На правах рукописи

ШАЛАГИН Сергей Викторович

МАРКОВСКИЕ АВТОМАТЫ НАД ПОЛЕМ ГАЛУА И ИХ МОДЕЛИРОВАНИЕ В БАЗИСЕ ПРОГРАММИРУЕМЫХ МАТРИЦ ЛОГИЧЕСКИХ ЭЛЕМЕНТОВ

05.13.18 Математическое моделирование, численные методы и комплексы программ

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени
кандидата технических наук

Казань – 2001

Работа выполнена в Казанском государственном техническом университете им. А.Н.Туполева (КАИ)

Научные руководители — доктор технических наук, профессор Захаров В.М.

Кандидат технических наук, доцент Нуруллин Ш.Р.

Официальные оппоненты — Доктор физико-математических наук, профессор Чугунов В.А.

Кандидат технических наук, доцент Якимов И.М.

Ведущая организация — Институт проблем информатики академии наук Республики Татарстан (г. Казань)

Защита состоится «23» ноября 2001 г. в 14[00] часов на заседании диссертационного совета Д 212.079.01 в Казанском государственном техническом университете им. А.Н. Туполева по адресу: 420111, г. Казань, ул. Карла Маркса, 10.

С диссертацией можно ознакомится в библиотеке университета

Автореферат разослан «17» октября 2001 г.

Ученый секретарь
диссертационного совета
д.ф-м.н., профессор — Н.Г. Данилаев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Известен ряд областей, где марковские последовательности широко используются при решении задач. К данным областям, в частности, относятся статистическое моделирование, распознавание образов, передача и защита информации в сетях ЭВМ. Для решения указанных задач необходимо вырабатывать широкий класс случайных последовательностей с заданными свойствами. В этом случае модели цепей Маркова часто используются в качестве базовых для построения различных вероятностных моделей автоматного типа.

Известны основополагающие работы ученых по теории моделирования марковских последовательностей и построению автоматных моделей генераторов цепей Маркова. Среди них - Анишин А.С., Альпин Ю.А., Бусленко Н.П., Бухараев Р.Г., Баканович Э.А., Гилл А., Гиоргадзе А.Х., Гладкий В.С., Глова В.И., Захаров В.М., Кемени Дж., Кирьянов Б.Ф., Кузнецов В.М., Летунов Ю.П., Лоренц А.А., Меньков А.В., Песошин В.А., Полляк Ю.Г., Поспелов Д.А., Романовский В.И., Салимов Ф.И., Столов Е.Л., Схиртладзе Р.Д., Хамитов Г.П., Ченцов В.М., Чирков М.К.

Несмотря на большое количество работ по данному направлению, задача построения автоматных моделей цепей Маркова (марковских автоматов) на основе теории конечных полей изучена недостаточно. Подход на основе теории полей Галуа позволяет синтезировать структурные модели генераторов конечных цепей Маркова (ЦМ), состоящие из однородных блоков. Оценки сложности и быстродействия для заданных блоков могут быть перенесены на всю структуру. Данная структура может быть реализована по современной технологии производства интегральных схем: в базисе программируемых матриц логических элементов (ПМЛЭ), имеющих однородную структуру, что делает реализацию генераторов ЦМ и на их основе различных вероятностных автоматных моделей более эффективной. При программной реализации ЦМ открывается возможность использовать модулярную и полиномиальную арифметику. Особый интерес представляют поля Галуа $GF(2^n)$. Вычисления в $GF(2^n)$ обладают определенными достоинствами: алгоритмы вычислений в $GF(2^n)$ допускают параллельную реализацию, дают возможность производить потоковые преобразования над n-мерными векторами; для данного поля обычно применяется в качестве модуля такой многочлен, который обеспечивает более простую реализацию быстрого умножения с приведением по модулю. Для приложений большое значение имеет задача синтеза устройств с перестраиваемой структурой. Эта задача может быть эффективно решена в базисе ПМЛЭ. В связи с отмеченным выше актуальна задача исследования возможности и эффективности построения марковских автоматов (МА) в полях Галуа и разработка методов анализа степени соответствия получаемых структур структуре программируемых однородных вычислительных сред. Решению данной задачи посвящена настоящая диссертация.

Цель работы: разработка комплекса моделей, методов, алгоритмов, методик и программных средств для построения и моделирования марковских автоматов над полем Галуа в однородных вычислительных средах класса программируемых матриц логических элементов.

Достижение поставленной цели требует решения следующих задач:

- разработка математической модели представления марковских автоматов над полем Галуа $GF(2^n)$;
- разработка структурных моделей генераторов ЦМ над полем $GF(2^n)$ и получение оценок их сложности;
- исследование адекватности структурных реализаций многочленов над полем $GF(2^n)$, задающих генераторы ЦМ, структуре ПМЛЭ, на основе компьютерного моделирования;
- разработка модели многопараметрического анализа множеств стохастических матриц методами кластер анализа с целью уменьшения объема исходных данных для моделирования ЦМ с заданными свойствами;
- разработка комплекса прикладных программ для анализа и синтеза марковских автоматов.

Работа поддержана грантом Российского фонда фундаментальных исследований № 99-01-00163 «Энтропийно-сложностные свойства дискретных вычислительных моделей» и программой «Университеты России», проект № 015-04-01-52 «Синтез и сложность детерминированных и вероятностных дискретных вычислительных моделей».

Методы исследований. Для решения поставленных задач использованы методы теории вероятностей и математической статистики, теории вероятностных автоматов, теории чисел, аппарат конечных полей, линейной алгебры и дискретной математики, методы многомерной классификации, программные интегральные системы моделирования.

Научная новизна работы

- Дана постановка задачи построения марковских автоматов над полем Галуа. Введено понятие «полиномиальная модель однородной конечной простой цепи Маркова» над полем $GF(2^n)$. Установлена взаимосвязь ЦМ и полиномов над полем Галуа. Предложен метод и разработаны алгоритмы и методика синтеза марковских автоматов в виде суперпозиции полиномиальных функций над полем Галуа. Предложены и разработаны альтернативные структурные реализации генераторов ЦМ на основе полиномиальных функций над полем $GF(2^n)$, получены их сложностные и временные оценки.

- Разработаны алгоритмы минимизации количества ненулевых коэффициентов полиномиальной функции над полем $GF(2^n)$ и метод представления генератора дискретной случайной величины (ДСВ) полиномиальными функциями над полем Галуа.
- Получены оценки сложности полиномиальных моделей ЦМ в базисе программируемых матриц логических элементов.
- Дана постановка задачи классификации стохастических эргодических матриц методами многомерной математической статистики и предложена методика классификации.
- Дано обобщение результатов решения задачи полиномиального представления марковских моделей на постановку задачи синтеза автономных вероятностных автоматов с выходом.

Достоверность полученных результатов определяется следующим. Разработанные математические и структурные модели обоснованы доказательством соответствующих утверждений. Данные подтверждаются математическим моделированием с использованием современных компьютерных технологий.

Практическая значимость. Предложенная полиномиальная модель марковского автомата над полем Галуа расширяет область применения модулярной и полиномиальной арифметик на задачи моделирования случайных процессов. Полученные оценки аппаратных затрат, представленные описания алгоритмов и программ дают разработчикам возможность их непосредственного использования при моделировании и проектировании специализированных автоматных моделей по современной технологии ПМЛЭ. Предложенный метод представления марковских моделей полиномиальными функциями над полем Галуа может быть применён для решения задач синтеза более широкого класса вероятностных автоматных моделей. Разработанная методика многопараметрической классификации стохастических матриц позволяет получать новые их характеристики, которые могут быть использованы для представления класса марковских моделей одной полиномиальной функцией над полем Галуа и соответственно - для уменьшения объема исходных данных при моделировании цепей Маркова.

Результаты использованы в НИР за 2000г. по гранту РФФИ № 99-01-00163 «Энтропийно-сложностные свойства дискретных вычислительных моделей» и по проекту № 015-04-01-52 «Синтез и сложность детерминированных и вероятностных дискретных вычислительных моделей» программы «Университеты России», в ФНПЦ «Радиоэлектроника» (г. Казань), в центре новейших информационных технологий (ЦНИТ) РТ (г. Казань), в ГИБДД МВД Республики Татарстан (г. Казань) и

в учебном процессе кафедры ЭВМ Казанского государственного технического университета.

На защиту выносятся следующие результаты, полученные лично:

- полиномиальная модель марковского автомата над полем Галуа $GF(2^n)$, метод построения структурных моделей марковских автоматов в виде суперпозиции полиномиальных функций в полях Галуа, однородные схемы генераторов ЦМ;
- алгоритм минимизации количества ненулевых коэффициентов полиномиальной функции, определенной в поле Галуа, метод реализации генератора дискретной случайной величины полиномиальными функциями над полем Галуа;
- оценки сложности структурных моделей умножителей над полем Галуа и методика анализа их адекватности логической структуре ПМЛЭ;
- модель и методика многопараметрического анализа марковских моделей методами кластерного анализа;
- комплекс прикладных программ для реализации алгоритмов синтеза и анализа марковских автоматов.

Апробация работы. Основные положения и результаты докладывались и обсуждались на III-й Республиканской научно-технической конференции молодых учёных и специалистов (Казань, 1997г.); Всероссийских студенческих Туполевских чтениях «Актуальные проблемы авиастроения» (Казань, 1998г.); I-й Всероссийской научно-технической конференции «Компьютерные технологии в науке, проектировании и производстве» (Нижний Новгород, 1999г.); III-ем Всероссийском семинаре «Теория сеточных методов для нелинейных краевых задач» (Казань, 2000г.); Всероссийской научно-технической конференции «Туполевские чтения студентов» (Казань, 2000г.); Всероссийской научно-методической конференции «Интеграция образования, науки и производства - главный фактор повышения эффективности инженерного образования» (Казань, 2000г.); Итоговой научной конференции Казанского государственного университета (Казань, 2001г.); VII-м Международном семинаре «Дискретная математика и её приложения» (Москва, 2001г.), городском семинаре «Методы моделирования» (Казань, 2001г.), ряде семинаров кафедры Теоретической кибернетики Казанского государственного университета (Казань, 2001г.).

Публикации. Содержание диссертации опубликовано в 23 работах, включая 7 статей, 15 тезисов и 1 учебное пособие.

Структура и объём диссертации. Диссертационная работа изложена на 175 страницах машинописного текста, содержит 55 рисунков и 25 таблиц, состоит из введения, пяти глав, заключения и списка литературы из 134 наименований и двух приложений на 11 страницах.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертации, формируются цель и задачи исследования, приводится перечень основных результатов, выносимых на защиту. Дана структура диссертации.

В первой главе «Базовые определения и понятия» рассмотрены автоматные марковские модели (АММ), задающие генераторы ЦМ. В качестве базовой модели определен марковский автомат, задаваемый системой $A=(S,P)$, где $S=\{s_1,s_2,\ldots,s_m\}$ - конечное множество состояний автомата, P - стохастическая матрица (СМ) размера m, задающая функцию переходов автомата. Содержатся необходимые сведения из аппарата полей Галуа. Рассмотрены ПМЛЭ, а также специализированная САПР: XACT - Xilinx Advanced CAD Technology, позволяющая моделировать схемы вычислителей в полях Галуа и используемая для оценки адекватности указанных вычислителей структуре ПМЛЭ. Кратко описаны методы кластерного (КА), дискриминантного (ДА) и факторного анализа (ФА), а также «Интегрированная система STATISTICA 5.0», реализующая данные методы с целью многомерной классификации множества стохастических матриц, задающих марковские модели. Показаны взаимосвязь решаемых задач и подходы к их решению.

Во второй главе «Синтез структур марковских моделей над полем Галуа» разработаны математические и структурные модели генераторов ЦМ над полем Галуа. Показана принципиальная возможность полиномиального представления над полем $GF(2^n)$ модели ЦМ. Результат обоснован теоремой 2.1. Обозначим как $\hat{\mu}$ дискретную случайную величину вида $\hat{\mu}=\begin{pmatrix}\mu_1, & \mu_2, & \ldots, & \mu_l\\ p_1, & p_2, & \ldots, & p_l\end{pmatrix}$, где μ_i, $i=\overline{1,l}$, значения $\hat{\mu}$ и p_i - их вероятности, $0\le p_i\le 1$, $\sum_{i=1}^{l} p_i=1$. Стохастическнй вектор $(p_1,p_2,\ldots,p_l)$ обозначим символом $\overline{P}$.

Зададим конечную однородную цепь Маркова (ЦМ) системой

$$P_{(m)}=(S,P,\pi_0), \tag{1}$$

где $S=\{s_1,s_2,\ldots,s_m\}$ - множество состояний ЦМ, P - стохастическая матрица размера m определяет закон ЦМ, π_0 - m-мерный стохастический вектор, определяющий начальное распределение вероятностей состояний ЦМ. Пусть $G=GF(2^n)$. Введём в рассмотрение отображение $\varphi: G\times G\to G$ как многочлен $f(x,q)$ над этим полем:

$$f(x,q)=\sum_{i,j=0}^{r} a_{ij}x^i q^j,\ r=2^n-1,\ x,q,a_{ij}\in G. \tag{2}$$

Теорема 2.1 (синтеза). Для заданной системы (S, P, π_0) можно указать случайную величину $\hat{\mu}$ и полиномиальную функцию (2) степени $r \geq l$, $l \leq (m^2 - m + 1)$, со случайным начальным значением одной из переменных и коэффициентами $a_{ij} \in G$ такими, что случайная величина $\hat{\mu}$ может быть преобразована функцией (2) в заданную ЦМ значений функции.

Следствие из теоремы 2.1: задание ЦМ в виде системы

$$(\hat{\mu}, f(x,q), \pi_0), \tag{3}$$

где $f(x,q)$ - полиномиальная функция (ПФ) вида (2), эквивалентно заданию системы (1).

Система (3) определена в работе как полиномиальная модель (ПМ) цепи Маркова.

Справедливо и обратное:

Теорема 2.2 (анализа). Пусть заданы $f(x,q) = \sum_{i,j=0}^{r} a_{ij} x^i q^j$, $r = 2^n - 1$, $a_{ij}, x, q \in G$ с множеством $\{x_i\}$, $i = \overline{1,l}$ значений переменной x и множеством $\{q_j\}$, $j = \overline{1,m}$ значений переменной q, случайная величина $\hat{\mu}$ с множеством значений $\{x_i\}$ и со стохастическим вектором $\overline{P}$ и вектор π_0. Тогда последовательность вычисленных значений полинома (2) является реализацией простой однородной ЦМ с множеством состояний $\{q_j\}$, описываемой стохастической матрицей P размера $|\{q_j\}|$, элементы которой однозначно определяются вектором $\overline{P}$ и полиномом (2).

Теоремы 2.1 и 2.2 устанавливают взаимосвязь стохастических матриц и полиномиальных функций над полем Галуа. На их основе даны методы перехода от (1) к (3) и от (3) к (1).

Рассмотрено представление ПФ $f(x,q)$ на уровне структурной модели и предложена реализация на её основе генератора ЦМ по схеме, изображенной на рис. 1, где блок 1 - генератор ДСВ $\hat{\mu}$, значения которой совпадают со значениями переменной x, блок 2 выполняет функцию $f(x,q)$, коэффициенты которой a_i, $i = \overline{0,r}$ поступают из памяти (блок 4), блок 3 синхронизирует итерационный процесс вычисления значения q. Пара переменных (x,q) обозначена символом z. Возможности генерации ЦМ схемой на рис. 1 определяются следующими положениями, вытекающими из теорем 2.1 и 2.2:

1) если модель (3) задана на основе системы (1), то последовательность значений q есть ЦМ с законом, описываемым заданной СМ P;

2) если модель (3) задана непосредственно парой ($f(x,q)$, $\hat{\mu}$), в соответствии с ограничениями, определяемыми теоремой 2.2, то последовательность значений q есть ЦМ, закон которой однозначно определяется по исходным данным (ДСВ $\hat{\mu}$ и полиномом относительно z, обозначенным как $\delta'(z)$);

3) используя в модели (3) в качестве исходных данных различные стохастические векторы $\overline{P}$ или меняя коэффициенты a_i, $i=\overline{0,r}$, полинома $\delta'(z)$, или меняя одновременно стохастический вектор и коэффициенты ПФ $\delta'(z)$, можно с помощью схемы получать различные семейства простых конечных ЦМ.

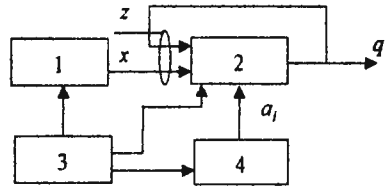

Рис. 1. Структурная модель генератора цепи Маркова

Решена задача структурной реализации $f(x,q)$ для блока 2 на рис. 1. Пусть значения $f(x,q)$ и её аргументов x и q определены в поле $GF(2^n)$ и она представлена в виде отображения $L(z)$: $GF(2^{2n}) \to GF(2^{2n})$. При этом

$$L(z)=z',\ z,z' \in GF(2^{2n}),\ z=(x,q)^T,\ z'=(x',q')^T. \qquad (4)$$

В результате (4), эквивалентное $f(x,q)$, представляется ПФ от одной переменной $L(z)$. Значение $f(x,q)$ отображается посредством n двоичных разрядов $2n$-разрядной величины $z' \in GF(2^{2n})$, обозначенных в (4) как q'. Другая половина разрядов z' - x' - может принимать произвольные значения.

Решена задача структурного представления ПФ $f(x,q)$ (и эквивалентной ей ПФ $L(z)$) - параллельной, систолической векторной, систолической и последовательностной структурами. Приведены оценки сложности и времени вычисления значения ПФ для предложенных структур блока 2 схемы на рис. 1. Оценки сложности определены по числу схем, реализующих операции умножения и сложения над полем Галуа.

Предложен алгоритм[1] минимизации ПМ $f(x,q)$ в случае её представления в виде (4) над полем $GF(2^{2n})$ путем уменьшения количества блоков Π_i,

[1] Алгоритм предложен на основе метода минимизации структуры полиномиальной функции, развитого в работах Столова Е.Л. и Нурутдинова Ш.Р. (1988).

$i = \overline{0, r-1}$, $r = 2^{2n} - 1$. Решение задачи - в увеличении числа нулевых коэффициентов $L(u)$. Алгоритм состоит из 10 процедур.

1. Ввод элементов множеств входных сигналов (X) мощностью b и внутренних состояний (Q) размерности d, а также отображения $q' = \delta(x, q)$.
2. Кодирование элементов множеств X, Q элементами поля $GF(2^p)$.
3. Составление исходной таблицы соответствий $q' = \delta(x, q)$, где $q, q', x \in GF(2^p)$.
4. Построение матрицы $\mathbf{Z}$, имеющей структуру вида

$$\mathbf{Z} = \begin{pmatrix} t_{00} & t_{01} & \cdots & t_{0(d-1)} & \sigma_{00} & \cdots & \sigma_{0(b-1)} \\ t_{10} & t_{11} & \cdots & t_{1(d-1)} & \sigma_{10} & \cdots & \sigma_{1(b-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ t_{r0} & t_{r1} & \cdots & t_{r(d-1)} & \sigma_{r0} & \cdots & \sigma_{r(b-1)} \end{pmatrix}, \; r = 2^{2n} - 1,$$

с целью построения системы уравнений $A = C^{-1}\mathbf{Z}$, где A - матрица коэффициентов минимального многочлена, а C^{-1} имеет вид

$$C^{-1} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \xi^{r-1} & \cdots & \xi^{i(r-1) \bmod (r)} & \xi \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \xi^{2} & \cdots & \xi^{2i \bmod (r)} & \xi^{r-2} \\ 0 & 1 & \xi & \cdots & \xi^{i} & \xi^{r-1} \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{pmatrix}, \quad 1 \le i \le r-1,$$

где ξ - примитивный элемент поля $GF(2^p)$.

5. Разбиение матрицы $\mathbf{Z}$ на T_i, D_j, где

$$T_i = \begin{pmatrix} t_{0i} \\ t_{1i} \\ \cdots \\ t_{ri} \end{pmatrix}, \; i = \overline{0, d-1}. \qquad D_j = \begin{pmatrix} \sigma_{0j} \\ \sigma_{1j} \\ \cdots \\ \sigma_{rj} \end{pmatrix}, \; j = \overline{0, b-1}, \; d + b = p.$$

6. Разбиение матрицы вида C^{-1} на составляющие $C_0, C_1, \ldots, C_{p-1}$. Здесь C^{-1} представлена выражением $C^{-1} = C_0\xi^0 + C_1\xi + \ldots + C_{p-1}\xi^{p-1}$
7. Построение системы уравнений $A = C^{-1}\mathbf{Z}$.
8. Исключение противоречивых и одинаковых уравнений из системы.
9. Решение системы уравнений.
10. Вывод результатов п. 3 и коэффициентов минимального многочлена.

Разработана программа, реализующая данный алгоритм, в которой (см. процедуру 8) предложен диалоговый подход к решению системы вида $A = C^{-1}\mathbf{Z}$. С целью описания работы программы, рассмотрим отображение $\delta'(z) = z'$, где $z = (x, q)^T$, $z' = (x', q')^T$. Вектор z' содержит компоненту x', которая в дальнейших вычислениях

не участвует и может принимать произвольные значения. Следовательно, отображению δ можно поставить в соответствие не одно отображение δ', а их семейство - $\Delta:(x,q)^T \to (x',q')^T$, где $x \in X$, $q,q' \in Q$ и $\forall x' \in GF(2^n)$. Δ содержит 2^n отображений - по одному для каждого x'. Цель работы алгоритма - выделение на множестве Δ такого отображения, для которого многочлен $\delta'(z)$ имеет минимальное число ненулевых коэффициентов.

Предложен алгоритм реализации n-разрядной ДСВ $\hat{\mu}$, заданной полиномом от одной переменной над полем $GF(2^n)$ вида $f_{\hat{\mu}}(x) = \sum_{i=0.}^{s-1} a_i x^i$, $s = 2^n$, посредством двух ПФ степени $s' = 2^m$ над полем $GF(2^m)$, $m = \frac{n}{2}$, на входы которых подаются равномерно распределённые m-разрядные ДСВ. Данный алгоритм может быть использован при синтезе генератора n-разрядной ДСВ $\hat{\mu}$ на основе k h-разрядных ДСВ для $n = k * h$, $k \geq 2$

Возможность представления ДСВ $\hat{\mu}$ полиномиальной функцией $f_{\hat{\mu}}$ позволяет описать схему на рис. 1 суперпозицией вида $f \bullet f_{\hat{\mu}}$.

Решена задача синтеза на основе базового элемента - полиномиальной модели вида (3) - более широкого класса вероятностных моделей автоматного типа - автономного вероятностного автомата с выходом.

В третьей главе «Компьютерное моделирование полиномиальных моделей в структуре ПМЛЭ» решается задача исследование адекватности отображения предложенных в главе 2 однородных структур, реализующих генераторы ЦМ на архитектуру ПМЛЭ (серия XC4000E), с помощью САПР «ХАСТ».

Определены в качестве базовых известные математические модели умножителей в поле Галуа, а также предложены математические модели умножителей, когда один из множителей - постоянный (умножителей на константу). Рассмотрена структурная модель умножителя - СУ/G_1 над полем $G_1 = GF(2^n)$ и предложена структурная схема СУ/G_2 над полем $G_2 = GF(2^{4k})$, $k = 1, 3, 5$. Для них рассчитаны оценки сложности по числу двухвходовых элементарных схем (ЭС). Рассматриваются сложностные аспекты реализации схем умножения (СУ) элементов в полях Галуа. Решены следующие задачи:

1) сравнительная оценка сложности СУ/G_1 и СУ/G_2 при реализации умножения элементов одинаковой размерности;
2) оценка реальных затрат при реализации СУ/G_1 и СУ/G_2 в базисе ПМЛЭ;
3) оценка доли ресурсов взаимосвязи, необходимых для реализации СУ на ПМЛЭ и минимизация этой доли;

4) сравнительная оценка быстродействия СУ/G_1 и СУ/G_2 при реализации операции умножения элементов одинаковой размерности;
5) оценка быстродействия одного уровня ЭС СУ, представленной теоретически на основе реальной логической структуры СУ, с целью оценки эффективности её реализации на ПМЛЭ по времени.

Для оценки сложности СУ, определим функцию $f(n)$ вида

$$f(n) = \sum_{i=1}^{2n-1}(s_i - 1), \tag{5}$$

где s_i - число единичных элементов в i-й строке матрицы $\hat{D}'$, получаемой из $\hat{D} = (I, A, \ldots, A^{n-1})^T$ путём вычёркивания повторных строк. $\hat{D}'$ содержит не более $(2n-1)$ различных строк (Нурутдинов Ш.Р., 1992).

Утверждение 3.1. Оценка сложности СУ/G_1, рассчитанная на основе числа ЭС, составляет

$$Q^{(1)} = n^2 + n(n-1) + f(n). \tag{6}$$

$f(n)$ вычислена согласно (5).

Структурная модель СУ/G_1 реализуется схемой, представленной на рис. 2. Блок КС включает в себя линейные комбинационные схемы, реализующие умножение вектора β на матрицы A^i, $i = \overline{0, n-1}$. Ключевые схемы AND управляются разрядами вектора $\alpha = (a_0, a_1, \ldots, a_{n-1})$. Сумматор Σ, осуществляет поразрядное суммирование по модулю 2 векторов, поступающих с выходов ключевых схем AND.

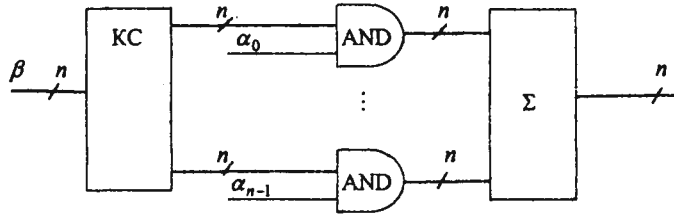

Рис. 2

Блок-схема структурной модели СУ/G_2, приведена на рис. 3. КС$_1$ и КС$_2$ представляют собой схемы сложения элементов в $GF(2^k)$. Новизна этой модели состоит в том, что с целью реализации операции умножения в $GF(2^k)$ предложено для построения блока MLT (блок умножителей) использовать СУ/G_1.

Утверждение 3.2. Оценка сложности СУ/G_2, измеряемая в ЭС, определяется величиной

$$Q^{(2)} = 9(k^2 + k(k-1) + f(k)) + 21k. \qquad (7)$$

В (7) $f(k)$ рассчитана на основе (5), а сложность элемента блока MLT (рис. 3) получена согласно (6).

Сравнение оценок (6) и (7) характеризуется коэффициентом вида

$$K = \begin{cases} \dfrac{Q^{(1)} - Q^{(2)}}{Q^{(1)}} \times 100\% & \text{при} \quad Q^{(1)} > Q^{(2)} \\ -\dfrac{Q^{(2)} - Q^{(1)}}{Q^{(2)}} \times 100\% & \text{при} \quad Q^{(2)} \le Q^{(1)} \end{cases} \qquad (8)$$

Значение K принадлежит интервалу [-100%, 100%]. Оценки сложности для случаев n = 4, 12, 20 и k = 1, 3, 5 приведены в табл. 1 Наблюдается рост K при увеличении размерности поля Галуа. Увеличение K для n = 12 и k = 3 (по сравнению со случаем для n = 20 и k = 5) связано с большим значением $f(n)$ в (6).

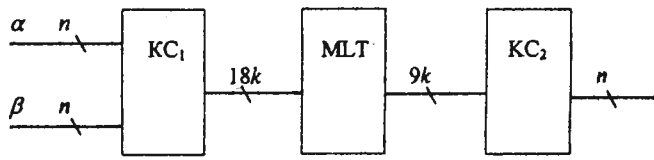

Рис. 3

Предложены верхние оценки сложности для умножителей на константу: (СУ/G_1)$_{const}$ и (СУ/G_2)$_{const}$. По аналогии со сложностью СУ, они составляют $\tilde{Q}^{(1)} = n(n-1) + f(n)$ и $\tilde{Q}^{(2)} = 9(k(k-1) + f(k)) + 16k$. Значения для $\tilde{Q}^{(1)}$ и $\tilde{Q}^{(2)}$ при n = 4, 12, 20 и k = 1, 3, 5 приведены в табл. 2. K_{const} вычисляется аналогично K согласно (8). Для n = 4, k = 1 значение $\tilde{Q}^{(1)}$ для (СУ/G_1)$_{const}$ уменьшилось за счет элементов AND, тогда как для (СУ/G_2)$_{const}$ их число не изменилось. Поэтому K_{const} - отрицательный. Увеличение K_{const} для n = 12 и k = 3 (по сравнению со случаем для n = 20 и k = 5) связано с ростом числа ЭС, необходимого для реализации КС в (СУ/G_1)$_{const}$.

Таблица 1

n	k	$Q^{(1)}$	$Q^{(2)}$	K
4	1	31	30	3%
12	3	317	216	32%
20	5	801	555	31%

Таблица 2

N	K	$\tilde{Q}^{(1)}$	$\tilde{Q}^{(2)}$	K_{const}
4	1	15	16	- 6%
12	3	173	120	31%
20	5	401	305	24%

Предложена методика оценки реальных аппаратных затрат СУ путем их компьютерного моделирования в базисе ПМЛЭ. Для отражения логической ёмкости (логических ресурсов) ПМЛЭ введено понятие логической единицы (ЛЕ) - базис ПМЛЭ. Оценки аппаратных затрат, измеряемых в ЛЕ, для СУ/G_1 и СУ/G_2 определяются соответственно на основе (6) и (7) по формулам:

$$Q_{1T} = \left]\frac{1}{8}Q^{(1)}\right[, \qquad Q_{2T} = \left]\frac{1}{8}Q^{(2)}\right[. \tag{9}$$

Обозначим генераторы, реализующие булевы функции от i, $i = 3, 4$, переменных, в составе конфигурируемых логических блоков (КЛБ) в структурной схеме ПМЛЭ, как ГФ(i), а количество ГФ(i), задействованных при реализации СУ - $N_{ГФ(i)}$.

Утверждение 3.3. Логическая емкость СУ, измеряемая количеством ГФ(i), $i = 3, 4$, составляет

$$Q_{ЛЕ} = Q_{КЛБ} = \left]\frac{1}{9}\left(4N_{ГФ(4)} + N_{ГФ(3)}\right)\right[. \tag{10}$$

Соотношение (10) характеризует эквивалентность реальных аппаратных затрат СУ, измеряемых в ГФ(i), оценкам сложности, выраженным в ЛЕ.

При оценке сложности СУ согласно (10) предполагается, что логическая ёмкость каждого КЛБ задействована в полном объёме. При реальном представлении СУ на ПМЛЭ, часть логических ресурсов тратиться на обеспечение взаимосвязи между КЛБ - на ресурсы взаимосвязи (РВ). Кроме того, внутри КЛБ может быть задействована лишь часть логических ресурсов. В результате, оценки реальных аппаратных затрат логических ресурсов ПМЛЭ для СУ, выше оценок, полученных теоретически. Q_{1T}, Q_{2T} есть нижние оценки сложности реализации соответствующих СУ. Оценки реальных затрат (10) с учетом РВ для СУ/G_1 и СУ/G_2, обозначим, соответственно, как Q_1 и Q_2. Сравнение Q_{iT} и Q_i, $i = 1, 2$, позволяет получить количественные оценки доли РВ, а, следовательно, и количественно оценить адекватность реализации СУ в базисе ПМЛЭ. Коэффициент вида

$$K_{PT} = \frac{Q_i - Q_{iT}}{Q_i} \times 100\%, \; i = 1, 2,$$

характеризует отношение реальных затрат СУ в базисе ПМЛЭ к теоретическим. Коэффициент K_{PT}, который принимает значения от 0 до 100%, будем называть критерием адекватности. Значение K_{PT} указывает, насколько адекватно СУ вписывается в однородную структуру ПМЛЭ. Увеличение значения K_{PT} характеризует увеличение доли РВ в общих затратах логических ресурсов. Q_{1T}, Q_1 и K_{PT} при $i = 1$ для СУ/G_1 приведены в табл. 3 ($n = 4, 12, 20$), а для СУ/G_2 ($k = 1, 3, 5$) - Q_{2T}, Q_2 и K_{PT}, при $i = 2$ - в табл. 4. Так, для СУ/G_2 при $k = 3$, доля РВ меньше, чем для остальных

СУ. Данные из табл. 3 и 4 позволяют сравнить сложность СУ/G_1 и СУ/G_2. Так, для $n = 12$ и $k = 3$ различие оценок Q_1 и Q_2 составляет 49%.

В результате проектировщик (пользователь САПР) получает возможность оценки доли неэффективно используемых аппаратных ресурсов ПМЛЭ при реализации СУ. На основе $K_{РТ}$ может быть выявлена потенциальная возможность минимизации сложности СУ, за счёт более полного использования ресурсов КЛБ.

Таблица 3

n	Q_{1T}	Q_1	$K_{РТ}$
4	4	5	20%
12	44	57	23%
20	100	124	19%

Таблица 4

k	Q_{2T}	Q_2	$K_{РТ}$
1	4	5	20%
3	27	29	7%
5	69	106	35%

Получены временные оценки и результаты моделирования СУ с учетом временных задержек ЭС в базисе ПМЛЭ.

Утверждение 3.4. Оценка времени выполнения операции умножения СУ/G_1 равна

$$T^1_{\otimes}(n) = \left(\left\lceil \log_2 (\max_i s_i) \right\rceil + \left\lceil \log_2 n \right\rceil + 1 \right) t_{ЭС}, \qquad (11)$$

где s_i - число «1» в i-й строке матрицы $\hat{D}'$, $t_{ЭС}$ - время задержки функционирования ЭС.

Оценка времени выполнения операции умножения для СУ/G_2 ($T^2_{\otimes}(n)$) вычисляется на основе (11) и имеет вид:

$$T^2_{\otimes}(n) = T^1_{\otimes}(k) + 5t_{ЭС}.$$

Реальные значения задержек для СУ/G_1 и СУ/G_2, полученные при использовании САПР, равны $\hat{T}_1$ и $\hat{T}_2$, соответственно, и приведены в табл. 5. Они определяют время задержки не только КЛБ, но и программируемых межсоединений внутри ПМЛЭ.

Таблица 5

n	K	T_1	T_2	$\hat{T}_1$ (нс)	$\hat{T}_2$ (нс)	$t^1_{ЭС}$ (нс)	$t^2_{ЭС}$ (нс)
4	1	4	6	18,6	17,6	4,64	2,93
12	3	8	9	29,8	27,1	3,73	3,01
20	5	8	11	36,5	43,5	4,56	3,96

Среднее время задержки одного уровня схемы для СУ, представленной теоретически на основе ЭС - $t^1_{ЭС}$ и $t^2_{ЭС}$ - при указанных значениях n и k находится как $t^i_{ЭС} = T_i / \hat{T}_i$, $i = \overline{1,2}$ (см. табл. 5). Значения $t^1_{ЭС}$ и $t^2_{ЭС}$ позволяют судить об эффективности реализации СУ в базисе ПМЛЭ по быстродействию; на основании этих значений

выведена закономерность: СУ/G_2 реализуется на ПМЛЭ более эффективно, чем СУ/G_1. Данный факт объясняется большей адекватностью структуры СУ/G_2 структуре ПМЛЭ, чем структуры СУ/G_1.

В четвёртой главе «Кластерный анализ марковских моделей» решены задачи многопараметрической классификации СМ P, задающих марковские модели, методами многомерной математической статистики - КА, ДА и ФА. При реализации семейства случайных последовательностей возникает вопрос хранения больших массивов исходных данных, характеризующих каждую из моделей генераторов заданного класса. Решение этой задачи особенно актуально при реализации генераторов ЦМ в перестраиваемых структурах на базе ПМЛЭ. Предложен подход сокращения объема данных, основанный на двух этапах. Этап 1- классификация моделей по их законам (по СМ): классификация СМ (объектов) на основании признаков, характеризующих различные их свойства методами кластерного анализа. Производится проверка адекватности классификации и информативность каждого из указанных признаков. Этап 2 - определение СМ - типичного представителя (типичную СМ) для каждого из полученных подклассов (кластеров). Среди основных решенных задач следующие:

1) задача типизации, когда для заданного множества объектов число кластеров не известно (классификация и определение типичного представителя группы);
2) задача определения структуры естественного (обусловленного классификационными признаками) расслоения множества объектов различных типов на классы;
3) задача кластеризации объектов различных типов при помощи количественных признаков;
4) задачи сравнительной оценки качества признаков, оценки качества и определения достоверности полученных кластерных решений.

Предложено объединение методов КА и ДА, что расширяет возможности анализа модели данных, приводит к коррекции результатов. Объекты для классификации - стохастические матрицы размерности $(m \times m)$ класса эргодических (ЭСМ), сгенерированы на основе программы, реализованной по схеме на рис. 1. Положительные элементы ЭСМ представлены с дискретностью $D = 0{,}5 * 10^{-5}$ в диапазоне $[D;\ 1\text{-}D]$. Основная цель данной главы - разработка методики решения отмеченных задач на основе КА, ДА и ФА, с использованием «Интегрированной системы STATISTICA 5.0». Для этого в качестве примера классифицируемого множества объектов выбран класс $A = П \cup Д \cup ЛП$ в состав которого входят два подкласса ЭСМ, сходные между собой и подкласс, существенно отличающийся от остальных. Объем выборки для A составляет 900 ЭСМ, по 300 - для каждого подкласса. $П$ - положительные ЭСМ, элементы которых удовлетворяют условию $p_{ij} > 0$, $i, j = \overline{1, m}$. $Д$ - дважды стохасти-

ческие матрицы, удовлетворяющие ограничениям вида: $\sum_{j=1}^{m} p_{ij} = 1,\ p_{ij} > 0,\ i,j = \overline{1,m}$.

ЛП - матрицы, задающие локальные вероятностные переходы. При этом подклассы *П* и *Д* имеют сходство в том, что они содержат положительные матрицы (*Д* включён в состав *П*), а матрицы из подкласса *ЛП* характеризуются значительным количеством нулей. Тем самым *ЛП* существенно отличается от *П* и *Д*.

При решении задач классификации отмеченного класса объектов рассматриваются следующие свойства *P*:

1) асимптотические (мультипликативные) свойства матрицы *P*, определяемые структурой матрицы, получаемой возведением *P* в степень *t* (*t*- натуральное число) при $t \to \infty$;
2) уровень, характеризуемый мерой отклонения положительных элементов матрицы *P* от нуля;
3) рассеяние (разброс) элементов в строках и столбцах матрицы *P* относительно средних;
4) энтропия матрицы *P*, характеризующая отклонение матрицы *P* от матрицы, в которой элементы $p_{ij} = 1/m,\ i,j = \overline{1,m}$.

Разработано множество признаков *V*, отражающее данные свойства. Так, свойство 1) отображают 4 признака, вычисленные по формулам вида:

$c_1 = M_a = \sum_{j=1}^{m} a_j j,\ c_2 = D_a = \sum_{j=1}^{m} (j - M_a)^2 a_j$, где $a = (a_1, a_2, ..., a_m)$ - предельный вектор для *P*. $c_3 = \sum_{j=1}^{m} \beta_j,\ c_4 = \sqrt{\sum_{j=1}^{m} (\beta_j)^2}$, где $\beta = (\beta_1, \beta_2, ..., \beta_m)$ есть вектор предельных дисперсий для времён пребывания в каждом состоянии ЦМ, заданной матрицей *P*. Свойства 2) и 3) характеризуют признаки c_5, c_6 и c_7, c_8, c_9 соответственно, которые вычисляются по формулам вида:

$c_5 = m \max_{ij} | p_{ij} |,\ c_6 = \sqrt{\sum_{i=1}^{m} \sum_{j=1}^{m} | p_{ij} |^2},\ c_7 = (m)^{-1} \sum_{i=1}^{m} \sum_{j=1}^{m} (j - M_i)^2 p_{ij}$,

где $M_i = \sum_{j=1}^{m} j p_{ij},\ c_8 = \sum_{i=1}^{m} \sum_{j=1}^{m} (p_{ij} - \bar{p})^2$, где $\bar{p} = 1/m,\ c_9 = \sum_{j=1}^{m} \sum_{i=1}^{m} (p_{ji} - \bar{p}_j)^2$,

где $\bar{p}_j = (m)^{-1} \sum_{i=1}^{m} p_{ij}$. Энтропия вычисляется как $c_{10} = -\sum_{i=1}^{m} \sum_{j=1}^{m} a_i p_{ij} \log_2 (p_{ij})$.

Описание данных для проведения многомерного анализа представлено в виде таблицы, строки которой соответствуют объектам из *A*, а столбцы - признакам (переменным) из *V*. Приведена схема КА. Ставятся и решаются следующие задачи:

1. Выявление кластерной структуры для объединения множеств объектов. Характеристика полученной кластерной структуры представлена в табл. 6, где показано: подкласс *ЛП* разделен на два кластера (№1 и №4), при этом *ЛП* выделяется в отдельные кластеры, а *П* и *Д* частично пересекаются; наибольшее Евклидово расстояние наблюдается между *ЛП* из кластера №1 и *П* (кластер №2). Ближе всего находятся *ЛП* из кластера №4 и ЭСМ *Д* и *П* из кластера №3.
2. Проведение сравнительной оценки качества признаков.
3. Задача типизации - определение типичного представителя для каждого кластера.

Таблица 6

	Состав кластеров (%%)			No. 1	No. 2	No. 3	No. 4
	П	Д	ЛП				
No. 1	0	0	7	0	1,81	1,80	1,24
No. 2	50	0	0	1,81	0	1,27	0,96
No. 3	50	99	0	1,80	1,27	0	0,92
No. 4	0	1	93	1,24	0,96	0,92	0

Решена задача оценки обоснованности (достоверности) результатов КА при использовании ДА.

Решена также задача оценки зависимости (корреляции) внутри множества признаков *V* при использовании ФА, алгоритм решения которой включает три этапа. Этап 1 - определение корреляции между признаками. Этап 2 - определение числа факторов и их интерпретация. Этап 3 - выводы по факторному решению.

В главе предложена методика решения задачи многопараметрического анализа ЭСМ на основе кластерного анализа с использованием методов ДА и ФА.

В пятой главе «Комплекс прикладных программ для реализации алгоритмов синтеза и анализа полиномиальных моделей» разработаны два пакета прикладных программ для реализации алгоритмов синтеза и анализа полиномиальных моделей, а также методика генерации таблицы «Объект-признак» *T*, содержащей данные для многомерного статистического анализа марковских моделей.

Первый пакет служит для анализа алгоритма минимизации числа ненулевых коэффициентов полиномиальных моделей вида (2) (ПМ) в зависимости от соответствующих им подклассов КДА. Второй пакет включает в себя программу разложения СМ *P*, задающей ПМ, на взвешенную сумму простых матриц, а также программы генерации ЦМ на основе СМ, задающей полиномиальную модель и получения укрупненной цепи Маркова на основе исходной ЦМ (при заданных ограничениях).

Разработанная методика генерации таблицы *T* реализуется посредством редактора электронных таблиц Microsoft Excel 97 и включает два этапа. На этапе 1 генерируется набор СМ, принадлежащих заданным подклассам - *П*, *Д* и *ЛП* (см. Главу

4). Этап 2 - вычисление на основе указанных СМ векторов значений - признаков из рабочего словаря *V*.

Указанные пакеты программ и методика использованы и апробированы при решении задач, поставленных в главах 2 и 4, а также прикладных задач: многомерной классификации и анализа последовательностей случайных чисел и разработки моделей данных для экспертных систем распознавания и диагностики.

В заключении сформулированы основные результаты диссертации.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Поставлена и решена задача синтеза МА в базисе полиномиальных функций над полем Галуа. Результатами решения являются: полиномиальная модель над полем $GF(2^n)$ конечной простой однородной цепи Маркова, теорема синтеза, задающая метод преобразования МА в полиномиальную модель и теорема анализа, обосновывающая обратное преобразование полиномиальной модели в МА. Полиномиальная модель устанавливает взаимосвязь стохастических матриц с полиномиальными функциями, что позволяет реализовать распараллеливание процесса обработки информации и реализовывать более адекватные структуры генераторов цепей Маркова в программируемых однородных вычислительных средах. Предложены альтернативные (по критериям сложности и быстродействия) структурные схемы - параллельного, систолического векторного, систолического и последовательностного типов - для реализации генераторов ЦМ в базисе полиномиальных функций.

2. Разработан алгоритм минимизации заданных полиномиальных функций на основе известного метода, а также предложен метод полиномиального представления ДСВ с заданным законом распределения над полем Галуа. Предложена структурная модель генератора ЦМ, основанная на преобразовании вида суперпозиция полиномиальных функций над полем Галуа. Показана возможность применения понятия «суперпозиция полиномиальных функций над полем Галуа» для построения автономных вероятностных автоматов с выходом, что позволяет расширить класс случайных последовательностей, генерируемых посредством полиномиальных функций, до класса функций конечных цепей Маркова. Совокупность полученных результатов дает методику синтеза марковских моделей автоматного типа в базисе полиномиальных функций над полем Галуа.

3. Предложены структурные модели схем умножения в поле Галуа (умножителей). Доказаны утверждения, определяющие теоретические оценки сложности и оценки реальных затрат при реализации умножителей в базисе ПМЛЭ, а также теоретические оценки времени выполнения операции умножения элементов поля Галуа. Предложена методика исследования адекватности структурных реализаций умножителей, задающих генераторы ЦМ, матричной архитектуре ПМЛЭ.

4. Разработана модель и соответствующая методика многопараметрического анализа стохастических матриц, задающих полиномиальную модель генераторов ЦМ, что позволяет решать задачу уменьшения объема исходных данных при моделировании семейств ЦМ.

5. Разработан комплекс прикладных программ для реализации алгоритмов синтеза и анализа полиномиальных моделей, задающих МА, с целью решения следующих задач: разложения стохастических матриц, задающих ПМ, на взвешенную сумму простых матриц, генерации ЦМ на основе заданной стохастической матрицы, вычисления укрупненной цепи Маркова, определения структуры полиномиальной модели на основе задающей ее СМ. Комплекс программ использован при решении прикладных задач в ряде организаций.

Основное содержание диссертации опубликовано в работах:

1. Шалагин С.В. Синтез генераторов тестов в базисе программируемых логических интегральных схем // Тезисы докладов «Актуальные проблемы авиастроения» VIII Всероссийские Туполевские чтения студентов - Казань, 1998. - С. 70.
2. Шалагин С.В. Система анализа и синтеза вероятностных сетей // Тезисы докладов «Актуальные проблемы авиастроения» VIII Всероссийские Туполевские чтения студентов - Казань, 1998. - С. 80.
3. Глова В.И., Захаров В.М., Песошин В.А., Шалагин С.В. Моделирование. Дискретные вероятностные модели. Учебное пособие. - Казань: Изд-во АБАК, 1998. - 50 с.
4. Захаров В.М., Шалагин С.В. Анализ стохастических сетей на основе модели поглощающей цепи Маркова // Тезисы докладов. Первая Всероссийская научно-техническая конф. «Компьютерные технологии в науке, проектировании и производстве». - Н.Новгород, 1999. - Ч. XVII.- С.3.
5. Шалагин С.В. Моделирование конечнозначных случайных последовательностей на линейных автоматах // Тезисы докладов. Международная молодёжная научная конференция «XXV Гагаринские чтения». - М.: Изд-во «Латмэс», 1999. - С. 179-180.
6. Захаров В.М., Соколов С.Ю., Шалагин С.В. К задаче синтеза вероятностных преобразователей информации в однородных вычислительных структурах // Тезисы докладов. 4-я Всероссийская научно-технич. конференция студентов, молодых учёных и специалистов «Новые информационные технологии в научных исследованиях и образовании» – Рязань, 1999. - С.78.
7. Бахарев А.Н. Захаров В.М. Песошин В.А. Шалагин С.В. Новые технологии автоматизированного проектирования цифровых устройств в учебном процессе // Тезисы докладов. Всероссийская научно-методическая конф. «Проблемы высшего технического образования». – Казань, 1999. – С. 144.

8. Глова В.И. Захаров В.М. Песошин В.А. Шалагин С.В. Моделирование вычислительных систем на вероятностных дискретных моделях // Тезисы докладов. Всероссийская научно-методическая конференция «Проблемы высшего технического образования». – Казань, 1999. – С. 160.
9. Шалагин С.В. К задаче анализа стохастических сетей на основе модели поглощающей цепи Маркова // Тезисы докладов. II Всероссийская научно-техническая конф. «Компьютерные технологии в науке, проектировании и производстве». - Н.Новгород, 2000. - Ч. V. - С. 16.
10. Фаттахов Н.Г. Шалагин С.В. К задаче аппаратно-программной реализации в однородных вычислительных структурах методов стохастической геометрии для распознавания образов // Тезисы докладов. II Всероссийская научно-техническая конф. «Компьютерные технологии в науке, проектировании и производстве». - Н.Новгород, 2000. - Ч.VI. - С. 30.
11. Нурутдинов Ш.Р., Шалагин С.В. Вычисление произведения элементов поля Галуа // Теория сеточных методов для нелинейных краевых задач. Материалы Третьего Всеросс. семинара. - Казань: Изд-во Казанского мат. общества, 2000. - С. 94 - 96.
12. Шалагин С.В. Кластерный анализ стохастических эргодических матриц. - Деп. в ВИНИТИ 31.10.00. № 2750 - В00. - 42 с.
13. Захаров В.М., Нурмеев Н.Н., Салимов Ф.И., Шалагин С.В. Классификация стохастических эргодических матриц методами кластерного и дискриминантного анализа // Сб. «Исследования по информатике». Вып. 2. Научно-практическое издание. Институт проблем информатики АН РТ. - Казань: Отечество, 2000. - С. 91-106.
14. Захаров В.М., Нурутдинов Ш.Р., Шалагин С.В. Синтез автономных вероятностных автоматов на основе полей Галуа // Сб. «Исследования по информатике». Вып. 2. Научно-практическое издание. Институт проблем информатики АН РТ. - Казань: Отечество, 2000. - С. 107-116.
15. Нурутдинов Ш.Р., Шалагин С.В. Минимизация количества элементов однородной вычислительной структуры // Сб. «Исследования по информатике». Вып. 2. Научно-практическое издание. Институт проблем информатики АН РТ. - Казань: Отечество, 2000. - С. 117-124.
16. Шалагин С.В. Синтез управляемых генераторов случайных кодов на программируемых логических интегральных схемах // Тезисы докладов второй Всероссийской. научно-технической конференции (Computer-Based Conference) «Информационные технологии в науке, проектировании и производстве». - Н.Новгород, 2000. - С. 16-17.
17. Захаров В.М., Нурмеев Н.Н., Салимов Ф.И., Шалагин С.В. Автоматизированный анализ стохастических эргодических матриц методами многомерной математи-

ческой статистики // Интеграция образования, науки и производства - главный фактор повышения эффективности инженерного образования: Всероссийская научно-методическая конференция. Тезисы докладов. - Казань: Изд-во Казанского гос. техн. ун-та, 2000. - С. 330.

18. Захаров В.М., Нурутдинов Ш.Р. Шалагин С.В. Синтез автоматов марковского типа в конечных полях Галуа // Интеграция образования, науки и производства - главный фактор повышения эффективности инженерного образования: Всероссийская научно-методическая конференция. Тезисы докладов. - Казань: Изд-во КГТУ, 2000. - С. 331.
19. Захаров В.М., Нурутдинов Ш.Р. Шалагин С.В. Построение модели умножителя в полях Галуа // Материалы VII Международного семинара «Дискретная математика и ее приложения». Часть I. - М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2001. - С. 62 - 65.
20. Захаров В.М., Нурмеев Н.Н., Салимов Ф.И., Шалагин С.В. Анализ стохастических матриц методами многомерной классификации // Материалы VII Международного семинара «Дискретная математика и ее приложения». Часть I. - М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2001. - С. 156 - 159.
21. Захаров В.М., Нурутдинов Ш.Р. Шалагин С.В. Аппаратная реализация умножения элементов поля Галуа на программируемых микросхемах архитектуры FPGA // Вестник Казанского государственного технического университета. - Казань: Изд-во КГТУ им. А.Н.Туполева, 2001. - №1. - С. 36-41.
22. Захаров В.М., Нурутдинов Ш.Р. Шалагин С.В. Представление стохастических матриц полиномиальными функциями над полем Галуа // Научно-практическая конф. по актуальным вопросам информатики, вычислительной техники и информационной безопасности. Тезисы докладов. - Казань: Изд-во Казан. гос. техн. ун-та, 2001. - С. 82.

Формат 60x84 1/16. Бумага газетная. Печать офсетная.
Печ. л. 1,25. Усл. печ. л. 1,16. Усл. кр.-отт. 1,16. Уч.-изд.л. 1,0.
Тираж 100. Заказ 6123.

Типография Издательства Казанского государственного технического университета
420111, Казань, К.Маркса, 10.

2-