# ИНТЕРВАЛЬНАЯ АРИФМЕТИКА НАД ПОЛЕМ $GF(p)$ *

Л. В. Куприянова, Д. В. Сперанский, В. Г. Самойлов
*Саратовский государственный университет, Россия*

The arithmetic operations on the intervals, which consist of elements of field $GF(p)$, where $p$ is a prime number, are introduced. Important properties of entered arithmetic are proved, some equations are considered.

## Введение

Интервальная арифметика является эффективным средством при вычислениях с использованием приближенных чисел, при наличии ошибок округления и т.п. Иными словами, речь идет о вычислениях при наличии некоторых неопределенностей, источники возникновения которых весьма многообразны. В частности, такими источниками могут быть ограниченность разрядной сетки компьютера, ошибки преобразования (к примеру, преобразования чисел из одной системы счисления в другую), ошибки измерений из-за естественного несовершенства измерительных приборов.

Методы интервального анализа, развитые к настоящему времени, базируются на использовании арифметических операций с вещественными и комплексными числами. В предлагаемой статье вводится интервальная арифметика над конечными полями $GF(p)$, где $p$ — простое число. Необходимость такой интервальной арифметики обусловлена потребностями развития методов теории дискретных систем.

В качестве примера приведем теорию линейных последовательностных машин (ЛПМ) [1], которые определены над конечными полями $GF(p)$. Линейные последовательностные машины представляют собой математические модели широко распространенных реальных дискретных систем, осуществляющих кодирование и декодирование информации, сигнатурный анализ выходных реакций устройства для его технического диагностирования и т. п.

С физической точки зрения уровни значений напряжений для входных и выходных значений сигналов, а также уровни значений состояний элементов памяти электронных устройств, описываемых математическими моделями ЛПМ, можно измерять в “квантованных” единицах. Поскольку по техническим условиям значения напряжений имеют ограничения сверху, предельное значение этого напряжения, выраженное в “квантованных” единицах, и дает характеристику $p$ поля $GF(p)$. Отсюда же возникает и необходимость оперировать квантованными значениями напряжений в арифметике по модулю $p$.

*Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, грант №010100080.

Заметим, что уровни напряжений измеряются приборами с некоторой погрешностью, и поэтому вместо точных значений уровней сигналов могут возникнуть интервалы, в пределах которых находятся их действительные значения. Разнообразные задачи, возникающие в теории ЛПМ, сводятся, в частности, к решению различных разностных уравнений и систем, имеющих интервальные коэффициенты.

Работы по интервальной арифметике над конечными полями в настоящее время отсутствуют, и предлагаемая статья может отчасти заполнить эту нишу.

# 1. Обозначения и основные определения

Строчные греческие буквы $\alpha$, $\beta$, $\gamma$, ..., а также латинские с чертой снизу или сверху $\underline{a}$, $\overline{a}$, $\underline{b}$, $\overline{b}$, ... будут далее обозначать элементы поля $GF(p) = \{0, 1, \ldots, p-1\}$, где $p$ — простое число.

Каждый элемент поля $GF(p) = \{0, 1, \ldots, p-1\}$ представляет собой класс вычетов по модулю $p$. Выберем из каждого класса вычетов одного представителя, являющегося минимальным целым неотрицательным числом. Введем на множестве этих представителей порядок как на множестве целых чисел. Для полученного упорядоченного множества $\{0, 1, \ldots, p-1\}$ сохраним ранее использованное обозначение $GF(p)$.

Подмножество $\boldsymbol{a} \subseteq GF(p)$ такое, что $\boldsymbol{a} = [\underline{a}, \overline{a}] = \{\alpha \mid \underline{a} \leq \alpha \leq \overline{a}; \underline{a}, \overline{a} \in GF(p)\}$ будем называть правильным интервалом, где $\underline{a}$ и $\overline{a}$ – соответственно его нижняя и верхняя границы.

Запись вида $\boldsymbol{b} = \left[\underline{b}, \overline{b}\right]$, где $\underline{b} > \overline{b}$, будем интерпретировать как множество $GF(p) \backslash \left[\overline{b}+1, \underline{b}-1\right]$, где $\backslash$ — операция разности в теоретико-множественном смысле, и называть это множество неправильным интервалом.

Интервал вида $[\underline{a}, \overline{a}]$, где $\underline{a} = \overline{a}$, будем называть вырожденным и интерпретировать его как элемент поля $GF(p)$.

**Определение 1.** *Все правильные, неправильные и вырожденные интервалы называются обычными интервалами.*

Зарезервируем латинские буквы за обозначениями интервалов.

Исходя из интерпретации неправильного интервала $\left[\underline{b}, \overline{b}\right]$ как множества "внешних" элементов $GF(p)$ по отношению к правильному интервалу $\left[\overline{b}+1, \underline{b}-1\right]$ любой неправильный интервал может быть представлен в следующем виде:

$$[\underline{b}, \overline{b}] = [0, \overline{b}] \cup [\underline{b}, p-1]. \tag{1}$$

**Определение 2.** *Два интервала $\boldsymbol{a} = [\underline{a}, \overline{a}]$ и $\boldsymbol{b} = [\underline{b}, \overline{b}]$ называются равными (и записывается это как $\boldsymbol{a} = \boldsymbol{b}$), если они равны в теоретико-множественном смысле.*

Из этого определения следует, что $\underline{a} = \underline{b}$ & $\overline{a} = \overline{b} \rightarrow \boldsymbol{a} = \boldsymbol{b}$, но обратная импликация, в отличие от случая вещественных интервалов, места не имеет. Например, при $p = 5$ интервалы $[2, 1]$ и $[3, 2]$ равны как множества, однако их границы не совпадают. Легко видеть, что для любого $\alpha \in GF(p)$ справедливо равенство $[\alpha, \alpha - 1] = [0, p-1]$.

Очевидно, что отношение равенства над полем $GF(p)$ рефлексивно, симметрично и транзитивно.

Введем операции над обычными интервалами. Далее знаками $+$, $-$, $\cdot$, $/$ будем обозначать соответствующие арифметические операции над вещественными числами и интервалами над $GF(p)$, а знаками $\oplus$, $\ominus$, $\odot$, $\oslash$ — операции над элементами поля $GF(p)$.

**Определение 3.** *Пусть* $\circledast \in \{\oplus, \ominus, \odot, \oslash\}$ *— бинарная арифметическая операция над элементами поля* $GF(p)$*. Если* $\boldsymbol{a}, \boldsymbol{b}$ *— обычные интервалы, то*

$$\boldsymbol{a} * \boldsymbol{b} = \{\alpha \circledast \beta \mid \alpha \in \boldsymbol{a}, \beta \in \boldsymbol{b}\} \tag{2}$$

*определяет бинарную арифметическую операцию над обычными интервалами. (В случае деления предполагаем, что* $0 \notin \boldsymbol{b}$*.)*

Очевидно, что операции сложения и умножения коммутативны.

Если интерпретировать поле $GF(p)$ как точки числовой оси, то каждый правильный интервал $[\underline{a}, \overline{a}]$ — это множество точек, расположенных вплотную одна за другой между $\underline{a}$ и $\overline{a}$.

Отметим, что результатом операции над обычными интервалами может оказаться множество точек, не являющееся одним интервалом, а представляющее собой объединение нескольких интервалов, разбросанных по числовой оси. Например, для $p = 7$ $[1, 2] \cdot [2, 3] = [2, 4] \cup [6, 6]$.

**Определение 4.** *Подмножество* $\boldsymbol{A} \subseteq GF(p)$ *такое, что*

$$\boldsymbol{A} = \bigcup_{i \in I} \boldsymbol{a}_i, \tag{3}$$

*где* $\boldsymbol{a}_i$ *— обычный интервал,* $I$ *— конечное множество индексов и для* $i \neq j$*,* $\boldsymbol{a}_i \cap \boldsymbol{a}_j = \emptyset$*, называется мультиинтервалом поля* $GF(p)$*.*

Мультиинтервал будем обозначать прописной буквой. Понятно, что обычный интервал является частным случаем мультиинтервала. Множество всех мультиинтервалов обозначим как $IGF(p)$.

Введем бинарные операции над мультиинтервалами.

**Определение 5.** *Пусть* $* \in \{+, -, \cdot, /\}$ *— бинарная операция. Если*

$$\boldsymbol{A} = \bigcup_{i \in I} \boldsymbol{a}_i \ , \boldsymbol{B} = \bigcup_{j \in J} \boldsymbol{b}_j,$$

*где* $\boldsymbol{a}_i, \boldsymbol{b}_j$ *— обычные интервалы поля* $GF(p)$*, то*

$$\boldsymbol{A} * \boldsymbol{B} = \left(\bigcup_{i \in I} \boldsymbol{a}_i\right) * \left(\bigcup_{j \in J} \boldsymbol{b}_j\right) = \bigcup_{i \in I, j \in J} \boldsymbol{a}_i * \boldsymbol{b}_j. \tag{4}$$

Заметим, что множество $IGF(p)$ мультиинтервалов является замкнутым относительно введенных бинарных операций.

Как следует из формулы (4), любая бинарная операция над мультиинтервалами в конечном счете сводится к соответствующей операции над обычными интервалами поля $GF(p)$.

Введем унарную операцию над обычным интервалом $\boldsymbol{x} = [\underline{x}, \overline{x}] \in IGF(p)$:

$$-\boldsymbol{x} = [-\overline{x}, -\underline{x}],$$

где $-\xi$ — это элемент $GF(p)$, обратный элементу $\xi$ по сложению, т. е. такой, что $\xi \oplus (-\xi) = 0$. Аналогичную операцию для мультиинтервала

$$\boldsymbol{X} = \bigcup_{i \in I} \boldsymbol{x}_i$$

определим так:

$$-\boldsymbol{X} = \bigcup_{i \in I} (-\boldsymbol{x}_i).$$

С использованием этой операции бинарная операция вычитания выражается через операцию сложения:

$$\boldsymbol{A} - \boldsymbol{B} = \boldsymbol{A} + (-\boldsymbol{B}). \tag{5}$$

Например, при $p = 5$ $\boldsymbol{a} = [0, 1]$, $\boldsymbol{b} = [4, 1]$, тогда

$$\boldsymbol{a} - \boldsymbol{b} = [0, 1] - [4, 1] = [0, 1] + (-[4, 1]) = [0, 1] + [4, 1] = [4, 2].$$

Введем операцию умножения элемента $\alpha \in GF(p)$ на мультиинтервал $\boldsymbol{X}$:

$$\alpha \cdot \boldsymbol{X} = \bigcup_{\xi \in \boldsymbol{X}} [\alpha \odot \xi, \alpha \odot \xi]. \tag{6}$$

Используя эту операцию, бинарную операцию умножения мультиинтервалов можно записать в виде

$$\boldsymbol{A} \cdot \boldsymbol{B} = \bigcup_{\alpha \in \boldsymbol{A}} \alpha \cdot \boldsymbol{B}. \tag{7}$$

Например, при $p = 5$, $\boldsymbol{a} = [2, 4]$, $\boldsymbol{b} = [1, 2]$ имеем

$$\boldsymbol{a} \cdot \boldsymbol{b} = 2 \cdot [1, 2] \cup 3 \cdot [1, 2] \cup 4 \cdot [1, 2] = [2, 2] \cup [4, 4] \cup [3, 3] \cup [1, 1] \cup [3, 4] = [1, 4].$$

И, наконец, операцию деления мультиинтервалов можно записать в виде

$$\boldsymbol{A}/\boldsymbol{B} = \boldsymbol{A} \cdot \left( \bigcup_{\beta \in \boldsymbol{B}} 1/\beta \right), \tag{8}$$

где $1/\beta$ — это элемент $GF(p)$, обратный элементу $\beta$ по умножению, т. е. такой, что $\beta \odot (1/\beta) = 1$. Например, если $p = 5$, $\boldsymbol{a} = [1, 3]$, $\boldsymbol{b} = [3, 4]$, то

$$\boldsymbol{a}/\boldsymbol{b} = [1, 3]/[3, 4] = [1, 3] \cdot (1/3 \cup 1/4) = [1, 3] \cdot (2 \cup 4) =$$

$$= 2 \cdot [1, 3] \cup 4 \cdot [1, 3] = [1, 2] \cup [4, 4] \cup [2, 4] = [1, 4].$$

## 2. Свойства арифметических операций в $IGF(p)$

В классической интервальной арифметике [2]

$$\zeta = f(\xi, \eta),$$

где $f(\xi, \eta) = \xi * \eta$, $* \in \{+, -, \cdot, /\}$, $\xi \in \boldsymbol{x}$, $\eta \in \boldsymbol{y}$, $\boldsymbol{x}, \boldsymbol{y} \in I(R)$ (при делении $0 \notin \boldsymbol{y}$) — непрерывные функции на компактном множестве, и потому $f(\xi, \eta)$ принимает как наименьшее, так и наибольшее значения.

Таким образом, $\boldsymbol{x} * \boldsymbol{y}$ есть также замкнутый вещественный интервал, полностью заполненный вещественными числами, являющимися результатами упомянутых бинарных

операций над соответствующими числами. При этом границы результата выражаются через операции с границами операндов. Некоторая, но не полная аналогия имеет место и в интервальной арифметике над полем $GF(p)$. Исходя из указанной аналогии найдем формулы, позволяющие выражать результаты бинарных операций над обычными интервалами через их границы.

Введем понятие ширины мультиинтервала

$$\boldsymbol{X} = \bigcup_{i \in I} \boldsymbol{x}_i$$

и обычного интервала $\boldsymbol{x}_i = [\underline{x_i}, \overline{x_i}]$, обозначаемой далее как $\mathrm{wid}\,(\boldsymbol{X})$ и $\mathrm{wid}\,(\boldsymbol{x}_i)$ соответственно:

$$\mathrm{wid}\,(\boldsymbol{X}) = \sum_{i \in I} \mathrm{wid}\,(\boldsymbol{x}_i),$$

$$\mathrm{wid}\,(\boldsymbol{x}_i) = \begin{cases} \overline{x_i} - \underline{x_i} + 1, & \text{если } x_i \text{ — правильный интервал,} \\ \overline{x_i} - \underline{x_i} + p + 1, & \text{если } x_i \text{ — неправильный.} \end{cases}$$

Понятно, что $\mathrm{wid}\,(\boldsymbol{x}_i)$ и $\mathrm{wid}\,(\boldsymbol{X})$ — это числа элементов в соответствующих интервалах. Очевидно также, что $\mathrm{wid}\,(\boldsymbol{x}_i) = \overline{x_i} \ominus \underline{x_i} + 1$ в любом случае.

Пусть $\boldsymbol{a} = [\underline{a}, \overline{a}], \boldsymbol{b} = [\underline{b}, \overline{b}]$ — обычные интервалы поля $GF(p)$, тогда для сложения интервалов справедлива следующая формула:

$$\boldsymbol{a} + \boldsymbol{b} = \begin{cases} [\underline{a} \oplus \underline{b}, \overline{a} \oplus \overline{b}], & \text{если } \mathrm{wid}\,(\boldsymbol{a}) + \mathrm{wid}\,(\boldsymbol{b}) \le p, \\ [0, p-1] & \text{в противном случае.} \end{cases}$$

Перейдем к доказательству этой формулы, для чего рассмотрим все случаи использования в качестве операндов правильных и неправильных интервалов. Заметим, что в справедливости соотношения $\boldsymbol{a} + \boldsymbol{b} = [0, p-1]$ при $\mathrm{wid}\,(\boldsymbol{a}) + \mathrm{wid}\,(\boldsymbol{b}) > p$ можно убедиться непосредственной проверкой.

1. Пусть $\boldsymbol{a}, \boldsymbol{b}$ — правильные интервалы. Тогда $0 \le \underline{a} \le \overline{a} < p$ и $0 \le \underline{b} \le \overline{b} < p$, следовательно,

$$0 \le \underline{a} + \underline{b} \le \overline{a} + \overline{b} < 2p, \tag{9}$$

$$-p \le \underline{a} + \underline{b} - p \le \overline{a} + \overline{b} - p < p\ : \tag{10}$$

(а) если $\underline{a} + \underline{b} < p$, $\overline{a} + \overline{b} < p$, то $\boldsymbol{a} + \boldsymbol{b} = [\underline{a} + \underline{b}, \overline{a} + \overline{b}] = [\underline{a} \oplus \underline{b}, \overline{a} \oplus \overline{b}]$ и результирующий интервал является правильным;

(б) если $\underline{a} + \underline{b} < p$, $\overline{a} + \overline{b} \ge p$, то $\boldsymbol{a} + \boldsymbol{b} = [\underline{a} + \underline{b}, p-1] \cup [0, \overline{a} + \overline{b} - p] = [\underline{a} \oplus \underline{b}, \overline{a} \oplus \overline{b}]$ и результатом является неправильный интервал;

(в) если $\underline{a} + \underline{b} \ge p$, $\overline{a} + \overline{b} \ge p$, то $\boldsymbol{a} + \boldsymbol{b} = [\underline{a} + \underline{b} - p, \overline{a} + \overline{b} - p] = [\underline{a} \oplus \underline{b}, \overline{a} \oplus \overline{b}]$ и результатом является правильный интервал;

(г) случай $\underline{a} + \underline{b} \ge p$, $\overline{a} + \overline{b} < p$ невозможен, поскольку тогда $\overline{a} + \overline{b} < p \le \underline{a} + \underline{b}$, что противоречит (9).

2. Пусть $\boldsymbol{a}$ — неправильный, а $\boldsymbol{b}$ — правильный интервалы, $\mathrm{wid}\,(\boldsymbol{a}) + \mathrm{wid}\,(\boldsymbol{b}) \le p$. Тогда

$$\mathrm{wid}\,(\boldsymbol{a}) + \mathrm{wid}\,(\boldsymbol{b}) \le p \Leftrightarrow \overline{a} - \underline{a} + p + 1 + \overline{b} - \underline{b} + 1 \le p \Rightarrow \overline{a} + \overline{b} < \underline{a} + \underline{b}. \tag{11}$$

Кроме того,

$$\boldsymbol{a} + \boldsymbol{b} = ([0, \overline{a}] \cup [\underline{a}, p-1]) + [\underline{b}, \overline{b}] = [\underline{b}, \overline{a} \oplus \overline{b}] \cup [\underline{a} \oplus \underline{b}, \overline{b} \ominus 1]\ : \tag{12}$$

(а) если $\underline{a}+\underline{b} \geq p$, $\overline{a}+\overline{b} < p$, то $\boldsymbol{a}+\boldsymbol{b} = [\underline{b}, \overline{a} \oplus \overline{b}] \cup [\underline{a}+\underline{b}-p, \overline{b}-1] = [\underline{a} \oplus \underline{b}, \overline{a} \oplus \overline{b}]$ — правильный интервал;

(б) если $\underline{a}+\underline{b} \geq p$, $\overline{a}+\overline{b} \geq p$ и в соответствии с (11) $\overline{a}+\overline{b} < \underline{a}+\underline{b}$, тогда интервал $[\underline{b}, \overline{a} \oplus \overline{b}]$ — неправильный. Отсюда следует, что $[\underline{b}, \overline{a} \oplus \overline{b}] = [\underline{b}, p-1] \cup [0, \overline{a}+\overline{b}-p]$, а $[\underline{a}+\underline{b}-p, \overline{b}-1]$ — правильный интервал и $\underline{b} \leq \overline{b}$. Из этого вытекает, что $[\underline{a} \oplus \underline{b}, \overline{b}-1] \cup [\underline{b}, p-1] = [\underline{a} \oplus \underline{b}, p-1]$. На основании этого получаем $\boldsymbol{a}+\boldsymbol{b} = [\underline{b}, p-1] \cup [0, \overline{a}+\overline{b}-p] \cup [\underline{a} \oplus \underline{b}, \overline{b}-1] = [0, \overline{a} \oplus \overline{b}] \cup [\underline{a} \oplus \underline{b}, p-1] = [\underline{a} \oplus \underline{b}, \overline{a} \oplus \overline{b}]$, результирующий интервал является неправильным;

(в) если $\underline{a}+\underline{b} < p$, $\overline{a}+\overline{b} < p$, будем полагать $\overline{b} \neq 0$ (иначе $\boldsymbol{b} = 0$ и формула тривиальна), тогда с учетом (11) и (12) $[\underline{b}, \overline{a}+\overline{b}]$ — правильный, а $[\underline{a}+\underline{b}, \overline{b}-1]$ — неправильный интервалы. На основании этого получаем $[\underline{a}+\underline{b}, \overline{b}-1] = [0, \overline{b}-1] \cup [\underline{a}+\underline{b}, p-1]$. С использованием формулы (12) получаем $\boldsymbol{a}+\boldsymbol{b} = [\underline{b}, \overline{a}+\overline{b}] \cup [\underline{a}+\underline{b}, \overline{b}+p-1] = [\underline{b}, \overline{a}+\overline{b}] \cup [0, \overline{b}-1] \cup [\underline{a}+\underline{b}, p-1] = [0, \overline{a}+\overline{b}] \cup [\underline{a}+\underline{b}, p-1] = [\underline{a} \oplus \underline{b}, \overline{a} \oplus \overline{b}]$, результирующий интервал является неправильным.

3. Пусть $\boldsymbol{a}$, $\boldsymbol{b}$ — неправильные интервалы и $\operatorname{wid}(\boldsymbol{a}) + \operatorname{wid}(\boldsymbol{b}) \leq p \Leftrightarrow \overline{a}-\underline{a}+p+1+\overline{b}-\underline{b}+p+1 \leq p \Rightarrow \overline{a}+\overline{b} < \underline{a}+\underline{b}-p-2 < \underline{a}+\underline{b}-p < \underline{a}+\underline{b}$. Кроме того, не нарушая общности, будем считать $\overline{a} \neq 0$, $\overline{b} \neq 0$. С учетом этого получаем $\boldsymbol{a}+\boldsymbol{b} = ([0, \overline{a}] \cup [\underline{a}, p-1]) + ([0, \overline{b}] \cup [\underline{b}, p-1]) = ([0, \overline{a}]+[0, \overline{b}]) \cup ([0, \overline{a}]+[\underline{b}, p-1]) \cup ([\underline{a}, p-1]+[0, \overline{b}]) \cup ([\underline{a}, p-1]+[\underline{b}, p-1]) = [0, \overline{a} \oplus \overline{b}] \cup [\underline{b}, \overline{a} \oplus p \ominus 1] \cup [\underline{a}, \overline{b} \oplus p \ominus 1] \cup [\underline{a} \oplus \underline{b}, 2 \odot (p \ominus 1)] = [0, \overline{a} \oplus \overline{b}] \cup [\underline{a} \oplus \underline{b}, p \ominus 2] \cup [0, \max\{\overline{a}, \overline{b}\} \ominus 1] \cup [\min\{\underline{a}, \underline{b}\}, p-1] = [\underline{a} \oplus \underline{b}, \overline{a} \oplus \overline{b}]$.

Аналогично для операции вычитания обычных интервалов справедлива следующая формула:

$$\boldsymbol{a} - \boldsymbol{b} = \begin{cases} [\underline{a} \ominus \overline{b}, \overline{a} \ominus \underline{b}], & \text{если } \operatorname{wid}(\boldsymbol{a}) + \operatorname{wid}(\boldsymbol{b}) \leq p, \\ [0, p-1] & \text{в противном случае.} \end{cases}$$

Произведение интервалов в общем случае не удается представить через операции с границами сомножителей. Например, при $p = 5$: $[1,3] \cdot [3,4] = [1,4] \neq [3,2]$ ($1 \odot 3 = 3$, $3 \odot 4 = 2$). В общем случае не выполняется даже включение $\boldsymbol{a} \cdot \boldsymbol{b} \not\subseteq [\underline{a} \odot \underline{b}, \overline{a} \odot \overline{b}]$. Например, для $p = 5$: $[1,3] \cdot [1,2] = [1,4] \not\subseteq [1,1]$. Однако при некоторых ограничениях на ширину сомножителей выполняется включение

$$\boldsymbol{a} \cdot \boldsymbol{b} \subseteq [\underline{a} \odot \underline{b}, \overline{a} \odot \overline{b}]. \tag{13}$$

Чтобы получить условия, при которых верна формула (13), рассмотрим сначала умножение интервала $\boldsymbol{a} \in IGF(p)$ на число $\lambda \in GF(p)$. Включение

$$\lambda \cdot \boldsymbol{a} \subseteq [\lambda \odot \underline{a}, \lambda \odot \overline{a}] \tag{14}$$

выполняется при условии $\lambda(\operatorname{wid}(\boldsymbol{a}) - 1) < p - 1$. В самом деле, пусть $\underline{a} \leq \overline{a}$, тогда

$$\boldsymbol{a} = [\underline{a}, \overline{a}] = \{\underline{a}, \underline{a}+1, \ldots, \overline{a}\},$$

$\lambda\boldsymbol{a} = \{\lambda \odot \underline{a}, \lambda \odot \underline{a} \oplus \lambda, \lambda \odot \underline{a} \oplus 2 \odot \lambda, \ldots, \lambda \odot \overline{a}\} \subset \{\lambda \odot \underline{a}, \lambda \odot \underline{a} \oplus 1, \lambda \odot \underline{a} \oplus 2, \ldots, \lambda \odot \overline{a}\} = [\lambda \odot \underline{a}, \lambda \odot \overline{a}]$.

По-другому это можно записать как

$$\lambda\boldsymbol{a} = \lambda \cdot [\underline{a}, \overline{a}] \subseteq \underbrace{[\underline{a}, \overline{a}] + [\underline{a}, \overline{a}] + \cdots + [\underline{a}, \overline{a}]}_{\lambda \text{ раз}} = [\lambda \odot \underline{a}, \lambda \odot \overline{a}].$$

Последнее равенство верно при условии, что сумма $\lambda$ интервалов $\boldsymbol{a}$ не покрывает все поле $GF(p)$, т. е. ее ширина меньше $p$:

$$(\lambda\overline{a} - \lambda\underline{a} + 1 < p) \Leftrightarrow (\lambda \operatorname{wid}(\boldsymbol{a}) - \lambda < p - 1) \Leftrightarrow (\lambda(\operatorname{wid}(\boldsymbol{a}) - 1) < p - 1).$$

Для $\underline{a} > \overline{a}$ доказательство аналогично, учитывая, что в этом случае $[\underline{a}, \overline{a}] = [0, \overline{a}] \cup [\underline{a}, p-1]$.

Произведение интервалов $\boldsymbol{a}, \boldsymbol{b} \in IGF(p)$ можно представить как объединение произведений интервала на число, т. е. для $\underline{a} \le \overline{a}$

$$\boldsymbol{a} \cdot \boldsymbol{b} = \underline{a}b \cup (\underline{a}+1)b \cup \cdots \cup \overline{a}b.$$

Продолжая рассуждения, как и в предыдущем случае, получим в результате включение (13), которое выполняется при условии, что ширина интервала $[\underline{ab}, \overline{a}\overline{b}]$ не превышает $p$.

Обозначим $\sigma(\boldsymbol{a}) = \underline{a} + \overline{a}$, $\sigma(\boldsymbol{b}) = \underline{b} + \overline{b}$, тогда

$$\operatorname{wid}([\underline{ab}, \overline{a}\overline{b}]) = \overline{a}\overline{b} - \underline{ab} + 1 = \overline{a}(\overline{b} - \underline{b}) + \overline{a}\underline{b} + \underline{a}(\overline{b} - \underline{b}) - \underline{a}\overline{b} + 1 =$$

$$= \overline{a}(\operatorname{wid}(\boldsymbol{b}) - 1) + \underline{b}(\overline{a} - \underline{a}) + \underline{ab} + \underline{a}(\operatorname{wid}(\boldsymbol{b}) - 1) + \overline{b}(\overline{a} - \underline{a}) - \overline{a}\overline{b} + 1 =$$

$$= (\operatorname{wid}(\boldsymbol{b}) - 1)\sigma(\boldsymbol{a}) + (\operatorname{wid}(\boldsymbol{a}) - 1)\sigma(\boldsymbol{b}) - (\overline{a}\overline{b} - \underline{ab} + 1) + 2 =$$

$$= \sigma(\boldsymbol{a})(\operatorname{wid}(\boldsymbol{b}) - 1) + \sigma(\boldsymbol{b})(\operatorname{wid}(\boldsymbol{a}) - 1) - \operatorname{wid}([\underline{ab}, \overline{a}\overline{b}]) + 2,$$

$$(\operatorname{wid}([\underline{ab}, \overline{a}\overline{b}]) < p) \Leftrightarrow \sigma(\boldsymbol{a})(\operatorname{wid}(\boldsymbol{b}) - 1) + \sigma(\boldsymbol{b})(\operatorname{wid}(\boldsymbol{a}) - 1) + 2 < 2p \Leftrightarrow$$

$$\Leftrightarrow \sigma(\boldsymbol{a})(\operatorname{wid}(\boldsymbol{b}) - 1) + \sigma(\boldsymbol{b})(\operatorname{wid}(\boldsymbol{a}) - 1) < 2(p-1). \tag{15}$$

Для $\underline{a} > \overline{a}$ доказательство аналогично.

Мы доказали, что включение (13) выполняется при условии (15). Таким образом, для точного вычисления произведения интервалов или числа и интервала приходится переходить к поэлементному умножению, что приводит к увеличению объема вычислений. Однако, если не требуется высокая точность вычислений или нужно получить любую внешнюю оценку произведения, можно ограничиться умножением интервальных границ при определенных ограничениях, накладываемых на ширину и величину интервальных сомножителей.

Отметим некоторые свойства введенных операций.

**Теорема 1.** *Пусть $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \in IGF(p)$, тогда:*

*1) $\boldsymbol{A} + \boldsymbol{B} = \boldsymbol{B} + \boldsymbol{A}$, $\boldsymbol{A} \cdot \boldsymbol{B} = \boldsymbol{B} \cdot \boldsymbol{A}$ (коммутативность);*

*2) $(\boldsymbol{A} + \boldsymbol{B}) + \boldsymbol{C} = \boldsymbol{A} + (\boldsymbol{B} + \boldsymbol{C})$, $(\boldsymbol{A} \cdot \boldsymbol{B}) \cdot \boldsymbol{C} = \boldsymbol{A} \cdot (\boldsymbol{B} \cdot \boldsymbol{C})$ (ассоциативность);*

*3) $(\forall \boldsymbol{A} \in IGF(p))$ $\boldsymbol{A} = \boldsymbol{A} + [0,0] = [0,0] + \boldsymbol{A}$, $\boldsymbol{A} = \boldsymbol{A} \cdot [1,1] = [1,1] \cdot \boldsymbol{A}$, т. е. $[0,0]$ и $[1,1]$ являются единственными нейтральными элементами для сложения и умножения соответственно;*

*4) $IGF(p)$ не имеет делителей нуля;*

*5) произвольный невырожденный интервал из $IGF(p)$ не имеет обратного ни по сложению, ни по умножению, но $0 \in \boldsymbol{A} - \boldsymbol{A}$, $1 \in \boldsymbol{A}/\boldsymbol{A}$;*

*6) $\boldsymbol{A} \cdot (\boldsymbol{B} + \boldsymbol{C}) \subseteq \boldsymbol{A} \cdot \boldsymbol{B} + \boldsymbol{A} \cdot \boldsymbol{C}$ (субдистрибутивность);*

*7) $\lambda \cdot (\boldsymbol{A} + \boldsymbol{B}) = \lambda\boldsymbol{A} + \lambda\boldsymbol{B}$, где $\lambda \in GF(p)$ (дистрибутивность умножения на число);*

*8) $\forall \alpha \in GF(p)$ $[\alpha, \alpha - 1] = [0, p-1]$;*

*9) $\operatorname{wid}(\boldsymbol{A} * \boldsymbol{B}) \le \operatorname{wid}(\boldsymbol{A}) \cdot \operatorname{wid}(\boldsymbol{B})$, где $* \in \{+, -, \cdot, /\}$;*

*10) $\operatorname{wid}(\boldsymbol{a} + \boldsymbol{b}) = \operatorname{wid}(\boldsymbol{a} - \boldsymbol{b}) = \operatorname{wid}(\boldsymbol{a}) + \operatorname{wid}(\boldsymbol{b}) - 1$, если $\boldsymbol{a}, \boldsymbol{b}$ — обычные интервалы и $\operatorname{wid}(\boldsymbol{a}) + \operatorname{wid}(\boldsymbol{b}) < p$;*

*11) $\operatorname{wid}(\lambda\boldsymbol{A}) = \operatorname{wid}(\boldsymbol{A})$, $\lambda \in GF(p)$ и $\lambda \ne 0$.*

**Доказательство.** Заметим, что доказательства пп. 1 – 6 теоремы почти дословно повторяют доказательства соответствующих утверждений из теоремы 4 в [2].

Следующий пример показывает справедливость п. 6 теоремы. Пусть $p = 5$, $\boldsymbol{a} = [0, 1]$, $\boldsymbol{b} = [1, 2]$, $\boldsymbol{c} = [3, 4]$, тогда $\boldsymbol{b} + \boldsymbol{c} = [4, 1]$, $\boldsymbol{a} \cdot (\boldsymbol{b} + \boldsymbol{c}) = [4, 1]$, $\boldsymbol{a} \cdot \boldsymbol{b} = [0, 2]$, $\boldsymbol{a} \cdot \boldsymbol{c} = [3, 0]$, $\boldsymbol{a} \cdot \boldsymbol{b} + \boldsymbol{a} \cdot \boldsymbol{c} = [3, 2] = [0, 4]$, откуда и следует требуемое включение.

Докажем п. 7. Пусть $\lambda \in GF(p)$, $\boldsymbol{A} = \{\alpha_1, \ldots, \alpha_m\}$, $\boldsymbol{B} = \{\beta_1, \ldots, \beta_n\}$. $\lambda(\boldsymbol{A} + \boldsymbol{B}) = \lambda(\{\alpha_1, \ldots, \alpha_m\} + \{\beta_1, \ldots, \beta_n\}) = \lambda\{\alpha_1 \oplus \beta_1, \alpha_1 \oplus \beta_2, \ldots, \alpha_1 \oplus \beta_n, \alpha_2 \oplus \beta_1, \alpha_2 \oplus \beta_2, \ldots, \alpha_2 \oplus \beta_n, \ldots, \alpha_m \oplus \beta_1, \alpha_m \oplus \beta_2, \ldots, \alpha_m \oplus \beta_n\} = \{\lambda \odot (\alpha_1 \oplus \beta_1), \lambda \odot (\alpha_1 \oplus \beta_2), \ldots, \lambda \odot (\alpha_1 \oplus \beta_n), \ldots, \lambda \odot (\alpha_m \oplus \beta_1), \ldots, \lambda \odot (\alpha_m \oplus \beta_n)\} = \{\lambda \odot \alpha_1, \ldots, \lambda \odot \alpha_m\} + \{\lambda \odot \beta_1, \ldots, \lambda \odot \beta_n\} = \lambda\boldsymbol{A} + \lambda\boldsymbol{B}$.

Справедливость п. 8 следует из определения неправильного интервала. Справедливость п. 9 легко заметить, если представить результат арифметической операции $* \in \{+, -, \cdot, /\}$ в виде таблицы, приведенной ниже.

| $\boldsymbol{B}$ \| $\boldsymbol{A}$ | $\alpha_1$ | $\alpha_2$ | $\ldots$ | $\alpha_m$ |
|---|---|---|---|---|
| $\beta_1$ | $\alpha_1 \circledast \beta_1$ | $\alpha_2 \circledast \beta_1$ | $\ldots$ | $\alpha_m \circledast \beta_1$ |
| $\beta_2$ | $\alpha_1 \circledast \beta_2$ | $\alpha_2 \circledast \beta_2$ | $\ldots$ | $\alpha_m \circledast \beta_2$ |
| $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ | $\ldots$ |
| $\beta_n$ | $\alpha_1 \circledast \beta_n$ | $\alpha_2 \circledast \beta_n$ | $\ldots$ | $\alpha_m \circledast \beta_n$ |

Если $\operatorname{wid}(\boldsymbol{A}) = m$, $\operatorname{wid}(\boldsymbol{B}) = n$ и среди $\alpha_i \circledast \beta_j$ нет совпадений, то ширина результата максимальна $\operatorname{wid}(\boldsymbol{A} * \boldsymbol{B}) = mn$; если есть совпадения, то получим строгое неравенство.

Докажем п. 10 теоремы. Если $\boldsymbol{a}, \boldsymbol{b} \in IGF(p)$ — обычные интервалы, т. е. $\boldsymbol{a} = [\underline{a}, \overline{a}]$, $\boldsymbol{b} = [\underline{b}, \overline{b}]$ и $\operatorname{wid}(\boldsymbol{a}) + \operatorname{wid}(\boldsymbol{b}) < p$, то справедливо равенство $\boldsymbol{a} + \boldsymbol{b} = [\underline{a} \oplus \underline{b}, \overline{a} \oplus \overline{b}]$, тогда $\operatorname{wid}(\boldsymbol{a} + \boldsymbol{b}) = \overline{a} \oplus \overline{b} \ominus \underline{a} \ominus \underline{b} + 1 = (\overline{a} \ominus \underline{a} + 1) \oplus (\overline{b} \ominus \underline{b} + 1) - 1 = \operatorname{wid}(\boldsymbol{a}) + \operatorname{wid}(\boldsymbol{b}) - 1$. Учитывая, что $\operatorname{wid}(-\boldsymbol{b}) = \operatorname{wid}(\boldsymbol{b})$, получим аналогично равенство для ширины разности интервалов.

Докажем п. 11 теоремы:
$\operatorname{wid}(\lambda\boldsymbol{A}) = \operatorname{wid}(\{\lambda \odot \alpha_1, \lambda \odot \alpha_2, \ldots, \lambda \odot \alpha_n\}) = \operatorname{wid}(\{\alpha_1, \ldots, \alpha_n\}) = \operatorname{wid}(\boldsymbol{A})$, так как $(\alpha_i \neq \alpha_j) \Rightarrow (\lambda \odot \alpha_i \neq \lambda \odot \alpha_j \ \forall \lambda \in GF(p)(\lambda \neq 0))$. ■

Заметим, что $IGF(p)$ с введенными операциями сложения и умножения на число не является линейным пространством и даже квазилинейным (см. определение квазилинейного пространства в [3]), так как не выполняется аксиома линейности $(\lambda + \mu)\boldsymbol{A} = \lambda\boldsymbol{A} + \mu\boldsymbol{A}$, где $\lambda, \mu \in GF(p), \boldsymbol{A} \in IGF(p)$.

П р и м е р. При $p = 11$
$(1 + 2) \cdot [1, 3] = 3 \cdot [1, 3] = [3, 3] \cup [6, 6] \cup [9, 9]$,
$1 \cdot [1, 3] + 2 \cdot [1, 3] = [1, 3] + [2, 2] \cup [4, 4] \cup [6, 6] = [3, 9]$,
$(1 + 2) \cdot [1, 3] \subset 1 \cdot [1, 3] + 2 \cdot [1, 3]$.

# 3. Множества решений уравнений в $IGF(p)$

Рассмотрим уравнение относительно $X$

$$f(A, X) = B, \tag{16}$$

зависящее от некоторых параметров $(\boldsymbol{A}_1, \ldots, \boldsymbol{A}_s)^T = \boldsymbol{A}$, где $\boldsymbol{A}_i, \boldsymbol{B} \in IGF(p)$, $i = \overline{1, s}$, $f(\boldsymbol{A}, \boldsymbol{X})$ — рациональное выражение, состоящее из интервалов $\boldsymbol{A}, \boldsymbol{X}$, соединенных знаками арифметических операций.

**Определение 6.** *Назовем формальным решением уравнения (16) такой мультиинтервал $\boldsymbol{X} \in IGF(p)$, что при его подстановке в (16) получается точное равенство.*

Пусть, например, $p = 5$ и рассматривается уравнение $[1, 2] + \boldsymbol{X} = [4, 2]$. Можно убедиться в том, что интервалы $\boldsymbol{X}_1 = [0, 0] \cup [3, 3]$ и $\boldsymbol{X}_2 = [3, 0]$ ($[3, 0] = [0, 0] \cup [3, 3] \cup [4, 4]$), подставленные в заданное уравнение, дают точное равенство, т. е. оба этих интервала являются формальными решениями. Из этого примера следует, что формальное решение уравнения $\boldsymbol{A} + \boldsymbol{X} = \boldsymbol{B}$ в общем случае неединственно.

Следующие определения множеств решений были введены С. П. Шарым в [4] и R. B. Kearfott в [5] для множеств решений интервальных систем линейных алгебраических уравнений, здесь множества решений определяются для уравнения (16).

**Определение 7.** *Назовем объединенным множеством решений уравнения (16) следующее множество элементов:*

$$\boldsymbol{X}_{\exists\exists} = \{\xi \in GF(p) \mid (\exists \alpha \in \boldsymbol{A})(\exists \beta \in \boldsymbol{B})\ f(\alpha, \xi) = \beta\}.$$

Так, для примера уравнения, рассмотренного выше, $\boldsymbol{X}_{\exists\exists} = [0, 4]$.

**Определение 8.** *Назовем допустимым множеством решений уравнения (16) следующее множество:*

$$\boldsymbol{X}_{\forall\exists} = \{\xi \in GF(p) \mid (\forall \alpha \in \boldsymbol{A})(\exists \beta \in \boldsymbol{B})\ f(\alpha, \xi) = \beta\}.$$

Для рассмотренного выше примера $\boldsymbol{X}_{\forall\exists} = [3, 0]$, т. е. для этого уравнения имеет место включение $\boldsymbol{X}_{\forall\exists} \subset \boldsymbol{X}_{\exists\exists}$. Легко показать, что такое включение справедливо и в общем случае. Кроме того, $\boldsymbol{X}_{\forall\exists} = \boldsymbol{X}_2$ (одному из формальных решений).

**Определение 9.** *Назовем управляемым множеством решений уравнения (16) следующее множество:*

$$\boldsymbol{X}_{\exists\forall} = \{\xi \in GF(p) \mid (\forall \beta \in \boldsymbol{B})(\exists \alpha \in \boldsymbol{A})\ f(\alpha, \xi) = \beta\}.$$

П р и м е р. Для $p = 5$ уравнение $[1, 3] + \boldsymbol{X} = [0, 1]$ имеет управляемое множество решений $\boldsymbol{X}_{\exists\forall} = [3, 4]$.

**Теорема 2.** *Линейное уравнение $\boldsymbol{a} + \boldsymbol{X} = \boldsymbol{b}$, где $\boldsymbol{a}, \boldsymbol{b}$ — обычные интервалы над полем $GF(p)$, имеет формальное решение $\boldsymbol{X}$ в виде мультиинтервала тогда и только тогда, когда* $\operatorname{wid}(\boldsymbol{a}) \le \operatorname{wid}(\boldsymbol{b})$.

**Доказательство.** Необходимость. Докажем ее от противного. Пусть $\operatorname{wid}(\boldsymbol{a}) > \operatorname{wid}(\boldsymbol{b})$. Покажем, что в этом случае рассматриваемое уравнение решения не имеет. Пусть $\boldsymbol{a} = \{\alpha_1, \ldots, \alpha_\mu\}$. Выберем произвольный элемент $\xi \in GF(p)$ и построим множество $\boldsymbol{a}_\xi = \{\alpha_1 \oplus \xi, \ldots, \alpha_\mu \oplus \xi\}$. Очевидно, что в $\boldsymbol{a}_\xi$ все элементы попарно различны, т. е. $\operatorname{wid}(\boldsymbol{a}_\xi) = \mu$. Элемент $\xi \notin \boldsymbol{X}$, поскольку среди элементов $\boldsymbol{a}_\xi$ существует по крайней мере один такой элемент $\alpha_i \oplus \xi \notin \boldsymbol{b}$, так как $\operatorname{wid}(\boldsymbol{b}) < \mu$. Из произвольности элемента $\xi$ следует, что в $\boldsymbol{X}$ нет ни одного элемента $GF(p)$, т. е. формальное решение пусто.

Достаточность. Пусть $\operatorname{wid}(\boldsymbol{a}) \le \operatorname{wid}(\boldsymbol{b})$, тогда формальное решение есть $\boldsymbol{X} = [\underline{b} \ominus \underline{a}, \overline{b} \ominus \overline{a}]$, $\boldsymbol{a} + \boldsymbol{X} = [\underline{a}, \overline{a}] + [\underline{b} \ominus \underline{a}, \overline{b} \ominus \overline{a}] = [\underline{a} \oplus \underline{b} \ominus \underline{a}, \overline{a} \oplus \overline{b} \ominus \overline{a}] = [\underline{b}, \overline{b}] = \boldsymbol{b}$, при этом по свойству 11 (теорема 1) $\operatorname{wid}(\boldsymbol{b}) = \operatorname{wid}(\boldsymbol{a} + \boldsymbol{X}) = \operatorname{wid}(\boldsymbol{a}) + \operatorname{wid}(\boldsymbol{X}) - 1 \Rightarrow \operatorname{wid}(\boldsymbol{b}) - \operatorname{wid}(\boldsymbol{a}) = \operatorname{wid}(\boldsymbol{X}) - 1$. Отсюда, учитывая, что $\operatorname{wid}(\boldsymbol{a}) \le \operatorname{wid}(\boldsymbol{b})$, получим $\operatorname{wid}(\boldsymbol{X}) \ge 1$, т. е. множество $\boldsymbol{X}$ непусто. ■

Заметим, что теорема 2 для случая, когда в уравнении $\boldsymbol{A} + \boldsymbol{X} = \boldsymbol{B}$ вместо обычных интервалов использованы мультиинтервалы, неверна. В самом деле, пусть $p = 7$, $\boldsymbol{A} = [1, 1] \cup [3, 3] \cup [5, 5]$, $\boldsymbol{B} = [6, 2]$. Перебором можно проверить, что уравнение в этом случае формального решения не имеет.

Для существования формального решения уравнения $\boldsymbol{AX} = \boldsymbol{B}$ условие $\operatorname{wid}(\boldsymbol{A}) \leq \operatorname{wid}(\boldsymbol{B})$ является необходимым, но не является достаточным, даже для случая, когда $\boldsymbol{A}$ и $\boldsymbol{B}$ — обычные интервалы. Например, при $p = 7$, $[2,4] \cdot \boldsymbol{X} = [3,6]$, $\operatorname{wid}(\boldsymbol{A}) = 3$, $\operatorname{wid}(\boldsymbol{B}) = 4$, но формального решения не существует, хотя объединенное множество решений $\boldsymbol{X}_{\exists\exists} = [1,6]$, допустимое множество решений $\boldsymbol{X}_{\forall\exists} = [6,6]$.

Для уравнения

$$\boldsymbol{A} + \boldsymbol{X} = \boldsymbol{B} \tag{17}$$

введенные множества решений определяются следующим образом:

$$\boldsymbol{X}_{\exists\exists} = \bigcup_{\alpha\in\boldsymbol{A}} \bigcup_{\beta\in\boldsymbol{B}} (\beta \ominus \alpha) = \boldsymbol{B} - \boldsymbol{A}, \tag{18}$$

$$\boldsymbol{X}_{\forall\exists} = \bigcap_{\alpha\in\boldsymbol{A}} \bigcup_{\beta\in\boldsymbol{B}} (\beta \ominus \alpha), \tag{19}$$

$$\boldsymbol{X}_{\exists\forall} = \bigcap_{\beta\in\boldsymbol{B}} \bigcup_{\alpha\in\boldsymbol{A}} (\beta \ominus \alpha). \tag{20}$$

Для уравнения

$$\boldsymbol{A} \cdot \boldsymbol{X} = \boldsymbol{B}, \tag{21}$$

где $0 \notin \boldsymbol{A}$, множества решений определяются аналогично:

$$\boldsymbol{X}_{\exists\exists} = \bigcup_{\alpha\in\boldsymbol{A}} \bigcup_{\beta\in\boldsymbol{B}} (\beta \oslash \alpha) = \boldsymbol{B}/\boldsymbol{A}, \tag{22}$$

$$\boldsymbol{X}_{\forall\exists} = \bigcap_{\alpha\in\boldsymbol{A}} \bigcup_{\beta\in\boldsymbol{B}} (\beta \oslash \alpha), \tag{23}$$

$$\boldsymbol{X}_{\exists\forall} = \bigcap_{\beta\in\boldsymbol{B}} \bigcup_{\alpha\in\boldsymbol{A}} (\beta \oslash \alpha). \tag{24}$$

Равенства (18) – (20), (22) – (24) следуют из определения множеств $\boldsymbol{X}_{\exists\exists}$, $\boldsymbol{X}_{\forall\exists}$, $\boldsymbol{X}_{\exists\forall}$ и определения операций $\bigcup$ и $\bigcap$, понимаемых в обычном смысле как операции объединения и пересечения множеств соответственно.

Рассмотрим пример: при $p = 7$, $[2,4] \cdot \boldsymbol{X} = [2,5]$. Для наглядности построим таблицу деления $\beta \oslash \alpha$, где $\beta \in [2,5]$, $\alpha \in [2,4]$.

| $\alpha$ \| $\beta$ | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| 2 | 1 | 5 | 2 | 6 |
| 3 | 3 | 1 | 6 | 4 |
| 4 | 4 | 6 | 1 | 3 |

Объединение всех элементов строк (столбцов) таблицы составляет объединенное множество решений $\boldsymbol{X}_{\exists\exists} = [1,6]$. Пересечение элементов строк таблицы составляет допустимое множество решений $\boldsymbol{X}_{\forall\exists} = [1,1] \cup [6,6]$. Пересечение элементов столбцов таблицы пусто, поэтому $\boldsymbol{X}_{\exists\forall} = \emptyset$ и управляемых решений уравнение не имеет.

**Теорема 3.** *Все множества решений уравнений (17) и (21) и формальное решение, если оно существует, включаются в объединенное множество решений, т. е. в* $\boldsymbol{B} - \boldsymbol{A}$ *для уравнения (17) и в* $\boldsymbol{B}/\boldsymbol{A}$ *для уравнения (21).*

**Доказательство** следует из равенств (18) – (20), (22) – (24) для множеств решений. Для формального решения очевидно, что если оно существует, то все его элементы являются допустимыми решениями и, следовательно, принадлежат также и объединенному множеству решений. ■

## Список литературы

[1] Гилл А. Последовательностные линейные машины. М.: Наука, 1974.

[2] Алефельд Г., Херцбергер Ю. Введение в интервальные вычисления. М.: Мир, 1987.

[3] Калмыков С. А., Шокин Ю. И., Юлдашев З. Х. Методы интервального анализа. Новосибирск: Наука, 1986.

[4] Shary S. P. Algebraic approach to the linear static identification, tolerance and control problems, or One more application of Kaucher arithmetic // Reliable Computing. 1996. Vol. 2, No. 1. P. 3–33.

[5] Kearfott R. B. Rigorous Global Search: Continuous Problems. Dordrecht: Kluwer, 1996.

*Поступила в редакцию 7 марта 2002 г.,*
*в переработанном виде — 31 июля 2002 г.*