На правах рукописи

ЭМИНОВ Булат Фаридович

МЕТОДЫ И АЛГОРИТМЫ ПОСТРОЕНИЯ И АНАЛИЗА ПОЛИНОМИАЛЬНЫХ ФУНКЦИЙ НАД КОНЕЧНЫМ ПОЛЕМ НА ОСНОВЕ СТОХАСТИЧЕСКИХ МАТРИЦ

05.13.18 - Математическое моделирование,
численные методы и комплексы программ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Казань - 2008

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

Научный руководитель: доктор технических наук, профессор Захаров Вячеслав Михайлович

Официальные оппоненты: доктор физико-математических наук, профессор Аблаев Фарид Мансурович

доктор технических наук, профессор Крашенинников Виктор Ростиславович

Ведущая организация: Новгородский государственный университет им. Ярослава Мудрого (г. Великий Новгород)

Защита состоится " 6" июня 2008 г. в 14 часов на заседании диссертационного совета Д 212.079.01 в Казанском государственном техническом университете им. А.Н. Туполева по адресу: 420111, г. Казань, ул. К.Маркса, 10.

С диссертацией можно ознакомиться в библиотеке Казанского государственного технического университета им. А.Н. Туполева.

Автореферет разослан "___" _____ 2008 г.

Ученый секретарь диссертационного совета, доктор физико-математических наук, профессор П.Г. Данилаев

0-770045

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. Одним из подходов моделирования цепей Маркова (ЦМ) и марковских функций является подход, использующий теорию конечных полей. Перспективность этого подхода определяется приложением функций конечных ЦМ, возрастающей сложностью вероятностных дискретных моделей и эффективностью арифметики конечных полей в задачах цифровой обработки информации. Аппарат конечных полей используется для решения задач синтеза вероятностных автоматов и генераторов случайных двоичных последовательностей, для моделирования случайных линейных зависимых процессов в конечном поле и некоторых типов ЦМ (Аблаев Ф.М., Бухараев Р.Г., Гавел Я., Кирьянов Б.Ф., Кознов Ф.В., Крашенинников В.Р., Кузнецов В.М., Латыпов Р.Х., Мансуров Р.М., Осмоловский С.А., Песошин В.А., Столов Е.Л., Taylor L.).

В работах Захарова В.М., Нурутдинова Ш.Р., Соколова С.Ю., Шалагина С.В. (2000-2006 г.г.) предложен подход моделирования дискретных случайных процессов на полиномиальных моделях, описываемых полиномиальными функциями над полем $GF(2^n)$. Полиномиальные функции рассматриваются как модели дискретных преобразователей цепей Маркова. Разработаны методы представления полиномиальными функциями над полем $GF(2^n)$ простых и сложных ЦМ и определенных функций однородных и неоднородных ЦМ. Задача представления решается как задача вычисления коэффициентов полиномов над полем $GF(2^n)$ на основе заданных стохастических матриц. Решена важная прикладная задача отображения полиномиальных моделей в однородные вычислительные среды, позволяющие реализовать параллельные алгоритмы вычисления и проводить потоковые преобразования над n-мерными векторами при моделировании дискретных случайных процессов. Однако, в этом направлении существуют недостаточно исследованные вопросы и нерешенные задачи, имеющие теоретическое и практическое значение.

Для дальнейшего развития и повышения эффективности методов моделирования дискретных случайных процессов в конечном поле актуальным является исследование вопросов, связанных с повышением точности полиномиальных моделей, определением их свойств и вероятностных характеристик, расширением класса случайных последовательностей, представляемых полиномиальными функциями над полем $GF(2^n)$ и конечным полем $GF(q_c)$ характеристики $q_c \geq 2$, с получением оценок порядка поля в зависимости от точности задания закона цепи Маркова и структуры стохастических матриц, а также ряд других вопросов, связанных с построением (вычислением коэффициентов) и анализом полиномиальных функций над конечным полем.

Объект исследования. Модели и аналитические методы моделирования случайных последовательностей над конечным полем.

Предмет исследования. Полиномиальные модели, порождающие функции цепей Маркова в конечном поле, свойства и характеристики этого класса моделей.

Научная задача. Разработка новых аналитических методов построения полиномиальных функций и анализа свойств полиномиальных функций, порождающих случайные последовательности в конечном поле на основе стохастических матриц (СМ), с учетом структурных свойств СМ и точности задания

переходных вероятностей.

Цель работы: развитие полиномиальных моделей, аналитических методов и построение эффективных методик для моделирования цепей Маркова и их функций в конечном поле.

Решение общей научной задачи и достижение поставленной цели связано с решением следующих задач.

1. Разработка метода и алгоритмов представления стохастических матриц полиномиальными функциями над полем GF(2^n). Определение оценок порядка поля GF(2^n) с учетом точности задания элементов стохастических матриц.

2. Разработка метода и алгоритмов моделирования расширенных цепей Маркова (РЦМ) полиномиальными функциями над полем GF(2^n). Определение порядка поля GF(2^n) с учетом структуры стохастической матрицы РЦМ.

3. Разработка метода представления неразложимых стохастических матриц с заданной точностью полиномами минимальной степени над конечным полем GF(q_c) характеристики $q_c \geq 2$.

4. Разработка метода вычисления характеристик полиномиальных моделей, предназначенных для получения случайных последовательностей из класса функций цепей Маркова.

5. Статистический анализ цепей Маркова по критерию линейной сложности последовательностей. Исследование взаимосвязи энтропии неразложимых стохастических матриц с линейной сложностью реализаций цепей Маркова.

6. Разработка комплекса методик и программ, реализующих предлагаемые методы и алгоритмы.

Методы исследований. Для решения поставленных задач использованы методы теории чисел, теории вероятностей, математической статистики, теории детерминированных и вероятностных автоматов, теории графов, аппарат конечных полей, линейной и полиномиальной алгебры, дискретной математики.

Научная новизна работы и значимость результатов.

- Новые метод и алгоритмы представления стохастических матриц с двоично-рациональными элементами полиномиальными функциями над полем GF(2^n), с учетом точности задания переходных вероятностей. Сформулированы и доказаны теоремы, обосновывающие метод.

- Новые метод и алгоритмы получения и отображения закона расширенных цепей Маркова в полиномиальную функцию над полем GF(2^n). Сформулированы и доказаны теоремы, обосновывающие метод.

- Новый метод представления стохастических матриц с заданной точностью и моделирования случайных последовательностей из класса неоднородных цепей Маркова полиномами минимальной степени над полем GF(q_c) характеристики $q_c \geq 2$. Доказана теорема, устанавливающая линейную связь между точностью задания стохастической матрицы и величиной минимальной степени полинома.

- Новый метод определения вероятностных характеристик случайных последовательностей из класса функций однородных цепей Маркова, порождаемых полиномиальными нелинейными динамическими моделями над полем GF(2^n). Доказаны теоремы, устанавливающие формулы для вычисления асимптотических вероятностных характеристик случайных последовательностей.

- Методика исследования однородных простых и сложных цепей Маркова на основе критерия линейной сложности. Сформулирован критерий нахождения длин реализаций марковских последовательностей при заданной точности представления матриц цепей Маркова. Определены стохастические зависимости линейной сложности реализаций цепей Маркова от энтропии стохастических матриц.

Достоверность результатов работы. Основные полученные результаты сформулированы в виде теорем и утверждений, приведены их доказательства. Предложенные аналитические методы и алгоритмы обоснованы доказательством теорем. Адекватность предложенных моделей подтверждается компьютерным моделированием и сравнением с известными результатами.

Практическая значимость.

- Решение задачи представления РЦМ полиномиальными функциями над полем $GF(2^n)$ расширяет класс дискретных случайных процессов, получаемых на полиномиальных моделях, и позволяет определить свойства данных процессов и стохастических матриц РЦМ.

- Предложенные алгоритмы разложения СМ ЦМ на имплицирующий вектор (ИВ) и множество стохастических булевых матриц (СБМ) позволяют определить вычислительную и комбинационную сложности вероятностных автоматов, синтезируемых в некотором логическом базисе.

- Полученные формулы определения предельного распределения вероятностей символов случайных последовательностей (СП), порождаемых полиномиальными нелинейными динамическими моделями дискретных преобразователей информации, и фундаментальная матрица для СМ позволяют на их основе получить ряд других характеристик СП, например, матрицу средних времен достижения, векторы предельных дисперсии и корреляции.

- Метод моделирования СП на основе минимального полинома позволяет: воспроизводить на линейных регистрах сдвига реализации ЦМ; расширить функциональное использование линейных регистров сдвига.

- Методика исследования линейной сложности (ЛС) марковских последовательностей расширяет класс задач применения ЛС, дает возможность моделировать ЦМ на основе линейных и нелинейных полиномов минимальных степеней, позволяет выявлять свойства ЛС марковских функций.

- Комплекс программ, алгоритмов и методик является инструментальным средством для моделирования СП и исследования свойств полиномиальных функций над конечным полем.

Результаты работы используются:

- в подсистеме временного прогнозирования производственно-экономических показателей состояния предприятия (на базе разработанной в диссертации программной реализации математического аппарата числовых стохастических матриц), включенной в состав автоматизированного рабочего места менеджера предприятия, введенного в опытную эксплуатацию в ОАО "ICL-КПО ВС", г. Казань (справка об использовании результатов);

- в учебном процессе кафедры Компьютерных систем (предыдущее название (до 2006 года) - Компьютерные системы и информационная безопасность) и кафедры Систем информационной безопасности КГТУ им. А.Н. Туполева в форме учебного

электронного пособия "Лабораторный практикум по вычислениям в конечных полях" (акт внедрения).

На защиту выносятся следующие результаты:

- метод и алгоритмы определения закона и свойств РЦМ по СМ исходной простой ЦМ, теоремы, обосновывающие метод и алгоритмы;
- метод представления заданного закона РЦМ минимизированной автоматной моделью и полиномиальной функцией над полем GF(2^n), теоремы, обосновывающие метод и свойства стохастических матриц РЦМ;
- метод и алгоритмы разложения СМ ЦМ с двоично-рациональными элементами на ИВ и множество СБМ, теоремы, обосновывающие метод и алгоритмы;
- аналитический метод определения характеристик СП из класса функций однородных ЦМ, порождаемых полиномиальными нелинейными динамическими моделями над полем GF(2^n), теоремы, обосновывающие метод;
- статистический метод исследования однородных простых и сложных ЦМ на основе критерия ЛС;
- аналитический метод представления СМ с заданной точностью и моделирования СП из класса неоднородных ЦМ полиномами минимальной степени над полем GF(q_c), теорема, обосновывающая метод;
- комплекс методик и программ, реализующий предложенные методы и алгоритмы.

Апробация работы. Основные результаты докладывались и обсуждались на следующих конференциях и семинарах: X-XV Всероссийские молодежные научные конференции "Туполевские чтения" (Казань, 2002-2007); Всероссийская научная конференция студентов и аспирантов (Таганрог, 2004); XIV Международная конференция "Проблемы теоретической кибернетики" (Пенза, 2005); Региональная научно-методическая конференция "Профессиональные компетенции в структуре модели современного инженера" (Нижнекамск, 2005); 6-ая Международная конференция молодых ученых и студентов (Самара, 2005); Международная научно-практическая конференция "Инфокоммуникационные технологии глобального информационного общества" (Казань,2005); Региональная научно-методическая конференция "Информационная культура в системе подготовки будущего инженера" (Нижнекамск, 2006); Всероссийский семинар "Ситуационные исследования" (Казань, 2006); Региональная научно-техническая конференция по вопросам информатики, вычислительной техники и информационной безопасности (Казань, 2006); Региональная научно-практическая конференция "Наука и профессиональное образование" (Нижнекамск, 2007); 9-ый Международный семинар "Дискретная математика и ее приложения" (Москва, 2007); Всероссийская научная конференция студентов, аспирантов и молодых ученых "Наука, технологии, инновации" (Новосибирск, 2007); Республиканский научный семинар "Методы моделирования" при КГТУ им. А.Н. Туполева (Казань, 2004-2008).

Публикации. Содержание работы опубликовано в 29 работах, включая 3 статьи, опубликованные в изданиях, входящих в перечень ВАК, 16 статей в других изданиях, 9 тезисов докладов и одну работу, зарегистрированную в отраслевом фонде алгоритмов и программ.

Структура и объем диссертации. Диссертационная работа состоит из введения,

четырех глав, заключения и списка использованной литературы, включающего 250 наименований, изложена на 153 страницах машинописного текста, содержит 44 рисунка и 12 таблиц, приложение на 10 страницах.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертации, дается определение цели и задач исследования, приводится перечень основных результатов, выносимых на защиту. Дана структура диссертации.

В **первой главе** "Связь цепей Маркова, вероятностных автоматов и полиномиальных функций в конечном поле" дан обзор результатов, определяющих связь ЦМ, вероятностных автоматов и полиномиальных моделей над полем GF(2^n). Вводятся известные понятия, теоремы и модели, необходимые для изложения решаемых задач. Уточняется постановка задач.

Связь цепей Маркова, вероятностных автоматов и полиномиальных функций над полем GF(2^n) определяется на основе представления СМ P размера $m \times m$ линейной стохастической комбинацией ИВ и множества СБМ вида $P = \sum_{a=0}^{l-1} q_a B^{(a)}$, (1.1) где $l \le m^2 - m + 1$ (для минимаксного алгоритма); q_a - элементы ИВ $\tilde{q}$, $a = \overline{0, l-1}$; $B^{(a)}$ - СБМ (авторы: Бухараев Р.Г., Габбасов Н.З., Gelenbe S.E., Гиоргадзе А.Х., Davis A.C., Захаров В.М., Костромин Г.Я., Кузнецов С.Е., Метра И.А., Паршенков Н.Я., Поспелов Д.А., Нурмеев Н.Н., Салимов Ф.И., Сачков В.Н., Ченцов В.М., Чирков М.К., Шилкевич Т.П. и др.). Размер ИВ зависит от алгоритма разложения и определяет сложность автоматных моделей марковских функций и рассматриваемых полиномиальных моделей над GF(2^n).

В известных полиномиальных моделях, основанных на использовании полиномиальных функций

- от одной переменной $g(y) = \sum_{i=0}^{r_f} a_i^{(f)} y^i, r_f = 2^n - 1, a_i^{(f)}, y \in GF(2^n)$ (1.2)

- от двух переменных $f(x,q) = \sum_{i=0}^{r_f}\sum_{j=0}^{r_f} a_{ij}^{(f)} x^i q^j, r_f = 2^n - 1, a_{ij}^{(f)}, x, q \in GF(2^n)$ (1.3)

минимальный порядок поля GF(2^n) определяется из условия $2^n \ge l$.

Пусть задана конечная простая ЦМ системой $(S, P, \overline{\pi_0})$, (1.4) где $S = \{s_i\}$ - конечное множество состояний ЦМ; $P = (p_{ij})$, $i, j = \overline{0, m-1}$ - СМ; $\overline{\pi_0}$ - вектор размера m начального распределения вероятностей состояний. Величина U - дискретная случайная величина (ДСВ), принимающая конечное число значений $x_0, \ldots, x_{l-1}$ с вероятностями из ИВ $\tilde{q} = \{q_i\}$ размера l, $\sum_{i=0}^{l-1} q_i = 1$.

***Теорема* 1.1** [1]. Существуют такие ДСВ U и функция $f(x, q)$ (1.3) со случайным начальным значением и коэффициентами $a_{ij}^{(f)} \in$GF(2^n), что U может быть преобразована $f(x, q)$ в заданную ЦМ вида (1.4). Минимальный порядок поля GF(2^n) выбирается из условия $2^n \ge l$.

---

[1] Захаров В.М., Нурутдинов Ш.Р., Шалагин С.В. Полиномиальное представление цепей Маркова над полем Галуа // Вестник КГТУ им. А.Н. Туполева, 2001, №3. - С. 27-31.

Теорема 1.1 обосновывает полиномиальную модель $(U; f(x, q))$, (1.5) где U - ДСВ со множеством значений $\{x_i\}$ с вероятностями из ИВ $\tilde{q}$; $f(x, q)$ - функция (1.3) со множеством $\{x_i\}$ значений переменной x и множеством $\{q_j\}$ значений переменной q для моделирования ЦМ в поле GF(2^n), $i = \overline{0, l-1}$, $j = \overline{0, m-1}$. Теорема определяет связь порядка поля с размерами матрицы P. Связь порядка поля GF(2^n) со структурой и точностью представления матриц P является малоисследованной задачей (например, исследуемые в главе 2 разреженные матрицы РЦМ).

Дана постановка задачи представления ЦМ над конечным полем GF(q_c), основанная на понятии "линейная сложность". Данное понятие связано с понятием линейных рекуррентных последовательностей над конечным полем. Исследования псевдослучайных и случайных последовательностей с помощью ЛС имеют следующие направления: разработка методов улучшения ЛС периодических последовательностей, исследование качества случайных чисел в моделировании; применение алгоритма Берлекэмпа "решения ключевого уравнения над произвольным полем" для кодирования информации; тестирование работоспособности цифровых схем; тестирование качества поточных шифров и исследование аналитической сложности генераторов чисел в криптологии (авторы: Алферов А.П., Берлекэмп Э., Иванов М.А., Куракин В.Л., Jansen C. J., Klapper A., Massey J. L., Reeds J.A., Rueppel R. A., Schaub T., Sloane N.J.A., Smeets B., Zong-duo Dai). В меньшей степени ЛС исследована в теории моделирования марковских последовательностей (МП) над конечным полем.

Во **второй главе** "Методы представления случайных последовательностей полиномиальными функциями над конечным полем" решаются задачи 1-3.

В **разделе 2.1** "Представление стохастических матриц полиномиальными функциями над полем GF(2^n) с учетом точности представления элементов матриц" предложен метод представления СМ с двоично-рациональными элементами полиномиальными функциями над полем GF(2^n). Метод основан на предложенных трех алгоритмах двоично-рационального разложения СМ на комбинацию ИВ и множества СБМ. Получены оценки порядка поля GF(2^n) в зависимости от точности представления элементов СМ. Доказаны теоремы, определяющие оценки вычислительной сложности (ВС) и размера l ИВ для предложенных алгоритмов.

Рассмотрены следующие алгоритмы минимаксного и двоично-рационального подходов разложения (1.1) матрицы P: алгоритм 1, использующий метод минимакса; предлагаемые алгоритмы 2-4, базирующиеся на двоично-рациональном представлении элементов матрицы P; алгоритм 2 основан на методе двоично-рационального разложения матриц (Бухараев Р.Г., Захаров В.М., 1978). Доказаны конечность предложенных алгоритмов и факт различия всех формируемых ими СБМ. Данные алгоритмы позволяют снизить ВС разложения (1.1) и получить точную оценку размера ИВ для заданных матриц и точности представления матриц. В алгоритмах 3 и 4 отсутствуют ограничения на класс двоично-рациональных СМ, выявленных в алгоритме 2.

Все элементы матриц P рассматриваются в виде двоично-рациональной дроби с h разрядами. Используются следующие формы представления СБМ: в виде квадратных бинарных матриц (способ 1) размера $m \times m$ и в виде векторов $B = \{b_i\}$ (способ 2)

размера m, $i, b_i = \overline{0, m-1}$, где позиции элементов p_{ib_i} в матрицах P задают позиции равных единице элементов СБМ.

Предложена модификация алгоритма 2 (алгоритм 2м), позволяющая снизить ВС со значения $O(m^4b^3)$ до $O(m^3b^2)$ при хранении СБМ способом 2 и исключении операции сравнения получаемых СБМ с ранее найденными.

Пусть $\widetilde{P}(m, b)$ - класс СМ с двоично-рациональными элементами, представленными с точностью $\varepsilon = 2^{-b}$.

***Теорема* 2.1**. Алгоритм 2 для класса матриц $\widetilde{P}(m, b)$ не результативен (не создается искомый ИВ), если матрица $P \in \widetilde{P}(m, b)$, $P = (p_{ij})$, $i, j = \overline{0, m-1}$, обладает одним из следующих свойств:

1) $\exists k = \overline{0, b-1}$, для которого не выполняется равенство: $\sum_{j=0}^{m-1} c_{0jk} = \ldots = \sum_{j=0}^{m-1} c_{(m-1)jk}$, где c_{ijk} - значение k-го разряда p_{ij}, $i = \overline{0, m-1}$,

2) $\exists\, p_{ij} = 1$, где $i, j = \overline{0, m-1}$.

Показано, что задача вычисления размера l ИВ для алгоритма 2 сводится к задаче нахождения экстремума числа двоичных единиц в разрядах элементов по строкам матрицы P.

***Теорема* 2.2**. Размер l ИВ, получаемого при разложении (1.1) матрицы P по алгоритму 2, определяется условиями

$$l \le \sum_{j=0}^{m-1} \sum_{k=0}^{b-1} c_{ijk}, \sum_{j=0}^{m-1} \sum_{k=0}^{b-1} c_{ijk} = const, i = \overline{0, m-1}, \text{ и } \begin{cases} 2 \le l \le 2^b, \text{ при } m \ge 2^b \\ 2 \le l \le m^2 - m + 1, \text{ при } m < 2^b \end{cases}.$$

В алгоритме 3 координаты единичных элементов СБМ задаются координатами выбранных последовательно по одному из каждой строки, при минимальном j, элементов $p_{ij} > 0$ матрицы P, $i, j = \overline{0, m-1}$, а каждый элемент ИВ равен 2^{-b}.

Предложен алгоритм 4, обладающий следующими особенностями:
- устраняются ограничения (теорема 2.1) на класс матриц алгоритма 2;
- его ВС минимальна для обоих подходов и зависит от m и b;
- дает точную оценку параметра l для конкретной матрицы P.

Алгоритм 4 состоит из следующих пунктов.

1. Из исходной матрицы P формируются матрицы $W^{(k)} = (w_{ij}^{(k)})$, $w_{ij}^{(k)} = \overline{0, 2^{k+1}}$, $i, j = \overline{0, m-1}$, $k = \overline{0, b-1}$, по правилу: при $p_{ij} = 1$, то $w_{ij}^{(0)} = 2$; иначе $w_{ij}^{(k)} = c_{ijk}$. Необходимый объем памяти для матриц $W^{(k)}$ равен $m^2b(b+1)/2$ бит.

2. При не соблюдении условия $d = 0$, $d = \sum_{j=0}^{m-1} w_{ij}^{(k)} - \min\limits_{c=\overline{0,m-1}} \sum_{j=0}^{m-1} w_{cj}^{(k)}$, $k = \overline{0, b-2}$, значения d любых элементов $w_{ij}^{(k)} > 0$ с удвоением переносятся в соответствующие элементы $w_{ij}^{(k+1)}$ матрицы $W^{(k+1)}$, так как справедливо равенство $1/2^a = 2^k/2^{a+k}$, где a - натуральное число.

3. Текущая СБМ $B^{(l)}$ для $\forall k = \overline{0, b-1}$ формируется из элементов $w_{ij}^{(k)} > 0$ матрицы $W^{(k)}$ при минимальном j. Осуществляется проверка повторения матрицы $B^{(l)}$ в матрицах $W^{(j)}$, $j = \overline{k+1, b-1}$. При получении $B^{(l)}$ в $W^{(j)}$ к q_l добавляется

$\min_{0\le i\le m-1} w_{i\,b_i^{(l)}}^{(j)} \cdot 2^{-(j+1)}$, иначе в ИВ $\tilde{q}$ добавляется элемент $q_l = \min_{0\le i\le m-1} w_{i\,b_i^{(l)}}^{(k)} \cdot 2^{-(k+1)}$.

***Теорема* 2.3**. Размер l ИВ, получаемого при разложении (1.1) матрицы P по алгоритму 4, определяется условиями

$$l \le \sum_{j=0}^{m-1}\sum_{k=0}^{b-1} w_{ij}^{(k)},\ \sum_{j=0}^{m-1}\sum_{k=0}^{b-1} w_{ij}^{(k)} = const, \text{ и } \begin{cases} 2 \le l \le 2^b, \text{ при } m \ge 2^b \\ 2 \le l \le m^2 - m + 1, \text{ при } m < 2^b \end{cases}, \quad (2.1)$$

где $w_{ij}^{(k)}, i = \overline{0, m-1}$ - элементы матриц $W^{(k)}$, полученные к пункту 3 алгоритма.

Параметры ВС и l (таблица) алгоритмов двоично-рационального подхода зависят не только от размера m и энтропии $H(P)$ матриц P, как в минимаксном подходе, но и от числа разрядов b представления элементов. Размер l ИВ для алгоритма 4 при b-const с ростом размера m матриц увеличивается, а при достижении соотношения $m^2 - m + 1 > 2^b$ становится константой. Уменьшение ВС в рассматриваемых алгоритмах осуществляется за счет: последовательного выбора элементов из строк; представления СБМ в виде вектора чисел и исключения сравнения полученных СБМ с ранее найденными; снижения точности представления элементов матрицы P. Например, вычислительная сложность снижается от 6561 (алгоритм 1) операций к 5652 (алгоритм 4) для СМ размера 9×9 и при числе двоичных разрядов $b = 4$ представления элементов.

Алгоритм	Оценка ВС	Оценка l
алгоритм 1	$O(m^4)$	известные оценки $1 \le l \le m^2 - m + 1$ и (2.2) $\max_{0\le i\le m-1} \sigma_i \le l \le \sum_{i=0}^{m-1} \sigma_i - m + 1$, (2.3) σ_i - число ненулевых элементов в строке i
алгоритм 2	$O(m^4 b^3)$	$l \le \sum_{j=0}^{m-1}\sum_{k=0}^{b-1} c_{ijk}$, $\sum_{j=0}^{m-1}\sum_{k=0}^{b-1} c_{ijk} = const$, $i = \overline{0, m-1}$, и $\begin{cases} 2 \le l \le 2^b, \text{ при } m \ge 2^b \\ 2 \le l \le m^2 - m + 1, \text{ при } m < 2^b \end{cases}$
алгоритм 2м	$O(m^3 b^2)$	
алгоритм 3	$O(m^3)$	$1 \le l \le m^2 - m + 1$
алгоритм 4 (соавторство с Нурмеевым Н.Н.)	$O(mb(17m+b))$	$l \le \sum_{j=0}^{m-1}\sum_{k=0}^{b-1} w_{ij}^{(k)}$, $\sum_{j=0}^{m-1}\sum_{k=0}^{b-1} w_{ij}^{(k)} = const$, $i = \overline{0, m-1}$, и $\begin{cases} 2 \le l \le 2^b, \text{ при } m \ge 2^b \\ 2 \le l \le m^2 - m + 1, \text{ при } m < 2^b \end{cases}$

***Теорема* 2.4**. Порядок n поля GF(2^n) в системе (1.5) для класса СМ $\tilde{P}(m, b)$, представленных в виде (1.1) по алгоритму 4, определяется из условия $2^n \ge max(l, m)$, где l - размер ИВ, удовлетворяющего условию (2.1).

Опишем метод представления СМ с двоично-рациональными элементами полиномиальными функциями над полем GF(2^n), с учетом точности задания переходных вероятностей.

1. Выполняется разложение (1.1) матрицы P с помощью алгоритма 4 на ИВ $\tilde{q}$ и множество СБМ. Размер ИВ $\tilde{q}$ удовлетворяет условию теоремы 2.3.

2. ИВ $\tilde{q}$ и множество СБМ преобразуются в автоматную таблицу конечного

детерминированного автомата (КДА).

3. По автоматной таблице вычисляется функция $f(x, q)$ вида (1.3) над полем GF(2^n), порядок которого определяется теоремой 2.4.

Шаги метода детально описаны в диссертации, в главе 4.

В разделе 2.2 "Представление расширенных цепей Маркова над полем GF(2^n)" решены задачи синтеза и анализа модели расширенных цепей Маркова над полем GF(2^n). Доказана теорема (2.5), обосновывающая алгоритм вычисления закона РЦМ по заданной СМ исходной простой ЦМ. Предложен метод (теоремы 2.5, 2.7, 2.8) представления заданного стохастического закона РЦМ в определенную полиномиальную функцию над полем GF(2^n). Предложены полиномиальные модели РЦМ, определены свойства структуры матрицы РЦМ (в частности, теорема 2.6 и следствие 2.1). Определены оценки размера ИВ, получаемого при разложении (1.1) матрицы РЦМ, исходя из результатов раздела 2.1. Получены оценки порядка поля GF(2^n).

Пусть задана последовательность состояний $s_{j1}, s_{j2}, \ldots$ простой однородной ЦМ с конечным множеством состояний $S = \{s_j\}$ и матрицей $P = (p_{ij})$ размера $m \times m$, $i, j = \overline{0, m-1}$. Составим цепочки символов s_j длины $r = \nu + \kappa \geq 2$, $\nu \geq 1$, $\kappa \geq 0$, имеющие вид $(s_{j1}, \ldots, s_{j\nu}, s_{j\nu+1}, \ldots, s_{j\nu+\kappa})$. Смежные цепочки, содержащие $\kappa = r - \nu$ общих символов и ν отличающихся символов, будем рассматривать как один шаг перехода расширенной ЦМ с $m^{\nu+\kappa}$ состояниями A_i, $i = \overline{0, m^{\nu+\kappa} - 1}$, определяемой матрицей Q размера $m^{\nu+\kappa} \times m^{\nu+\kappa}$. Определим матрицу Q РЦМ (задача анализа) через матрицу P исходной ЦМ при $\nu \geq 2$, $\kappa \geq 2$. Пусть E и ξ_m - единичные матрица и вектор-столбец размеров $m^{r-2} \times m^{r-2}$ и m соответственно; $\otimes$ - символ операции кронекерово произведения матриц; $C = |B_0 B_1 \ldots B_{m-1}|$ - матрица размера $m \times m^2$, являющаяся последовательной конкатенацией матриц $B_i = (b_{aj}^{(i)})$, $i, j, a = \overline{0, m-1}$, где

$$b_{aj}^{(i)} = \begin{cases} p_{aj}, \text{ если } a = i \\ 0, \text{ если } a \neq i \end{cases}.$$

***Замечание* 2.1**. Пусть дана матрица $P = (p_{ij})$, $i, j = \overline{0, m-1}$. Тогда по формуле $W = \xi_m \otimes E \otimes C$ определяется "промежуточная" стохастическая матрица $W = (w_{cd})$, $c, d = \overline{0, m^r - 1}$, размера $m^{\nu+\kappa} \times m^{\nu+\kappa}$, на основе которой вычисляется матрица Q.

***Утверждение* 2.1**. Пусть дана матрица $P = (p_{ij})$, $\forall p_{ij} > 0$, $i, j = \overline{0, m-1}$, и на ее основе получена матрица $W = (w_{cd})$, $a, d = \overline{0, m^r - 1}$, с цепочками длины $r = \nu + \kappa$, $\nu > 1$, $\kappa > 1$. Тогда для $W^r = (w_{ij}^{(r)})_{m^r \times m^r}$: $\forall w_{ad}^{(r)} > 0$.

***Теорема* 2.5**. Пусть W^ν - ν-я степень матрицы W, $\nu \geq 1$, $\kappa \geq 0$. Тогда переходная матрица Q РЦМ вида

$$(s_{j1}, \ldots, s_{j\nu}, s_{j\nu+1}, \ldots, s_{j\nu+\kappa}) \to (s_{j\nu+1}, \ldots, s_{j\nu+\kappa}, \ldots, s_{j2\nu+\kappa}) \to \ldots$$

равна $$Q = W^\nu. \qquad (2.4)$$

***Теорема* 2.6**. Пусть дана матрица $P = (p_{ij})$, $\forall p_{ij} > 0$, $i, j = \overline{0, m-1}$, и на ее основе получена матрица Q РЦМ размера $m^r \times m^r$, $r = \nu + \kappa \geq 2$, $\nu \geq 1$, $\kappa \geq 0$. Тогда РЦМ - эргодическая.

***Следствие* 2.1**. Пусть дана матрица $P=(p_{ij})$ ЦМ, и $\exists p_{ij}=0$, $i,j=\overline{0,m-1}$; на основе P получена матрица Q РЦМ размера $m^r\times m^r$, $r\geq 2$, $v\geq 1$, $\kappa\geq 0$. Тогда РЦМ не является эргодической.

***Утверждение* 2.2**. Если РЦМ, заданная матрицей Q размера $m^r\times m^r$, с длиной цепочек $r=v+\kappa$, образована матрицей P с одинаковыми строками, то данная цепь является цепью Маркова-Брунса.

Предложен **алгоритм** вычисления матрицы Q РЦМ по матрице P. Исходные данные: матрица P размера $m\times m$; переменные κ, v, $r\geq 2$. Результат вычислений: матрица Q размера $m^r\times m^r$.

1. Вычисляются ненулевые элементы матрицы W по формуле

$$w_{i,(i\cdot m \bmod m^r+d)}=p_{(i \bmod m),d},\ i=\overline{0,m^r-1},\ d=\overline{0,m-1}, \tag{2.5}$$

где i - текущий номер строки матрицы W, d - текущий номер столбца P.

2. Вычисляется соотношение (2.4).

Поставим в соответствие матрице Q размера $m^r\times m^r$ полиномиальную модель (1.5) - $(U, f(x, q))$, где $f(x, q)$ - функция (1.3), принимающая m^r значений; переменные x и q принимают соответственно l и m^r значений.

Структурная схема построенной автоматной модели (1.5) для РЦМ представлена на рис.2.1 (рис.2.2 - схема полиномиальной модели (1.5)), где Г - генератор ДСВ U; М - КДА, со множеством состояний A_j, $j=\overline{0,m^r-1}$, входным алфавитом $\{x_0, \ldots, x_{l-1}\}$ и функцией переходов, полученной по Q.

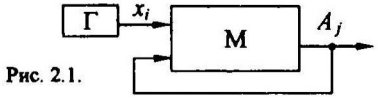

Рис. 2.1.

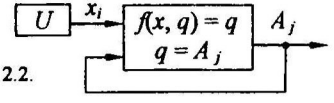

Рис. 2.2.

***Утверждение* 2.3**. Пусть задана матрица Q РЦМ размера $m^r\times m^r$, $r\geq 2$. Тогда для ИВ $\tilde{q}$ матрицы Q, получаемого по минимаксному алгоритму, с учетом числа ненулевых элементов, размер l лежит в диапазоне

$$m^v\leq l\leq m^r-m^\kappa+1. \tag{2.6}$$

С учетом структуры СМ РЦМ, порядок поля, необходимого для построения полиномиальной модели РЦМ, был снижен с $(m^r)^2$ к m^r.

***Теорема* 2.7**. Пусть задана матрица Q РЦМ размера $m^r\times m^r$, $r\geq 2$. Тогда порядок поля $GF(2^n)$ для модели (1.5) определяется из условия $2^n\geq m^r$, где n - наименьшее целое.

Учитывая разреженность матриц РЦМ осуществим синтез автоматной модели РЦМ на основе принципа приведения множества состояний A_j.

***Теорема* 2.8**. Алгоритм i-эквивалентных разбиений сводит число h состояний автоматной модели РЦМ, заданной матрицей Q, к значению m.

Схема построенной автоматной модели РЦМ изображена на рис.2.3 (рис.2.4 - полиномиальная модель). Блок 1 - КДА с множеством состояний приведенного автомата, y_c - состояние КДА. Блок 2 - Г для моделирования системы из m случайных величин. Блок 3 - регистр сдвига (РС), образующий цепочки z_c символов $s_i\in S$ длины v, $i=\overline{0,m-1}$. Цепочки из s_i образуют текущее состояние A_j РЦМ, $j=\overline{0,m^r-1}$.

***Теорема* 2.9**. Пусть задана РЦМ матрицей Q размера $m^r \times m^r$ и параметрами ν, κ. Тогда последовательность состояний РЦМ представляется последовательностью значений функции $\psi = f_2 \times f_1$ - суперпозиции полиномов вида (1.3) над полем GF(2^n), где n - наименьшее целое, удовлетворяющее условию $2^n \geq l$, а l удовлетворяет неравенству (2.6).

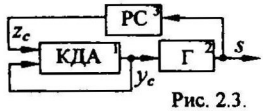

Рис. 2.3.

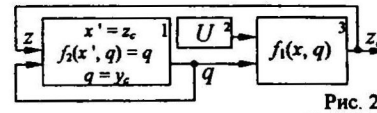

Рис. 2.4.

Теорема 2.9 дает следующий метод построения полиномиальной модели над полем GF(2^n) для моделирования РЦМ.

1. Вычисляется матрица Q РЦМ по алгоритму (раздел 2.2).

2. По матрице Q задается автоматная модель, представленная на рис.2.3.

3. По автоматной модели определяется функция $\psi = f_2 \times f_1$ и строится полиномиальная модель, представленная на рис.2.4, где блоки 1 и 3 соответствуют блокам 1 и 3 автоматной модели, а блок 2 моделирует ДСВ с числом значений l из (2.6).

В **разделе 2.3** "Моделирование случайных последовательностей минимальными полиномами над конечным полем по заданной стохастической матрице" предложен метод моделирования случайных последовательностей из класса неоднородных ЦМ над полем GF(q_c), где $q_c \geq 2$ - простое число. Предлагаемый метод позволяет по заданной матрице P получать семейство реализаций СП фиксированной длины на основе минимальных полиномов $f(x)$ (полиномов минимальной степени) над полем GF(q_c); доказана теорема, обосновывающая метод.

Пусть заданы $P = (p_{ij})$, $i, j = \overline{0, m-1}$, и $\bar{\pi} = (\pi_0, \ldots, \pi_{m-1})$ - предельный вектор для P; $\varphi = (s_{i1}, \ldots, s_{iN})$ - последовательность длины N в алфавите S, обладающую следующими свойствами: для любого i буква s_i входит $a_i \geq 1$ раз в φ; буква s_j следует $a_{ij} \geq 0$ раз за s_i (и за s_{iN} следует s_{i1}); выполняются

$$\sum_{j=0}^{m-1} a_{ij} = \sum_{j=0}^{m-1} a_{ji} = a_i \geq 1 \text{ и } \sum_{i=0}^{m-1} a_i = N. \qquad (2.7)$$

С φ свяжем неразложимую матрицу $P_\varphi = (p_{ij}^{(\varphi)})$, $p_{ij}^{(\varphi)} = a_{ij}/a_i$, удовлетворяющую (2.7), и предельный вектор $\overline{\pi_\varphi} = (\pi_i^{(\varphi)})$, $\pi_i^{(\varphi)} = a_i/N$.

Положим: 1) точность приближения матрицы $P = (p_{ij})$ матрицей $P_\varphi = (p_{ij}^{(\varphi)})$, $i, j = \overline{0, m-1}$, удовлетворяет условию $|p_{ij}^{(\varphi)} - p_{ij}| \leq \varepsilon$, $0 < \varepsilon < 1$; 2) длина N последовательности φ определяется из условия $N \geq N^*$, N^* - максимальное из $\max\limits_{i,j=\overline{0,m-1};\ p_{ij}\pi_i \neq 0} (p_{ij}\pi_i)^{-1}$ и $\max\limits_{i=\overline{0,m-1}} (1 + p_{ij} + \varepsilon)/(\pi_i \varepsilon)$. Требуется построить минимальный полином $f(x)$ над GF(q_c), вырабатывающий последовательность u_N длины $N \geq N^*$. Матрица P_φ, соответствующая u_N, должна с заданной величиной $\varepsilon > 0$ аппроксимировать исходную матрицу P.

***Теорема* 2.10**. Пусть заданы неразложимая СМ $P = (p_{ij})$ размера $m \times m$ и числа $0 < \varepsilon < 1$, $N \geq N^*$. Тогда существует минимальный полином $f(x)$ над полем GF(q_c),

вырабатывающий последовательность $u_{N'+1}$ длины $N'+1$ с законом $P_\varphi=(p_{ij}^{(\varphi)})$, который удовлетворяет условиям

$$|N^{'}-N|\le m-1, \tag{2.8}$$

$$|p_{ij}^{(\varphi)}-p_{ij}|\le\varepsilon \text{ и } p_{ij}^{(\varphi)}=\begin{cases}0, \text{если } p_{ij}=0\\ >0, \text{если } p_{ij}>0\end{cases}, \; i,j=\overline{0,m-1}, \tag{2.9}$$

$$|\pi_i^{(\varphi)}-\pi_i|N\le 1+\pi_i|N'-N|, \tag{2.10}$$

и степень L полинома $f(x)$ удовлетворяет условию $2L\le N'+1$.

***Следствие* 2.2** (из теоремы 2.10). Число последовательностей $u_{N'+1}$, полученных по матрице P_φ размера $m\times m$ и удовлетворяющих условиям (2.8)-(2.10) теоремы 2.10, ограничено сверху величиной m^L, где $L=\begin{cases}(N^{'}+1)/2, \text{если } N^{'} - \text{нечетное};\\ ((N^{'}+1)+1)/2, \text{если } N^{'} - \text{четное}\end{cases}$

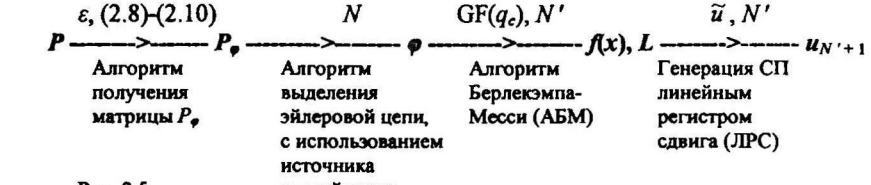

Рис. 2.5.

Представим на рис. 2.5 метод моделирования СП на основе полинома $f(x)$: входные параметры, необходимые для преобразований, надписаны в верхней части; величины, над которыми выполняются преобразования - посередине; известные алгоритмы, выполняющие преобразования - внизу.

Благодаря алгоритму получения матрицы P_φ, для аппроксимации исходной матрицы P с заданной точностью необходима реализация ЦМ длиной не в N^2 символов, а в N.

Третья глава "Методы анализа полиномиальных функций, моделирующих случайные последовательности в конечном поле", состоит из двух разделов, в которых исследуются свойства полиномиальных нелинейных динамических моделей преобразователей функций ЦМ и линейной сложности МП (решаются задачи 4, 5).

В **разделе 3.1** "Анализ нелинейных моделей преобразователей случайных последовательностей над полем GF(2^n) на основе стохастических матриц" решена задача анализа полиномиальных нелинейных динамических моделей (ПНДМ) над полем GF(2^n), порождающих случайные последовательности (СП) из класса функций конечных однородных ЦМ. Задача анализа состоит в определении характеристик СП. Основными определяемыми характеристиками являются стохастические векторы, характеризующие асимптотику распределений вероятностей символов СП. Доказаны теоремы, обосновывающие аналитическое определение искомых характеристик СП. Для четырех последовательно усложняемых ПНДМ, описывающих классы СП, определены их полиномиальные функции над полем GF(2^n) и структурные схемы.

Определение базовых полиномиальных функций над полем GF(2^n). Введем в рассмотрение ЦМ, заданную системой (1.4), и полиномиальные функции $g(y)$ (1.2) и $f(x, q)$ (1.3) над полем GF(2^n); значения этих функций обозначим соответственно β и α,

$\alpha, \beta \in GF(2^n)$. Поставим в соответствие матрице P полиномиальную модель (1.5) - $(U, f(x, q))$, где $f(x, q)$ - функция (1.3), принимающая m значений, а переменные x и q - соответственно l и m значений.

***Утверждение* 3.1**. Порядок поля $GF(2^n)$ в (1.5) определяется из условия $2^n \geq l_1$, где n - наименьшее целое, а l_1 - размер ИВ для матриц P, у которых $\exists p_{ij} = 0$, определяемый условием (2.3).

Полиномиальные нелинейные динамические модели, порождающие функции цепей Маркова

1. Зададим следующие ограничения на систему (1.5).

1) Пусть значение $\alpha(t+1)$ функции $f(x, q)$, полученное в момент времени $t+1$, есть состояние ЦМ, определяемое переменными $x(t)$ и $q(t) = \alpha(t)$ во время t.

2) Значение q в момент $t = 0$ определяется вектором $\overline{\pi_0}$.

При этих ограничениях системе (1.5) соответствует ПНДМ над полем $GF(2^n)$ вида
$$(U, \alpha(t+1) = f(x(t), q(t)), \overline{\pi_0}). \quad (3.1)$$

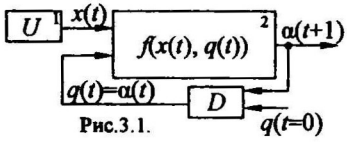

Рис.3.1.

Последовательность значений $f(x(t), q(t))$ в системе (3.1) в моменты $t = 1, 2, \ldots$ является простой однородной ЦМ, определяемой P и $\overline{\pi_0}$. На структурной схеме модели (3.1) (рис.3.1) функциональное назначение блоков 1, 2 соответствует системе (3.1); блок 1 - генератор ДСВ U; блок D - элемент задержки на единицу времени $t = 1$. Пусть $\overline{P_\alpha}(t) = (p_{\alpha i}(t))$ - вектор распределения вероятностей значений $f(x(t), q(t))$ для времени t; $\overline{\pi}$ - предельный вектор эргодической ЦМ.

***Теорема* 3.1**. Для СП, порождаемой моделью (3.1):
$$\overline{P_\alpha}(t) = \overline{\pi_0} P^t = \overline{\pi_0} \prod_{i=1}^{t} P, \overline{P_\alpha}(t+1) = \overline{P_\alpha}(t) P \text{ и } \overline{\pi} P = \overline{\pi}. \quad (3.2)$$

2. Разобьем множество S системы (1.4) на непересекающиеся подмножества
$$C_0, \ldots, C_{h_s-1}; \bigcup_{j=0}^{h_s-1} C_j = S; C_a \cap C_j = 0, a \neq j, a, j = \overline{0, h_s - 1}, \quad (3.3)$$
и выполним отображение
$$\mu(s): S \to B_t = \{b_0^{(t)}, \ldots, b_{h_s-1}^{(t)}\}, \quad (3.4)$$
где $B_t = \{b_i^{(t)}\}$ - функция конечной ЦМ с h_s значениями, определяемая условием $b_i^{(t)} = j$, если в момент времени t ЦМ находится в каком-либо состоянии s_i подмножества C_j, $i = \overline{0, m-1}$.

По аналогии с (3.1) функцию B_t будем моделировать над полем $GF(2^n)$ ПНДМ вида:
$$(U, \psi_1(t+1) = g(y(t+1)); f(x(t), q(t)), \overline{\pi_0}), \quad (3.5)$$
где $2^n \geq l_1$; $q(t) = \alpha(t)$; функция $g(y(t+1))$ реализует отображение $\mu(s)$; ψ_1 - суперпозиция функций $f(x, q)$ и $g(y)$; последовательность значений β функции ψ_1 в моменты t представляет функцию B_t.

Пусть $\overline{P_\beta}(t) = (p_{\beta i}(t))$ и $\overline{P_\beta}$ - вектор и предельный вектор распределения вероятностей значений β функции $\psi_1(t)$. Зададим бинарную матрицу $\Lambda = (\lambda_{ij})$, где $\lambda_{ij} = 1$, если $s_i \in C_j$, $i = \overline{0, m-1}$, $j = \overline{0, h_s - 1}$.

***Теорема* 3.2**. Для ПНДМ (3.5), заданной системой ((1.4), (3.4)) = (S, P, B_t, $\mu(s)$, $\overline{\pi_0}$), векторы $\overline{P_\beta}(t)$ и $\overline{P_\beta}$ вычисляются по формулам

$$\overline{P_\beta}(t) = \overline{\pi_0}P^t\Lambda = \overline{P_\alpha}(t)\Lambda \text{ и } \overline{P_\beta} = \overline{\pi}\Lambda . \qquad (3.6)$$

На систему (3.5) наложим следующие ограничения.

a_1) $l \le r_f$ определяет порядок поля, а функции $f(x, q)$ соответствует матрица коэффициентов $A_f = (a_{ij}^{(f)})$, $a_{ij}^{(f)} \in GF(2^n)$, $i, j = \overline{0, r_f}$.

a_2) Заданы ДСВ U с ИВ $\overline{q}$ размера l, $l \le r_f$, и вектор $\overline{\pi_0}$ размера m.

a_3) Переменная x и функция $f(x, q)$ принимают соответственно l и m значений, а множества значений $q(t)$, α и $y(t+1)$ совпадают.

a_4) Функция $g(y)$ реализует отображение $\mu(s)$.

***Следствие* 3.1**. Пусть задана система (3.5) с ограничениями a_1) - a_4). Тогда для нее однозначно определяются матрица P, векторы

$$\overline{P_\alpha}(t) = \overline{\pi_0}P^t, \ \overline{P_\beta}(t) = \overline{P_\alpha}(t)\Lambda \text{ и } \overline{P_\beta} = \overline{\pi}\Lambda . \qquad (3.7)$$

3. Зададим функцию ЦМ системой ((1.4), Z, $\mu(z/s)$), (3.8)

где функция $\mu(z/s)$ задается матрицей $P_{(z/s)} = (p_{(z_i/s_j)})$, $i = \overline{0, m-1}$, $j = \overline{0, |Z|-1}$, а элемент $p_{(z_i/s_j)}$ определяет вероятность появления буквы $z_j \in Z$ при состоянии s_i.

Системе (3.8), по теореме 3.2, поставим в соответствие ПНДМ

$$(U, U', \psi_2(t+1) = f_2[x'(t+1), q'(t+1)]f_1[x(t), q(t)], \overline{\pi_0}), \qquad (3.9)$$

где $2^n \ge \max(l_1, l_2)$; l_2 - размер ИВ, полученного при разложении матрицы $P_{(z/s)}$; U и U' - ДСВ, определяемые по разложению (1.1) матриц P и $P_{(z/s)}$; $\psi_2(t+1)$ - задает процесс Z_t и является суперпозицией функций f_2 и f_1 вида (1.3). $\overline{P_z}(t)$ и $\overline{P_z}$ - вектор и предельный вектор распределения вероятностей значений $\psi_2(t)$.

***Следствие* 3.2**. Если в системе (3.8) ЦМ - эргодическая, то для модели (3.9), заданной по системе (3.8), векторы $\overline{P_z}(t)$ и $\overline{P_z}$ вычисляются по формулам

$$\overline{P_z}(t) = \overline{\pi_0}P^t P_{(z/s)} \text{ и } \overline{P_z} = \overline{\pi}P_{(z/s)} . \qquad (3.10)$$

Рассмотрим систему (3.9) при следующих ограничениях.

c_1) Пусть заданы вектор $\overline{\pi_0}$; ДСВ U и U', состоящие соответственно из l_1 и l_2 значений.

c_2) Заданы порядок n поля $GF(2^n)$ из условия $2^n \ge max(l_1, l_2)$ и матрицы коэффициентов для $f_1(x, q)$ и $f_2(x', q')$.

c_3) Задано ограничение a_3) на функцию $f_1(x, q)$.

c_4) Переменная x' в $f_2(x', q')$ и функция $f_2(x', q')$ принимают соответственно l_2 и $|Z|$ значений, а множества значений $q'(t)$ и $f_1(x, q)$ совпадают.

***Следствие* 3.3**. Пусть задана система (3.9) с ограничениями c_1) - c_4). Тогда для процесса Z_t однозначно определяются матрицы P и $P_{(z/s)}$, вектор $\overline{P_z}(t)$ (3.10) и, если полученная ЦМ является эргодической, то и вектор $\overline{P_z}$ (3.10).

4. Введем систему $M_{z/b^{(t)}}$ вида $M_{z/b^{(t)}} = ((1.4), (3.4), Z, \mu(z/b^{(t)}))$, (3.11)

где $\mu(z/b^{(t)})$ задается матрицей $P_{(z/b^{(t)})} = (p_{(z_i/b_j^{(t)})})$, $i = \overline{0, h_z - 1}$, $j = \overline{0, |Z| - 1}$, а $p_{(z_i/b_j^{(t)})}$ определяет вероятность появления буквы $z_j \in Z$ от буквы $b_i^{(t)}$.

Заданную системой (3.11) функцию ЦМ можно моделировать ПНДМ вида

$$(U, U', \psi_3(t+1) = f_2[x'(t+1); q'(t+1)] \cdot \psi_1(t+1), \overline{\pi_0}), \qquad (3.12)$$

где $\psi_3(t)$ - суперпозиция функций f_2 и ψ_1, а последовательность значений функции $\psi_3(t)$ задает процесс Z'_t (рис.3.2 - структурная схема модели (3.12)).

Пусть $\overline{P_{z/b^{(t)}}}(t)$ и $\overline{P_{z/b^{(t)}}}$ - вектор и предельный вектор распределения вероятностей значений $\psi_3(t)$.

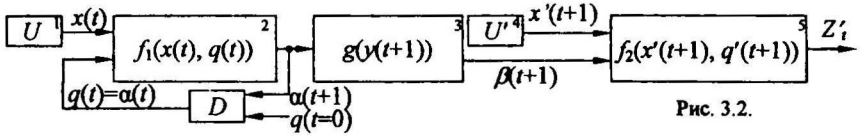

Рис. 3.2.

***Следствие* 3.4**. Для модели (3.12), заданной по системе (3.11), векторы $\overline{P_{z/b^{(t)}}}(t)$ и $\overline{P_{z/b^{(t)}}}$ равны $\overline{P_{z/b^{(t)}}}(t) = \overline{\pi_0} P^t \Lambda P_{(z/b^{(t)})}$ и $\overline{P_{z/b^{(t)}}} = \overline{\pi} \Lambda P_{(z/b^{(t)})}$. (3.13)

Совокупность формул (3.2), (3.6), (3.7), (3.10), (3.13), определяемых теоремами (3.1, 3.2) и следствиями (3.1-3.4), образует метод вычисления характеристик ПНДМ вида (3.1), (3.5), (3.9) и (3.12) над полем $GF(2^r)$, порождающих СП из класса функций ЦМ.

В <u>разделе 3.2</u> "Статистический анализ линейной сложности регулярных цепей Маркова" предложен метод статистического анализа однородных простых и сложных ЦМ по критерию ЛС (с использованием результатов раздела 2.3). Определены статистические критерии нахождения необходимых для исследования ЛС длин реализаций МП при заданной точности представления СМ, рассмотрены их отличия и особенности. Показана взаимосвязь ЛС и энтропии СМ: определены оценки математического ожидания $M(L(l_c))$ и дисперсии $D(L(l_c))$ МП, моделируемых по заданным матрице P и энтропии $H(P)$, где $L(l_c)$ - значение ЛС МП длины l_c; определены оценки $M(L(l_c))$ и $D(L(l_c))$, характеризующие подклассы МП с определенной величиной $H(P)$; определен профиль ЛС МП.

ЛС линейной рекуррентной последовательности (ЛРП) определяет минимальную длину ЛРС, реализующего данную последовательность. Алгоритмом вычисления ЛС заданной ЛРП и нахождения полинома $f(x)$ является АБМ. Функция $L(i)$ называется *профилем* ЛС последовательности u, где $L(i)$ задает ЛС последовательности $u = (s_0, s_1, \ldots, s_{i-1})$ для $\forall i = \overline{1, l_c}$.

Пусть у ЦМ с алфавитом состояний S стохастическая матрица $P = (p_{ij})$ размера $m \times m$ ($m^r \times m^r$ - для r-сложных ЦМ) принадлежит классу регулярных матриц M_R; предельный вектор $\overline{\pi}$, матрица частот P', вектор $\overline{\pi}' = (a_i / l_c)$ соответствуют обозначениям $\overline{\pi}$, P_φ и $\overline{\pi_\varphi}$ раздела 2.3. Опишем метод статистического анализа однородных простых и сложных ЦМ по критерию ЛС.

1. Строятся матрицы $P \in M_R$ методом статистического моделирования при

условиях: стохастичности по строкам, регулярности СМ и соответствия P одной из трех, равных по величине, групп энтропии $H_i(P)$, $i = \overline{1,3}$.

2. Вычисляется точность ε отображения свойств исходной ЦМ реализацией ЦМ из условия $2(1-\lambda)^d \le \varepsilon.$ (3.14)

Выражение (3.14) вытекает из неравенства Бернштейна: $\sum_{i=0}^{m-1} | p_i^d - \pi_i | \le 2(1-\lambda)^d$, где $\lambda = \min_{i,j=\overline{0,m-1}} p_{ij}$, p_i^d - вероятность перехода ЦМ в состояние $s_i \in S$ за d шагов, $d = 1, 2, \ldots$

3. Параллельно со статистическим моделированием реализаций ЦМ определяется l_c, с остановкой при выполнении $|\pi_i - a_i / l_c| \le \varepsilon, \forall i = \overline{0, m-1},$ (3.15)

- критерия, задающего длины $l_c = \sum_{i=0}^{m-1} a_i$ последовательностей, достаточных для отображения с точностью ε свойств ЦМ, и отражающего закономерности и предельные свойства P. Для реализации ЦМ вычисляется ее ЛС (с помощью АБМ) и строится профиль ЛС.

4. В пункте 3 генерируются реализации ЦМ, число которых соответствует заданному уровню точности, и по ним вычисляются оценки $M(L(l_c))$ и $D(L(l_c))$, строятся плотность и функция распределения величины $L(l_c)$.

ВС АБМ для двоичной последовательности длины l_c составляет оценку $O(l_c^3)$. Правильность работы программной реализации метода анализа проверялась на основе анализа следующих последовательностей: псевдослучайных двоичных, полученных на ЛРС; случайных чисел; реализаций ЦМ при $H_{max}(P)$; полученных аффинными преобразованиями.

Для простых и сложных ЦМ получены следующие оценки (по критерию (3.15)), близкие к случайным последовательностям с равномерным распределением:
$M(L(l_c)) \to l_c/2 + \omega, \omega < 1$ - коэффициент,
$D(L(l_c)) \to 86/81$ при $H(P) \in [0{,}5 \cdot H_{max}(P); 0{,}9 \cdot H_{max}(P)]$ и $H_{max}(P) = \log_2 m$,
распределение случайной величины ЛС с ростом объема выборки стремится к нормальному закону.

Показано, что среди сложных и простых ЦМ, матрицы которых равны, ЛС больше у сложных ЦМ из-за избыточности двоичного кодирования состояний. ЛС зависит от $H(P)$ и не зависит от m. Если на данном этапе построения профиля ЛС наблюдается горизонтальный тренд, то изменяется $f(x)$ без увеличения L или для АБМ являются предсказуемыми символы последовательности. Значение ЛС растет при повторе символов последовательности, не начинающихся с начала последовательности. Полученные оценки ЛС ЦМ могут служить оценками необходимой величины минимальной степени полинома при моделировании ЦМ над полем $GF(q_c)$ (раздел 2.3).

В **четвертой главе** "Комплекс методик и программ для решения задач построения и анализа полиномиальных функций и моделирования случайных последовательностей" описывается разработанный комплекс методик и программ, реализующий методы и алгоритмы, предложенные в диссертации. Комплекс позволяет решать следующие задачи: преобразование закона цепи Маркова в полиномиальную модель с использованием двоично-рационального разложения СМ и

представление марковских функций полиномиальными моделями; тестирование предложенных полиномиальных моделей; получение закона расширенной цепи Маркова; исследование характеристик марковских и псевдомарковских циклических последовательностей с помощью АБМ.

Основные результаты работы

1. Разработан новый метод моделирования расширенных цепей Маркова в поле GF(2^n), основанный на предложенном методе определения закона расширенной цепи Маркова по заданной стохастической матрице простой цепи Маркова. Доказаны теоремы, устанавливающие новые свойства (структурные, асимптотические) стохастических матриц расширенных цепей Маркова и оценки минимального порядка поля GF(2^n) для представления расширенных цепей Маркова полиномиальными функциями.

2. Предложены новые алгоритмы разложения двоично-рациональных стохастических матриц на имплицирующий вектор и множество стохастических булевых матриц, позволяющие снизить вычислительную сложность разложения и получить точную оценку размера имплицирующего вектора и порядка поля GF(2^n) для описания полиномиальных функций. Доказаны теоремы, обосновывающие алгоритмы и оценки.

3. Предложен новый метод моделирования случайных последовательностей фиксированной длины N из класса неоднородных цепей Маркова, заданных стохастическими матрицами, на основе полиномов минимальной степени над конечным полем GF(q_c), $q_c \geq 2$, позволяющий повысить точность представления стохастических матриц полиномами пропорционально величине $1/N$. Доказана теорема, устанавливающая существование минимальных полиномов для представления стохастических матриц с заданной точностью.

4. Сформулированы и доказаны теоремы, составляющие основу предложенного аналитического метода вычисления характеристик полиномиальных нелинейных динамических моделей над полем GF(2^n), порождающих случайные последовательности из класса функций конечных однородных цепей Маркова.

5. Предложена новая методика статистического анализа однородных простых и сложных цепей Маркова по критерию линейной сложности. Статистическим моделированием получены оценки линейной сложности реализаций цепей Маркова.

6. Разработан комплекс методик и программ, реализующий предложенные методы и алгоритмы.

Список публикаций по теме диссертации.

I. Статьи по теме диссертации, опубликованные в журналах из перечня ВАК.

1. Захаров В.М., Эминов Б.Ф. Анализ нелинейных моделей преобразователей случайных последовательностей над полем GF(2^n) на основе стохастических матриц // Вестник Казанского государственного технического университета им. А.Н. Туполева. - Казань: КГТУ им. А.Н. Туполева, 2006, №3. - С. 41-46.

2. Эминов Б.Ф. Метод моделирования случайных последовательностей класса неоднородных цепей Маркова полиномами минимальной степени над полем GF(q) // Системы управления и информационные технологии. Вып. 4.1(30). - Воронеж: Изд-во "Научная книга", 2007. - С. 203-207.

3. Захаров В.М., Эминов Б.Ф. Анализ алгоритмов разложения двоично-рациональных

стохастических матриц на комбинацию булевых матриц // Информационные технологии, №3. - М.: Изд-во Новые технологии, 2008. - С. 54-59.

II. Статьи в сборниках и материалах научно-технических конференций.

4. Эминов Б.Ф. К задаче анализа полиномиальных моделей автономных вероятностных автоматов // XII Туполевские чтения: Международная молодежная научная конференция. Том 3. - Казань: КГТУ им. А.Н. Туполева, 2004. - С. 60-62.

5. Захаров В.М., Эминов Б.Ф. Автоматное моделирование расширенных цепей Маркова // Актуальные проблемы современной науки: Труды 1-го Международного форума молодых ученых и студентов.Ч.18.-Самара: Изд-во Самар.гос.техн.ун-та, 2005.- С.146-148.

6. Эминов Б.Ф. Программный комплекс обучающих средств "Основы криптографической защиты информации" // Прикладная информатика - 2004: Доклады факультетской научно-технической конференции. - Казань: КГТУ им. А.Н. Туполева, 2005. - С. 84-88.

7. Эминов Б.Ф. Анализ полиномиальных моделей автономных вероятностных автоматов // Прикладная информатика - 2004: Доклады факультетской научно-технической конференции. - Казань: КГТУ им. А.Н. Туполева, 2005. - С. 36-40.

8. Дьячков В.В., Эминов Б.Ф. Временное прогнозирование функционирования предприятия на нейронных сетях // Информационная культура в системе подготовки будущего инженера: Материалы региональной научно-методической конференции. Нижнекамск. - Казань: КГТУ им. А.Н. Туполева, 2006. - С. 64-66.

9. Эминов Б.Ф. Построение имплицирующего вектора на основе двоично-рационального представления элементов стохастических матриц // Информационная культура в системе подготовки будущего инженера: Материалы региональной научно-методической конференции, Нижнекамск. - Казань: КГТУ им. А.Н. Туполева, 2006. - С. 222-224.

10. Эминов Б.Ф. Модели ситуационного управления как инструмент познания // Всероссийский семинар Ситуационные исследования: вып. 2. Типология ситуаций // Под ред. Н.М.Солодухо. - Казань: КГТУ им.А.Н.Туполева, 2006. - С. 84-94.

11. Эминов Б.Ф. Минимизация автоматной модели расширенной цепи Маркова методом /-эквивалентных преобразований//XIV Туполевские чтения:Международная молодежная науч. конференция,том 4.-Казань:КГТУ им.А.Н.Туполева,2006.-С.74-76.

12. Захаров В.М., Эминов Б.Ф. Статистический анализ линейной сложности регулярных цепей Маркова // Исследования по информатике. Выпуск 10. ИПИ АН РТ.-Казань: Отечество,2006.-С. 37-50.

13. Эминов Б.Ф. Влияние точности представления двоично-рациональных элементов стохастических матриц на размер имплицирующего вектора // Научно-техническая конференция по вопросам информатики, вычислительной техники и информационной безопасности. - Казань: КГТУ им. А.Н. Туполева, 2006. - С. 122-125.

14. Эминов Б.Ф. Получение стохастической матрицы расширенной цепи Маркова//Наука и профессиональное образование: Материалы региональной научно-практической конференции, Нижнекамск.- Казань: КГТУ им. А.Н.Туполева, 2007.-С.225-230.

15. Захаров В.М., Эминов Б.Ф. Представление расширенных цепей Маркова над полем $GF(2^n)$ // Моделирование процессов. Труды Казанского научного семинара "Методы моделирования".Вып.3. - Казань:КГТУ им.А.Н.Туполева, 2007. - С. 270-286.

16. Эминов Б.Ф. Моделирование случайных последовательностей минимальными полиномами над конечным полем по заданной стохастической матрице // Информационные технологии моделирования и управления. Научно-технический журнал. Вып. 7 (41). - Воронеж: Изд-во Научная книга, 2007. - С. 811-818.

17. Эминов Б.Ф. Применение алгоритма Берлекемпа-Месси к синтезу и анализу рекуррентных двоичных последовательностей//XV Туполевские чтения: Международная

молодежная науч.конф.Том 3.-Казань:КГТУ им.А.Н.Туполева,2007.-С.90-92.

18. Эминов Б.Ф. Вычислительная сложность и имплицирующий вектор стохастических матриц с двоично-рациональными элементами // XV Туполевские чтения: Международная молодежная научная конференция. Том 3. - Казань: КГТУ им.А.Н.Туполева, 2007. - С. 87-90.

19. Эминов Б.Ф. Представление стохастических неразложимых матриц с заданной точностью минимальными полиномами над конечным полем // Наука, технологии, инновации. Материалы всероссийской научной конференции молодых ученых. Часть 1. - Новосибирск: Изд-во НГТУ, 2007. - С. 107-109.

III. Тезисы в сборниках и материалах научно-технических конференций.

20. Соколов С.Ю., Шамсетдинов М.И., Эминов Б.Ф. К задаче программной реализации вычисления произведения элементов поля Галуа // X Всероссийские Туполевские чтения студентов. Том 2. - Казань: КГТУ им.А.Н.Туполева, 2002. - С.32.

21. Соколов С.Ю., Эминов Б.Ф. К задаче программной реализации полиномиальной модели конечного детерминированного автомата // XI Туполевские чтения: Всероссийская молодежная научная конференция. Том 3. - Казань: КГТУ им. А.Н. Туполева, 2003. - С. 27.

22. Эминов Б.Ф. Анализ линейной сложности эргодических цепей Маркова // Всероссийская научная конференция студентов и аспирантов. - Таганрог: Изд-во Таганрогского гос. радио-техн. ун-та, 2004. - С. 242-243.

23. Эминов Б.Ф. Программный комплекс обучающих средств "Основы криптографической защиты информации" // XII Туполевские чтения: Международная молодежная научная конференция. Том 3. - Казань: КГТУ им.А.Н.Туполева,2004.-С.88-89.

24. Эминов Б.Ф. Сравнительный анализ линейной сложности марковских и псевдомарковских последовательностей // XII Туполевские чтения: Международная молодежная научная конференция. Том 3. - Казань: КГТУ им.А.Н.Туполева,2004.-С.62-63.

25. Эминов Б.Ф. Программный комплекс лабораторного практикума для вычислений в полях Галуа // Материалы региональной научно-методической конференции Профессиональные компетенции в структуре модели современного инженера. - Нижнекамск: КГТУ им. А.Н.Туполева, 2005. - С. 104-105.

26. Захаров В.М., Эминов Б.Ф. Статистический анализ линейной сложности цепных последовательностей из класса регулярных цепей Маркова // Инфокоммуникационные технологии глобального информационного общества: Тезисы докладов 3-ей ежегодной международной научно-практической конференции. - Казань: Изд-во КГУ им. В.И. Ульянова-Ленина, 2005. - С. 82-84.

27. Эминов Б.Ф. Автоматный метод моделирования расширенных цепей Маркова // Туполевские чтения: Международная молодежная научная конференция. Том 3. - Казань: КГТУ им. А.Н. Туполева, 2005. - С. 59-60.

28. Захаров В.М., Эминов Б.Ф. Статистические оценки линейной сложности марковских последовательностей по критерию энтропии // Проблемы теоретической кибернетики: Тезисы докладов XIV международной конференции. - М.: Изд-во механико-математического фак-та МГУ, 2005.-С. 49.

IV. Работы, зарегистрированные в фонде алгоритмов и программ.

29. Захаров В.М., Эминов Б.Ф. Электронное учебное пособие "Лабораторный практикум вычислений в конечных полях" // Регистрация в отраслевом фонде алгоритмов и программ, № 10018. - М., 2008.

Формат 60×84 1/16. Бумага офсетная. Печать офсетная.
Печ.л. 1,25. Усл.печ.л. 1,16. Усл.кр.-отт. 1,16. Уч.-изд.л. 1,04.
Тираж 100. Заказ Л 73.

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

10-2