

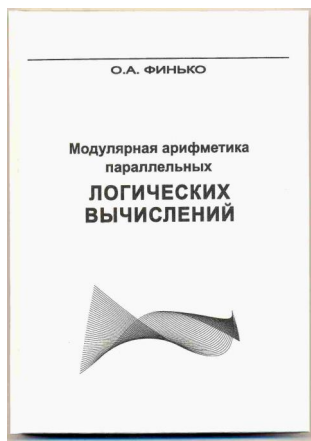
УДК 519.7

ББК 22.18

**Финько О.А.**<sup>2</sup>

Ф59

Модулярная арифметика параллельных логических вычислений: Монография / Под. ред. В.Д. Малюгина; – М.: ИПУ РАН, 2003. – 224 с.



Монография<sup>3</sup> посвящена новому направлению математической логики — реализации параллельных логических вычислений посредством арифметико-логических форм. Впервые рассматривается отображение классической логики на модулярную арифметику, которое открывает уникальные возможности по достижению высоких уровней производительности и отказоустойчивости средств гибких логических вычислений.

Для специалистов в области защиты информации, прикладной математики, математической кибернетики, информатики и вычислительной техники, аспирантов и студентов соответствующих специальностей.

## Рецензенты:

- ◆ лауреат Государственной премии СССР, академик Казахстанской НАН, доктор технических наук, профессор В.М. АМЕРБАЕВ;
- ◆ проректор Чувашского государственного ун-та по информатизации и образовательным технологиям, доктор технических наук, профессор Е.К. ЛЕБЕДЕВ.

---

<sup>1</sup>Книга выпущена на средства Министерства обороны РФ. Заинтересованные юридические и физические лица и организации могут получить книгу **БЕСПЛАТНО**. Книга не может быть использована с целью получения прибыли. Для получения книги необходимо выслать на имя руководителя организации соответствующее письмо с ходатайством и мотивацией предоставления книги. Адрес организации: 350035. г. Краснодар, ул. Красина, д. 4. Краснодарское высшее военное училище (военный институт). Начальнику военного училища.

<sup>2</sup> © Автор. Просьба замечания и отзывы на книгу направлять автору: E-mail: ofinko@yandex.ru.

<sup>3</sup> С монографией можно ознакомиться в библиотеках ИПУ РАН (г. Москва) и Московского государственного института электронной техники (технический ун-т) (Зеленоград).

# Оглавление

Предисловие редактора

Введение

Обозначения

## 1 Основные положения арифметической логики

- 1.1 Представление булевых функций арифметическими полиномами
- 1.2 Преобразование булевых формул в арифметические полиномы
- 1.3 Линейные арифметические полиномы
- 1.4 Конъюнктивные преобразования
- 1.5 Арифметический аналог логического ряда Тейлора
- 1.6 Выводы

## 2 Введение в модулярные формы арифметической логики

- 2.1 Модулярные полиномиальные формы
- 2.2 Конъюнктивные модулярные преобразования
- 2.3 Модулярная форма логического ряда Тейлора
- 2.4 Выводы

## 3 Многомерные формы, основанные на Китайской теореме

- 3.1 Полиномиальные многомерные формы, основанные на Китайской теореме
- 3.2 Конъюнктивные многомерные преобразования, основанные на Китайской теореме
- 3.3 Выводы

## 4 Организация вычислений в больших числовых диапазонах

- 4.1 Принцип больших модулей
- 4.2 Принцип групп модулей
- 4.3 Многоступенчатые многомерные формы
- 4.4 Выводы

## 5 Обобщение модулярных форм на $k$ -значную логику

- 5.1 Полиномиальная арифметика  $k$ -значной логики
- 5.2 Модулярные формы  $k$ -значной логики
- 5.3 Теоретико-числовые преобразования на  $k$ -значной логике
- 5.4 Реализация систем  $k$ -значных функций
- 5.5 Выводы

## 6 Альтернативные арифметико-логические формы

- 6.1 Мультипликативно-кодированные арифметико-логические формы
- 6.2 Модулярно-кодированные арифметико-логические формы
- 6.3 Выводы

## 7 Восстановление позиционной формы числа

- 7.1 Теорема о восстановлении для двух модулей

- 7.2 Применение специальных модулей
- 7.3 Обобщения для произвольного количества модулей
- 7.4 Использование полиадической системы счисления
- 7.5 Выводы

## **8 Оператор s-арного модулярного суммирования**

- 8.1 Традиционный «горизонтальный» метод s-арного суммирования
- 8.2 «Вертикальный» метод s-арного суммирования
- 8.3 «Вертикальный» метод s-арного преобразования
- 8.4 s-арное модулярное умножение
- 8.5 Счетчики единиц по модулю
- 8.6 Использование избыточных позиционных представлений чисел
- 8.7 Выводы

## **9 Контроль ошибок логических вычислений и отказоустойчивые структуры**

- 9.1 Контроль ошибок избыточными модулярными кодами
- 9.2 Реконфигурация вычислительных структур
- 9.3 Контроль дефектов методом тестирования
- 9.4 Выводы

## **Заключение**

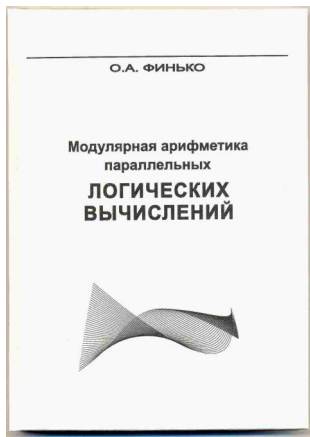
## **Приложения**

- A Необходимые положения теории чисел
- B Таблица индексов для модуля 13

## **Литература**

## **Предметный указатель**

**Finko O.A.** Modular arithmetics of parallel logic evaluations. Under Maljugin's VD edition. Institute of problems of control of the Russian academy of sciences, Moscow, 2003.



The monography<sup>5</sup> is devoted to a new direction of a mathematical logic – to implementation of parallel logical computations by means of arithmetic-logic forms. For the first time map of classical logic to modular arithmetics which opens unique possibilities on reaching high levels of efficiency and fault tolerance of tools of flexible logical computations is considered.

The monography intends for usage by experts in the field of a guard of the information, an applied mathematics, mathematical cybernetics, computer science and computer facilities, post-graduate students and students of appropriate specialities

## Reviewers:

- ◆ The winner of the State premium of the USSR, the academician of the Kazakhstan national academy of sciences, Dr.Sci.Tech., the professor V. Amerbaev;
- ◆ The pro-rector of the Chuvash state university on informatization and educational process engineerings, Dr.Sci.Tech., the professor E. Lebedev.

---

<sup>4</sup> The edition of the book financed the Ministry of Defence of the Russian Federation. The interested legal and physical persons and the organizations can receive the book **FREE-OF-CHARGE**. The book cannot be used with the purpose of reception of the profit. For reception of the book it is necessary to send addressed to the head of the organization the corresponding letter with the petition and motivation of granting of the book. The address of the organization: an index 350035. city of Krasnodar, street Khrasina, the house 4. Krasnodar high military school (military institute). To the chief of military school.

<sup>5</sup> It is possible to familiarize with the monography in libraries IPU of the Russian Academy of Science (Moscow) and the Moscow state institute of electronic technics (Technical university) (Zelenograd).

# Contents

## **Preface of the editor**

## **Introduction**

## **Labels**

### **1 Substantive provisions of arithmetical logic**

- 1.1 Representation of Boolean functions by arithmetical polynomials
- 1.2 Conversion of Boolean formulas in arithmetical polynomials
- 1.3 Linear arithmetical polynomials
- 1.4 Conjunctive conversions
- 1.5 Arithmetical analog of logical lines of Taylor
- 1.6 Summary

### **2 Introduction to modular forms of arithmetical logic**

- 2.1 Modular polynomial forms
- 2.2 Conjunctive modular conversions
- 2.3 The modular form of logical lines of Taylor
- 2.4 Summary

### **3 Multivariate forms based on the Chinese theorem**

- 3.1 Polynomial the multivariate forms based on the Chinese theorem
- 3.2 The conjunctive multivariate conversions based on the Chinese theorem
- 3.3 Summary

### **4 Organization of computations in the big numerical ranges**

- 4.1 A principle of the big units
- 4.2 A principle of groups of units
- 4.3 Multistage multivariate forms
- 4.4 Summary

### **5 Generalization of modular forms on $k$ -unit logic**

- 5.1 Polynomial arithmetics of  $k$ -unit logic
- 5.2 Modular forms of  $k$ -unit logic
- 5.3 Number-theoretic conversions on  $k$ -unit logic
- 5.4 Implementation of systems of  $k$ -unit functions
- 5.5 Summary

### **6 Alternate arithmetic-logic forms**

- 6.1 It is multiplicative - coded arithmetic-logic forms
- 6.2 Модулярно-coded arithmetic-logic forms
- 6.3 Summary

### **7 Restoring of the item form of number**

- 7.1 The theorem of restoring for two units
- 7.2 Application of special units
- 7.3 Generalizations for an arbitrary amount of units
- 7.4 Usage polyadic number systems

## 7.5 Summary

### **8 Operator $s$ -ary modular totting**

- 8.1 A traditional "horizontal" method  $s$ -ary tottings
- 8.2 The "Vertical" method  $s$ -ary tottings
- 8.3 The "Vertical" method  $s$ -ary conversions
- 8.4  $s$ -ary modular multiplying
- 8.5 Counters of units modulo
- 8.6 Usage of surplus item representations of numbers
- 8.7 Summary

### **9 Error checkings of logical computations and fault-tolerant structures**

- 9.1 Error checking by surplus modular codes
- 9.2 Reconfiguration of computing structures
- 9.3 Monitoring imperfections by a method of testing
- 9.4 Summary

### **Inference**

#### **Applications**

- Necessary positions of a number theory
- The table of indexes for the module 13

### **References**

### **Index**