, where $'1/\xi'$ is an element of $GF(p)$, inverse to ξ on multiplication. Let's introduce operation of multiplication of an interval X on α, an element of a field $GF(p)$:

$$\alpha * X = (\bigcup_{\xi \in X} [\alpha \cdot \xi, \alpha \cdot \xi],$$

As width of a usual interval $x = [\underline{x}, \overline{x}]$ we shall call a value

$$w(x) = \begin{cases} \overline{x} - \underline{x} + 1, & \text{if } x \text{ is interior,} \\ \overline{x} - \underline{x} + p + 1, & \text{if } x \text{ is exterior.} \end{cases}$$

Width of the generalized interval is $w(x) = \sum\limits_{i \in I} w(x_i)$.

3 Properties of Arithmetic Operations in $IGF(p)$

Let a, b be a usual intervals of a field $GF(p)$, A, B is generalized intervals, $\lambda, \mu \in GF(p)$, then the following formul as allowing to calculate or to estimate results of arithmetic operations over intervals with the help of operations with bounds of intervals are valid:

$$a + b = ft \begin{cases} [\underline{a} + \underline{b}, \overline{a} + \overline{b}], & \text{if } w(a) + w(b) \le p, \\ [0, p-1], & \text{otherwise.} \end{cases}$$

$$a - b = \begin{cases} [\underline{a} - \overline{b}, \overline{a} - \underline{b}], & \text{if } w(a) + w(b) \le p, \\ [0, p-1], & \text{otherwise.} \end{cases}$$

$$\lambda \cdot a \subseteq [\lambda \underline{a}, \lambda \overline{a}], \text{ if } \lambda(w(a) - 1) < p - 1,$$

$$a \cdot b \subseteq [\underline{a}\underline{b}, \overline{a}\overline{b}], \text{ if } \sigma(a)(w(b) - 1) + \sigma(b)(w(a) - 1) < 2(p - 1),$$

where $\sigma(a) = \underline{a} + \overline{a}$, $\sigma(b) = \underline{b} + \overline{b}$.

Besides known properties, having a place for real interval arithmetics (commutativity and associativity for adition and multiplication, absence opposite on addition and multiplication for the majority of elements, subdistributivity, etc.), the following properties are valid:

1. $\lambda(A + B) = \lambda A + \lambda B$ (distributivity of multiplication to number);
2. $(\lambda + \mu)A \subseteq \lambda A + \mu A$;
3. $w(A * B) \le w(A) \cdot w(B)$, where $* \in +, -, \cdot, /$;
4. $w(a + b) = w(a - b) = w(a) + w(b) - 1$, if a, b is usual intervals and $w(a) + w(b) < p$;
5. $w(\lambda A) = w(A)$, if $\lambda \neq 0$.

4 Solution Sets of the Equations in $IGF(p)$

As the algebraic solution of the equation relative to X

$$f(A, X) = B, \tag{1}$$

dependent from some parameters $(A_1, \dots, A_s)^T = A$, where $A_i, B \in IGF(p)$, $i = 1, \dots, s$, we shall call s uch generalized interval $X \in IGF(p)$, that at its substitution in the equation the correct equality turns out.

For the equation (1) we shall define also following solution sets.
$X_{\exists\exists} := \{\xi | (\exists\alpha \in a)(\exists\beta \in b) f(\alpha, \xi) = \beta\}$ is a united solution set;
$X_{\forall\exists} := \{\xi | (\forall\alpha \in a)(\exists\beta \in b) f(\alpha, \xi) = \beta\}$ is a tolerable solution set;
$X_{\exists\forall} := \{\xi | (\forall\beta \in b)(\exists\alpha \in a) f(\alpha, \xi) = \beta\}$ is a controlled solution set.

All solution sets and an algebraic solution, if they exist, are included in the united solution set. Also it is obvious the algebraic solution, that all its elements are the tolerable solutions, and therefore, the algebraic solution is included in tolerable solution set.

The linear equation $a + X = b$, where $a,\ b$ are usual intervals over a field $GF(p)$, has the algebraic solution X if and only if $w(a) \leq w(b)$.