Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

УДК 004.31: 519.714: 681.5.04

ГОРОДЕЦКИЙ
Данила Андреевич

МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ СИНТЕЗА ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВ МОДУЛЯРНОЙ АРИФМЕТИКИ

Автореферат диссертации
на соискание ученой степени кандидата технических наук
по специальности 05.13.05 – «Элементы и устройства
вычислительной техники и систем управления»

Минск 2011

Работа выполнена в Белорусском государственном университете

Научный руководитель: СУПРУН Валерий Павлович,
кандидат технических наук, доцент, доцент кафедры математической кибернетики Белорусского государственного университета

Официальные оппоненты: САДЫХОВ Рауф Хосровович,
доктор технических наук, профессор, заведующий кафедрой электронных вычислительных машин учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

САДОВ Василий Сергеевич,
кандидат технических наук, доцент, доцент кафедры интеллектуальных систем Белорусского государственного университета

Оппонирующая организация: Филиал НТЦ «Белмикросистемы» ОАО «ИНТЕГРАЛ»

Защита состоится 1 декабря 2011 года в 16.00 на заседании совета по защите диссертаций Д 02.15.01 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки 6, корп. 1, ауд. 232. e-mail: dissovet@bsuir.by, тел. (017) 293-89-89

ВВЕДЕНИЕ

Прогресс в области проектирования и производства вычислительной техники связан с повышением ее быстродействия. Физический предел стимулирует поиск принципиально новых подходов для решения этой задачи. Параллельные системы обработки информации являются эволюционным шагом в повышения быстродействия устройств вычислительной техники. Однако отсутствие «параллельной» математики, сложность программной и аппаратной реализации таких систем существенно ограничивают их применение. Одним из подходов к преодолению этих трудностей является использование модулярной арифметики (МА) и непозиционной системы счисления – системы остаточных классов (СОК).

К настоящему времени не найдено общих принципов организации параллельных систем обработки информации, однако применение аппарата МА обеспечивает повышение эффективности при решении весьма широкого круга теоретических и практических задач, которые возникают, например, при реализации нейропроцессорных вычислителей, устройств мультимедиа и систем обработки данных в реальном времени. Устройства, реализованные на основе алгоритмов МА, обладают не только более высокой скоростью обработки данных по сравнению с иными формами параллелизма, но часто являются более эффективными с точки зрения надежности и потребления мощности.

Естественный параллелизм устройств, функционирующих на основе СОК, позволяет распараллелить процесс вычислений как на программном, так и на аппаратном уровне, а модульность и однородность обеспечивает эффективное проектирование систем на кристалле.

Основными вычислительными операциями, за счет которых достигается высокое быстродействие устройств МА, являются операции сложения и умножения. В отечественной и зарубежной литературе широко исследуется вопрос построение модулярных сумматоров и модулярных умножителей для узко ограниченного множества значений модуля, однако вопрос проектирования таких вычислителей для произвольных значений модуля практически не освящен. Отсутствие широкой элементной базы и формальных описаний устройств МА на языках проектирования также является сдерживающим фактором к их широкому применению в вычислительной технике.

Диссертационная работа направлена на решение задач аналитического описания устройств, реализующих арифметические операции МА, а также на разработку методов синтеза логических схем таких устройств.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами и темами

Диссертационная работа выполнялась на кафедре уравнений математической физики (с 2010 г. – кафедра математической кибернетики) Белорусского государственного университета. Исследования, проведенные автором в рамках диссертационной работы, были отражены в рамках следующих научных тем и программ:

– НИР по теме «Разработка математических методов логического синтеза вычислительных устройств модулярной арифметики в базисе интегральных схем», № гос. регистрации 20061250 (2006–2010 гг.);

– ГПФНИ «Математические модели – 27», тема «Комбинаторные и теоретико-графовые методы и алгоритмы построения и анализа дискретных моделей», № гос. регистрации 20061787 (2006–2010 гг.);

– ГКПНИ «Научные основы информационных технологий и систем» «Инфотех – 06», тема «Модели и методы алгоритмического и функционально-логического проектирования управляющих и вычислительных систем на базе сверхбольших интегральных схем», № гос. регистрации 20061971 (2006–2010 гг.).

Цель и задачи исследования

Целью исследований является разработка математических моделей и методов синтеза одноуровневых и двухуровневых логических схем вычислительных устройств, реализующих арифметические операции МА для произвольного значения модуля и числа операндов. Для достижения поставленной цели требуется решить следующие задачи:

– разработать математические модели устройств, реализующих операции модулярного сложения (для произвольного числа операндов и произвольного значения модуля), а также модулярного умножения (для двух операндов и произвольного значения модуля);

– разработать метод синтеза логических схем устройств, реализующих операции модулярного сложения (для произвольного числа операндов и произвольного значения модуля) и модулярного умножения (для двух операндов и произвольного значения модуля);

– разработать метод синтеза логических схем устройств МА, реализующих различные суперпозиции арифметических операций;

– на основе предложенных моделей и методов разработать VHDL-описания элементов и устройств МА, а также провести экспериментальные исследования и анализ их эффективности.

Объектом исследований являются вычислительные устройства МА. Предметом исследований являются математические модели и методы синтеза логических схем вычислительных устройств МА.

Положения, выносимые на защиту

На защиту выносятся:

– математические модели и метод синтеза одноуровневых и двухуровневых логических схем модулярных сумматоров и модулярных умножителей; логические схемы, синтезированные на основе применения этого метода;

– метод блочно-структурного синтеза вычислительных устройств МА, реализующих различные суперпозиции основных модулярных операций (операций сложения, умножения и возведения в степень); логические схемы, синтезированные на основе применения этого метода;

– новые аналитические представления бисимметрических булевых функций, метод синтеза устройств для их вычисления; логические схемы, синтезированные с помощью этого метода.

Разработанные математические модели и методы синтеза логических схем ориентированы на представление данных (операндов) двоичными позиционными и унитарными кодами. Применение разработанных методов позволяет синтезировать более эффективные логические схемы устройств МА по сравнению с существующими аналогами (в том числе синтезированными посредством САПР) как по сумме входов логических элементов, так и по числу уровней соответствующих логических схем.

Личный вклад соискателя

Все результаты, выносимые на защиту и включенные в диссертацию, получены лично соискателем. Результаты, опубликованные в соавторстве, получены на паритетных началах, и в диссертацию включены лишь те из них, которые получены лично соискателем.

Апробация результатов диссертации

Основные теоретические и практические результаты диссертационной работы докладывались на:

– 62-й, 63-й, 64-й и 65-й научных конференциях студентов и аспирантов Белорусского государственного университета, Минск, Беларусь, 2005, 2006, 2007 и 2008 гг.;

– 10-й, 11-й, 12-й и 13-й Республиканских научных конференциях студентов и аспирантов «Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях», Гомель, Беларусь, 2007, 2008, 2009 и 2010 гг.;

– четвертой и пятой Международных научно-технических конференциях «Проблемы проектирования и производства радиоэлектронных средств», Новополоцк, Беларусь, 2006 и 2008 гг.;

– восьмой и одиннадцатой Международных научно-технических конференциях «Интеллектуальные системы» и «Интеллектуальные САПР», Дивноморское, Россия, 2008 и 2011 гг.;

– 10-й Белорусской математической конференции, Минск, Беларусь, 2008 г.;

– Международной научной конференции «Дискретная математика, алгебра и их приложения», Минск, Беларусь, 2009 г.;

– восьмой научно-практической конференции «Исследование, разработка и применение высоких технологий в промышленности», Санкт-Петербург, Россия, 2009 г.;

– шестой Международной конференции «Информационные технологии в промышленности», Минск, Беларусь, 2010 г.;

– седьмой Международной конференции «Автоматизация проектирования дискретных систем», Минск, Беларусь, 2010 г.

Опубликованность результатов

По материалам диссертационных исследований опубликовано 49 печатных работ, в том числе 6 статей в рецензируемых научных журналах, 13 публикаций в сборниках материалов Международных научных и научно-технических конференций и 30 Патентов на изобретение Республики Беларусь. Общее количество опубликованных статей составляет 20 авторских листов, из них 1,9 авторских листа в изданиях, соответствующих пункту 18 Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь, 1,2 авторский лист в материалах конференций и 16,9 в Патентах на изобретение Республики Беларусь. Результаты работы включены в 3 отчета по завершенным НИР.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, четырех глав, заключения, списка использованных источников, списка публикаций соискателя и приложений. В первой главе описывается современный уровень развития вычислительной техники, реализованной на основе МА, и актуальность исследований, приводятся основные понятия МА и теории синтеза логических схем; рассматриваются задачи синтеза логических схем устройств для вычисления бисимметрических булевых функций и распознавания юнатных (однородных) булевых функций. Вторая и третья главы посвящены разработке математических моделей и метода синтеза модулярных сумматоров для случая представления данных в позиционных кодах, модулярных сумматоров и модулярных умножителей для случая представления данных в унитарных кодах. В третьей главе также рассматривается метод синтеза схем устройств МА, предназначенных для реализации различных суперпозиций модулярных операций сложения, умножения и возведения в степень; рассматриваются устройства с управляющими входами, синтезированные на основе этого метода. В четвертой главе проводится анализ результатов синтеза VHDL-описаний устройств МА, реализованных на основе предложенных математических моделей и методов синтеза.

Полный объем диссертации составляет 189 страниц, в том числе 28 иллюстраций и 12 таблиц на 20 страницах, 6 приложений на 56 страницах, библиографический список из 192 источников (в том числе 49 авторских) на 18 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во ***введении*** приведены основные направления развития вычислительной техники на основе применения МА, определено направление проводимых исследований.

В ***первой главе*** рассматриваются основные положения в проектировании дискретных модулярных систем, а также элементы теории синтеза логических схем устройств, в основу которых положено использование симметрических и пороговых булевых функций.

Для модулярных вычислительных систем характерны два типа выполняемых операций – модульные и немодульные. К немодульным относятся операции преобразования из позиционного представления в модулярное и обратно, к модульным – операции сложения и умножения.

За счет выполнения модульных операций устройства МА обладают более высокой скоростью обработки информации по сравнению со своими аналогами,

реализованными на основе использования позиционных систем счисления. Высокое быстродействие достигается посредством параллельного выполнения вычислений над числами, разрядность которых меньше разрядности исходных чисел. Уменьшение разрядности исходных чисел достигается за счет их деления на взаимно простые модули с целью выполнения вычислений над полученными остатками. Такой подход представления чисел носит название СОК и ассоциируется с модулярными принципами обработки информации.

Среди основных ограничений использования МА при реализации вычислительных структур является отсутствие широкой элементной базы устройств МА, а также методов проектирования устройств, предназначенных для вычислений произвольного значения модуля и числа складываемых или умножаемых операндов.

Диссертационные исследования посвящены разработке математических моделей и методов синтеза логических схем устройств, реализующих модульные арифметические операции.

Одним из основных направлений развития вычислительной техники на основе применения МА являются нейрокомпьютеры, элементарным вычислительным элементом которых является искусственный нейрон, реализующий при определенной настройке пороговую или симметрическую булеву функцию (соответственно ПБФ и СБФ).

В научно-технической литературе широко представлены теоретические и практические результаты, направленные на применение свойств ПБФ и СБФ в вычислительной технике. Однако вопросы их применения при реализации устройств МА исследованы слабо. Известные результаты, как правило, не предназначены для широкого практического применения из-за узкого диапазона рассматриваемых значений модулей и фиксированного числа операндов, над которыми происходят вычисления.

Приводятся основные понятия теории булевых функций, относящихся к ПБФ и СБФ, рассматриваются полиномиально-однородные симметрические (ПОСБФ), бисимметрические (БиСБФ) и однородные (юнатные) булевы функции. Исследуются их свойства и приводятся различные виды разложений.

Описывается процедура *симметрирования* функции $F = F(x_1, x_2, ..., x_n)$, суть которой состоит в представлении функции F посредством СБФ, зависящей от $2^n - 1$ переменных:

$$F^* = F^*(x_1, x_2, x_2, ..., \underbrace{x_i, .., x_i}_{2^{i-1}}, ..., \underbrace{x_n, ..., x_n}_{2^{n-1}}).$$

Известно, что $w(F) = \pi(F^*)$, где $w(F) = (w_0, w_1, ..., w_{2^n-1})$ – вектор коэффициентов совершенной дизъюнктивной нормальной формы (СДНФ) булевой функции F, а $\pi(F^*) = (\pi_0, \pi_1, ..., \pi_{2^n-1})$ – локальный код СБФ F^*.

Произвольную СБФ $F = F(x_1, x_2, ..., x_n)$ можно представить посредством дизъюнкции фундаментальных симметрических булевых функций (ФСБФ), т.е.

$$F(x_1, x_2, ..., x_n) = \bigvee_{i=0}^{n} \pi_i \cdot F_n^i(x_1, x_2, ..., x_n), \quad (1)$$

где π_i – значение функции F на любом наборе значений n переменных, содержащем i единиц, $0 \le i \le n$.

Если отношение частичной симметрии переменных произвольной булевой функции $F = F(X)$ разбивает единственным образом множество переменных $X = \{x_1, x_2, ..., x_n\}$ на два класса симметрии $X_1 = \{x_1, x_2, ..., x_r\}$ и $X_2 = \{x_{r+1}, x_{r+2}, ..., x_n\}$, то $F = (X_1, X_2)$ называется БиСБФ типа «r, $n-r$».

Если полином Жегалкина СБФ $F = F(x_1, x_2, ..., x_n)$ содержит (все) элементарные конъюнкции, ранг которых равен k $(0 \le k \le n)$, то функция F называется ПОСБФ и обозначается как $F = E_n^k(x_1, x_2, ..., x_n)$.

Рассматриваются задачи построения аналитических представлений БиСБФ и синтеза логических схем для их вычисления [3]. Для БиСБФ $F = (X_1, X_2)$ известны формулы, имеющие вид дизъюнктивного и полиномиального разложений

$$F(X_1, X_2) = \bigvee_{j=0}^{r^*-1} \omega_j \cdot F_r^{j_1}(X_1) \cdot F_{n-r}^{j_2}(X_2) \quad (2)$$

и

$$F(X_1, X_2) = \sum_{j=0}^{r^*-1} \oplus \alpha_j \cdot E_r^{j_1}(X_1) \cdot E_{n-r}^{j_2}(X_2), \quad (3)$$

которые, соответственно, можно представить в следующем виде:

$$F(X_1, X_2) = F_r^0(X_1) \cdot G_0(X_2) \vee F_r^1(X_1) \cdot G_1(X_2) \vee ... \vee F_r^r(X_1) \cdot G_r(X_2) \quad (4)$$

и

$$F(X_1, X_2) = E_r^0(X_1) \cdot H_0(X_2) \oplus E_r^1(X_1) \cdot H_1(X_2) \oplus ... \oplus E_r^r(X_1) \cdot H_r(X_2), \quad (5)$$

где $F_r^{j_1}(X_1)$ – ФСБФ, зависящая от r переменных множества X_1, и рабочее число которой равно j_1 (функции $F_{n-r}^{j_2}(X_2)$, $F_r^0, F_r^1, ..., F_r^r$ определяются аналогично); $G_0(X_2), G_1(X_2), ..., G_r(X_2)$ – некоторые СБФ, зависящие от $n-r$ переменных множества X_2; $E_r^{j_1}(X_1)$ – ПОСБФ r переменных множества X_1 (функции $E_{n-r}^{j_2}(X_2)$, $E_r^0, E_r^1, ..., E_r^r$ определяются аналогично); $H_0(X_2), H_1(X_2), ..., H_r(X_2)$ – СБФ $n-r$ переменных множества X_2,

которые зависят от функций $G_0(X_2), G_1(X_2), \ldots, G_r(X_2)$; $\omega(F)=(\omega_0,\omega_1,\ldots,\omega_{r^*-1})$ – локальный код БиСБФ F; $\alpha(F)=(\alpha_0,\alpha_1,\ldots,\alpha_{r^*-1})$ – вектор коэффициентов полинома Жегалкина БиСБФ F; $j=j_1\cdot(n-r+1)+j_2$, $r^*=(r+1)\cdot(n-r+1)$, $0\le j_1\le r$ и $0\le j_2\le n-r$.

Используя формулу (5), можно синтезировать эффективные логические схемы для вычисления произвольных БиСБФ типа «$r, n-r$». Так, например, были синтезированы логические схемы устройств для вычисления 512 БиСБФ типа «2, 2» и 4096 БиСБФ типа «3, 2» [3].

Аналитические представления БиСБФ использовались, в частности, для описания структуры модулярных сумматоров.

Рассматривается задача синтеза устройства $\mathrm{D}(n)$, предназначенного для распознавания юнатных (однородная) булевых функций n переменных [15]. Схема устройства $\mathrm{D}(n)$ состоит из n подсхем, предназначенных для сравнения двух 2^{n-1} – разрядных двоичных наборов. На входы $\mathrm{D}(n)$ поступают значения вектора коэффициентов СДНФ $w(F)=(w_0,w_1,\ldots,w_{2^n-1})$ булевой функции $F=F(x_1,x_2,\ldots,x_n)$. В результате сравнения компонент вектора $w(F)$ на первом выходе $\mathrm{D}(n)$ формируется значение 1, если функция F является юнатной, и значение 0 – в противном случае. Если функция F юнатная, то на остальных n выходах $\mathrm{D}(n)$ формируются значения двоичного вектора юнатности $q(F)=(q_1,q_2,\ldots,q_n)$. Компонента $q_i=1$ тогда и только тогда, когда $w(F_0^i)\le w(F_1^i)$, где $F_0^i=F(x_i=0)$, $F_1^i=F(x_i=1)$.и $i=\overline{1,n}$.

Во ***второй главе*** приводятся математические модели, предназначенные для реализации устройств МА, выполняющих операции модулярного сложения и модулярного умножения [4, 5, 12–14, 16, 18].

Операнды, над которыми производятся вычисления $X_1,X_2,\ldots,X_N$, а также результат их сложения S и умножения R, представляются в двоичных позиционных и унитарных кодах, где операнды $X_1,X_2,\ldots,X_N,S,R$ принимают целочисленные значения.

Число $X \pmod P$, где $X\in \mathrm{Z}_+$, задается двумя способами:

– позиционным кодом $X=(x_1,x_2,\ldots,x_\delta)$, т.е.

$$X \pmod P=\sum_{i=1}^{\delta}2^{i-1}x_i=2^0\cdot x_1+2^1\cdot x_2+\ldots+2^{\delta-1}\cdot x_\delta,$$

где $x_1,x_2,\ldots,x_\delta\in\{0,1\}$ и $\delta=[\log_2 P]+1$;

– унитарным кодом $X=(x_0,x_1,\ldots,x_{P-1})$, т.е.

$$X \pmod P=\sum_{i=0}^{P-1}i\cdot x_i=0\cdot x_0+1\cdot x_1+\ldots+(P-1)\cdot x_{P-1},$$

где $x_0, x_1, ..., x_{P-1} \in \{0,1\}$ и $x_0 + x_1 + ... + x_{P-1} = 1$.

Предлагаемые математические модели модулярных сумматоров и модулярных умножителей имеют вид системы дизъюнкций ФСБФ.

Например [4, 16], в результате выполнения операции сложения по модулю три в позиционных кодах $\sum_{n=1}^{N} X_n = \sum_{n=1}^{N} \left(x_1^n + 2x_2^n\right) = s_1 + 2s_2 = S \pmod 3$ формируются две булевы функции $S_1 = S_1\left(x_1^1, x_2^1, x_1^2, x_2^2, ..., x_1^N, x_2^N\right)$ и $S_2 = S_2\left(x_1^1, x_2^1, x_1^2, x_2^2, ..., x_1^N, x_2^N\right)$, принимающие значения s_1 и s_2 результата сложения $S = (s_1, s_2)$.

Результат сложения $X_1 + X_2 + ... + X_N = S^* = S \pmod 3$, где $S^* \in \{0,1,2,...,2N\}$, можно представить с помощью двоичной матрицы $M\left(S^*\right) = \left[s_{i,j}\right]$, где $i \pmod 3 = s_{i,1} + 2s_{i,2}$, $i = \overline{0,2N}$ и $j = \overline{1,2}$.

Функция $S_1 = 1$ тогда и только тогда, когда $s_{i,1} = 1$; функция $S_2 = 1$ тогда и только тогда, когда $s_{i,2} = 1$.

Применив процедуру *симметрирования* к функциям $S_1 = S_1(Y_1, Y_2)$ и $S_2 = S_2(Y_1, Y_2)$, где $Y_1 = \left\{x_1^1, x_1^2, ..., x_1^N\right\}$ и $Y_2 = \left\{x_2^1, x_2^2, ..., x_2^N\right\}$, получим СБФ S_1^* и S_2^*, зависящие от $3N$ переменных. Тогда функции $S_1 = S_1^*(Y_1, Y_2, Y_2)$ и $S_2 = S_2^*(Y_1, Y_2, Y_2)$, а S_1^* и S_2^* взаимнооднозначно задаются локальными кодами $\pi\left(S_1^*\right) = \left(\pi_0^1, \pi_1^1, ..., \pi_{2N}^1, \pi_{2N+1}^1, ..., \pi_{3N}^1\right)$ и $\pi\left(S_2^*\right) = \left(\pi_0^2, \pi_1^2, ..., \pi_{2N}^2, \pi_{2N+1}^2, ..., \pi_{3N}^2\right)$.

Так как $0 \le S^* \le 2N$, то $\pi_\nu^1 = \pi_\nu^2 = 0$, где $2N + 1 \le \nu \le 3N$. Тогда локальные коды СБФ S_1^* и S_2^* могут быть записаны в виде $\pi\left(S_1^*\right) = \left(\pi_0^1, \pi_1^1, ..., \pi_{2N}^1\right)$ и $\pi\left(S_2^*\right) = \left(\pi_0^2, \pi_1^2, ..., \pi_{2N}^2\right)$ или в виде $\pi\left(S_1^*\right) = \left(s_{0,1}, s_{1,1}, ..., s_{2N,1}\right)$ и $\pi\left(S_2^*\right) = \left(s_{0,2}, s_{1,2}, ..., s_{2N,2}\right)$. В таком случае значения $\pi\left(S_1^*\right)$ и $\pi\left(S_2^*\right)$ соответствуют первому и второму столбцам матрицы $M\left(S^*\right)$, где $w(S_2) = \pi\left(S_1^*\right)$ и $w(S_2) = \pi\left(S_2^*\right)$.

Применяя разложение (1), получим представления функции S_1 и S_2 посредством дизъюнкции ФСБФ [4].

Утверждение. Если $N \ge 2$, то

$$S_1(Y_1, Y_2) = \bigvee_{i=0}^{2N} \pi_i^1 \cdot F_{3N}^i(Y_1, Y_2, Y_2),$$

$$S_2(Y_1, Y_2) = \bigvee_{i=0}^{2N} \pi_i^2 \cdot F_{3N}^i(Y_1, Y_2, Y_2). \qquad (6)$$

Отсюда следует, что

$$S_1 = \begin{cases} 1, \textit{ если } \sum_{n=1}^{N} X_n = \sum_{n=1}^{N} \left(x_1^n + 2x_2^n \right) = i \cdot \pi_i^1; \\ 0 - \textit{в противном случае}, \end{cases}$$

$$S_2 = \begin{cases} 1, \textit{ если } \sum_{n=1}^{N} X_n = \sum_{n=1}^{N} \left(x_1^n + 2x_2^n \right) = i \cdot \pi_i^2; \\ 0 - \textit{в противном случае}. \end{cases} \quad (7)$$

Аналитические представления (6) и (7) обобщаются на случай произвольного $P \geq 3$.

Аналогично решается задача построения математических моделей модулярных сумматоров и модулярных умножителей в унитарных кодах, реализующих операции $X_1 + X_2 + ... + X_N = S \pmod{P}$ и $X_1 \cdot X_2 = R \pmod{P}$ соответственно [5, 12, 13–18].

В ***третьей главе*** описываются методы синтеза схем вычислительных устройств МА:

– метод синтеза двухуровневых логических схем модулярных сумматоров в позиционных кодах для произвольного числа операндов и значения модуля $S(N,3)$ и $S(N,P)$ [4, 16], одноуровневых логических схем модулярных сумматоров в унитарных кодах для двух операндов и произвольного значения модуля $S(2,P)$ [5, 13], двухуровневых логических схем модулярных сумматоров в унитарных кодах для произвольного числа операндов и значения модуля $S(N,P)$ [12, 18], одноуровневых логических схем модулярных умножителей в унитарных кодах для двух операндов и произвольного значения модуля $R(2,P)$ [14];

– метод блочно-структурного синтеза логических схем вычислительных устройств МА [2, 7–11, 19].

Эффективность логических схем оценивается числом логических элементов схемы, сложностью по Квайну L (суммой входов элементов схемы), глубиной (числом уровней) T схемы и числом ее внешних выводов M.

Схемы модулярных сумматоров и модулярных умножителей, синтезированных с помощью описанных методов, состоят из двух типов элементов: элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом и элементов ИЛИ. Результат выполнения этих модулярных операций можно представить системой СБФ. Полученную систему реализует логическая схема, состоящая либо из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом и элементов ИЛИ для $S(N,P)$, где $P \geq 3$, в позиционных и унитарных кодах, либо только из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом для $S(2,P)$ и $R(2,P)$ в унитарных кодах.

Под элементом ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом a понимается логический элемент, на входы которого поступают значения двоичных переменных $x_1, x_2, ..., x_\delta$, а на его выходе формируются значения ФСБФ

$$F_n^a(x_1, x_2, ..., x_\delta) = \begin{cases} 1, \text{ если } x_1 + x_2 + ... + x_\delta = a; \\ 0 - \text{в противном случае.} \end{cases}$$

Логическая схема $S(N,3)$, реализующая операцию модулярного сложения в позиционных кодах $\sum_{n=1}^{N} X_n = \sum_{n=1}^{N} \left(x_1^n + 2x_2^n\right) = s_1 + 2s_2 = S \pmod 3$, состоит из двух подсхем $S_1(N,3)$ и $S_2(N,3)$. Подсхемы $S_1(N,3)$ и $S_2(N,3)$ реализуют СБФ S_1^* и S_2^*, соответственно, где $w(S_2) = \pi(S_1^*)$ и $w(S_2) = \pi(S_2^*)$, функции S_1 и S_2 описываются посредством дизъюнкции ФСБФ (6).

Подсхемы $S_1(N,3)$ и $S_2(N,3)$ состоят из элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом и элемента ИЛИ. На ходы элементов ИСКЛЮЧАЮЩЕЕ ИЛИ с порогом поступают значения двоичных переменных N операндов, а выходы соединены с входами первого и второго элементов ИЛИ. На выходе первого элемента ИЛИ формируются значения функции S_1, а на выходе второго элемента ИЛИ – значения функции S_2. Подсхемы $S_1(N,3)$ и $S_2(N,3)$ функционируют в соответствии с системами уравнений (7).

Метод синтеза $S(N,3)$ обобщается на случай $S(N,P)$, где $P \geq 3$, в позиционных кодах. По аналогии описывается метод синтеза модулярных сумматоров $S(N,P)$ и модулярных умножителей $R(2,P)$ в унитарных кодах [5, 12, 13, 14, 18].

Характеристики логических схем, синтезируемых на основе применения предложных методов приведены в таблице 1, где $|\pi(S_k)|$ – вес локального кода $\pi(S_k)$ и $k = \overline{1,\delta}$.

На основе предложенных методов были синтезированы схемы устройств МА, реализующие в позиционных и унитарных кодах, например, такие арифметические операции, как $X_1 + X_2 = S \pmod 3$ [35, 44], $X_1 \cdot X_2 = R \pmod 3$ [36, 40].

Описывается метод блочно-структурного синтеза логических схем вычислительных устройств МА [2, 7–11, 19]. Метод предназначен для синтеза устройств МА $\mathbb{R}$, реализующих суперпозицию операций МА – $X_1 + X_2 = S \pmod P$, умножения $X_1 \cdot X_2 = R \pmod P$ и возведения в степень $X_1^{X_2} = Q \pmod P$.

Общая идея блочно-структурного метода состоит в построении структуры устройства $\mathbb{R}$ из заранее разработанных логических схем – «блоков», реализующих операции модулярного сложения, умножения или

возведения в степень. Эти «блоки» логических схем подбираются таким образом, чтобы после их подстановки в структуру устройства $\mathfrak{R}$ можно было объединить на «стыках» одноименные логические элементы, обладающие свойством ассоциативности (например, элементы И, ИЛИ и СЛОЖЕНИЕ ПО МОДУЛЮ ДВА), уменьшая тем самым сложность и/или глубину логической схемы вычислительного устройства $\mathfrak{R}$, реализующего первоначально заданную суперпозицию операций. Кроме того, если использовать логические схемы «блоков» с меньшим числом внешних выводов, то появляется возможность удалить из схемы часть логических элементов.

Таблица 1 – Таблица характеристик схем устройств МА

Тип модулярного устройства	Сложность схемы по числу логических элементов, L_1	Сложность схемы по Квайну, L_2	Число уровней, T
Данные представляются в позиционных кодах			
$S(N,3)$	$\left[\frac{2N+2}{3}\right]+\left[\frac{2N+1}{3}\right]+2$	$L_1\cdot(3N+1)$	2
$S(N,P)$	$N\cdot(P-1)-\left[\frac{N\cdot(P-1)}{P}\right]+\delta-1$	$(L_1-\delta+1)\cdot(2^{\delta}-1)\cdot N+\sum_{k=1}^{\delta}\lvert\pi(S_k)\rvert$	2
Данные представляются в унитарных кодах			
$S(2,P)$	P	$P^2\cdot(P+1)$	1
$S(N,P)$	$N\cdot(P-1)+P+1$	$(L_1+N)\cdot\left(\frac{P\cdot(P-1)}{2}+1\right)$	2
$R(2,P)$	P	$P\cdot(P-1)^2+2$	1

Очевидно, что эффективность применения метода блочно-структурного синтеза зависит от номенклатуры логических схем – «блоков», отличающихся друг от друга типом использованных логических элементов, сложностью, глубиной и/или числом внешних выводов. На основе предложенного метода были синтезированы схемы устройств МА, реализующие в позиционных и унитарных кодах, например, такие арифметические операции, как $X_1\cdot X_2+X_3=S$ (mod 3) [20], $X_1\cdot X_2+X_3\cdot X_4=S$ (mod 3) [21, 36, 34], $(X_1+X_2)\cdot(X_3+X_4)=S$ (mod 3) [22, 26, 37], $X_1+X_2+X_3+X_4=S$ (mod 3) [23, 24].

Рассматривается задача синтеза схем устройств с управляющими входами, реализующими различные виды модулярных операций [10, 11]. Для

этих целей также предлагается использовать метод блочно-структурного синтеза. На основе предложенного метода были синтезированы схемы устройств МА, реализующие в позиционных и унитарных кодах, например, операции $X_1^n \pm X_1^m = S \pmod 3$ [25, 31, 46], $X_1^{Y_1} \cdot X_2^{Y_2} \cdot \ldots \cdot X_N^{Y_N} = S \pmod 3$ [30], $(X_1 \cdot X_2 \cdot \ldots \cdot X_N)^Y = S \pmod 3$ [33], $X_1^n + X_1^m = S \pmod 3$ [42], $(X_1 + X_2)^n = S \pmod 3$ [47].

Четвертая глава посвящена экспериментальным исследованиям VHDL-описаний элементов и устройств МА, полученных на основе разработанных математических моделей и методов синтеза. При проведении экспериментальных исследований были использованы системы ModelSim, Leonardo и ISE.

Целью первой части главы было сравнение логических схем [20–29, 31–36, 38–42], синтезированных на основе применения предложенных методов, с их аналогами, полученными с помощью выбранных САПР [1, 17].

Автоматизированный синтез проводился в двух библиотеках, одна из которых была специально для этого разработана. Множество логических элементов разработанной библиотеки составляет совокупность подмножеств элементов, использованных при проектировании устройств [20–29, 31–36, 38–42]. Синтез устройств также проводился в библиотеке элементов, используемой при проектировании базовых матричных кристаллов и заказных СБИС.

Устройства задавались двумя формами на языке VHDL: структурной, т.е. в виде совокупности компонентов и связей между ними, и функциональной – в виде VHDL-описаний, аналогичных таблице истинности, описывающей поведение функций выхода устройств.

В результате экспериментальных исследований было выявлено, что сложность и число уровней только пяти из двадцати одной синтезированные логических схем, сравнимы со своими аналогами, синтезированными на основе применения предложенных моделей и методов, и незначительно им уступают, в то время, как остальные существенно проигрывают авторским решениям по выбранным критериям.

На основе применения предложенных математических моделей были разработаны VHDL-описания модулярных сумматоров алгоритмического (*ALG*) и адресного (*ADR* и *ADR_BR*) типов [6].

На входы сумматора *ALG* поступают значения N операндов по модулю P. На промежуточном выходе формируется результат их сложения $X_1 + X_2 + \ldots + X_N = S^*$. Затем этот результат S^* поступает на вход блока модулярного преобразователя, на выходе которого формируется результат сложения $S \pmod P$.

Сумматор *ADR* вместо блока аппаратного деления содержит дешифратор и таблицу всевозможных значений, которые может принимать результат сложения операндов по модулю P. Таблица содержит $N(P-1)$ строк для N – операндного сумматора, осуществляющего сложение по модулю P.

Адресная модель модулярного сумматора была реализована двумя способами. Сумматор *ADR* ориентирован на реализацию всех элементов сумматора таблицами состояний LUT. Каждая таблица, содержащая $N(P-1)$ строк, сумматора *ADR_BR* прописывается в блочную память.

Полученные на FPGA структуры модулярных сумматоров сравнивались по быстродействию и сложности (по числу LUT) для сумматоров *ALG* и *ADR*. Экспериментальные исследования проводились для четырех систем модулей $M_1 = \{5,7,9\}$, $M_2 = \{15,17,31,37\}$, $M_3 = \{7,13,15,29,31,59,61\}$, $M_4 = \{17,19,23,25,27,29,31\}$ и для числа операндов, равного $N = 2,7,11,16,32$.

В результате реализации алгоритмических описаний *ALG* модулярных сумматоров были получены схемы меньшей сложности, но работающие с меньшей скоростью и наоборот, схемы, синтезированные по VHDL-описаниям адресных сумматоров, которые характеризуются большей скоростью вычислений, однако их аппаратная сложность значительно превышает аналогичный параметр алгоритмических сумматоров.

По мере роста числа операндов увеличивается разница в быстродействии алгоритмических и адресных сумматоров. Эта разница увеличивается как с увеличением разрядности операндов, так и с увеличением разрядности внутри системы модулей.

Применение системы оснований M_4, модули которой имеют одинаковою разрядность, приводит к реализации модулярных сумматоров, функционирующих с большей скоростью, чем их аналоги, реализованные в системе модулей с различной разрядностью – M_3. Кроме того, реализация в системе M_4 сопровождается меньшими аппаратными затратами.

В приложениях к диссертации приводятся VHDL-описания модулярных сумматоров алгоритмического (*ALG*) и адресного (*ADR* и *ADR_BR*) типов, а также разработанная для экспериментальных исследований библиотека элементов.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

Диссертационная работа посвящена разработке математических моделей и методов синтеза вычислительных устройств МА, а также реализации VHDL-описаний этих устройств посредством САПР [1, 6, 17]. При выполнении работы были получены следующие результаты.

1. Разработаны математические модели и метод синтеза а) двухуровневых логических схем модулярных сумматоров для произвольного числа операндов и значения модуля при условии представления данных в позиционных и унитарных кодах [4, 5, 12, 16, 18]; б) одноуровневых логических схем модулярных сумматоров и умножителей для двух операндов и произвольного значения модуля при условии представления данных в унитарных кодах [13, 14]. Предложены логические схемы вычислительных устройств, реализующие арифметические операции модулярного сложения и модулярного умножения, защищенные Патентами на изобретение Республики Беларусь [34–37, 40, 44, 48, 49].

2. Разработан метод блочно-структурного синтеза устройств МА, предназначенный для реализации а) суперпозиции модулярных операций (операций сложения, умножения и возведения в степень) [2, 7–9, 19]; б) вычислительных устройств МА с управляющими входами [10, 11]. Предложены логические схемы вычислительных устройств, реализующие различные суперпозиции модулярных операций сложения, умножения и возведения в степень, защищенные Патентами на изобретение Республики Беларусь [20–33, 36–39, 41–43, 45–47].

3. Предложены новые аналитические представления бисимметрических булевых функций; метод синтеза устройств для вычисления бисимметрических булевых функций [3]. Предложена логическая схема устройства для распознавания однородных булевых функций [15].

Рекомендации по практическому использованию результатов

Выполнение арифметических операций выгодно отличает модулярные структуры от своих аналогов, реализованных на основе использования позиционных систем счисления. Разработанные математические модели и методы синтеза направлены на синтез эффективных по сложности и глубине (быстродействию) логических схем вычислительных устройств МА.

Предложенные в диссертации VHDL-описания модулярных сумматоров, могут быть использованы при проектировании модулярных вычислительных структур с применением САПР.

Полученные в рамках диссертационных исследований результаты, выполненные в рамках фундаментальных и научно-практических исследований, нашли свое теоретическое и практическое применение: внедрены в учебный процесс механико-математического факультета Белорусского государственного университета и используются при проектировании вычислительной техники НТЦ «Белмикросистемы», УП «Интеграл-КАРТ» и лабораторией логического проектирования ОИПИ НАН Беларуси.

В рамках диссертационной работы были разработаны логические схемы вычислительных устройств МА, эффективность и мировая новизна которых подтверждена 30 Патентами на изобретение Республики Беларусь [20–49].

Некоторые из представленных результатов были отмечены Дипломом на 7-й Международной конференции «Автоматизация проектирования дискретных систем».

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи в научных журналах

1. Бибило, П.Н. Автоматизированный синтез устройств модулярной арифметики: может ли САПР заменить изобретателя / П.Н. Бибило, Д.А. Городецкий // Автоматика и вычислительная техника. – 2009. – № 2. – С. 15-27 (*Переведена на английский язык:* Automatic Control and Computer Sciences. – 2009. – Vol. 43, № 2. – P. 63-73).

2. Супрун, В.П. Метод блочно-структурного синтеза вычислительных устройств модулярной арифметики / В.П. Супрун, Д.А. Городецкий // Информатика. – 2009. – № 4. – С. 74-80.

3. Супрун, В.П. Реализация бисимметрических булевых функций логическими схемами / В.П. Супрун, Д.А. Городецкий // Известия ВУЗов. Приборостроение. – 2010. – № 5. – С. 17-25.

4. Супрун, В.П. Синтез n – операндных сумматоров по модулю три / В.П. Супрун, Д.А. Городецкий // Автоматика и вычислительная техника. – 2010. – № 3. – С. 72–80 (*Переведена на английский язык:* Automatic Control and Computer Sciences. – 2010. – Vol. 44, № 3. – P. 171-177).

5. Супрун, В.П. Реализация операций сложения и умножения в унитарных кодах / В.П. Супрун, Д.А. Городецкий // Автоматика и вычислительная техника.

– 2010. – № 5. – С. 59-71 (*Переведена на английский язык:* Automatic Control and Computer Sciences. – 2010. – Vol. 44, № 5. – P. 292-301).

6. Бибило, П.Н. О реализации модулярных сумматоров на FPGA / П.Н. Бибило, Д.А. Городецкий // Информатика. – 2011. – № 1. – С. 62-67.

Тезисы докладов и материалы конференций

7. Городецкий, Д.А. Проектирование устройств модулярной арифметики / Д.А. Городецкий // 63-я научная конференция студентов и аспирантов Белгосуниверситета: сб. раб., Минск, 23-26 мая 2006 г.: в 3 ч. / Белорус. гос. ун-т.; редкол.: Л.М. Томильчик [и др.]. – Минск, 2006. – Ч. 1. – С. 15-18.

8. Городецкий, Д.А. Вычислительные устройства унитарных кодов по модулю три с минимальным числом внешних выводов / Д.А. Городецкий, А.М. Седун, В.П. Супрун // Проблемы проектирования и производства радиоэлектронных средств: сб. материалов 4 Междунар. науч-практ. конф., Новополоцк, 25-26 мая 2006 г.: в 2 т. / Полоц. гос. ун-т; редкол.: А.П. Достанко [и др.]. – Новополоцк, 2006. – Т. 2. – С. 34-38.

9. Городецкий, Д.А. Блочно-структурный метод синтеза вычислительных устройств модулярной арифметики / Д.А. Городецкий // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: материалы 10 Республ. науч. конф. студ. и аспир., Гомель, 12–14 марта 2007 г. / Гомельск. гос. ун-т им. Ф. Скорины: редкол.: Д.Г. Лин [и др.]. – Гомель, 2007. – С. 246-247.

10. Городецкий, Д.А. Многофункциональные вычислительные устройства по модулю три / Д.А. Городецкий // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: материалы 11 Республ. науч. конф. студ. и аспир., Гомель, 17–19 марта 2008 г.: в 2 ч. / Гомельск. гос. ун-т им. Ф. Скорины: редкол.: О.М. Демиденко [и др.]. – Гомель, 2008. – Ч. 2. – С. 36-37.

11. Супрун, В.П. Вычислительные устройства унитарных кодов по модулю три с управляющими входами / В.П. Супрун, Д.А. Городецкий // Проблемы проектирования и производства радиоэлектронных средств: сб. материалов 5 Междунар. науч-практ. конф., Новополоцк, 29-30 мая 2008 г.: в 3 т. / Полоц. гос. ун-т; редкол.: А.П. Достанко [и др.]. – Новополоцк, 2008. – Т. 3. – С. 98-102.

12. Городецкий, Д.А. Сумматоры унитарных кодов по модулю P / Д.А. Городецкий, В.П. Супрун // Интеллектуальные системы (AIS'08) и Интеллектуальные САПР (CAD–2008): труды Междунар. науч-техн. конф., Дивноморское, 3–10 сент. 2008 г.: в 4 т. – М.: Физматлит, 2008. – Т. 2. – С. 391-395.

13. Супрун, В.П. Математическая модель сумматора унитарных кодов по модулю *P* / В.П. Супрун, Д.А. Городецкий // 10 Белорусская математическая конференция: тез. докл. Междунар. науч. конф., Минск, 3–7 ноября 2008 г.: в 5 ч. / Инст. матем. НАН Беларуси. – Минск, 2008. – Ч. 5. – С. 100-101.

14. Городецкий, Д.А. Модулярные умножители унитарных кодов / Д.А. Городецкий // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: материалы 12 Республ. науч. конф. студ. и аспир., Гомель, 16–18 марта 2009 г.: в 2 ч. / Гомельск. гос. ун-т им. Ф. Скорины: редкол.: О.М. Демиденко [и др.]. – Гомель, 2009. – Ч. 2. – С. 19-20.

15. Gorodecky, D.A. A synthesis of logical devices for identification the unite Boolean functions // D.A. Gorodecky, V.P. Suprun // Discrete mathematics, algebra and their applications: thesis of the Intern. scient. conf., Minsk, 19–22 Oct. / Inst. of Math. NAS of Belarus. – Minsk, 2009. – P. 138-140.

16. Супрун, В.П. Метод синтеза устройства для сложения и вычитания чисел по модулю три / В.П. Супрун, Д.А. Городецкий // Исследование, разработка и применение высоких технологий в промышленности: сб. тр. 8 Междунар. науч.–практ. конф., Санкт-Петербург, 27–28 окт. 2009 г.: / под. ред. А.П. Кудинова – СПб.: Изд-во Политехн. ун-та, 2009. – С. 44-45.

17. Городецкий, Д.А. VHDL-модели устройств модулярной арифметики / Д.А. Городецкий // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: материалы 13 Республ. науч. конф. студ. и аспир., Гомель, 15–17 марта 2010 г.: в 2 ч. / Гомельск. гос. ун-т им. Ф. Скорины: редкол.: О.М. Демиденко [и др.]. – Гомель, 2010. – Ч. 1. – С. 74-75.

18. Супрун, В.П. Реализация операции модулярного сложения в унитарных кодах / В.П. Супрун, Д.А. Городецкий // Информационные технологии в промышленности: тез. докл. 6 Междунар. конф., Минск, 27-29 октября 2010 г. / ОИПИ НАН РБ. – Минск, 2010 – С. 105-106.

19. Супрун, В.П. Реализация основных арифметических операций в унитарных кодах / В.П. Супрун, Д.А. Городецкий // Автоматизация проектирования дискретных систем (CAD DD'10): сб. мат. 7 Междунар. конф., Минск, 16-17 ноября 2010 г. / ОИПИ НАН РБ. – Минск, 2010. – С. 182-187.

Патенты на изобретение Республики Беларусь

20. Вычислительное устройство унитарных кодов по модулю три: пат. 9189 Респ. Беларусь, МКИ G 06 F 7/49 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № а 20050241; заявл. 15.03.2005; опубл.

30.04.2007 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2007. – № 2. – С. 153-154.

21. Вычислительное устройство унитарных кодов по модулю три: пат. 9341 Респ. Беларусь, МКИ G 06 F 7/38, 7/48 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20050342; заявл. 05.04.2005; опубл. 30.06.2007 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2007. – № 3. – С. 141.

22. Вычислительное устройство унитарных кодов по модулю три: пат. 9477 Респ. Беларусь, МКИ G 06 F 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20050475; заявл. 17.05.2005; опубл. 30.06.2007 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2007. – № 3. – С. 141-142.

23. Сумматор унитарных кодов по модулю три: пат. 9600 Респ. Беларусь, МКИ G 06 F 7/38, 7/48 / Д.А. Городецкий, А.М. Седун, В.П. Супрун; заявитель Белорус. гос. ун-т. – № a 20050565; заявл. 07.06.2005; опубл. 30.08.2007 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2007. – № 4. – С. 165.

24. Сумматор унитарных кодов по модулю три: пат. 10201 Респ. Беларусь, МКИ G 06 F 7/38, 7/48 / Д.А. Городецкий, А.М. Седун, В.П. Супрун; заявитель Белорус. гос. ун-т. – № a 20060155; заявл. 23.02.2006; опубл. 28.02.2008 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2008. – № 1. – С. 152-153.

25. Вычислительное устройство унитарных кодов по модулю три: пат. 10221 Респ. Беларусь, МКИ G 06 F 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20060423; заявл. 05.05.2006; опубл. 28.02.2008 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2008. – № 1. – С. 150.

26. Вычислительное устройство унитарных кодов по модулю три: пат. 10350 Респ. Беларусь, МКИ G 06 F 7/38 / Д.А. Городецкий, А.М. Седун, В.П. Супрун; заявитель Белорус. гос. ун-т. – № a 20060214; заявл. 13.03.2006; опубл. 28.02.2008 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2008. – № 1. – С. 149-150.

27. Вычислительное устройство унитарных кодов по модулю три: пат. 10659 Респ. Беларусь, МКИ G 06 F 7/00, 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20061008; заявл. 17.10.2006; опубл. 30.06.2008 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2008. – № 3. – С. 161.

28. Сумматор унитарных кодов по модулю пять: пат. 10834 Респ. Беларусь, МКИ G 06 F 7/38 / Д.А. Городецкий, А.М. Седун, В.П. Супрун; заявитель Белорус. гос. ун-т. – № a 20061007; заявл. 17.10.2006; опубл. 30.06.2008 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2008. – № 3. – С. 161.

29. Вычислительное устройство унитарных кодов по модулю три: пат. 11172 Респ. Беларусь, МКИ G 06 F 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20070509; заявл. 04.05.2007; опубл. 30.10.2008 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2008. – № 5. – С. 137-138.

30. Устройство для умножения N чисел в унитарных кодах по модулю три: пат. 11286 Респ. Беларусь, МКИ G 06 F 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20070559; заявл. 14.05.2007; опубл. 30.10.2008 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2008. – № 5. – С. 138-139.

31. Вычислительное устройство унитарных кодов по модулю три: пат. 11462 Респ. Беларусь, МКИ G 06 F 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20070142; заявл. 09.02.2007; опубл. 30.12.2008 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2008. – № 6. – С. 145.

32. Вычислительное устройство унитарных кодов по модулю пять: пат. 11473 Респ. Беларусь, МКИ G 06 F 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20070914; заявл. 18.07.2007; опубл. 30.10.2008 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2008. – № 6. – С. 145-146.

33. Вычислительное устройство унитарных кодов по модулю три: пат. 11783 Респ. Беларусь, МКИ G 06 F 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20071231; заявл. 09.10.2007; опубл. 30.04.2009 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2009. – № 6. – С. 128.

34. Устройство для умножения унитарных кодов по модулю три: пат. 12000 Респ. Беларусь, МКИ G 06 F 7/38 / Д.А. Городецкий, А.М. Седун, В.П. Супрун; заявитель Белорус. гос. ун-т. – № a 20071442; заявл. 27.11.2007; опубл. 30.06.2009 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2009. – № 3. – С. 167-168.

35. Сумматор по модулю три: пат. 12003 Респ. Беларусь, МКИ G 06 F 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20071483; заявл. 30.11.2007; опубл. 30.06.2009 // Афіцыйны бюл. / Нац, цэнтр інтэлектуал. уласнасці. – 2009. – № 3. – С. 168.

36. Вычислительное устройство по модулю три: пат. 12200 Респ. Беларусь, МКИ G 06 F 7/38 / Д.А. Городецкий, А.М. Седун, В.П. Супрун; заявитель Белорус. гос. ун-т. – № a 20071526; заявл. 10.12.2007; опубл. 30.08.2009 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2009. – № 4. – С. 157-158.

37. Вычислительное устройство по модулю три: пат. 12201 Респ. Беларусь, МКИ G 06 F 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20071532; заявл. 12.12.2007; опубл. 30.08.2009 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2009. – № 4. – С. 158.

38. Вычислительное устройство унитарных кодов по модулю пять: пат. 12202 Респ. Беларусь, МКИ G 06 F 7/38 / Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20071633; заявл. 28.12.2007; опубл. 30.08.2009 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2009. – № 4. – С. 159.

39. Вычислительное устройство унитарных кодов по модулю три: пат. 12289 Респ. Беларусь, МКИ G 06 F 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20080210; заявл. 25.02.2008; опубл. 30.08.2009 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2009. – № 4. – С. 160.

40. Устройство для умножения унитарных кодов по модулю три: пат. 12448 Респ. Беларусь, МКИ G 06 F 7/00 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20080299; заявл. 14.03.2008; опубл. 30.10.2009 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2009. – № 5. – С. 132.

41. Вычислительное устройство для возведения в степень по модулю пять: пат. 12561 Респ. Беларусь, МКИ G 06 F 7/38 / П.Н. Бибило, Д.А. Городецкий; заявитель гос. нав. вуч. Аб. інст. прабл. інфырмат. НАН Беларусі – № a 20071056; заявл. 23.08.2007; опубл. 30.10.2009 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2009. – № 5. – С. 132.

42. Вычислительное устройство унитарных кодов по модулю три: пат. 12901 Респ. Беларусь, МКИ G 06 F 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20080458; заявл. 10.04.2008; опубл. 28.02.2009 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2010. – № 1. – С. 128-129.

43. Вычислительное устройство по модулю три: пат. 12977 Респ. Беларусь, МКИ G 06 F 7/00 / П.Н. Бибило, Д.А. Городецкий; заявитель гос. нав. вуч. Аб. інст. прабл. інфырмат. НАН Беларусі – № a 20071651; заявл. 29.12.2007; опубл. 30.04.2010 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2010. – № 2. – С. 136.

44. Сумматор унитарных кодов по модулю три: пат. 13247 Респ. Беларусь, МКИ G 06 F 7/00 / Д.А. Городецкий, А.М. Седун, В.П. Супрун; заявитель Белорус. гос. ун-т. – № a 20081321; заявл. 21.10.2008; опубл. 30.06.2010 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2010. – № 3. – С. 131-132.

45. Вычислительное устройство унитарных кодов по модулю три: пат. 13278 Респ. Беларусь, МКИ G 06 F 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20081173; заявл. 12.09.2008; опубл.

30.06.2010 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2010. – № 3. – С. 131.

46. Вычислительное устройство унитарных кодов по модулю три: пат. 13288 Респ. Беларусь, МКИ G 06 F 7/00 / Д.А. Городецкий, А.М. Седун, В.П. Супрун; заявитель Белорус. гос. ун-т. – № a 20080926; заявл. 15.07.2008; опубл. 30.06.2010 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2010. – № 3. – С. 129-130.

47. Вычислительное устройство унитарных кодов по модулю три: пат. 13307 Респ. Беларусь, МКИ G 06 F 7/38 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20081608; заявл. 15.12.2008; опубл. 30.06.2010 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2010. – № 3. – С. 132.

48. Устройство для умножения унитарных кодов по модулю пять: пат. 13493 Респ. Беларусь, МКИ G 06 F 7/38 / Д.А. Городецкий, А.М. Седун, В.П. Супрун; заявитель Белорус. гос. ун-т. – № a 20081463; заявл. 19.11.2008; опубл. 30.08.2010 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2010. – № 4. – С. 147.

49. Сумматор унитарных кодов по модулю пять: пат. 13821 Респ. Беларусь, МКИ G 06 F 7/00 / В.П. Супрун, Д.А. Городецкий; заявитель Белорус. гос. ун-т. – № a 20090059; заявл. 19.01.2009; опубл. 30.12.2010 // Афіцыйны бюл. / Нац. цэнтр інтэлектуал. уласнасці. – 2010. – № 6. – С. 125-126.

РЭЗЮМЭ

Гарадзецкі Даніла Андрэевіч

МАТЭМАТЫЧНЫЯ МАДЭЛІ І МЕТАДЫ СІНТАЗУ ВЫЛІЧАЛЬНЫХ ПРЫЛАД МАДУЛЯРНАЙ АРЫФМЕТЫКІ

Ключавыя словы: мадулярная арыфметыка, лагічная схема, мадулярны суматар, мадулярны памнажальнік, сіметрычная булева функцыя, парогавая булева функцыя.

Мэтай працы з'яўляецца распрацоўка матэматычных мадэляў і метадаў сінтэзу аднаўзроўневых і двухузроўневых лагічных схем вылічальных прылад, якія рэалізуюць арыфметычныя аперацыі мадулярнай арыфметыкі.

Прапанаваны матэматычныя мадэлі і метад сінтэзу:

– двухузроўневых лагічных схем мадулярных суматараў у пазіцыйных кодах для адвольнага ліку аперандаў і значэння модуля;

– аднаўзроўневых лагічных схем мадулярных суматараў ва ўнітарных кодах для двух аперандаў і адвольнага значэння модуля;

– двухузроўневых лагічных схем мадулярных суматараў ва ўнітарных кодах для адвольнага ліку аперандаў і значэння модуля;

– аднаўзроўневых лагічных схем мадулярных памнажальнікаў ва ўнітарных кодах для двух аперандаў і адвольнага значэння модуля.

Прапанаваны метад сінтэзу лагічных схем вылічальных прылад мадулярнай арыфметыкі, якія рэалізуюць розныя суперпазіцыі мадулярных аперацый (аперацый складання, множання і ўзвядзення ў ступень).

Прапанаваны новыя аналітычныя прадстаўленні сіметрычных булевых функцый.

Прыведзены лагічныя схемы, сінтэзаваныя з дапамогай распрацаваных метадаў, і лагічныя схема прылады, прызначанай для распазнання юнатных (аднародных) булявых функцый.

Эфектыўнасць і сусветная навізна лагічных схем мадулярнай арыфметыкі, распрацаваных у рамках дысертацыйнай работы, пацверджана 30 Патэнтамі на вынаходства Рэспублікі Беларусь.

Праводзяцца эксперыментальныя даследаванні VHDL-апісанняў элементаў і прылад мадулярнай арыфметыкі, атрыманых на аснове распрацаваных матэматычных мадэляў і метадаў сінтэзу. Прапанаваны VHDL-апісанні мадулярных суматараў.

РЕЗЮМЕ

Городецкий Данила Андреевич

МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ СИНТЕЗА ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВ МОДУЛЯРНОЙ АРИФМЕТИКИ

Ключевые слова: модулярная арифметика, логическая схема, модулярный сумматор, модулярный умножитель, симметрическая булева функция, пороговая булева функция.

Целью работы является разработка математических моделей и методов синтеза одноуровневых и двухуровневых логических схем вычислительных устройств, реализующих арифметические операции модулярной арифметики.

Предложены математические модели и метод синтеза:

– двухуровневых логических схем модулярных сумматоров в позиционных кодах для произвольного числа операндов и значения модуля;

– одноуровневых логических схем модулярных сумматоров в унитарных кодах для двух операндов и произвольного значения модуля;

– двухуровневых логических схем модулярных сумматоров в унитарных кодах для произвольного числа операндов и значения модуля;

– одноуровневых логических схем модулярных умножителей в унитарных кодах для двух операндов и произвольного значения модуля.

Предложен метод синтеза логических схем вычислительных устройств модулярной арифметики, реализующих различные суперпозиции модулярных операций (операций сложения, умножения и возведения в степень).

Предложены новые аналитические представления бисимметрических булевых функций.

Приведены логические схемы, синтезированные с помощью разработанных методов, и логическая схема устройства, предназначенного для распознавания юнатных (однородных) булевых функций.

Эффективность и мировая новизна логических схем модулярной арифметики, разработанных в рамках диссертационной работы, подтверждена 30 Патентами на изобретение Республики Беларусь.

Проводятся экспериментальные исследования VHDL-описаний элементов и устройств модулярной арифметики, полученных на основе разработанных математических моделей и методов синтеза. Предложены VHDL-описания модулярных сумматоров.

SUMMARY

Gorodetsky Danila Andreyavich

MATHEMATICAL MODELS AND SYNTHESIS METHODS OF COMPUTING DEVICES IN MODULAR ARITHMETIC

Keywords: modular arithmetic, logical scheme, modular summator, modular multiplier, symmetric Boolean function, threshold Boolean function.

The purpose of the dissertation is development of mathematical models and methods for synthesis of one- and two-level logical schemes for computational devices, which are realizing the arithmetical operations in modular arithmetic.

The mathematical models and the method of synthesis are proposed for:

– two-level logical schemes of modular summators in position codes for arbitrary number of operands and arbitrary value of module;

– one-level logical schemes of modular summators in unitary codes for two operands and arbitrary value of module;

– two-level logical schemes of modular summators in unitary codes for arbitrary number of operands and arbitrary value of module;

– one-level logical schemes of modular multipliers in unitary codes for two operands and arbitrary value of module.

A method for synthesis of logical schemes realizing various superpositions of main arithmetic operations (operands of sum, multiplication and involution) in modular arithmetic has been proposed.

New analytical representations of bisymmetrical Boolean functions have been proposed.

Logical schemes synthesized by the means of the developed methods are considered along with the logical scheme of device developed for recognition of unite (homogeneous) Boolean functions.

Efficiency and worldwide novelty of logical schemes in modular arithmetic developed upon the dissertation bounds have been confirmed by awarding 30 patents for inventions of The Republic of Belarus.

The experimental research of VHDL-descriptions of elements and devices in modular arithmetic designed on the basic of the developed mathematical models and synthesis methods have been considered. VHDL-descriptions of modular summators have been proposed.

Научное издание

ГОРОДЕЦКИЙ Данила Андреевич

МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ СИНТЕЗА ВЫЧИСЛИТЕЛЬНЫХ УСТРОЙСТВ МОДУЛЯРНОЙ АРИФМЕТИКИ

Специальность 05.13.05 – «Элементы и устройства вычислительной техники и систем управления»

Автореферат диссертации на соискание ученой степени кандидата технических наук

Подписано в печать 21.10.2011.	Формат 60x84 $^{1}/_{16}$.	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л. 1,86.
Уч.-изд. л. 1,6.	Тираж 60 экз.	Заказ 683.