

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2014

№1(23)

Свидетельство о регистрации: ПИ №ФС 77-33762
от 16 октября 2008 г.



ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

**РЕДАКЦИОННАЯ КОЛЛЕГИЯ ЖУРНАЛА
«ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА»**

Агибалов Г. П., д-р техн. наук, проф. (председатель); Девянин П. Н., д-р техн. наук, проф. (зам. председателя); Парватов Н. Г., д-р физ.-мат. наук, доц. (зам. председателя); Черемушкин А. В., д-р физ.-мат. наук, чл.-корр. Академии криптографии РФ (зам. председателя); Панкратова И. А., канд. физ.-мат. наук, доц. (отв. секретарь); Алексеев В. Б., д-р физ.-мат. наук, проф.; Бандман О. Л., д-р техн. наук, проф.; Быкова В. В., д-р физ.-мат. наук, проф.; Глухов М. М., д-р физ.-мат. наук, академик Академии криптографии РФ; Евдокимов А. А., канд. физ.-мат. наук, проф.; Закревский А. Д., д-р техн. наук, проф., чл.-корр. НАН Беларуси; Колесникова С. И., д-р техн. наук; Костюк Ю. Л., д-р техн. наук, проф.; Логачев О. А., канд. физ.-мат. наук, доц.; Салий В. Н., канд. физ.-мат. наук, проф.; Сафонов К. В., д-р физ.-мат. наук, проф.; Фомичев В. М., д-р физ.-мат. наук, проф.; Чеботарев А. Н., д-р техн. наук, проф.; Шойтов А. М., д-р физ.-мат. наук, чл.-корр. Академии криптографии РФ; Шоломов Л. А., д-р физ.-мат. наук, проф.

Адрес редакции: 634050, г. Томск, пр. Ленина, 36

E-mail: vestnik_pdm@mail.tsu.ru

В журнале публикуются результаты фундаментальных и прикладных научных исследований отечественных и зарубежных ученых, включая студентов и аспирантов, в области дискретной математики и её приложений в криптографии, компьютерной безопасности, кибернетике, информатике, программировании, теории надежности, интеллектуальных системах.

Периодичность выхода журнала: 4 номера в год.

Редактор *Н. И. Шидловская*

Верстка *И. А. Панкратовой*

Подписано к печати 11.03.2014.

Формат 60 × 84¹/₈. Усл. п. л. 13,4. Уч.-изд. л. 15. Тираж 300 экз.

Издательство ТГУ. 634029, Томск, ул. Никитина, 4

СОДЕРЖАНИЕ

ПАМЯТИ УЧИТЕЛЯ	5
ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ	
Аборнев А. В. Построение подстановок с использованием разрядно-подстановочных преобразований модуля над кольцом Галуа характеристики 4.....	9
Фомичев В. М. Эквивалентные по Фробениусу примитивные множества чисел	20
МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ	
Рожков М. И. Биективные отображения, порождаемые фильтрующим генератором....	27
Шушуев Г. И. Поиск оптимального линейного приближения сетей Фейстеля	40
МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ	
Сорокин С. Н. Метод обнаружения атак типа «отказ в обслуживании» на web-приложения.....	55
ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ	
Покровский А. В. О весовых спектрах одного класса линейных кодов.....	65
Таранников Ю. В. О рангах подмножеств пространства двоичных векторов, допускающих встраивание системы Штейнера $S(2, 4, v)$	73
ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ	
Дорохова А. М., Фомичев В. М. Уточнённые оценки экспонентов перемешивающих графов биективных регистров сдвига над множеством двоичных векторов	77
Корниенко А. С. Структура функциональных графов для циркулянтов с линейными булевыми функциями в вершинах	84
ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ	
Дюкова Е. В., Прокофьев П. А. Об асимптотически оптимальном перечислении неприводимых покрытий булевой матрицы	96
Pottosin Yu. V., Kardash S. N. Pipelining combinational circuits	106
ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ	
Афанасьев И. В. Применение КА-модели для исследования влияния загрязнений на динамику популяций голомянок и макрогектопуса в озере Байкал	114
СВЕДЕНИЯ ОБ АВТОРАХ	124
АННОТАЦИИ СТАТЕЙ НА АНГЛИЙСКОМ ЯЗЫКЕ	125

CONTENTS

TO TEACHER'S MEMORY	5
THEORETICAL BACKGROUNDS OF APPLIED DISCRETE MATHEMATICS	
Abornev A. V. Permutations induced by digit-permutable transformations of a module over a Galois ring of characteristic 4	9
Fomichev V. M. Primitive sets of numbers being equivalent by Frobenius	20
MATHEMATICAL METHODS OF CRYPTOGRAPHY	
Rozhkov M. I. Bijective mappings generated by filtering generator	27
Shushuev G. I. Finding the optimal linear approximation of Feistel network	40
MATHEMATICAL BACKGROUNDS OF COMPUTER SECURITY	
Sorokin S. N. Intrusion detection method for denial of service attacks on the web-applications	55
APPLIED CODING THEORY	
Pokrovskiy A. V. On the weight spectrum in linear codes of a class	65
Tarannikov Y. V. On ranks of subsets in the space of binary vectors admitting an embedding of a Steiner system $S(2, 4, v)$	73
APPLIED GRAPH THEORY	
Dorokhova A. M., Fomichev V. M. Improvement of exponent estimates for mixing graphs of bijective shift registers over a set of binary vectors	77
Kornienko A. S. Structure of functional graphs for circulants with linear Boolean functions at the vertices	84
COMPUTATIONAL METHODS IN DISCRETE MATHEMATICS	
Djukova E. V., Prokofjev P. A. On asymptotically optimal enumeration for irreducible coverings of Boolean matrix	96
Pottosin Yu. V., Kardash S. N. Pipelining combinational circuits	106
DISCRETE MODELS FOR REAL PROCESSES	
Afanasyev I. V. Cellular automata model application for investigation of pollution influence on population dynamics of comephorus and macrohectopus in Lake Baikal	114
BRIEF INFORMATION ABOUT THE AUTHORS	124
PAPER ABSTRACTS	125

ПАМЯТИ УЧИТЕЛЯ



25 февраля 2014 года не стало **Аркадия Дмитриевича Закревского** — выдающегося советского и белорусского учёного в области дискретной математики, информатики и кибернетики, профессора Томского государственного университета, создателя Русского языка программирования ЛЯПАС, члена-корреспондента НАН Беларуси, основателя ведущих научных школ Прикладной дискретной математики в ТГУ и Логического проектирования в ОИПИ НАН Беларуси, внёсших заметный вклад в развитие науки, в том числе по обеспечению безопасности Союзного государства.

22 мая 2013 г. ему исполнилось 85 лет. Родом из Ленинграда, он с 1936 по 1951 г. жил в Красноярске, в семье инженера-лесопатолога Закревского Дмитрия Филипповича, вместе с мамой (Анной Андреевной), учительницей младших классов, и старшим братом Валей. В военном 1942 г. умерли отец (от туберкулёза) и брат (от болезни поджелудочной железы). Спасаясь от голода, Аркадий бросил школу, не окончив семи классов. Пошёл в двухгодичное ремесленное училище связи, на специальность радиста. Там давали обед и 800 граммов хлеба в день! Учился работать на ключе, часами выстукивая сообщения в азбуке Морзе. Кроме обучения искусству радиооператора, ещё слесарил, делая отвёртки для винтовок. Учился в кружке фехтования на рапире.

В начале 1943 г. в Красноярск прибыла эвакуированная из Ленинграда радиолaborатория полярника Кренкеля, зимовавшего в 1937 г. на Северном полюсе в составе знаменитой четвёрки, прославившейся на весь мир, — Папанин, Кренкель, Фёдоров, Ширшов. Лаборатория прибыла в Красноярск без сотрудников, имея лишь оборудование на несколько миллионов рублей. Его передали ремесленному училищу связи, а заведующим назначили 15-летнего Аркадия. На примерах радиogramм Кренкеля он совершенствуется в азбуке Морзе. Кренкель отстукивал радиogramмы со скоростью 180 знаков в минуту, и Аркадий старался приблизиться к этой цифре. Сделал самостоятельно простейший длинноволновый радиоприемник, благо деталей было навалом, и он заработал!

К лету 1943 г. бросил училище связи и без документов сбежал в Норильскую экспедицию Желдорпроекта, принадлежавшую ГУЛАГу — Главному управлению лагерей МВД — и занимавшуюся проектированием железных дорог в Заполярье, в районах вечной мерзлоты. Ей нужны были радисты для летних полевых работ. В зиму 1944/45 г. Аркадия не успели вывезти с базы под Игаркой на большую землю, и он остался в тундре на долгую зимовку, на шесть месяцев, в совершенном одиночестве, питаясь зайцами, которых ловил петлями из отождённой проволоки от антенных растяжек. В апреле 1945 г. его забрасывают самолётом в Ангутиху — рыболовецкий посёлок на Енисее, недалеко от Туруханска. Утром 9 мая Аркадий получил радиogramму с сообщением о конце войны, радостный ходил с ней по посёлку и зачитывал. В начале зимы 1945 г. возвращается в Красноярск, в штаб Сибирского отделения Желдорпроекта. Работает на радиостанции этого отделения. Встретил одноклассников. Они уже окончили школу, учились в институте. А он? За всю Норильскую экспедицию не прочёл ни одной строчки! Аркадий идёт в вечернюю школу, в восьмой класс. Учится по старым самоучителям, которые нашёл в домашней библиотеке отца.

Весной 1946 г. его пригласили в Читинскую экспедицию, занимавшуюся проектированием железной дороги, соединяющей Транссибирскую магистраль с трассой БАМа — Байкало-Амурской магистрали, её планирование было начато ещё в 1938 г. Направили радистом в отряд, осуществлявший топологическую разведку и планирование участка железной дороги по берегу Витима, притока Лены.

С марта 1948 г. работает в Селенгинской экспедиции, которая проектирует железную дорогу из Советского Союза через Наушки и Улан-Батор в Пекин. 18 мая его перевели на базу экспедиции в Улан-Баторе — там потребовался радист. Пошёл в советскую среднюю школу. Познакомился с директором и договорился о сдаче выпускных экзаменов вместе со школьниками. Начало — 20 мая. Берёт учебники, спит по пять часов в сутки, интенсивно готовится по три дня к каждому экзамену. Все предметы выпускных экзаменов сдал успешно, по остальным, которые заносятся в аттестат, с его согласия поставили тройки. Получил полноценный аттестат зрелости. Не тратя времени, послал заявление с документами в Москву, в Институт иностранных языков.

Оно шло больше двух месяцев из-за бдительности почты, которая строго выполняла правила борьбы с утечкой информации. В сентябре пришёл отказ — заявление поступило слишком поздно.

С 1949 г. ещё одна экспедиция в Заполярье. Снова Игарка. В конце зимы 1950/51 г. призвали в армию. Уволился с работы, собрался. Но пришла оттепель, испортился аэродром, не смогли вывезти и отпустили, чтобы не кормить. Продолжил работать на рации.

Жаждал учиться! Сдал в местной школе экзамены экстерном — второй раз, для тренировки. Получил ещё один аттестат — лучше предыдущего, полученного в Улан-Баторе, исправив некоторые тройки.

Решил поступать в радиотехнический институт в Москве. В первых числах июля 1951 г. взял отпускные за шесть месяцев и отправился в Москву — сначала до Архангельска самолётом полярной авиации. Едва взлетели, самолёт забарахлил, вернулись в Игарку. Полёт отменили. Решил лететь в Красноярск, а далее — поездом до Москвы.

В Красноярске в привокзальной кассе — две длинные очереди и одна короткая, человек пять, — студенческая, как ему объяснили. Посоветовали обратиться в ГорОНО за соответствующей справкой. Её сразу же дали, вписав его фамилию в стандартный бланк. Вернулся к кассе и попросил билет до Москвы. Не дают! Оказалось, что в справке указан Томск.

Так он совершенно случайно попал в Томск. На вокзале в Томске билеты в Москву продаются свободно. Утро, а поезд уходит вечером. Раз уж попал сюда, надо познакомиться с городом, отправился на прогулку. Томск ему понравился, уютный, весь в зелени, на улицах много молодёжи, студентов. Подумал-подумал и решил остаться.

Зашёл в политехнический институт, узнал, что в нём имеется радиотехнический факультет, решил, что он ему подходит. Сдал документы.

До вступительных экзаменов ещё далеко. Зашёл в Университетскую рощу и в университет (ТГУ), побывал в Сибирском физико-техническом институте при университете, прослушал там лекцию для абитуриентов. Понравилась. Решил для надёжности сдавать экзамены одновременно в два вуза, благо у него были два аттестата зрелости.

Однако, когда подошёл август, обнаружил, что первый экзамен проводится в обоих вузах одновременно. Выбрал университет, пошёл забирать аттестат из политехнического. Не отдают! «Чёрт с вами, у меня есть ещё один аттестат, Улан-Баторский». Экзамены на физический факультет ТГУ сдал легко. Сбылась его мечта!

С 1951 по 1971 г. Аркадий Дмитриевич прошёл последовательно все ступени учебной, научной и педагогической деятельности в ТГУ — от студента до заведующего кафедрой, получив учёную степень доктора технических наук и учёное звание профессора. Здесь в начале 1960-х годов под его руководством родился алгоритмический язык ЛЯПАС — Логический Язык для Представления Алгоритмов Синтеза, названный американцами русским языком программирования — Russian programming language. Это было время, когда в западном мире ещё только вступали в обиход первые языки программирования — Фортран и Алгол.

В Советском Союзе язык ЛЯПАС был реализован на всех отечественных ЭВМ, начиная с одноадресной машины «Урал-1» и кончая БЭСМ-6, а также на ЭВМ семейств ЕС, СМ и VAX и на персональных компьютерах первых поколений; на нём написан ряд крупных систем автоматического синтеза дискретных управляющих систем для многочисленных предприятий министерств электронной и радиопромышленности СССР. Его изучали, реализовывали и применяли также за рубежом — в США, ФРГ, Польше, Югославии, Чехословакии, ГДР; странами-участницами СЭВ он был принят

в качестве международного языка программирования. Позднее, на волне демократии, с ликвидацией военно-промышленного комплекса страны и производства отечественных ЭВМ интерес к ЛЯПАСу пропал. Сейчас же, когда осознание необходимости для национальной безопасности России собственного программно-аппаратного обеспечения компьютерных систем стало свершившимся фактом, стал насущным вопрос возрождения родного языка программирования и его ориентации на криптографические приложения. С этой задачей успешно справляется кафедра защиты информации и криптографии, хранитель научной школы А. Д. Закревского в ТГУ. Теперь мы снова, как и четверть века назад, обучаем студентов программированию на ЛЯПАСе и совместно с ними разрабатываем доверенное системное и прикладное программное обеспечение на этом языке для автоматического синтеза безопасных компьютерных систем логического управления критически важными объектами и технологическими процессами в промышленности, на транспорте, в энергетике, науке и образовании и для криптографической защиты управляющей информации в них.

С 1972 г. Аркадий Дмитриевич жил и работал в Минске. В последнее время он — главный научный сотрудник Объединённого института проблем информатики Национальной академии наук Беларуси, член-корреспондент этой академии, академик Международной академии информатизации, информационных процессов и технологий. Автор около 500 научных статей и 15 монографий. По его собственному признанию, наибольший вклад он внёс в развитие следующих направлений научных исследований.

1. Логическая теория дискретных устройств (помехоустойчивое кодирование в синтезе надёжных логических схем, минимизация булевых функций от большого числа переменных, эффективное представление слабо определённых булевых функций полиномами Жегалкина и Рида — Маллера, эффективные методы логического анализа, синтеза и диагностики программируемых логических матриц).

2. Автоматизация программирования логических задач (русский язык программирования — ЛЯПАС, системное и прикладное программное обеспечение на его основе для решения алгоритмических задач дискретной математики).

3. Логические основы интеллектуальных систем (решение больших систем логических уравнений, распространение методов теории булевых функций на конечные предикаты, методы индуктивного и дедуктивного вывода в распознавании образов).

4. Автоматическое проектирование систем логического управления (язык ПРАЛУ для описания параллельных алгоритмов логического управления и основанные на нём математические методы алгоритмического проектирования дискретных управляющих систем, элементы теории параллельных автоматов).

5. Комбинаторные проблемы дискретной математики (новые методы решения многих комбинаторных задач на графах и матрицах).

От себя добавлю, что и в криптографии Аркадий Дмитриевич сделал революционный шаг, предложив ещё в 1959 г. симметричное шифрование на основе конечных автоматов с функциями выходов, инъективными в каждом состоянии автомата. Теперь такие автоматы называются обратимыми с нулевой задержкой.

С кафедрой защиты информации и криптографии ТГУ у Аркадия Дмитриевича всегда было тесное и плодотворное сотрудничество, тёплые человеческие отношения. Коллектив кафедры глубоко сожалеет и скорбит об уходе своего Учителя, дорогого Аркадия Дмитриевича, и заверяет в дальнейшем развитии его научных достижений на благо Отечества.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/23/2

УДК 512.6

ПОСТРОЕНИЕ ПОДСТАНОВОК С ИСПОЛЬЗОВАНИЕМ РАЗРЯДНО-ПОДСТАНОВОЧНЫХ ПРЕОБРАЗОВАНИЙ МОДУЛЯ НАД КОЛЬЦОМ ГАЛУА ХАРАКТЕРИСТИКИ 4

А. В. Аборнев

ООО «Центр сертификационных исследований», г. Москва, Россия

E-mail: abconf.c@gmail.com

Решается задача построения нелинейных подстановок на пространстве большой размерности с использованием только матрицы над кольцом Галуа характеристики 4 и разрядной функции этого кольца. Каждая такая подстановка может быть представлена как вектор-функция, у которой координатными функциями являются многочлены над полем. Ранее был анонсирован результат о построении подстановок из рассматриваемого класса, у которых ровно две координатные функции являются нелинейными. Здесь приводится полное доказательство этого результата.

Ключевые слова: разрядно-подстановочная матрица, подстановка, кольцо Галуа.

Введение

Пусть $R = \text{GR}(q^2, p^2)$ — кольцо Галуа мощности q^2 , характеристики p^2 с полем вычетов $\bar{R} = R/pR = \text{GF}(q)$, $q = p^r$. В частности, при $r = 1$ имеем $R = \mathbb{Z}_{p^2}$. Подмножество $P = \Gamma(R) = \{a \in R : a^q = a\}$ называют *p-адическим координатным множеством*, или *координатным множеством Тейлмюллера* кольца R . Будем называть его также *разрядным* множеством.

Каждый элемент $a \in R$ однозначно представляется в виде

$$a = a_0 + pa_1, \quad a_s \in P, \quad s \in \{0, 1\},$$

называемом *p-адическим разложением элемента a*. Отображения

$$\gamma_s : R \rightarrow P, \quad \gamma_s(a) = a_s, \quad s \in \{0, 1\},$$

будем называть *разрядными функциями в разрядном множестве P*, а элементы $a_s = \gamma_s(a)$ — *p-адическими разрядами элемента a*.

Алгебра $(P, \oplus, \cdot)$ с операцией сложения $a \oplus b = \gamma_0(a + b)$, $a, b \in P$, является полем.

Понятия *p-адического разложения* и значения функции γ_s естественным образом (поэлементно) распространяются на матрицы $A \in R_{m \times m}$. При этом мы используем обозначение $A_s = \gamma_s(A) = (a_s(ij))$. Таким же естественным образом операции $\oplus, \cdot$ распространяются на матрицы над полем P , при этом операцию умножения матриц над полем обозначим через $\odot$.

Каждая матрица $A \in R_{m,m}$ определяет отображение $\pi_A : P^m \rightarrow P^m$

$$\pi_A(\mathbf{y}) = \gamma_1(\mathbf{y}A^T) = \gamma_1(\mathbf{y}A_0^T) \oplus (\mathbf{y} \odot A_1^T) = (\psi_1(\mathbf{y}), \dots, \psi_m(\mathbf{y})), \quad \mathbf{y} \in P^m, \quad (1)$$

где $\psi_1, \dots, \psi_m$ — координатные функции и T — оператор транспонирования. Будем говорить, что π_A — *нелинейное* отображение, если оно не является гомоморфизмом группы $(P^m, \oplus)$.

В работе [1] было впервые показано, что для любого $m > 1$ существует обратимая матрица A , такая, что π_A является нелинейной подстановкой на пространстве P^m .

Если π_A — подстановка, то система функций $\psi_1, \dots, \psi_m$ в (1) называется *ортогональной* [2], матрица A при этом называется *разрядно-подстановочной* (или *РП-матрицей*).

Координатные функции $\psi_1, \dots, \psi_m$ в (1) суть многочлены над полем P от переменных $\mathbf{y} = (y_1, \dots, y_m) \in P^m$ вида

$$\psi_i(\mathbf{y}) = \gamma_1(a_0(i1)y_1 + \dots + a_0(im)y_m) \oplus l_i(\mathbf{y}), \quad i = 1, \dots, m, \quad (2)$$

где $l_i(\mathbf{y}) = a_1(i1)y_1 \oplus \dots \oplus a_1(im)y_m$ — линейные функции; γ_1 — однородный многочлен степени q над P . Для $p = 2$ имеем

$$\gamma_1(a_0(i1)y_1 + \dots + a_0(im)y_m) = \sigma_2(a_0(i1)y_1, \dots, a_0(im)y_m)^h, \quad (3)$$

где $h = 2^{r-1}$, $\sigma_2(x_1, \dots, x_m) = \sum_{1 \leq j < k \leq m} \oplus x_j x_k$ — элементарная симметрическая функция порядка 2 [3].

Вообще говоря, координатная функция $\psi_i(\mathbf{y})$ не является линейной тогда и только тогда, когда i -я строка матрицы A содержит более чем один обратимый элемент.

Всюду далее $R = \text{GR}(q^2, 4)$. Пусть $q = 2^r$, $A = A_0 + 2A_1$, $A_s = (a_s(ij)) \in P_{m,m}$, $s = 0, 1$. Сделаем невырожденную замену переменных $x_j^2 = y_j$, $j = 1, \dots, m$, в (2). Пользуясь (3), получаем, что ортогональность исходной системы (1) эквивалентна ортогональности следующей системы квадратичных функций от переменных $\mathbf{x} = (x_1, \dots, x_m)$:

$$g_i(\mathbf{x}) = \sigma_2(a_0^h(i1)x_1, \dots, a_0^h(im)x_m) \oplus d_i(\mathbf{x}), \quad i = 1, \dots, m, \quad (4)$$

где $d_i(\mathbf{x}) = \sum_{j=1}^m \oplus a_1(ij)x_j^2$, $i = 1, \dots, m$, — *диагональные* квадратичные функции. Очевидно, любая ортогональная система (4) соответствует некоторой РП-матрице. Таким образом, задача построения РП-матриц в рассматриваемом случае эквивалентна задаче построения ортогональных систем (4).

В общем случае задача построения ортогональных систем многочленов не решена. Однако известны системы многочленов Диксона [2] и регулярные системы вида $g(\mathbf{x})$, $g(\mathbf{x}S)$, $\dots$, $g(\mathbf{x}S^{m-1})$, где g — квадратичная функция, существенно зависящая от переменных x_1, x_2, x_3 ; S — сопровождающая матрица некоторого многочлена степени m над P [4].

Основные результаты

Сначала опишем линейные преобразования, которые сохраняют свойство матрицы быть разрядно-подстановочной.

Рассмотрим множество Π_m всех разрядно-подстановочных матриц над кольцом R размера $m \times m$. Преобразование $\varphi : R_{m,m} \rightarrow R_{m,m}$ будем называть *Π-стабильным*, если выполнено условие

$$(A \in \Pi_m) \iff (\varphi(A) \in \Pi_m).$$

Утверждение 1. Множество линейных Π -стабильных преобразований содержит следующие элементарные преобразования:

- 1) перестановка строк (столбцов) матрицы;
- 2) умножение строки (столбца) матрицы на элемент из $\Gamma(R)^*$.

Доказательство. Для доказательства достаточно заметить, что матрица является разрядно-подстановочной тогда и только тогда, когда система координатных функций соответствующей подстановки ортогональна. Действительно, указанные преобразования строк матрицы A равносильны соответствующим преобразованиям многочленов в системе (2). Перестановка столбцов эквивалентна перестановке переменных $x_1, \dots, x_m$.

Пусть теперь φ — умножение k -го столбца матрицы A на $c \in \Gamma(R)^*$. Положим $A' = \varphi(A)$. В этом случае отображение $\pi_{A'}$ задается системой многочленов

$$\psi'_i(x_1, \dots, x_m) = a_1(i1)x_1 \oplus \dots \oplus ca_1(ik)x_k \oplus \dots \oplus a_1(im)x_m \oplus \bigoplus_{(j_1 \dots j_m) \in I(m,p)} \frac{1}{j_1! \dots j_m!} (a_0(i1)x_1)^{h_{j_1}} \dots (ca_0(ik)x_k)^{h_{j_k}} \dots (a_0(im)x_m)^{h_{j_m}},$$

где $i = 1, \dots, m$. Очевидно, невырожденная замена переменных $y_k = cx_k$, $y_j = x_j$, $j \neq k$ сохраняет свойство ортогональности системы многочленов. При этом полученная система многочленов $\psi_i(y_1, \dots, y_m)$, $i = 1, \dots, m$, является системой координатных функций преобразования π_A . ■

Будем называть преобразования матриц из теоремы 1 *мономиальными*. Назовём *мономиальной* матрицу вида

$$\begin{pmatrix} a_1 \vec{E}_{i_1} \\ \vdots \\ a_m \vec{E}_{i_m} \end{pmatrix},$$

где $(i_1, \dots, i_m)$ — перестановка чисел от 1 до m ; $\vec{E}_k$ — k -я строка единичной матрицы; $a_k \in \Gamma(R)^*$, $k = 1, \dots, m$.

Очевидно, мономиальное преобразование системы строк (столбцов) матрицы равносильно умножению её на соответствующую мономиальную матрицу слева (справа).

Следствие 1. Умножение матрицы A слева (справа) на мономиальную матрицу является Π -стабильным преобразованием.

Будем говорить, что матрицы $A, B \in R_{m,m}$ *мономиально-эквивалентны*, если B получается из A применением конечного набора мономиальных преобразований. Так как произведение мономиальных матриц и матрица, обратная к мономиальной, также есть мономиальная матрица, то отношение мономиальной эквивалентности рефлексивно, симметрично и транзитивно, и мономиальная эквивалентность матриц A, B равносильна условию $B = M_1 A M_2$, где M_1, M_2 — мономиальные матрицы.

В связи со сказанным для описания множества Π_m достаточно в каждом классе мономиально-эквивалентных матриц из $R_{m,m}$ найти удобный для анализа элемент и проверить его принадлежность множеству Π_m .

Приведём необходимые результаты из теории квадратичных функций [5, 6]. Для любой квадратичной функции $g : P^m \rightarrow P$ билинейная функция $f : P^m \times P^m \rightarrow P$ вида

$$f(\mathbf{x}, \mathbf{y}) = g(\mathbf{x} \oplus \mathbf{y}) \oplus g(\mathbf{x}) \oplus g(\mathbf{y}) \quad (5)$$

называется *билинейной функцией, ассоциированной с g* .

Множество всех квадратичных функций, ассоциированных с одной и той же билинейной функцией f , есть множество всех функций вида $g(\mathbf{x}) \oplus d(\mathbf{x})$, где $d : P^m \rightarrow P$ — диагональная квадратичная функция. Подпространство $V_f^\perp = \{\mathbf{a} \in P^m : f(P^m, \mathbf{a}) = 0\}$ называется *ядром* f . Из (5) получаем свойство полулинейности ограничения g на $V_f^\perp$:

$$\forall a, b \in P \quad \forall \mathbf{u} \in V_f^\perp \quad (g(a\mathbf{x} \oplus b\mathbf{u}) = a^2 g(\mathbf{x}) \oplus b^2 g(\mathbf{u})). \quad (6)$$

Пусть $g_1, \dots, g_k$ — некоторая система квадратичных функций с ассоциированными билинейными функциями $f_1, \dots, f_k$ соответственно. Обозначим через $\mathcal{L}(g_1, \dots, g_k)$ множество, состоящее из $\mathbf{0}$ и всех векторов $\mathbf{b} \in P^m$, удовлетворяющих условию

$$\exists (c_1, \dots, c_k) \in P^k \setminus \{\mathbf{0}\} \quad (\mathbf{b} \in V_{c_1 f_1 \oplus \dots \oplus c_k f_k}^\perp, (c_1 g_1 \oplus \dots \oplus c_k g_k)(\mathbf{b}) \neq 0).$$

В работе [1] предлагается следующий способ построения ортогональных систем квадратичных функций.

Рассмотрим систему

$$g_1(x_1, \dots, x_m), \dots, g_k(x_1, \dots, x_m) \quad (7)$$

квадратичных функций и систему диагональных квадратичных функций

$$d_{k+1}, \dots, d_m. \quad (8)$$

Заметим, что подпространство

$$K = \{\mathbf{x} : d_i(\mathbf{x}) = 0, i = k+1, \dots, m\} \quad (9)$$

удовлетворяет условию $\dim K \geq k$, и $\dim K = k$, если и только если система (8) линейно независима.

Теорема 1 [1]. Для системы (7) следующие утверждения эквивалентны:

- 1) Существует система диагональных квадратичных функций (8), такая, что система $g_1, \dots, g_k, d_{k+1}, \dots, d_m$ ортогональна.
- 2) Существует система диагональных квадратичных функций (8) такая, что подпространство (9) удовлетворяет условиям

$$\dim K = k, K \subseteq \mathcal{L}(g_1, \dots, g_k). \quad (10)$$

- 3) Существует подпространство $K \leq_P P^m$, удовлетворяющее (10).

Многочлен $g \in P[x_1, \dots, x_m]$ называется *сбалансированным*, если для каждого $a \in P$ уравнение $g(\mathbf{x}) = a$ имеет $|P|^{m-1}$ решений.

Дополнение уже двух квадратичных функций до ортогональной системы является более сложной задачей. Зафиксируем числа $1 < s \leq k < t \leq m$. Ниже для любого $m > 2$ описаны системы из двух квадратичных функций

$$\begin{cases} g_1(x_1, \dots, x_m) = \sigma_2(x_1, \dots, x_k) \oplus d_{11}x_1^2 \oplus \dots \oplus d_{1m}x_m^2, \\ g_2(x_1, \dots, x_m) = \sigma_2(x_s, \dots, x_t) \oplus d_{21}x_1^2 \oplus \dots \oplus d_{2m}x_m^2, \end{cases} \quad (11)$$

которые дополняются некоторыми диагональными квадратичными функциями $d_3, \dots, d_m$ до ортогональной системы

$$\begin{aligned} g_1 &= \sigma_2(x_1, \dots, x_k) \oplus d_{11}x_1^2 \oplus \dots \oplus d_{1m}x_m^2, \\ g_2 &= \sigma_2(x_s, \dots, x_t) \oplus d_{21}x_1^2 \oplus \dots \oplus d_{2m}x_m^2, \\ d_3 &= d_{31}x_1^2 \oplus \dots \oplus d_{3m}x_m^2, \\ &\vdots \\ d_m &= d_{m1}x_1^2 \oplus \dots \oplus d_{mm}x_m^2. \end{aligned} \quad (12)$$

Такая система определяет РП-матрицу $A = A_0 + 2A_1 \in R_{m,m}$, где $A_1 = (d_{ij})$, A_0 — обратимая матрица вида

$$A_0 = \begin{pmatrix} \underbrace{e \dots e}_k 0 \dots 0 \\ 0 \dots 0 \underbrace{e \dots e}_{t-s+1} 0 \dots 0 \\ \dots \end{pmatrix}$$

и каждая из строк A_0 с номерами $i \in \{3, \dots, m\}$ содержит ровно по одному ненулевому элементу.

Обозначим через $f_{n,l}(\mathbf{x}, \mathbf{y})$, $1 \leq n < l \leq m$, билинейную функцию, ассоциированную с $\sigma_2(x_n, \dots, x_l)$ в P^m . Для чисел s, k, t из (11) определим ядро: $V_0^\perp = V_{f_{1,k}}^\perp \cap V_{f_{s,t}}^\perp$.

Теорема 2. Для системы (11) тогда и только тогда существует система функций (12), такая, что

$$\Pi = (g_1, g_2, d_3, \dots, d_m) : P^m \rightarrow P^m \quad (13)$$

является биекцией, когда существует пара векторов $\mathbf{u}, \mathbf{v} \in P^m$, удовлетворяющая одному из следующих условий 1–6:

1. а) $\mathbf{u}, \mathbf{v} \in V_0^\perp$,
б) система векторов $\{(g_1(\mathbf{u}), g_2(\mathbf{u})), (g_1(\mathbf{v}), g_2(\mathbf{v}))\}$ линейно независима над P ;
2. а) $\mathbf{u} \in V_0^\perp$, $\mathbf{v} \in V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp \setminus V_0^\perp$ для некоторых $c_1, c_2 \in P$,
б) $(g_1(\mathbf{u}), g_2(\mathbf{u})) \neq (0, 0)$, $(c_1 g_1 \oplus c_2 g_2)(\mathbf{u}) = 0$, $(c_1 g_1 \oplus c_2 g_2)(\mathbf{v}) \neq 0$;
3. а) $s-1 \equiv t-k \equiv k-s+1 \equiv 1 \pmod{2}$ и

$$\begin{aligned} \mathbf{u} &= (0, \dots, 0, 0, \dots, 0, e, \dots, e, *, \dots, *), \\ \mathbf{v} &= (\underbrace{e, \dots, e}_{s-1}, \underbrace{0, \dots, 0}_{k-s+1}, \underbrace{0, \dots, 0}_{t-k+1}, *, \dots, *), \end{aligned}$$

- б) многочлен $D_1(x) = g_1(\mathbf{u}) \oplus x g_2(\mathbf{u}) \oplus x^2 g_1(\mathbf{v}) \oplus x^3 g_2(\mathbf{v})$ не имеет корней в P , $g_2(\mathbf{v}) \neq 0$;
4. а) $s-1 \equiv t-k \equiv 1 \pmod{2}$, $k-s+1 \equiv 0 \pmod{2}$ и

$$\begin{aligned} \mathbf{u} &= (e, \dots, e, e, \dots, e, \delta_1, \dots, \delta_1, *, \dots, *), \\ \mathbf{v} &= (\underbrace{\delta_2, \dots, \delta_2}_{s-1}, \underbrace{e, \dots, e}_{k-s+1}, \underbrace{e, \dots, e}_{t-k+1}, *, \dots, *), \end{aligned}$$

где $\delta_1 \neq e$, $\delta_2 \neq e$,

- б) многочлен $D_2(x) = g_1(\mathbf{u}) \oplus x \frac{\delta_2 \oplus e}{\delta_1 \oplus e} g_2(\mathbf{u}) \oplus x^2 g_1(\mathbf{v}) \oplus x^3 \frac{\delta_2 \oplus e}{\delta_1 \oplus e} g_2(\mathbf{v})$ не имеет корней в P , $g_2(\mathbf{v}) \neq 0$;
5. а) $s-1 \equiv 1 \pmod{2}$, $t-k \equiv k-s+1 \equiv 0 \pmod{2}$ и

$$\begin{aligned} \mathbf{u} &= (e, \dots, e, e, \dots, e, 0, \dots, 0, *, \dots, *), \\ \mathbf{v} &= (\underbrace{e, \dots, e}_{s-1}, \underbrace{0, \dots, 0}_{k-s+1}, \underbrace{0, \dots, 0}_{t-k+1}, *, \dots, *), \end{aligned}$$

- б) многочлен $D_3(x) = g_1(\mathbf{u}) \oplus x g_2(\mathbf{u}) \oplus x^2 g_1(\mathbf{v}) \oplus x^3 g_2(\mathbf{v})$ не имеет корней в P , $g_2(\mathbf{v}) \neq 0$;

6. а) $s - 1 \equiv 0 \pmod{2}$, $t - k \equiv 1 \pmod{2}$, $k - s + 1 \equiv 0 \pmod{2}$ и

$$\mathbf{u} = (\underbrace{0, \dots, 0}_{s-1}, \underbrace{0, \dots, 0}_{k-s+1}, \underbrace{e, \dots, e}_{t-k+1}, *, \dots, *),$$

$$\mathbf{v} = (0, \dots, 0, e, \dots, e, e, \dots, e, *, \dots, *),$$

- б) многочлен $D_4(x) = g_1(\mathbf{u}) \oplus xg_2(\mathbf{u}) \oplus x^2g_1(\mathbf{v}) \oplus x^3g_2(\mathbf{v})$ не имеет корней в P , $g_2(\mathbf{v}) \neq 0$.

Доказательство. По теореме 1, пара квадратичных функций g_1, g_2 дополняется некоторыми диагональными квадратичными функциями $d_3, \dots, d_m$ до биекции (13) тогда и только тогда, когда существует подпространство $K < P^m$, такое, что

$$K \subset \mathcal{L}(g_1, g_2), \quad \dim K = 2. \quad (14)$$

Заметим, что $\mathcal{L}(g_1, g_2)$ состоит из $\mathbf{0}$ и всех векторов $\mathbf{b} \in P^m$, удовлетворяющих условию

$$\exists (c_1, c_2) \in P^2 \setminus \{\mathbf{0}\} \quad \left(\mathbf{b} \in V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp, \quad (c_1 g_1 \oplus c_2 g_2)(\mathbf{b}) \neq 0 \right). \quad (15)$$

Достаточность. Для каждого пункта 1–6 теоремы покажем, что если выполнено условие подпункта а и $K = \langle \mathbf{u}, \mathbf{v} \rangle$, то (14) равносильно условию подпункта б. Тогда достаточность условий теоремы будет доказана.

1. Пусть $\mathbf{u}, \mathbf{v} \in V_0^\perp$ и $\varphi : P \rightarrow P$ — автоморфизм Фробениуса: $\varphi(x) = x^2$. Заметим, что $V_0^\perp = \bigcap_{(c_1, c_2) \neq (0,0)} V_{c_1 f_1 \oplus c_2 f_2}^\perp$. Следовательно, ввиду (15)

$$\forall \mathbf{b} \in V_0^\perp \quad (\mathbf{b} \in \mathcal{L}(g_1, g_2) \Leftrightarrow (g_1(\mathbf{b}), g_2(\mathbf{b})) \neq (0, 0)),$$

и из (6) получаем, что линейная независимость векторов $(g_1(\mathbf{u}), g_2(\mathbf{u})), (g_1(\mathbf{v}), g_2(\mathbf{v}))$ эквивалентна условию

$$\forall (c_1, c_2) \in P^2 \setminus \{\mathbf{0}\} \quad ((g_1(c_1^h \mathbf{u} \oplus c_2^h \mathbf{v}), g_2(c_1^h \mathbf{u} \oplus c_2^h \mathbf{v})) \neq (0, 0)),$$

где $h = q/2 = 2^{r-1}$, то есть $K = \langle \mathbf{u}, \mathbf{v} \rangle \subset \mathcal{L}(g_1, g_2)$ и $\dim K = 2$.

2. Пусть $\mathbf{u} \in V_0^\perp$, $\mathbf{v} \in V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp$ для $(c_1, c_2) \in P^2 \setminus \{\mathbf{0}\}$. Из (15) и условий $(g_1(\mathbf{u}), g_2(\mathbf{u})) \neq (0, 0)$, $(c_1 g_1 \oplus c_2 g_2)(\mathbf{v}) \neq 0$ следует, что $\mathbf{u} \in \mathcal{L}(g_1, g_2)$ и $\mathbf{v} \in \mathcal{L}(g_1, g_2)$. Пусть $K = \langle \mathbf{u}, \mathbf{v} \rangle$. Чтобы доказать (14), достаточно показать, что $\mathbf{u} \oplus c\mathbf{v} \in \mathcal{L}(g_1, g_2)$ для всех $c \in P^*$. Ввиду $\mathbf{u} \oplus c\mathbf{v} \in V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp$ требуется доказать соотношение

$$(c_1 g_1 \oplus c_2 g_2)(\mathbf{u} \oplus c\mathbf{v}) \neq 0.$$

По условию п. 2б теоремы и (6) получаем

$$(c_1 g_1 \oplus c_2 g_2)(\mathbf{u} \oplus c\mathbf{v}) = (c_1 g_1 \oplus c_2 g_2)(\mathbf{u}) \oplus c^2(c_1 g_1 \oplus c_2 g_2)(\mathbf{v}) = c^2(c_1 g_1 \oplus c_2 g_2)(\mathbf{v}) \neq 0.$$

Если же условие п. 2б не выполнено, то получаем $K \not\subset \mathcal{L}(g_1, g_2)$. Случай доказан.

Для доказательства остальных случаев понадобятся дополнительные обозначения и результаты. По определению (15) множество $\mathcal{M} = \bigcup_{(c_1, c_2) \in P^2 \setminus \{\mathbf{0}\}} V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp$ содержит

множество $\mathcal{L}(g_1, g_2)$. Поэтому для доказательства того, что некоторый вектор $\mathbf{b}$ принадлежит $\mathcal{L}(g_1, g_2)$, будем сначала доказывать, что $\mathbf{b} \in \mathcal{M}$. Нам понадобятся свойства векторов $\mathbf{b} \in \mathcal{M}$. Очевидно, что

$$\mathcal{M} = V_{f_{1,k}}^\perp \cup V_{f_{s,t}}^\perp \cup \left(\bigcup_{c \in P^*} V_{f_{1,k} \oplus c f_{s,t}}^\perp \right). \quad (16)$$

Нетрудно доказать, что для любой билинейной функции $f_{\overline{l,n}}$, ассоциированной с квадратичной функцией $\sigma_2(x_l, \dots, x_n)$, $1 \leq l < n \leq m$, выполняется

$$f_{\overline{l,n}}(\mathbf{x}, \mathbf{y}) = \sum_{i=l}^n \sum_{\substack{j=l \\ j \neq i}}^n x_i y_j = (x_l, \dots, x_n)(E \oplus I)(y_l, \dots, y_n)^T. \quad (17)$$

Для $\mathbf{b} \in P^m$ имеем

$$f_{\overline{l,n}}(\mathbf{b}, \mathbf{x}) = 0 \Leftrightarrow (b_l, \dots, b_n)(E \oplus I)(x_l, \dots, x_n)^T = 0 \Leftrightarrow (b_l, \dots, b_n)(E \oplus I) = \mathbf{0}.$$

Поэтому, пользуясь линейной алгеброй, можно доказать, что

$$\left((b_1, \dots, b_m) \in V_{f_{\overline{l,n}}}^\perp \right) \Leftrightarrow (b_l = \dots = b_n = (n - l + 1)\delta, \quad \delta \in P). \quad (18)$$

Для описания множества $\mathcal{M} \setminus \left(V_{f_{\overline{1,k}}}^\perp \cup V_{f_{\overline{s,t}}}^\perp \right)$ понадобятся две леммы.

Лемма 1. Если $\delta \in P$, $1 \leq l < n \leq m$, то

$$f_{\overline{l,n}}(\mathbf{x}, \mathbf{b}) = \delta \sum_{i=l}^n x_i \Leftrightarrow \exists a \in P (b_l = \dots = b_n = a, \delta = (n - l)a).$$

Доказательство. Не ограничивая общности, можно рассмотреть билинейную функцию $f_{\overline{1,m}}$. Тогда $f_{\overline{1,m}}(\mathbf{x}, \mathbf{b}) = \mathbf{x}(E \oplus I)\mathbf{b}$, где $I = (1)_{m \times m}$. Поэтому равенство $f_{\overline{1,m}}(\mathbf{x}, \mathbf{b}) = \delta \sum_{i=1}^m x_i$ эквивалентно уравнению

$$(E \oplus I)\mathbf{b} = (\delta, \dots, \delta)^T. \quad (19)$$

Заметим, что дефект матрицы $E \oplus I$ равен остатку от деления m на 2. Если m чётно, то $(E \oplus I)$ — обратимая матрица и $\mathbf{b} = (\delta, \dots, \delta)^T$ — единственное решение (19).

Пусть m нечётно. Если $\delta \neq 0$, то уравнение (19) не имеет решений, потому что $\mathbf{1}(E \oplus I) = \mathbf{0}$, но $\mathbf{1}(\delta, \dots, \delta)^T = \delta \neq 0$. Если $\delta = 0$, то $\mathbf{b} \in V_{f_{\overline{1,m}}}^\perp$. Таким образом, равенство (19) выполнено тогда и только тогда, когда $\delta = 0$ и существует $a \in P$, такое, что $b_1 = \dots = b_m = a$. ■

Лемма 2. При введённых выше обозначениях вектор $\mathbf{b} \in P^m$ принадлежит $V_{f_{\overline{1,k}} \oplus c f_{\overline{s,t}}}^\perp$, для данного $c \in P^*$, тогда и только тогда, когда существуют $a_1, a_2, a_3 \in P$, такие, что выполнены соотношения

$$\begin{aligned} 1) \quad & b_1 = \dots = b_{s-1} = a_1, \quad \sum_{j=s}^k b_j = s a_1; \\ 2) \quad & b_{k+1} = \dots = b_t = a_2, \quad \sum_{j=s}^k b_j = (t - k + 1) a_2; \\ 3) \quad & \begin{cases} (s-1)a_1 \oplus (t-k)a_2 = 0, & \text{если } c = e, \\ b_s = \dots = b_k = a_3, \quad \frac{(s-1)a_1 \oplus c(t-k)a_2}{(c \oplus e)} = (k-s)a_3, & \text{если } c \neq e. \end{cases} \end{aligned}$$

Доказательство. Пусть $\mathbf{b} \in V_{f_{\overline{1,k}} \oplus c f_{\overline{s,t}}}^\perp$ для некоторого $c \in P^*$, то есть

$$f_{\overline{1,k}}(\mathbf{x}, \mathbf{b}) \oplus c f_{\overline{s,t}}(\mathbf{x}, \mathbf{b}) = 0. \quad (20)$$

Из (17) имеем

$$\begin{aligned} f_{1,k}(\mathbf{x}, \mathbf{b}) \oplus c f_{s,t}(\mathbf{x}, \mathbf{b}) &= f_{1,s-1}(\mathbf{x}, \mathbf{b}) \oplus \sum_{j=s}^k b_j \sum_{i=1}^{s-1} x_i \oplus \sum_{j=1}^{s-1} b_j \sum_{i=s}^k x_i \oplus f_{s,k}(\mathbf{x}, \mathbf{b}) \oplus \\ &\oplus c \left(f_{s,k}(\mathbf{x}, \mathbf{b}) \oplus \sum_{j=k+1}^t b_j \sum_{i=s}^k x_i \oplus \sum_{j=s}^k b_j \sum_{i=k+1}^t x_i \oplus f_{k+1,t}(\mathbf{x}, \mathbf{b}) \right). \end{aligned}$$

Разбивая переменные на три группы, получаем, что равенство (20) эквивалентно следующим трём соотношениям:

$$f_{1,s-1}(\mathbf{x}, \mathbf{b}) = \sum_{j=s}^k b_j \sum_{i=1}^{s-1} x_i; \quad (21)$$

$$f_{k+1,t}(\mathbf{x}, \mathbf{b}) = \sum_{j=s}^k b_j \sum_{i=k+1}^t x_i; \quad (22)$$

$$\sum_{j=1}^{s-1} b_j \sum_{i=s}^k x_i \oplus f_{s,k}(\mathbf{x}, \mathbf{b}) = c \left(\sum_{j=k+1}^t b_j \sum_{i=s}^k x_i \oplus f_{s,k}(\mathbf{x}, \mathbf{b}) \right). \quad (23)$$

По лемме 1 равенство (21) равносильно условию 1 леммы 2. Аналогично, (22) эквивалентно условию 2 леммы 2.

Следовательно, (23) выполнено тогда и только тогда, когда

$$(s-1)a_1 \sum_{i=s}^k x_i \oplus f_{s,k}(\mathbf{x}, \mathbf{b}) = c \left((t-k)a_2 \sum_{i=s}^k x_i \oplus f_{s,k}(\mathbf{x}, \mathbf{b}) \right).$$

Если $c = e$, то имеем $((s-1)a_1 \oplus (t-k)a_2) \sum_{i=s}^k x_i = 0$, то есть $(s-1)a_1 \oplus (t-k)a_2 = 0$.

Если $c \in P \setminus \{0, e\}$, то

$$f_{s,k}(\mathbf{x}, \mathbf{b}) = \frac{(s-1)a_1 \oplus c(t-k)a_2}{e \oplus c} \sum_{i=s}^k x_i.$$

Применяя лемму 1, получаем условие 3 леммы 2. ■

Продолжение доказательства достаточности условий теоремы 2

3. Пусть условия п. 3 теоремы выполнены. Так как многочлен $D_1(x)$ не имеет корней в P , то $g_1(\mathbf{u}) \neq 0$. Из (18) имеем $\mathbf{u} \in V_{f_{1,k}}^\perp$, $\mathbf{v} \in V_{f_{s,t}}^\perp$, и так как $g_1(\mathbf{u}) \neq 0$, $g_2(\mathbf{v}) \neq 0$, получаем $\mathbf{u}, \mathbf{v} \in \mathcal{L}(g_1, g_2)$. Пусть $K = \langle \mathbf{u}, \mathbf{v} \rangle$. Теперь для доказательства условия (14) достаточно доказать, что $\mathbf{u} \oplus d\mathbf{v} \in \mathcal{L}(g_1, g_2)$ для любых $d \in P^*$. Действительно, для

$$\mathbf{b} = \mathbf{u} \oplus d\mathbf{v} = (\underbrace{d, \dots, d}_{s-1}, \underbrace{0, \dots, 0}_{k-s+1}, \underbrace{e, \dots, e}_{t-k+1}, *, \dots, *)$$

по лемме 2 получаем $\mathbf{b} \in V_{f_{1,k} \oplus d f_{s,t}}^\perp$. Из свойства (6) полулинейности имеем $(g_1 \oplus dg_2)(\mathbf{b}) = D_1(d)$. Следовательно, из условия п. 3б теоремы получаем $\mathbf{b} \in \mathcal{L}(g_1, g_2)$.

Очевидно, что если при условии п. 3а условие п. 3б не выполнено, то (14) неверно.

4. Пусть условия п. 4 теоремы выполнены. Из (18) имеем $\mathbf{u} \in V_{f_{1,k}}^\perp$, $\mathbf{v} \in V_{f_{s,t}}^\perp$. Как и в п. 3, пользуясь соотношениями $g_1(\mathbf{u}) \neq 0$, $g_2(\mathbf{v}) \neq 0$, получаем $\mathbf{u}, \mathbf{v} \in \mathcal{L}(g_1, g_2)$.

Пусть $K = \langle \mathbf{u}, \mathbf{v} \rangle$. Теперь для доказательства условия (14) достаточно доказать, что $\mathbf{u} \oplus d\mathbf{v} \in \mathcal{L}(g_1, g_2)$ для любого $d \in P^*$. Действительно,

$$\mathbf{b} = (\underbrace{e \oplus d\delta_2, \dots, e \oplus d\delta_2}_{s-1}, \underbrace{e \oplus d, \dots, e \oplus d}_{k-s+1}, \underbrace{\delta_1 \oplus d, \dots, \delta_1 \oplus d}_{t-k+1}, *, \dots, *).$$

Нетрудно убедиться, что $\mathbf{b}$ удовлетворяет условиям леммы 2 для $c = \frac{\delta_2 \oplus e}{\delta_1 \oplus e}d$, то есть $\mathbf{b} \in V_{f_{1,k} \oplus cf_{s,t}}^\perp$. Из (6) получаем $(g_1 \oplus cg_2)(\mathbf{b}) = D_2(d)$. Теперь из условия 4 теоремы следует, что $\mathbf{b} \in \mathcal{L}(g_1, g_2)$.

Если при условии п. 4а условие п. 4б не выполнено, то (14) неверно.

5. Пусть условия п. 5 теоремы выполнены. Из (18) имеем $\mathbf{u} \in V_{f_{1,k}}^\perp$, $\mathbf{v} \in V_{f_{s,t}}^\perp$. Пользуясь $g_1(\mathbf{u}) \neq 0$, $g_2(\mathbf{v}) \neq 0$, получаем, что $\mathbf{u}, \mathbf{v} \in \mathcal{L}(g_1, g_2)$. Пусть $K = \langle \mathbf{u}, \mathbf{v} \rangle$. Теперь для доказательства условия (14) достаточно доказать, что $\mathbf{u} \oplus d\mathbf{v} \in \mathcal{L}(g_1, g_2)$ для любого $d \in P^*$. Действительно,

$$\mathbf{b} = (\underbrace{e \oplus d, \dots, e \oplus d}_{s-1}, \underbrace{e, \dots, e}_{k-s+1}, \underbrace{0, \dots, 0}_{t-k+1}, *, \dots, *).$$

По лемме 2 получаем $\mathbf{b} \in V_{f_{1,k} \oplus df_{s,t}}^\perp$. Как в п. 3, пользуясь $(g_1 \oplus dg_2)(\mathbf{b}) = D_3(d)$ и условием п. 5 теоремы, получаем $\mathbf{b} \in \mathcal{L}(g_1, g_2)$.

Пункт 6 симметричен п. 5 относительно чётности чисел $s-1$, $t-k$.

Необходимость. Предположим, что существует подпространство $K = \langle \mathbf{u}, \mathbf{v} \rangle$, удовлетворяющее условию (14). Если один из векторов $\mathbf{u}, \mathbf{v}$ принадлежит множеству $V_0^\perp$, то выполнено условие п. 1 или 2 теоремы. В этом случае теорема доказана.

Если $\mathbf{u}, \mathbf{v} \in V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp \setminus V_0^\perp$ для некоторых $c_1, c_2 \in P$, то включение $K \subset \mathcal{L}(g_1, g_2)$ не выполнено в силу свойства (6) полулинейности и условия (15). Отсюда также следует, что если $\mathbf{u}, \mathbf{v} \in P^m \setminus V_0^\perp$, $K = \langle \mathbf{u}, \mathbf{v} \rangle$ и $K \subset \mathcal{L}(g_1, g_2)$, то для $c_1, c_2 \in P$

$$\dim \left(K \cap V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp \right) = 1, \quad (24)$$

и векторы $\mathbf{u}, \mathbf{v}$ могут быть выбраны так, что

$$\mathbf{u} \in V_{f_{1,k}}^\perp \setminus V_0^\perp, \quad \mathbf{v} \in V_{f_{s,t}}^\perp \setminus V_0^\perp. \quad (25)$$

Таким образом, для доказательства необходимости условия теоремы остаётся показать, что если $K = \langle \mathbf{u}, \mathbf{v} \rangle$, где $\mathbf{u}, \mathbf{v}$ выбраны в соответствии с (25), и верно (14), то выполнено одно из условий п. 3а–6а теоремы.

Сначала рассмотрим случаи, когда для чисел s, k, t не выполнены соотношения из условия теоремы. Они исчерпываются следующим списком:

- 1) $s-1 \equiv t-k \equiv 0 \pmod{2}$, $\mathbf{u}, \mathbf{v} \notin V_0^\perp$;
- 2) $s-1 \not\equiv t-k \pmod{2}$, $k-s+1 \equiv 1 \pmod{2}$, $\mathbf{u}, \mathbf{v} \notin V_0^\perp$.

Действительно, если, например, $\mathbf{u} \in V_0^\perp$, то имеет место случай 1 или 2 теоремы. Если не выполняются соотношения для чисел k, s, t , то имеет место один из случаев 3–6.

Покажем, что в этих двух случаях не выполняется условие (14). Для этого воспользуемся тем, что множество $\mathcal{M}$ из (16) содержит $\mathcal{L}(g_1, g_2)$, и применим лемму 2.

1. Пусть $s-1 \equiv t-k \equiv 0 \pmod{2}$, $\mathbf{u}, \mathbf{v} \notin V_0^\perp$.

По лемме 2 вектор $\mathbf{b}$ принадлежит ядру $V_{f_{1,k} \oplus cf_{s,t}}^\perp$ тогда и только тогда, когда выполнено соотношение

$$b_1 = \dots = b_{s-1} = \sum_{j=s}^k b_j = b_{k+1} = \dots = b_t = a_1, \quad (26)$$

и при $c \notin \{0, e\}$

$$\begin{cases} b_s = \dots = b_k = 0, & \text{если } k - s \equiv 1 \pmod{2}, \\ b_s = \dots = b_k, & \text{если } k - s \equiv 0 \pmod{2}. \end{cases}$$

Отсюда, если $c \notin \{0, e\}$, то

$$\begin{cases} b_1 = \dots = b_t = 0, & \text{если } k - s \equiv 1 \pmod{2}, \\ b_1 = \dots = b_t, & \text{если } k - s \equiv 0 \pmod{2}. \end{cases}$$

Последнее условие означает, что $\mathbf{b} \in V_0^\perp$. Поэтому если $P \neq \text{GF}(2)$, то получаем противоречие с равенством (24).

Рассмотрим случай, когда $P = \text{GF}(2)$. Имеем $K = \{\mathbf{0}, \mathbf{u}, \mathbf{v}, \mathbf{b}\}$, при этом для некоторых $a_1, a_2 \in P$

$$\begin{aligned} \mathbf{u} &= (a_1, \dots, a_1, a_1, \dots, a_1, *, \dots, *, *) \in V_{f_{1,k}}^\perp, \\ \mathbf{v} &= (*, \dots, *, a_2, \dots, a_2, a_2, \dots, a_2, *) \in V_{f_{s,t}}^\perp, \\ \mathbf{b} &= \mathbf{u} \oplus \mathbf{v} \in V_{f_{1,k} \oplus f_{s,t}}^\perp. \end{aligned}$$

Отсюда и равенств (26) получаем, что $b_s = \dots = b_k$ и для $c_1, c_2 \in P$

$$\begin{aligned} \mathbf{u} &= (a_1, \dots, a_1, a_1, \dots, a_1, c_1, \dots, c_1, *) \in V_{f_{1,k}}^\perp, \\ \mathbf{v} &= (c_2, \dots, c_2, a_2, \dots, a_2, a_2, \dots, a_2, *) \in V_{f_{s,t}}^\perp. \end{aligned}$$

Если $k - s + 1 \equiv 0 \pmod{2}$, то числа $k, t - s + 1$ также чётны, и из (18) следуют соотношения $a_1 = 0, a_2 = 0$. Отсюда $\mathbf{b} = (0, \dots, 0, 0, \dots, 0, 0, \dots, 0, *, \dots)$.

Если же $k - s + 1 \equiv 0 \pmod{2}$, то $\mathbf{b} = (b, \dots, b, b, \dots, b, b, \dots, b, *, \dots)$, $b \in P$.

В обоих случаях $\mathbf{b} \in V_0^\perp$ — противоречие.

2. Пусть теперь $s - 1 \not\equiv t - k \pmod{2}$, $k - s + 1 \equiv 1 \pmod{2}$, $\mathbf{u}, \mathbf{v} \notin V_0^\perp$. Не ограничивая общности, будем считать, что $s - 1$ чётно.

При данных s, k, t по лемме 2 вектор $\mathbf{b}$ принадлежит ядру $V_{f_{1,k} \oplus cf_{s,t}}^\perp$ тогда и только тогда, когда выполнено соотношение

$$b_1 = \dots = b_{s-1} = \sum_{j=s}^k b_j = b_{k+1} = \dots = b_t = 0, \quad (27)$$

и при $c \notin \{0, e\}$ получаем $b_s = \dots = b_k = a_3 \in P$. Отсюда, если $c \notin \{0, e\}$, то в силу нечётности $k - s + 1$ имеем $b_1 = \dots = b_t = 0$, то есть $\mathbf{b} \in V_0^\perp$.

Рассмотрим случай $P = \text{GF}(2)$. Аналогично получаем, что $b_s = \dots = b_k$, и так как $k - s + 1$ нечётно, то в силу равенств $b_s = \dots = b_k = 0$ и (27) имеем $\mathbf{b} \in V_0^\perp$. Это означает, что при условии (25) включение (14) не выполняется.

Пусть теперь $K = \langle \mathbf{u}, \mathbf{v} \rangle$, где $\mathbf{u}, \mathbf{v}$ выбраны в соответствии с (25), верно (14) и для чисел s, k, t выполнено одно из условий п. 3а–6а теоремы. Для завершения доказательства теоремы остаётся показать, что тогда векторы $\mathbf{u}, \mathbf{v}$ можно выбрать такими, как в условиях п. 3а–6а.

Проведём такое доказательство для случая 3. Остальные случаи разбираются аналогично. Пусть $s - 1 \equiv t - k \equiv k - s + 1 \equiv 1 \pmod{2}$. Порождающие векторы $\mathbf{u}, \mathbf{v}$ пространства K , как было показано выше, можно выбрать так, чтобы выполнялись условия (25).

Кроме того, из (24) следует, что для каждого $d \in P^*$ существует $c \in P^*$, такое, что $\mathbf{b} = \mathbf{u} \oplus d\mathbf{v} \in V_{f_{1,k} \oplus cf_{s,t}}^\perp$. При данных s, k, t по лемме 2 последнее включение равносильно системе соотношений

$$b_1 = \dots = b_{s-1} = a_1, \sum_{j=s}^k b_j = 0, b_{k+1} = \dots = b_t = a_2,$$

где, кроме того,

$$\begin{cases} a_1 = a_2, & \text{если } c = e, \\ b_s = \dots = b_k = a_3 \in P, \quad a_1 \oplus ca_2 = 0, & \text{если } c \notin \{0, e\}. \end{cases}$$

Отсюда, пользуясь свойством (18) и учитывая, что числа $k, t-s+1$ чётны, получаем, что для некоторых $u_1, v_1 \in P$

$$\begin{aligned} \mathbf{u} &= (0, \dots, 0, 0, \dots, 0, u_1, \dots, u_1, * \dots) \in V_{f_{1,k}}^\perp, \\ \mathbf{v} &= (v_1, \dots, v_1, 0, \dots, 0, 0, \dots, 0, * \dots) \in V_{f_{s,t}}^\perp. \end{aligned}$$

В качестве u_1, v_1 можно выбрать $e \in P$. Случай доказан.

Поступая аналогично в оставшихся случаях, получаем требуемые условия. ■

Заключение

Полученные в работе результаты показывают, что, используя только линейные преобразования модуля и разрядные функции кольца Галуа, можно строить эффективно реализуемые подстановки большой степени, у которых две координатные функции нелинейны. В дальнейшем интерес представляет изучение криптографических свойств описанных подстановок и расширение классов РП-матриц.

Автор выражает глубокую благодарность профессору А. А. Нечаеву за постановку задачи и внимание к проводимым исследованиям.

ЛИТЕРАТУРА

1. *Nechaev A. A. and Abornev A. V.* Nonlinear permutations on a space over a finite field induced by linear transformations of a module over a Galois ring // Математические вопросы криптографии. 2013. Т. 4. Вып. 2. С. 81–100.
2. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1. М.: Мир, 1988.
3. *Кузьмин А. С., Нечаев А. А.* Линейные рекуррентные последовательности над кольцами Галуа // Алгебра и Логика. 1995. Т. 34. № 2. С. 169–189.
4. *Никонов В. Г., Саранцев А. В.* О сложности реализации в базисе ДНФ регулярных систем булевых функций // Математические вопросы криптографии. 2010. Т. 1. Вып. 3. С. 45–65.
5. *Diedonné J. -A.* La Géométrie des Groupes Classiques. Ergebnisse der Mathematik und ihrer Grenzgebiete. B. 5. Springer, 1971.
6. *Kuzmin A. S. and Nechaev A. A.* Trace-function on a Galois ring in coding theory // LNCS. 1997. V. 1255. P. 277–290.

ЭКВИВАЛЕНТНЫЕ ПО ФРОБЕНИУСУ ПРИМИТИВНЫЕ МНОЖЕСТВА ЧИСЕЛ

В. М. Фомичев

Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия

E-mail: fomichev@nm.ru

Множества натуральных взаимно простых чисел $\{a_1, \dots, a_k\}$ и $\{b_1, \dots, b_l\}$ полагаются эквивалентными, если им соответствует одно и то же число Фробениуса, то есть $g(a_1, \dots, a_k) = g(b_1, \dots, b_l)$. Получены результаты, позволяющие для широкого класса множеств аргументов сократить вычисления при решении проблемы Фробениуса как в оригинальной постановке (определение числа Фробениуса $g(a_1, \dots, a_k)$), так и в расширенной постановке (определение множества всех чисел, не содержащихся в аддитивной полугруппе, порожденной множеством $\{a_1, \dots, a_k\}$).

Ключевые слова: *число Фробениуса, примитивное множество, порожденная множеством чисел аддитивная полугруппа.*

Введение

Основные обозначения:

$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, где $\mathbb{N}$ — множество всех натуральных чисел;

$(a_1, \dots, a_k)$ — наибольший общий делитель натуральных чисел $a_1, \dots, a_k$;

$\langle A \rangle$ — аддитивная полугруппа, порожденная множеством $A \subset \mathbb{N}$;

если $A = \{a_1, \dots, a_k\}$, $n \in \mathbb{N}_0$, то $nA = \{na_1, \dots, na_k\}$, $n + A = \{n + a_1, \dots, n + a_k\}$;

$A^{(i)} = \{a_1, \dots, a_i\}$, $C(A^{(i)}) = d_i \mathbb{N}_0 \setminus \langle A^{(i)} \rangle$, $d_i = (a_1, \dots, a_i)$, $i = 2, \dots, k$;

$z_i = \max C(A^{(i)})$, $\overline{\langle A^{(i)} \rangle} = \{a \in \langle A^{(i)} \rangle : a < z_i\}$, $i = 2, \dots, k$.

Диофантова проблема Фробениуса (ПФ) (другое название — Money Changing Problem) состоит в определении наибольшего натурального числа $t \notin \langle A \rangle$, то есть числа, не представимого линейной комбинацией (с неотрицательными целыми коэффициентами) взаимно простых чисел $a_1, \dots, a_k$.

Множество $A = \{a_1, \dots, a_k\}$ натуральных чисел, $k > 1$, называется примитивным, если $(a_1, \dots, a_k) = 1$. Следовательно, функция Фробениуса $g(a_1, \dots, a_k)$ определена на всех примитивных множествах $\{a_1, \dots, a_k\}$ равенством

$$g(a_1, \dots, a_k) = \max\{t \in \mathbb{N} : t \notin \langle A \rangle\}.$$

Определим $C(A) = C(A^{(k)})$ — множество всех натуральных чисел, не представимых линейными комбинациями чисел $a_1, \dots, a_k$, $k > 1$. Тогда число Фробениуса $g(A) = \max C(A)$. Задача определения множества $C(A)$ называется расширенной проблемой Фробениуса (РПФ).

Описание множества $C(A)$ и формула числа Фробениуса даны Сильвестром [1] для $k = 2$ ещё в 1884 г.: $|C(A)| = (g(a_1, a_2) + 1)/2$, где

$$g(a_1, a_2) = a_1 a_2 - a_1 - a_2. \quad (1)$$

При $k > 2$ активно изучался порядок множества $C(A)$ и некоторые его свойства [2, гл. 5]. В [3] анонсирован алгоритм РПФ на основе рекуррентного соотношения между множествами $C(A^{(k)})$, $k > 1$, и дана оценка его сложности.

Несмотря на то, что ПФ исследовалась намного активнее, формулы получены только для множеств частного вида при $k = 3, 4$. Объективные трудности в получении общей формулы обоснованы в [2], где показано, что уже при $k = 3$ нельзя разбить область определения на конечное число подобластей так, чтобы в каждой подобласти число Фробениуса $g(a_1, a_2, a_3)$ выражалось как значение полинома от аргументов.

Более продуктивным оказался алгоритмический подход к определению $g(a_1, \dots, a_k)$. Построен ряд алгоритмов как при $k = 3$ [4], так и при произвольном k . В [5, 6] разработан алгоритм вычисления функции Фробениуса при любом k с помощью экспоненцирования квадратной неотрицательной матрицы M порядка a_k и определения её показателя примитивности (экспонента) с использованием соотношения

$$g(a_1, \dots, a_k) = \exp M - a_k.$$

Вычислительная сложность алгоритма в битовых операциях равна $O(a_k^3)$, требуемая память — $O(a_k^2 \log a_k)$ битов. В [7] предложено улучшение этого алгоритма со сложностью $O(a_k^2)$, однако обоснование корректности алгоритма не представлено.

В [8] на основе теоретико-графового подхода построен алгоритм определения $g(a_1, \dots, a_k)$ со сложностью $O(a_1(k + \log a_1))$ арифметических операций. В [9] оценка сложности этого алгоритма снижена до величины порядка $O(ka_1)$ операций.

Данная работа посвящена сокращению вычислительной сложности РПФ и ПФ с использованием эквивалентности множеств аргументов функции Фробениуса. На основе исследования отношений эквивалентности РПФ и ПФ для исходного множества аргументов A редуцируются на его собственное подмножество порядка h , где $2 \leq h \leq \min(k, a_1)$. Это позволяет снизить оценку вычислительной сложности до величины $O(l(A) + ha_1)$ арифметических операций, где $l(A) \leq k$ и числа $l(A)$ и h в ряде случаев значительно меньше k .

1. Эквивалентность множества и подмножества

Примитивное множество чисел $A = \{a_1, \dots, a_k\}$ рассмотрим как возрастающую последовательность длины k , где $1 < a_1 < \dots < a_k$.

Множества A и A' называются эквивалентными (обозначается $A \cong A'$), если $\langle A \rangle = \langle A' \rangle$. Наименьшие числа эквивалентных множеств равны.

Примитивные множества A и A' называются g -эквивалентными (обозначается $A \stackrel{g}{\cong} A'$), если $g(A) = g(A')$. Из определения следуют свойства:

- 1) если $D \cong D'$, то $D \stackrel{g}{\cong} D'$;
- 2) $D \cong D' \Leftrightarrow C(D) = C(D')$;
- 3) $A^{(i)} \cong A^{(i-1)} \Leftrightarrow a_i \in \langle A^{(i-1)} \rangle$, необходимое условие этого $d_i = d_{i-1}$, $i = 2, \dots, k$.

Пусть $a \in \mathbb{N}$, $B \subseteq \mathbb{N}$. Положим, что a делит B (записывается $a \mid B$), если a делит без остатка некоторое число из B . В противном случае a не делит B (записывается $a \nmid B$).

Теорема 1. Примитивные множества $A^{(i)}$ и $A^{(i-1)}$ являются g -эквивалентными, если и только если $a_i \nmid (g(a_1, \dots, a_{i-1}) - \overline{\langle A^{(i-1)} \rangle})$.

Доказательство. Свойство $a_i \nmid (g(a_1, \dots, a_{i-1}) - \overline{\langle A^{(i-1)} \rangle})$ равносильно тому, что

$$g(a_1, \dots, a_{i-1}) \neq b + ra_i$$

при любом $b \in \langle A^{(i-1)} \rangle$ и любом натуральном r , то есть $g(a_1, \dots, a_{i-1}) \in C(A^{(i)})$. Вместе с тем, если $a > g(a_1, \dots, a_{i-1})$, то по определению $a \in \langle A^{(i-1)} \rangle$ и, значит, $a \in \langle A^{(i)} \rangle$.

Следовательно, $g(a_1, \dots, a_{i-1})$ — наибольшее натуральное число из множества $C(A^{(i)})$. Отсюда $g(a_1, \dots, a_{i-1}) = g(a_1, \dots, a_i)$. ■

Следствие 1. Пусть $(a_1, a_2) = 1$, тогда $\{a_1, a_2\} \stackrel{g}{\cong} \{a_1, a_2, a_3\}$, если и только если $a_3 \notin C(A^{(2)})$, где $C(A^{(2)}) = a_1 a_2 - a_1 - a_2 - \langle A^{(2)} \rangle$.

2. Эквивалентность, связанная с линейными соотношениями

Числа a_i и a_j множества A называются a_1 -эквивалентными, если $a_i \bmod a_1 = a_j \bmod a_1$. Примитивное множество $A = \{a_1, \dots, a_k\}$ разбивается на h классов a_1 -эквивалентности, где $2 \leq h \leq \min\{k, a_1\}$. Трансверсаль множества A по отношению a_1 -эквивалентности, состоящую из наименьших чисел классов, назовём a_1 -трансверсалью множества A и обозначим A/a_1 . Обозначим $W(A/a_1)$ последовательность порядковых номеров (начиная со второго) чисел a_1 -трансверсали.

Множество A называется приведённым, если $a_i \notin \langle A^{(i-1)} \rangle$, $i = 2, \dots, k$. Неприведённое примитивное множество A содержит приведённые примитивные подмножества. Приведённое подмножество B_A множества A , называемое A -базисом, строится последовательно: $a_1 \in B_A$; $a_2 \in B_A$, если и только если a_2 не кратно a_1 ; пусть из $\{a_1, \dots, a_{i-1}\}$ в подмножество B_A включены числа $b_1, \dots, b_j$, тогда $a_i \in B_A$, если и только если $d_{i-1} > d_i$ или $d_{i-1} = d_i$ и $a_i \in C(b_1, \dots, b_j)$, $i = 3, \dots, k$. Обозначим $W(B_A)$ последовательность порядковых номеров (кроме 1) чисел A -базиса, то есть таких $i \in \{2, \dots, k\}$, что $d_{i-1} > d_i$ или $d_{i-1} = d_i$ и $a_i \in C(a_1, \dots, a_{i-1})$.

Пример 1. Неприведённое множество $A = \{5, 14, 19, 28, 43, 49\}$ разбивается на три класса 5-эквивалентности: $C_0 = \{5\}$, $C_3 = \{28, 43\}$, $C_4 = \{14, 19, 49\}$. Здесь $A/5 = \{5, 14, 28\}$ есть 5-трансверсаль множества A ; A -базис есть множество $B_A = \{5, 14\}$; $W(B_A) = \{2\}$.

Неприведённое множество $A = \{7, 14, 23, 48, 56, 62\}$ разбивается на три класса 7-эквивалентности: $C_0 = \{7, 14, 56\}$, $C_2 = \{23\}$, $C_6 = \{48, 62\}$. Здесь $A/7 = B_A = \{7, 23, 48\}$ есть 7-трансверсаль множества A и A -базис, $W(B_A) = \{3, 4\}$.

Индексом примитивности множества A называется наименьшее натуральное число $p(A)$, такое, что $d_{p(A)} = 1$. Пусть $p(A) = p$, тогда $p \leq k$, $d_p = d_{p+1} = \dots = d_k = 1$. Последовательность порядковых номеров $i \in \{2, \dots, p\}$, таких, что $d_{i-1} > d_i$, обозначим $L(A)$.

Пример 2. Для множества $A = \{5, 14, 19, 28, 43, 49\}$: $p(A) = 2$, $L(A) = \{2\}$. Для множества $A' = \{6, 18, 27, 28, 42, 63, 79\}$: $p(A') = 4$, $L(A') = \{3, 4\}$.

Теорема 2. Для любого множества A выполнено:

- а) $B_A \subseteq A/a_1 \subseteq A$, $B_A \cong A/a_1 \cong A$;
- б) $L(A) \subseteq W(B_A) \subseteq W(A/a_1)$;
- в) $|B_A| \leq |A/a_1| \leq \min\{k, a_1\}$, и последняя оценка достижима.

Доказательство.

а) По построению $A/a_1 \subseteq A$ и $B_A \subseteq A$, покажем, что $B_A \subseteq A/a_1$, или, что равносильно, $A \setminus A/a_1 \subseteq A \setminus B_A$. Пусть $a_j \notin A/a_1$, тогда найдётся число $a_i \in A/a_1$, такое, что $a_i < a_j$ и $a_i \bmod a_1 = a_j \bmod a_1$. Тогда $a_j = a_i + r a_1$ при некотором $r \in \mathbb{N}$, следовательно, $a_j \notin B_A$.

Из доказанных включений следует, что $\langle B_A \rangle \subseteq \langle A/a_1 \rangle \subseteq \langle A \rangle$. Вместе с тем каждое из чисел множества $A \setminus B_A$ есть линейная комбинация чисел B_A , значит, $\langle A \rangle = \langle A/a_1 \rangle = \langle B_A \rangle$.

б) Включение $W(B_A) \subseteq W(A/a_1)$ следует из условия $B_A \subseteq A/a_1$. Если $i \in L(A)$, то $d_{i-1} > d_i$, значит, $i \in W(B_A)$. Следовательно, $L(A) \subseteq W(B_A)$.

в) По построению $|A/a_1| \leq k$. Вместе с тем $|A/a_1|$ не превышает числа наименьших неотрицательных вычетов по модулю a_1 . Достижимость оценки очевидна. ■

Следствие 2. Всякое примитивное множество $A = \{a_1, \dots, a_k\}$ содержит эквивалентное подмножество порядка не больше $\min\{k, a_1\}$.

3. Эквивалентность быстро возрастающих последовательностей

Далее положим, что примитивное множество $A = A/a_1$, то есть $k \leq a_1$ и числа $a_1, \dots, a_k$ несравнимы по модулю a_1 , где $a_1 \geq 3$.

Пусть $L(A) = \{n_2, \dots, n_r\}$, $1 < r < k$, то есть $d_{n_{j-1}} > d_{n_j}$, $j = 2, \dots, r$. Тогда последовательность разбивается на r отрезков $A_1, \dots, A_r$, где $A_j = (a_{n_j}, \dots, a_{n_{j+1}-1})$, $j = 1, \dots, r$, $n_1 = 1$, $n_r = p$, $n_{r+1} = k + 1$.

Обозначим: $J_1 = A_1 \setminus \{a_1\}$; $J(A)$ — множество чисел a_i из A , таких, что $d_{i-1} = d_i$ и a_i не делит множество $C(A^{(i-1)})$ (то есть $J(A) \subseteq \{n_2 + 1, \dots, k\} \setminus \{n_2, \dots, n_r\}$); $W(J)$ — возрастающая последовательность номеров чисел множества $J(A)$.

Отметим некоторые известные свойства:

- 1) если $B \subset A$ и $A \setminus B \subset \langle B \rangle$, то $A \cong B$;
- 2) множество $A^{(i)}/d_i = \{a_1/d_i, \dots, a_i/d_i\}$ примитивное, $\langle A^{(i)} \rangle = d_i \langle A^{(i)}/d_i \rangle$, $i = 2, \dots, k$;
- 3) $g(a_1, \dots, a_k) \leq (a_1 - 1)(a_k - 1) - 1$ [4, теорема 3.1.1].

Теорема 3. $A \cong A \setminus J(A)$; если $n_2 > 2$, то $A \cong A \setminus (J_1 \cup J(A))$.

Доказательство. Если $d_{i-1} = d_i$ и a_i не делит множество $C(A^{(i-1)})$, то $C(A^{(i)}) = C(A^{(i-1)})$, $i = n_2 + 1, \dots, k$. Отсюда если $a_i \in J(A)$, то $C(A^{(j)}) = C(B^{(j-1)})$ при любом $j \in \{i, \dots, k\}$, где $B = A \setminus \{a_i\}$. В частности, при $j = k$ получаем $C(A) = C(A \setminus \{a_i\})$, следовательно, $A \cong A \setminus \{a_i\}$.

Пусть $W(J) = \{i_1, \dots, i_t\}$. В силу произвольности рассмотренного множества A и числа $a_i \in J(A)$ рассуждения верны для множества A и числа a_{i_1} ; для множества $A \setminus \{a_{i_1}\}$ и числа a_{i_2} ; ..., для множества $A \setminus \{a_{i_1}, \dots, a_{i_{t-1}}\}$ и числа a_{i_t} . Значит,

$$A \cong A \setminus \{a_{i_1}\} \cong \dots \cong A \setminus \{a_{i_1}, \dots, a_{i_{t-1}}\} \cong A \setminus J(A).$$

Если $n_2 > 2$, то числа $a_2, \dots, a_{n_2-1}$ кратны a_1 . Следовательно, $J_1 \subset \langle a_1 \rangle$ и $J_1 \subset \langle (A \setminus J(A)) \setminus J_1 \rangle$. Тогда по утверждению а теоремы 2

$$A \setminus J(A) \cong (A \setminus J(A)) \setminus J_1 = A \setminus (J_1 \cup J(A)),$$

значит, $A \cong A \setminus (J_1 \cup J(A))$. ■

Далее без ущерба для общности считаем, что $n_2 = 2$.

Обозначим: $\gamma_j = d_{n_j}((a_1/d_{n_j} - 1)(a_{n_j}/d_{n_j} - 1) - 1)$, $l_1 = 1$, l_j — наибольший номер, такой, что $n_j \leq l_j < n_{j+1}$ и $a_{l_j} \leq \gamma_j$ (при $a_1 \geq 3$ корректность этих условий вытекает из утверждений б и в теоремы 2); $S_1 = (a_1)$, $S_j = (a_{n_j}, \dots, a_{l_j})$, то есть отрезок S_j составлен из первых (наименьших) $l_j - n_j + 1$ чисел отрезка A_j , $j = 2, \dots, r$; $S(A)$ есть конкатенация отрезков $S_1, S_2, \dots, S_r$; $l(A)$ — длина последовательности $S(A)$.

Следствие 3. $A \cong S(A)$, $l(A) \leq \min\{k, a_1 a_p - a_1 - 2a_p + p\}$, где $p = p(A)$.

Доказательство. При $j = 2, \dots, r$ выполнена цепь вложений $C(A^{(n_j)}) \supseteq \dots \supseteq C(A^{(n_{j+1}-1)})$. Тогда в соответствии с утверждениями б и в теоремы 2 каждое число

множеств $C(A^{(n_j)}), \dots, C(A^{(n_{j+1}-1)})$ не превышает γ_j . Если $l_j < n_{j+1} - 1$, то по определению числа l_j каждое из чисел $a_{l_j+1}, \dots, a_{n_{j+1}-1}$ больше γ_j и, следовательно, не делит ни одно из чисел множеств $C(A^{(n_j)}), \dots, C(A^{(n_{j+1}-1)})$. Тогда по теореме 1 $A \cong S(A)$.

По построению $l(A) \leq k$, так как $S(A) \subseteq A$. Заметим, что наибольшее число из $S(A)$ не превышает γ_p , где $\gamma_p = a_1 a_p - a_1 - a_p$, поэтому $l(A) \leq a_1 a_p - a_1 - a_p$. Вместе с тем $\{1, \dots, a_p\} \setminus \{a_1, \dots, a_p\} \cap A = \emptyset$; тогда, учитывая, что $\gamma_p > a_p$ при $a_1 \geq 3$, получаем $l(A) \leq \gamma_p - a_p + p = a_1 a_p - a_1 - 2a_p + p$. ■

Алгоритмы построения множеств A/a_1 и $A \setminus S(A)$ являются полиномиальными. Алгоритм построения множества $A \setminus J(A)$ экспоненциальный, по сложности он равен решению расширенной проблемы Фробениуса [4].

Наибольшее сокращение вычислительной сложности РПФ и ПФ достигается в тех случаях, когда $\{a_1, \dots, a_k\} \cong \{a_1, a_2\}$.

Пример 3. Пусть $A = \{5, 13, 18, 20, 57\}$. Вычисляем $A/5$: $5 = 20 = 0 \pmod{5}$, $13 = 18 = 3 \pmod{3}$, $57 = 2 \pmod{5}$. Тогда $A/5 = \{5, 13, 57\}$. Следовательно, $A \cong \{5, 13, 57\}$.

Вычисляем $J(A/5)$: $L(A/5) = \{13\}$, $r = 2$, $A_1 = \{5\}$, $A_2 = \{13, 52\}$, $\gamma_2 = 47 < 57$. Тогда $J(A/5) = \{57\}$, $(A/5) \setminus J(A/5) = \{5, 13\}$. Окончательно имеем $A \cong \{5, 13\}$.

4. Эквивалентность примитивных пар чисел

Обозначим: $[A]$ — класс g -эквивалентности, содержащий примитивное множество A ; $[A]_m$ — класс всех примитивных множеств порядка m , g -эквивалентных A , $m = 2, 3, \dots$

Теорема 4. Пусть $(a, b) = 1$. Тогда

$$[\{a, b\}]_2 = \{(a + \delta, b + \varepsilon) : a - b + 1 < \varepsilon < 0, \delta = (1 - a)\varepsilon / (b + \varepsilon - 1) \in \mathbb{N}, \\ 1 - a < \delta < 0, \varepsilon = (1 - b)\delta / (a + \delta - 1) \in \mathbb{N}\}.$$

Доказательство. Пусть $(a, b) \stackrel{g}{\cong} (a + \delta, b + \varepsilon)$, то есть $g(a, b) = g(a + \delta, b + \varepsilon)$, где $g(a, b) = ab - a - b$ в соответствии с (1). Тогда

$$b\delta + a\varepsilon + \delta\varepsilon - \delta - \varepsilon = 0. \quad (2)$$

Так как функция $g(a, b)$ монотонно возрастает при $a, b > 1$, то при заданных a, b уравнение (2) относительно δ, ε выполнено лишь при условии $\delta\varepsilon < 0$. Следовательно, множество $[\{a, b\}]_2$ состоит из примитивных пар вида $(a + \delta, b + \varepsilon)$, где $a + \delta < b + \varepsilon$ и $\delta\varepsilon < 0$. Пусть $\delta > 0$, $\varepsilon < 0$, тогда по условию задачи $a - b + 1 < \varepsilon < 0$ и из (1) следует

$$\delta = (1 - a)\varepsilon / (b + \varepsilon - 1). \quad (3)$$

Тогда $[\{a, b\}]_2$ включает все примитивные пары $(a + \delta, b + \varepsilon)$, где при $\varepsilon > a - b + 1$ число δ , определяемое формулой (3), является натуральным.

Пусть $\delta < 0$, $\varepsilon > 0$, тогда по условию задачи $1 - a < \delta < 0$ и из (2) следует

$$\varepsilon = (1 - b)\delta / (a + \delta - 1). \quad (4)$$

Тогда $[\{a, b\}]_2$ включает все примитивные пары $(a + \delta, b + \varepsilon)$, где при $1 - a < \delta < 0$ является натуральным число ε , определяемое формулой (4). ■

Следствие 4. Если $a > 2$, то $(2, g(a, b) + 2) \in [\{a, b\}]_2$; если $a > 3$, то $(3, (g(a, b) + 3)/2) \in [\{a, b\}]_2$.

Доказательство. Если $a > 2$, то при $\delta = 2 - a$ в соответствии с (4) получаем $\varepsilon = (1 - b)(2 - a) \in \mathbb{N}$. Следовательно, $\{a, b\} \stackrel{g}{\cong} \{2, g(a, b) + 2\}$.

Если $a > 3$, то при $\delta = 3 - a$ в соответствии с (4) получаем $\varepsilon = (1 - b)(3 - a)/2$. Хотя бы одно из чисел примитивной пары (a, b) нечётное. Следовательно, $\varepsilon \in \mathbb{N}$ и $\{a, b\} \stackrel{g}{\cong} \{3, (g(a, b) + 3)/2\}$. ■

Пример 4. Построим множество $[\{13, 22\}]_2$, где $g(13, 22) = 251$. При $\delta > 0$ имеем $-8 < \varepsilon < 0$, соответствующие значения δ приведены в табл. 1.

Таблица 1

 Значения δ

ε	-7	-6	-5	-4	-3	-2	-1
δ	6	72/15	60/16	48/17	2	24/19	12/20

Из табл. 1 следует, что $(\delta, \varepsilon) \in \{(2, -3), (6, -7)\}$. Пары $(13, 22)$ g -эквивалентна примитивная приведённая упорядоченная пара $(15, 19)$. Пара $(19, 15)$ не упорядочена, поэтому она исключена из класса $[\{13, 22\}]_2$.

При $\varepsilon > 0$ имеем $-12 < \delta < 0$; соответствующие значения ε приведены в табл. 2.

Таблица 2

 Значения ε

δ	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1
ε	231	105	63	42	147/5	21	15	84/8	7	42/10	21/11

Тогда $(\delta, \varepsilon) \in \{(-3, 7), (-5, 15), (-6, 21), (-8, 42), (-9, 63), (-10, 105), (-11, 231)\}$, и пара $(13, 22)$ g -эквивалентна семи примитивным приведённым упорядоченным парам: $(10, 29)$, $(8, 37)$, $(7, 43)$, $(5, 64)$, $(4, 85)$, $(3, 127)$ и $(2, 253)$. Итак, класс g -эквивалентности $[\{13, 22\}]_2$ содержит (вместе с самой парой $(13, 22)$) девять примитивных приведённых упорядоченных пар.

Заключение

Отношения эквивалентности примитивных множеств позволяют сократить сложность решения РПФ и ПФ путём редукции заданного примитивного множества к его собственному подмножеству, выполняемой с помощью полиномиального алгоритма.

Редукция множества A к множествам A/a_1 и $A \setminus S(A)$ позволяет понизить известные оценки сложности вычисления функции Фробениуса. В частности, сложность алгоритма экспоненцирования квадратной неотрицательной матрицы [5, 6] понижается до величины порядка $O(a^3)$, где a — наибольшее число редуцированного множества $(A/a_1) \setminus S(A/a_1)$. Оценка Боккера — Липтак [9] понижается до величины порядка $O(l(A) + ha_1)$, где h — порядок множества $(A/a_1) \setminus S(A/a_1)$, то есть в ряде случаев при больших значениях k оценка понижается до величины порядка $O(a_1)$.

ЛИТЕРАТУРА

1. *Sylvester J. J.* Problem 7382 // *Mathematical Questions from the Educational Times*. 1884. V. 37. P. 26.
2. *Curtis F.* On formulas for the Frobenius number of a numerical semigroup // *Math. Scand.* 1990. No. 67. P. 190–192.
3. *Фомичев В. М.* Эквивалентность примитивных множеств // *Прикладная дискретная математика. Приложение*. 2013. № 6. С. 20–24.

4. *Alfonsin J. R.* The Diophantine Frobenius Problem. Oxford University Press, 2005.
5. *Heap B. R. and Lynn M. S.* A graph-theoretic algorithm for the solution of a linear Diophantine problem of Frobenius // Numerische Math. 1964. No. 6. P. 346–354.
6. *Heap B. R. and Lynn M. S.* On a linear Diophantine problem of Frobenius: an improved algorithm // Numerische Math. 1965. No 7. P. 226–231.
7. *Bogart C.* Calculating Frobenius numbers with Boolean Toeplitz matrix multiplication // For Dr. Cull, CS 523, March 17, 2009. Oregon State University.
8. *Nijenhuis M.* A minimal-path algorithm for the “money changing problem” // Am. Math. Monthly. 1979. V. 86. P. 832–835.
9. *Bocker S. and Liptak Z.* The “money changing problem” revisited: computing the Frobenius number in time $O(ka_1)$. Technical Report No. 2004-2, Univ. of Bielefeld, Technical Faculty, 2004.

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

DOI 10.17223/20710410/23/4

УДК 519.4

БИЕКТИВНЫЕ ОТОБРАЖЕНИЯ, ПОРОЖДАЕМЫЕ
ФИЛЬТРУЮЩИМ ГЕНЕРАТОРОМ

М. И. Рожков

*Московский институт электроники и математики Национального исследовательского университета «Высшая школа экономики», г. Москва, Россия***E-mail:** rozhkov.m.i@yandex.ru

Рассматривается задача построения биективных отображений

$$B_{f,L}: (F_2)^n \rightarrow (F_2)^n, \quad B_{f,L}(x) = (f(x), f(\delta(x)), \dots, f(\delta^{n-1}(x))), \quad x \in (F_2)^n,$$

набор координатных функций которых задаётся преобразованием $\delta = \delta_L$ регистра сдвига большой длины n с функцией обратной связи L и нелинейной функцией выхода f от небольшого числа k аргументов ($k \ll n$). При этом биективность отображения $B_{f,L}$ равносильна ортогональности системы его координатных функций. В работе развивается метод, который сводит исходную задачу проверки биективности отображения $B_{f,L}$ при больших значениях длины регистра n к проверке его биективности применительно к регистрам сдвига ограниченной длины $n \leq n_0$, что позволяет эффективно использовать для её решения вычислительную технику. На основе данного метода в работе построены новые бесконечные классы биективных отображений для случая нелинейной функции f , зависящей от $k \leq 6$ переменных. Ранее аналогичные результаты были известны для случая, когда функция f зависит от $k = 3$ переменных. Полученные результаты могут быть полезны при построении и обосновании статистических свойств датчиков случайных чисел на основе фильтрующих генераторов. При этом особый практический интерес представляет выбор пар (f, L) , при которых одновременно обеспечивается биективность отображения $B_{f,L}$ и максимальность периода отображения δ_L .

Ключевые слова: ортогональные системы функций, регистр сдвига, фильтрующий генератор, понижающее множество.

1. Основные понятия и обозначения

Далее в работе будем придерживаться следующих основных понятий и обозначений (используемые алгебраические понятия изложены в [1]):

- F_2 — поле из двух элементов;
- $(f_1, f_2, \dots, f_m)$ — задание отображения $(F_2)^n \rightarrow (F_2)^m$ в виде системы координатных функций;
- $L(x_1, x_2, \dots, x_n) = L(x_1, x_2, \dots, x_{s(1)}, x_{n-s(2)+1}, x_{n-s(2)+2}, \dots, x_n)$ — функция обратной связи регистра сдвига длины $n \geq s(1) + s(2)$, линейная по переменной x_1 , ($s(1) \geq 1$, $s(2) \geq 0$ — заданные параметры);
- $\delta = \delta_L$ — преобразование векторов пространства $(F_2)^n$, осуществляемое регистром сдвига с функцией обратной связи $L(x_1, x_2, \dots, x_n)$, действующее на вектор

$(x_1, x_2, \dots, x_n) \in (F_2)^n$ по правилу

$$\delta(x_1, x_2, \dots, x_n) = (x_2, x_3, \dots, x_n, L(x_1, x_2, \dots, x_n));$$

- $f(x_1, x_2, \dots, x_k)$ — функция от k аргументов без запретов (являющаяся фильтрующей функцией съёма с соответствующего регистра сдвига);
- $B_{f,L}$ — преобразование двоичных векторов длины n (отображение $(F_2)^n \rightarrow (F_2)^n$), задаваемое системой координатных функций

$$B_{f,L} = (f(x), f(\delta(x)), \dots, f(\delta^{n-1}(x))), \quad x \in (F_2)^n.$$

В работе рассматриваются вопросы выбора нелинейной функции съёма f и функции обратной связи L , при которых преобразование $B_{f,L}$ является биективным. При этом биективность преобразования $B_{f,L}$ равносильна ортогональности системы его координатных функций [2]. В [2] показано, что при $n \geq 2^{k-1} + k - 1$ отсутствие запретов у функции $f = f(x_1, x_2, \dots, x_k)$ является необходимым условием биективности отображения $B_{f,L}$ (функции без запрета называют также функциями без потери информации, сильно равновероятными и совершенно уравновешенными [3–5]).

Известно [4], что для функции без запретов $f(x_1, x_2, \dots, x_k)$ при любом натуральном n существует ровно 2^{k-1} входных слов $x_1, x_2, \dots, x_{n+k-1}$, перерабатываемых данной функцией в любое фиксированное выходное слово $y(1), y(2), \dots, y(n)$ по закону

$$y(j) = f(x_j, x_{j+1}, \dots, x_{j+k-1}), \quad j = 1, 2, \dots, n.$$

Поэтому биективность преобразования $B_{f,L}$ равносильна тому, что среди этих 2^{k-1} входных слов ровно одно слово будет удовлетворять ограничениям

$$x_{n+1} = L(x) = L(x_1, x_2, \dots, x_n), \quad x_{n+2} = L(\delta_L(x)), \quad \dots, \quad x_{n+k-1} = L((\delta_L)^{k-2}(x)). \quad (1)$$

При этом $x_{n+1}, x_{n+2}, \dots, x_{n+k-1}$ как функции от независимых переменных $x_1, x_2, \dots, x_n$ (в силу ограничений на вид функции обратной связи L) зависят лишь от $k + s(1) - 2$ начальных переменных и от $s(2)$ последних переменных. Таким образом, выполняется ограничение 1 или нет для данного входного слова $x_1, x_2, \dots, x_{n+k-1}$, зависит только от его начального отрезка $x_1, x_2, \dots, x_{k+s(1)-2}$ длины $k + s(1) - 2$ и конечного отрезка $x_{n-s(2)+1}, \dots, x_n, x_{n+1}, x_{n+2}, \dots, x_{n+k-1}$ длины $k + s(2) - 1$.

Для заданных функции $f(x_1, x_2, \dots, x_k)$, натуральных $r, s \geq k - 1$ и выходного слова $Y = y(1), y(2), \dots, y(m)$ через $I = I(Y) = I_{r,s}(Y)$ обозначим систему пар векторов $(\alpha^{(i)}, \beta^{(i)})$, $i = 1, 2, \dots, 2^{k-1}$, где $\alpha^{(i)} = x_1, x_2, \dots, x_r$ и $\beta^{(i)} = x_{m+k-s}, x_{m+k-s+1}, \dots, x_{m+k-1}$ являются соответственно началами и концами входных слов $X = x_1, x_2, \dots, x_k, x_{k+1}, \dots, x_{k+m-1}$, перерабатываемых функцией f в выходное слово Y :

$$y(j) = f(x_j, x_{j+1}, \dots, x_{j+k-1}), \quad j = 1, 2, \dots, m.$$

Так как число различных входов X , отвечающих заданному выходу Y , в точности равно 2^{k-1} , то полагаем, что $I(Y)$ состоит из 2^{k-1} элементов. При этом соответствующие системы $I(Y)$ и $I(Z)$ считаем равными ($I(Y) = I(Z)$), если любой элемент $(\alpha, \beta) \in I(Y)$ встречается в $I(Z)$ ровно столько раз, сколько он встречается в $I(Y)$.

Определение 1. Двоичные последовательности $Y = y(1), y(2), \dots, y(n)$ и $Z = z(1), z(2), \dots, z(m)$ назовём эквивалентными (обозначим $Y \sim Z$), если $I_{k-1,k-1}(Y) = I_{k-1,k-1}(Z)$.

Пример 1. Для функции от трёх переменных $f(x_1, x_2, x_3) = x_1x_2 + x_2 + x_3$ выходным словам $Y_1 = (y(1), y(2), y(3), y(4)) = (0, 0, 0, 0)$ и $Z_1 = (z(1), z(2), z(3)) = (0, 0, 0)$ соответствуют следующие наборы входных слов:

$$(0, 0, 0, 0, 0, 0), (1, 0, 0, 0, 0, 0), (0, 1, 1, 0, 0, 0), (1, 1, 0, 0, 0, 0) \text{ для } Y_1, \\ (0, 0, 0, 0, 0), (1, 0, 0, 0, 0), (0, 1, 1, 0, 0), (1, 1, 0, 0, 0) \text{ для } Z_1.$$

Начала и окончания длины 2 входных векторов свидетельствуют, что

$$I_{2,2}(Y_1) = I_{2,2}(Z_1) = \{(00, 00), (10, 00), (01, 00), (11, 00)\}.$$

Следовательно, слова Y_1 и Z_1 являются эквивалентными. Аналогичным образом можно убедиться, что эквивалентны также слова $Y_2 = (0, 1, 0, 1, 0, 1)$ и $Z_2 = (0, 1)$, для которых

$$I_{2,2}(Y_2) = I_{2,2}(Z_2) = \{(00, 01), (10, 01), (01, 11), (11, 01)\}.$$

Определение 2. Упорядоченное множество натуральных чисел $\{h, t_1, t_2, \dots, t_\theta\}$, $h > t_1 > \dots > t_\theta$, $\theta \geq 1$, назовём *понижающим для функции* $f(x_1, x_2, \dots, x_k)$, если для любой последовательности Y длины h найдётся эквивалентная ей последовательность Z длины $t \in \{t_1, t_2, \dots, t_\theta\}$. Понижающее множество $\{h, t_1, t_2, \dots, t_\theta\}$ называем *равновесным*, если для любого $t \in \{t_1, t_2, \dots, t_\theta\}$ и любой последовательности Y длины t найдётся эквивалентная ей последовательность длины h . Понижающее множество $\{h, t\}$, состоящее из двух элементов, будем также называть *понижающей парой* и обозначать (h, t) .

Пример 2. Для функции от двух переменных $f(x_1, x_2) = x_1 + x_2$ выходным словам Y длины 1 и 2 соответствуют следующие множества входов: слову 0 — $\{(0, 0), (1, 1)\}$, слову 1 — $\{(0, 1), (1, 0)\}$, слову 00 — $\{(0, 0, 0), (1, 1, 1)\}$, слову 10 — $\{(0, 1, 1), (1, 0, 0)\}$, слову 01 — $\{(0, 0, 1), (1, 1, 0)\}$, слову 11 — $\{(0, 1, 0), (1, 0, 1)\}$. Отсюда получаем

$$I_{1,1}(Y = 0) \cup I_{1,1}(Y = 1) = \{\{(0, 0), (1, 1)\}, \{(0, 1), (1, 0)\}\}; \\ I_{1,1}(Y = 00) \cup I_{1,1}(Y = 10) \cup I_{1,1}(Y = 01) \cup I_{1,1}(Y = 11) = \{\{(0, 0), (1, 1)\}, \{(0, 1), (1, 0)\}\}.$$

Следовательно, для рассматриваемой функции множество $(h, t) = (2, 1)$ является равновесной понижающей парой.

Определение 3. *Длиной (расстоянием) эквивалентности* для заданной функции без запретов $f = f(x_1, x_2, \dots, x_k)$ назовём натуральное число n_0 , при котором любое слово длины $n > n_0$ эквивалентно некоторому слову длины $\leq n_0$.

Для функции из примера 2 расстояние эквивалентности, очевидно, равно 1.

Заметим, что если n_0 — длина эквивалентности функции f , то и любое $n > n_0$ также является её длиной эквивалентности. Кроме того, непосредственно из определения 3 вытекает: если n_0 — длина эквивалентности функции f , то множество

$$\{n_0 + 1, n_0, n_0 - 1, \dots, 2, 1\}$$

является для данной функции понижающим.

2. Вспомогательные утверждения

Лемма 1. Пусть $r, s \geq k - 1$, $I_{r,s}(Y) = I_{r,s}(Z)$, $\varepsilon \in \{0, 1\}$, $Y1 = \varepsilon Y$, $Z1 = \varepsilon Z$, $Y2 = Y\varepsilon$, $Z2 = Z\varepsilon$. Тогда $I_{r+1,s}(Y1) = I_{r+1,s}(Z1)$, $I_{r,s+1}(Y2) = I_{r,s+1}(Z2)$.

Доказательство. Пусть $X = x_1, x_2, \dots, x_k, x_{k+1}, \dots, x_{k+n-1}$ — произвольное входное слово, соответствующее выходному слову Y длины $|Y| = n$. Тогда входные слова, соответствующие выходному слову $Y2 = Y\varepsilon$, имеют следующий вид:

- 1) $X\sigma$, если имеется единственное значение $\sigma \in \{0, 1\}$, для которого

$$f(x_{n+1}, \dots, x_{n+k-1}, \sigma) = \varepsilon;$$

- 2) $X0, X1$, если $f(x_{n+1}, \dots, x_{n+k-1}, 0) = f(x_{n+1}, \dots, x_{n+k-1}, 1) = \varepsilon$;

- 3) таких входных слов не существует, если

$$f(x_{n+1}, \dots, x_{n+k-1}, 0) = f(x_{n+1}, \dots, x_{n+k-1}, 1) \neq \varepsilon.$$

Отсюда вытекает справедливость леммы для пары $Y2, Z2$. Аналогичным образом проводится доказательство и для пары $Y1, Z1$. ■

Лемма 2. Пусть $f(x_1, x_2, \dots, x_k) = \varphi(x_1, x_2, \dots, x_{k-1}) + x_k$. Двоичные последовательности $y(1), y(2), \dots, y(n)$ и $z(1), z(2), \dots, z(m)$ являются эквивалентными, если и только если при любом $\alpha \in (F_2)^{k-1}$

$$\delta_{y(n)}\delta_{y(n-1)}\dots\delta_{y(1)}(\alpha) = \delta_{z(m)}\delta_{z(m-1)}\dots\delta_{z(1)}(\alpha),$$

где $\delta_\varepsilon(x_1, x_2, \dots, x_{k-1}) = (x_2, x_3, \dots, x_{k-1}, \varphi(x_1, x_2, \dots, x_{k-1}) + \varepsilon)$.

Доказательство. Для функции $f(x_1, x_2, \dots, x_k) = \varphi(x_1, x_2, \dots, x_{k-1}) + x_k$ слова $X = x_1, x_2, \dots, x_{n+k-1}$, перерабатываемые этой функцией в фиксированное выходное слово $y(1), y(2), \dots, y(n)$, $y(j) = f(x_j, x_{j+1}, \dots, x_{j+k-1})$, $j = 1, 2, \dots, n$, задаются последовательностью векторов

$$\begin{aligned} \alpha_0 &= (x_1, x_2, \dots, x_{k-1}), \\ \alpha_1 &= (x_2, x_3, \dots, x_k), \quad x_k = \varphi(\alpha_0) + y(1) \Rightarrow \alpha_1 = \delta_{y(1)}(\alpha_0), \\ &\dots \\ \alpha_n &= (x_{n+1}, x_{n+2}, \dots, x_{n+k-1}), \quad x_{n+k-1} = \varphi(\alpha_{n-1}) + y(n) \Rightarrow \alpha_n = \delta_{y(n)}(\alpha_{n-1}). \end{aligned}$$

Отсюда и получаем утверждение леммы. ■

Лемма 3. Пусть $\{h, t_1, t_2, \dots, t_\theta\}$ — понижающее множество. Тогда

1. При любом натуральном ε множество $\{h + \varepsilon, t_1 + \varepsilon, t_2 + \varepsilon, \dots, t_\theta + \varepsilon\}$ также является понижающим. При этом оно будет равновесным, если таким является исходное множество.

2. При любом фиксированном $n_0 \geq t_\theta$ произвольное слово $Y = y(1), y(2), \dots, y(n)$ длины $n \geq n_0$ эквивалентно некоторому слову длины $t \in \{n_0, n_0 + 1, \dots, n_0 + h - t_\theta - 1\}$.

Доказательство. С учётом леммы 1 доказательство первой части леммы 3 легко проводится индукцией по ε . Докажем вторую часть. Пусть произвольное заданное слово $Y = y(1), y(2), \dots, y(n)$ длины $n \geq n_0$ эквивалентно некоторому слову $Z = z(1), z(2), \dots, z(t)$ длины $t \in \{n_0, n_0 + 1, \dots, n_0 + h - t_\theta - 1\}$. Тогда слово $Y_1 = (y(1), y(2), \dots, y(n), a) = Ya$ эквивалентно слову $Z_1 = Za$, длина которого

принадлежит множеству $\{n_0 + 1, n_0 + 2, \dots, n_0 + h - t_\theta\}$. Далее достаточно рассмотреть случай, когда длина слова Z_1 равна $t = n_0 + h - t_\theta$. Слово Z_1 можно представить в виде $Z_1 = VW$, где V — начало слова Z_1 (длины $(n_0 - t_\theta) \geq 0$), а W — его окончание длиной h . Тогда слово W эквивалентно некоторому слову W_1 длины $t \in \{t_1, t_2, \dots, t_\theta\}$. Значит, слово $Z_1 = VW$ эквивалентно слову VW_1 , длина которого равна $(n_0 - t_\theta + t) \in \{n_0, n_0 + 1, \dots, n_0 + t_1 - t_\theta\}$. Так как $n_0 + t_1 - t_\theta < n_0 + h - t_\theta$, то утверждение леммы верно и для слов длины $n + 1$. ■

3. Оценка длины эквивалентности

Утверждение 1. Пусть $f = f(x_1, x_2, \dots, x_k)$ — произвольная двоичная функция без запретов от k переменных. Тогда её минимальная длина эквивалентности не превосходит величины $n_0 = \binom{2^{2(k-1)} + 2^{k-1} - 1}{2^{k-1}} - 1$.

Доказательство. Через I_s обозначим множество $\cup I_{k-1, k-1}(Y)$, где объединение производится по всем словам Y длины s . Система $I_{k-1, k-1}(Y)$, соответствующая слову Y длины n , которое не имеет эквивалентных слов меньшей длины, очевидно, не принадлежит множеству $\cup I_{k-1, k-1}(Z)$, где объединение производится по всем словам Z длины меньше n (системы $I(Y)$ и $I(Z)$ при этом рассматриваются как отдельные элементы соответствующих объединений). В таком случае, учитывая очевидное равенство $|I_1| = 2$, получим соотношение

$$|\cup I_s| \geq |I_1| + \omega - 1 = \omega + 1. \quad (2)$$

(объединение по $s = 1, 2, \dots, \omega$, которые не являются длиной эквивалентности). Заметим далее, что общее число различных систем вида $I_{k-1, k-1}(Y)$ не превосходит числа вариантов выбора 2^{k-1} элементов из множества пар $(\alpha^{(i)}, \beta^{(i)})$, $\alpha^{(i)}, \beta^{(i)} \in (F_2)^{k-1}$, т. е. числа сочетаний с повторениями из $2^{2(k-1)}$ элементов по 2^{k-1} . С учётом (2) отсюда получаем, что при

$$\omega = \binom{2^{2(k-1)} + 2^{k-1} - 1}{2^{k-1}}$$

любое слово длины $\geq \omega$ эквивалентно некоторому слову длины $< \omega$. ■

Из данного утверждения вытекает, что длина эквивалентности имеется у любой двоичной функции без запретов. При этом важной задачей является нахождение минимальной длины эквивалентности.

Утверждение 2. Пусть функция без запретов от k переменных линейна по последней переменной: $f(x_1, x_2, \dots, x_k) = \varphi(x_1, x_2, \dots, x_{k-1}) + x_k$. Тогда её минимальная длина эквивалентности не превосходит величины $n_0 = d^d - 1$, $d = 2^{k-1}$.

Доказательство. В условиях данного утверждения (с учётом леммы 2) двоичные последовательности $y(1), y(2), \dots, y(n)$ и $z(1), z(2), \dots, z(m)$ являются эквивалентными, если и только если при любом $\alpha \in (F_2)^{k-1}$

$$\delta_{y(n)} \delta_{y(n-1)} \dots \delta_{y(1)}(\alpha) = \delta_{z(m)} \delta_{z(m-1)} \dots \delta_{z(1)}(\alpha),$$

где $\delta_\varepsilon(x_1, x_2, \dots, x_{k-1}) = (x_2, x_3, \dots, x_{k-1}, \varphi(x_1, x_2, \dots, x_{k-1}) + \varepsilon)$. Число различных систем $I_{k-1, k-1}(Y)$ не превосходит числа отображений множества $(F_2)^{k-1}$ в себя, которое равно d^d , $d = 2^{k-1}$. С учётом неравенства (2) отсюда и вытекает справедливость утверждения. ■

Утверждение 3. Пусть функция без запретов от k переменных линейна по обоим крайним переменным: $f(x_1, x_2, \dots, x_k) = x_1 + \lambda(x_2, x_3, \dots, x_{k-1}) + x_k$. Тогда её минимальная длина эквивалентности не превосходит величины $n_0 = (2^{k-1})! - 1$.

Доказательство проводится по аналогичной схеме с учётом того, что в условиях данного утверждения отображения δ_0 и δ_1 являются биективными, а число биективных отображений множества $(F_2)^{k-1}$ в себя равно $(2^{k-1})!$.

Замечание 1. Если функция линейна по обоим крайним переменным, то её длина эквивалентности, очевидно, связана с известными понятиями длины (и ширины) покрытия группы G , порождённой подстановками δ_0 и δ_1 [6].

Утверждение 4. Для любой двоичной функции без запретов от k переменных существует равновесная понижающая пара (h, t) , $t < h \leq H$, где $H = 2^n$, $n = \binom{2^{2(k-1)} + 2^{k-1} - 1}{2^{k-1}}$.

Доказательство. Рассмотрим последовательность $I_1, I_2, \dots$ множеств, введённых в доказательстве утверждения 1. Как уже отмечалось при доказательстве утверждения 1, множество I_s при любом $s = 1, 2, \dots$ является непустым подмножеством конечного множества M , мощность которого не превосходит величины $n = \binom{2^{2(k-1)} + 2^{k-1} - 1}{2^{k-1}}$. Следовательно, найдутся два индекса $h > t$, при которых $I_h = I_t$. При этом индекс h можно выбрать так, что он не превосходит числа всех подмножеств множества M , т. е. величины $H = 2^n$. ■

Замечание 2. Аналогичными рассуждениями можно показать, что если функция f удовлетворяет условиям утверждений 2 или 3, то она обладает равновесной понижающей парой (h, t) , $t < h \leq 2^n$, где $n = d^d$, $d = 2^{k-1}$ в условиях утверждения 2 и $n = (2^{k-1})!$ — в условиях утверждения 3.

Для заданной функции без запретов f через $O(f)$ обозначим множество функций

$$\{f(x), f(x) + 1, f(x + e), f(x + e) + 1, f(s(x)), f(s(x)) + 1, f(s(x) + e), f(s(x) + e) + 1\},$$

где e — двоичный вектор с единичными координатами (преобразование $x + e$ заключается в инвертировании координат двоичного вектора x); $s(x) = s(x_1, x_2, \dots, x_k) = (x_k, x_{k-1}, \dots, x_1)$.

Утверждение 5. Пусть функция без запрета $f(x_1, x_2, \dots, x_k)$ обладает равновесной понижающей парой (H, T) . Тогда (H, T) является равновесной понижающей парой для любой функции $\varphi \in O(f)$.

Доказательство. Для заданной функции без запрета $f(x_1, x_2, \dots, x_k)$ и выходного слова $Y = (y(1), y(2), \dots, y(n))$ через $f^{-1}(Y)$ обозначим множество входных слов

$$f^{-1}(Y) = \{x_1(j), x_2(j), \dots, x_{n+k-1}(j) : j = 1, 2, \dots, 2^{k-1}\},$$

перерабатываемых функцией f в слово Y :

$$y(t) = f(x_t(j), x_{t+1}(j), \dots, x_{t+k-1}(j)), \quad t = 1, 2, \dots, n; \quad j = 1, 2, \dots, 2^{k-1}.$$

Пусть $\varphi(x) = f(x + e)$. Тогда для любого слова Y множество векторов $\varphi^{-1}(Y)$ получено из векторов множества $f^{-1}(Y)$ путём их инвертирования. Следовательно, слова Y и Z эквивалентны относительно функции f в том и только в том случае,

если они эквивалентны относительно функции φ . А значит, если пара (H, T) является понижающей для функции f , то она будет понижающей и для функции φ .

Пусть $\varphi(x) = f(s(x))$. Для заданного слова $Y = (y(1), y(2), \dots, y(n))$ через $Y^* = (y(n), y(n-1), \dots, y(1))$ будем обозначать слово, полученное выписыванием в обратном порядке координат вектора Y . Соответственно через $f^{-1}(Y)^*$ обозначим множество двоичных последовательностей, полученных выписыванием в обратном порядке элементов последовательностей, содержащихся в множестве $f^{-1}(Y)$. Заметим, что $f^{-1}(Y)^* = \varphi^{-1}(Y^*)$. Значит, слово Y длины H эквивалентно слову Z длины T относительно функции f в том и только в том случае, когда слово Y эквивалентно слову Z относительно функции φ . Значит, пара (H, T) является понижающей для функции φ .

Пусть $\varphi(x) = f(x) + 1$. Тогда $\varphi^{-1}(Y + e) = f^{-1}(Y)$. Значит, слова Y и Z эквивалентны относительно функции f в том и только в том случае, если слова $(Y + e)$ и $(Z + e)$ эквивалентны относительно функции φ . А значит, пара (H, T) будет понижающей и для функции φ . Оставшиеся варианты рассматриваются по аналогичной схеме. ■

4. Условия биективности отображений $B_{f,L}$

Теорема 1. Пусть $\{h, t_1, t_2, \dots, t_\theta\}$ — понижающее множество для функции $f(x_1, x_2, \dots, x_k)$, $n_0 \geq t_\theta + s(1) + s(2) - 1$. Если отображение $B_{f,L}$ является биективным для всех $n \in \{n_0, n_0 + 1, \dots, n_0 + h - t_\theta - 1\}$, то оно биективно при любом $n \geq n_0$.

Доказательство. Для функции без запретов $f(x_1, x_2, \dots, x_k)$ существует ровно 2^{k-1} входных слов $x_1, x_2, \dots, x_{n+k-1}$, перерабатываемых данной функцией в фиксированное выходное слово $Y = y(1), y(2), \dots, y(n)$ по закону $y(j) = f(x_j, x_{j+1}, \dots, x_{j+k-1})$, $j = 1, 2, \dots, n$. Биективность отображения $B_{f,L}$ равносильна тому, что любому фиксированному выходному слову $y(1), y(2), \dots, y(n)$ соответствует единственное входное слово $x_1, x_2, \dots, x_{n+k-1}$ с ограничениями (1). Заметим, что выполнение (или невыполнение) условий (1) для входного слова зависит только от его начала $x_1, x_2, \dots, x_{k+s(1)-2}$ длины $k + s(1) - 2$ и конца $x_{n-s(2)+1}, x_{n-s(2)+2}, \dots, x_{n+k-1}$ длины $k + s(2) - 1$. С учётом леммы 3 в условиях теоремы для любого слова $Y = y(1), y(2), \dots, y(n)$ длины $n \geq n_0$ найдётся эквивалентное ему слово $Z = z(1), z(2), \dots, z(n_0)$, имеющее такие же начальный и конечный отрезки длины $s(1) - 1$ и $s(2)$:

$$y(j) = z(j), j \in \{1, 2, \dots, s(1) - 1\}, \quad y(n + 1 - j) = z(n_0 + 1 - j), j \in \{1, 2, \dots, s(2)\}.$$

В таком случае у этих слов одинаковы системы $I_{r,s}(Y) = I_{r,s}(Z)$ для $r = k + s(1) - 2$, $s = k + s(2) - 1$. Следовательно, и условия (1) применительно к данным последовательностям одновременно выполнены или нет. ■

Теорема 2. Пусть (h, t) — равновесная понижающая пара, $n_0 \geq t + s(1) + s(2) - 1$.

- 1) Если отображение $B_{f,L}$ является биекцией для $n = n_0$, то оно является биекцией при всех $n = n_0 + (h - t)d$, $d = 0, 1, \dots$
- 2) Если отображение $B_{f,L}$ не является биекцией для $n = n_0$, то оно не является биекцией ни при каком $n = n_0 + (h - t)d$, $d = 0, 1, \dots$
- 3) Задача нахождения биективных отображений $B_{f,L}$ при всех $n \geq t + s(1) + s(2) - 1$ эквивалентна задаче нахождения биективных отображений $B_{f,L}$ при $n = n_0 \in \{t + s(1) + s(2) - 1, t + s(1) + s(2), \dots, h + s(1) + s(2) - 2\}$.

Доказательство. Доказательство части 1 и 2 теоремы. Используя рассуждения, аналогичные доказательству теоремы 1, получим, что в условиях теоремы 2 для любого слова $Y = y(1), y(2), \dots, y(n)$ найдётся слово $Z = z(1), z(2), \dots, z(n_0)$, при котором $I_{r,s}(Y) = I_{r,s}(Z)$, $r = k + s(1) - 2$, $s = k + s(2) - 1$. Таким образом, если для выходного

слова $z(1), z(2), \dots, z(m)$ длины $m = n_0$ существует единственное входное слово с ограничениями (1), то это верно и для слова $y(1), y(2), \dots, y(n)$ длины $n = n_0 + (h - t)d$. С другой стороны, пусть для некоторого выходного слова $Z = z(1), z(2), \dots, z(m)$ длины $m = n_0$ нарушено условие единственности входного слова $x_1, x_2, \dots, x_{m+k-1}$ с ограничениями (1). Тогда в силу равновесности понижающей пары (h, t) для слова Z найдётся слово $Y = y(1), y(2), \dots, y(n)$ длины $n = n_0 + (h - t)d$, такое, что $I_{r,s}(Y) = I_{r,s}(Z)$, $r = k + s(1) - 2$, $s = k + s(2) - 1$. Следовательно, для слова Y также нарушено условие единственности входного слова $x_1, x_2, \dots, x_{n+k-1}$ с ограничениями (1). На этом доказательство частей 1 и 2 завершено. Справедливость третьей части вытекает из доказанных частей 1, 2 с учётом того, что в условиях теоремы любое натуральное число $n \geq t + s(1) + s(2) - 1$ представимо в виде

$$n = n_0 + (h - t)d, d \in \{0, 1, \dots\}, n_0 \in \{t + s(1) + s(2) - 1, t + s(1) + s(2), \dots, h + s(1) + s(2) - 2\}.$$

Теорема доказана. ■

Таким образом, наличие понижающего множества для функции $f(x_1, x_2, \dots, x_k)$ в принципиальном плане сводит вопрос о биективности отображений $B_{f,L}$ для всех достаточно больших n к исследованию соответствующих отображений при ограниченных значениях n . Особенно ярко это проявляется для понижающей пары (h, t) при $h = t + 1$. В этом случае биективность $B_{f,L}$ для $n = n_0 = t + s(1) + s(2) - 1$ равносильна его биективности при любом $n \geq n_0$.

5. Преобразования, сохраняющие биективность отображения $B_{f,L}$

Рассмотрим преобразования исходных функций (f, L) , при которых сохраняется биективность отображения $B_{f,L}$. Так, например, при биективности $B_{f,L}$ биективным будет и отображение $B_{f+1,L}$. Кроме того, биективным будет и отображение $B_{g,L}$, где $g(x) = f((\delta_L)^j(x))$, $j \in \{1, 2, \dots\}$.

Утверждение 6. Пусть при $f = f(x_1, x_2, \dots, x_n)$ и $L = x_1 + L_0(x_2, x_3, \dots, x_n)$ отображение $B_{f,L}$ является биективным. Тогда биективно и отображение $B_{g,H}$, где $g = f(x_1 + 1, x_2 + 1, \dots, x_n + 1)$, $H = x_1 + L_0(x_2 + 1, x_3 + 1, \dots, x_n + 1)$.

Доказательство. Справедливость утверждения вытекает из легко проверяемого равенства $\tau \delta_L^{-1} \tau^{-1} = \delta_H$, где преобразование τ заключается в инвертировании всех координат двоичного вектора. ■

Утверждение 7. Пусть при $f = f(x_1, x_2, \dots, x_k)$ и $L = x_1 + L_0(x_2, x_3, \dots, x_n)$, $k \leq n$, отображение $B_{f,L}$ является биективным. Тогда биективно и отображение $B_{g,H}$, где $g = f(x_k, x_{k-1}, \dots, x_1)$, $H = x_1 + L_0(x_n, x_{n-1}, \dots, x_2)$.

Доказательство. Рассмотрим случай $k = n$. В силу биективности отображения δ_L система функций $\{f(x), f((\delta_L)(x)), \dots, f((\delta_L)^{n-1}(x))\}$ будет ортогональной в том и только в том случае, когда такой будет система функций

$$\{z_1 = f((\delta_L)^{-1}(sx)), z_2 = f(sx), z_3 = f((\delta_L)(sx)), \dots, z_n = f((\delta_L)^{n-2}(sx))\},$$

где $s: (F_2)^n \rightarrow (F_2)^n$, $s(x_1, x_2, \dots, x_n) = (x_n, x_{n-1}, \dots, x_1)$. Из равенства $s\delta_L s^{-1} = (\delta_H)^{-1}$ следует, что

$$\begin{aligned} z_1 &= f((\delta_L)^{-1}s(x)) = f(s\delta_H(x)) = g(\delta_H(x)), \\ z_2 &= f(s(x)) = g(x), \end{aligned}$$

$$\begin{aligned} z_3 &= f((\delta_L)s(x)) = f(s(\delta_H)^{-1}(x)) = g((\delta_H)^{-1}(x)), \\ &\dots \\ z_n &= f((\delta_L)^{n-2}s(x)) = f(s(\delta_H)^{-n+2}(x)) = g((\delta_H)^{-n+2}(x)). \end{aligned}$$

Далее из ортогональности системы $\{z_1(x), z_2(x), \dots, z_n(x)\}$ следует ортогональность системы $\{z_1(B(x)), z_2(B(x)), \dots, z_n(B(x))\}$, где B — произвольная биекция на множестве векторов $(F_2)^n$. В частности, при $B = (\delta_H)^{n-2}$ получаем ортогональность системы $\{g((\delta_H)^{n-1}(x)), \dots, g(\delta_H(x)), g(x)\}$. Поскольку свойство ортогональности системы функций не зависит от порядка следования функций, на этом доказательство утверждения для $k = n$ завершено.

Пусть теперь $k < n$. Рассматривая функцию $f(x_1, x_2, \dots, x_k)$ как функцию от n переменных $x_1, x_2, \dots, x_n$, из доказанного выше получаем биективность отображения $B_{\varphi, H}$, где $\varphi = f(x_n, x_{n-1}, \dots, x_{n-k+1})$. В таком случае биективно и $B_{g, H}$, где $g = \varphi((\delta_H)^{n-k}(x)) = f(x_k, x_{k-1}, \dots, x_1)$, что и завершает доказательство. ■

6. Случай $k = 3$

Для заданной понижающей пары (h, t) и параметров $s(1), s(2)$ через M будем обозначать множество

$$M = \{t + s(1) + s(2) - 1, t + s(1) + s(2), \dots, h + s(1) + s(2) - 2\}.$$

Так как функции без запрета от трёх переменных $f(x_1, x_2, x_3)$ являются линейными по одной из крайних переменных, то с учётом утверждения 5 множество понижающих пар нелинейных функций задаётся понижающими парами (h, t) функции $f_1 = x_1x_2 + x_2 + x_3$, для которой $(h, t) = (6, 4)$, и функции $f_2 = x_1x_2 + x_3$, для которой $(h, t) = (11, 8)$. Для пары функций $f = x_1x_2 + x_2 + x_3$, $L = x_1 + x_{n-1}$ экспериментальными расчётами установлена биективность отображения $B_{f, L}$ при $n = 7 \in M = \{6, 7\}$. Следовательно, по теореме 2 отображение $B_{f, L}$ с указанными функциями f, L биективно при всех нечётных $n \geq 7$. Аналогичный результат другими методами ранее получен в [7].

7. Случай $k = 4$

Экспериментальные исследования на ЭВМ привели к нахождению биективных отображений $B_{f, L}$ для некоторых ограниченных значений $n = n_0 \in M$. С учётом теоремы 2 это позволило построить бесконечные перечни длин регистра, при которых биективно отображение $B_{f, L}$. В частности, биективные отображения исследуемого вида найдены для следующих четырёх функций f и соответствующих функций L :

$$\begin{aligned} f_1 &= x_1 + x_4 + x_1x_2 + x_1x_3 + x_1x_2x_3, & L &= x_1 + x_n; \\ f_2 &= x_3 + x_4 + x_1x_3 + x_2x_3 + x_1x_2x_3, & L &\in \{x_1 + x_{n-2}, x_1 + x_n\}; \\ f_3 &= x_4 + x_1x_2 + x_1x_3 + x_2x_3, & L &= x_1 + x_{n-1}; \\ f_4 &= x_2 + x_3 + x_1x_3 + x_3x_4 + x_1x_3x_4, & L &= x_1 + x_{n-2}. \end{aligned}$$

Общие характеристики функций f и L , значения $n = n_0 \in M$, а также бесконечные перечни длин регистра, при которых биективно отображение $B_{f, L}$, приведены в табл. 1.

Т а б л и ц а 1

Параметры биекций $B_{f,L}$, f от четырёх переменных

$f(x)$	$L(x)$	$s(1)$	$s(2)$	(h, t)	$n = n_0 \in M$ ($B_{f,L}$ — биекция)	Бесконечный перечень длин регистра ($B_{f,L}$ — биекция)
f_1	$x_1 + x_n$	1	1	(9, 6)	$n_0 = 8$	$n \equiv 2 \pmod 3, n \geq 8$
f_2	$x_1 + x_{n-2}$	1	3	(8, 5)	$n_0 = 10$	$n \equiv 1 \pmod 3, n \geq 10$
f_2	$x_1 + x_n$	1	1	(8, 5)	$n_0 = 8$	$n \equiv 2 \pmod 3, n \geq 8$
f_3	$x_1 + x_{n-1}$	1	2	(12, 8)	$n_0 = 11, 13$	$n \equiv 1 \pmod 2, n \geq 11$
f_4	$x_1 + x_{n-2}$	1	3	(6, 5)	$n_0 = 8$	$n \geq 8$

8. Случай $k = 5$

Примеры функций от пяти переменных и соответствующие им бесконечные классы биекций $B_{f,L}$ приведены в табл. 2 и 3.

Т а б л и ц а 2

Перечень функций f от пяти переменных, для которых найдены биекции $B_{f,L}$

$f(x) = f(x_0, x_1, x_2, x_3, x_4)$
$f_1 = x_0x_3 + x_0x_2x_3 + x_4$
$f_2 = x_1 + x_2 + x_3 + x_0x_1 + x_0x_3 + x_1x_2 + x_2x_3 + x_4$
$f_3 = x_1x_3 + x_0x_1x_3 + x_4$
$f_4 = x_0x_3 + x_1x_3 + x_2x_3 + x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_3 + x_4$
$f_5 = x_0 + x_3 + x_0x_1 + x_0x_2 + x_0x_3 + x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_3 + x_4$
$f_6 = x_2 + x_3 + x_0x_2 + x_1x_2 + x_1x_3 + x_0x_1x_2 + x_4$
$f_7 = x_0 + x_3 + x_0x_1 + x_0x_2 + x_0x_4 + x_0x_1x_2 + x_0x_1x_4 + x_0x_2x_4 + x_0x_1x_2x_4$
$f_8 = x_3 + x_2x_4 + x_0x_2x_4 + x_1x_2x_4 + x_0x_1x_2x_4$
$f_9 = x_3 + x_0x_4 + x_0x_1x_4$
$f_{10} = x_2 + x_3 + x_0x_3 + x_1x_3 + x_3x_4 + x_0x_1x_3 + x_0x_3x_4 + x_1x_3x_4 + x_0x_1x_3x_4$
$f_{11} = x_1 + x_0x_2 + x_1x_2 + x_2x_3 + x_2x_4 + x_3x_4 + x_0x_2x_3 + x_0x_2x_4 + x_0x_3x_4 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4$
$f_{12} = x_3 + x_0x_1 + x_1x_4 + x_0x_1x_2 + x_0x_1x_4 + x_1x_2x_4 + x_0x_1x_2x_4$

Т а б л и ц а 3

Параметры биекций $B_{f,L}$, f от пяти переменных

$f(x)$	$L(x)$	$s(1)$	$s(2)$	(h, t)	$n = n_0 \in M$ ($B_{f,L}$ — биекция)	Бесконечный перечень длин регистра ($B_{f,L}$ — биекция)
f_1	$x_0 + x_{n-2}$	1	2	(11, 7)	$n_0 = 9$	$n \equiv 1 \pmod 4, n \geq 9$
f_2	$x_0 + x_{n-2}$	1	2	(12, 8)	$n_0 = 11, 13$	$n \equiv 1 \pmod 4, n \geq 13$ $n \equiv 3 \pmod 4, n \geq 11$
f_3	$x_0 + x_{n-1}$	1	1	(10, 6)	$n_0 = 10$	$n \equiv 2 \pmod 4, n \geq 10$
f_4	$x_0 + x_{n-1}$	1	1	(14, 8)	$n_0 = 11, 14$	$n \equiv 2 \pmod 3, n \geq 11$
f_5	$x_0 + x_{n-1}$	1	1	(18, 12)	$n_0 = 14, 17$	$n \equiv 2 \pmod 3, n \geq 14$
f_6	$x_0 + x_{n-3}$	1	3	(10, 7)	$n_0 = 11$	$n \equiv 2 \pmod 3, n \geq 11$
f_7	$x_0 + x_{n-2}$	1	2	(12, 9)	$n_0 = 13$	$n \equiv 1 \pmod 3, n \geq 11$
f_8	$x_0 + x_{n-2}$	1	2	(7, 6)	$n_0 = 8$	$n \geq 8$
f_9	$x_0 + x_{n-2}$	1	2	(10, 8)	$n_0 = 10, 11$	$n \geq 10$
f_{10}	$x_0 + x_{n-3}$	1	3	(9, 8)	$n_0 = 11$	$n \geq 11$
f_{11}	$x_0 + x_{n-3}$	1	3	(8, 7)	$n_0 = 10$	$n \geq 10$
f_{12}	$x_0 + x_{n-1}$	1	1	(14, 9)	$n_0 = 10$	$n \equiv 0 \pmod 5, n \geq 10$

Замечание 3. Отсутствие запретов у функций $g \in \{f_7, \dots, f_{12}\}$ из табл. 2 следует из утверждения 3 работы [8] с учётом полученной с помощью экспериментальных расчётов равновероятности 16-грамм $(y_1, y_2, \dots, y_{16})$, где $y_j = g(x_j, x_{j+1}, \dots, x_{j+4})$, $j = 1, 2, \dots, 16$.

Замечание 4. Описание всех функций $f(x_1, x_2, \dots, x_k)$ без запрета при небольших значениях k можно проводить экспериментальными методами на основе результатов работ [8, 9]. Методы построения функций без запрета рассматриваются также в [4, 5, 10] и др.

9. Случай $k = 6$

В табл. 4 приведены параметры биективных отображений $B_{f,L}$ для следующих функций от шести переменных:

$$f_1 = x_1x_2 + x_1x_2x_3 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_2x_3x_5 + x_1x_2x_3x_4x_5 + x_6;$$

$$f_2 = x_1x_2 + x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_3x_4 + x_1x_2x_5 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_2x_3x_4x_5 + x_6;$$

$$f_3 = x_3 + x_4 + x_5 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_6;$$

$$f_4 = x_3 + x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_2x_5 + x_3x_5 + x_4x_5 + x_6.$$

Таблица 4

 Примеры биекций $B_{f,L}$, f от шести переменных

f	(h, t)	L	$s(1)$	$s(2)$	$n = n_0 \in M$ ($B_{f,L}$ — биекция)	Бесконечный перечень длин регистра ($B_{f,L}$ — биекция)
f_1	(14, 9)	$x_1 + x_{n-1}$	1	2	13	$n \equiv 3 \pmod{5}, n \geq 11$
f_1	(14, 9)	$x_1 + x_{n-1} + x_n$	1	2	13	$n \equiv 3 \pmod{5}, n \geq 11$
f_2	(14, 9)	$x_1 + x_n$	1	1	12, 13, 14	$n \geq 10$, $n \equiv 2 \pmod{5}$ или $n \equiv 3 \pmod{5}$ или $n \equiv 4 \pmod{5}$
f_2	(14, 9)	$x_1 + x_{n-1}$	1	2	13, 14	$n \geq 11$, $n \equiv 3 \pmod{5}$ или $n \equiv 4 \pmod{5}$
f_2	(14, 9)	$x_1 + x_{n-1} + x_n$	1	2	13, 14	$n \geq 11$, $n \equiv 3 \pmod{5}$ или $n \equiv 4 \pmod{5}$
f_3	(24, 16)	$x_1 + x_{n-3}$	1	4	21, 22, 23, 25, 26, 27	$n \not\equiv 0 \pmod{4}, n \geq 20$
f_4	(22, 14)	$x_1 + x_{n-1}$	1	2	17, 19, 21, 23	$n \equiv 1 \pmod{2}, n \geq 16$

Замечание 5. В работе приведены только классы биекций $B_{f,L}$, отвечающих функциям

$$L = L(x_1, x_2, \dots, x_{s(1)}, x_{n-s(2)+1}, x_{n-s(2)+2}, \dots, x_n) \neq x_1.$$

Приведённые классы биективных отображений не являются окончательными и могут быть расширены, в том числе путём дополнительных экспериментов на ЭВМ с целью поиска биекций $B_{f,L}$ в ограниченной области длин регистра $n = n_0$, $h + s(1) + s(2) - 2 \geq n_0 \geq t + s(1) + s(2) - 1$, при $s(1) + s(2) > 4$.

Замечание 6. Предлагаемый в работе метод построения биекций $B_{f,L}$ полностью применим и для случая нелинейной функции обратной связи L рассматриваемого вида.

Заключение

В работе развивается новый метод построения биективных отображений $B_{f,L}$, задаваемых регистром сдвига большой длины n с функцией обратной связи

$L(x_1, x_2, \dots, x_n)$, которая зависит от ограниченного числа крайних переменных, и нелинейной функцией-фильтром $f(x_1, x_2, \dots, x_k)$ от небольшого числа переменных $k \ll n$. Метод основан на поиске понижающих множеств функции f , наличие которых сводит исходную задачу для бесконечного множества длин генератора n к проверке биективности конечного числа отображений, отвечающих генераторам ограниченной длины $n \leq n_0$. На основе предложенного метода построены новые бесконечные классы биективных отображений $B_{f,L}$ для случая нелинейной функции $f = f(x_1, x_2, \dots, x_k)$ от $k \leq 6$ переменных. Ранее аналогичные результаты были известны для случая, когда f зависит от трёх переменных.

Полученные результаты могут быть полезны при построении и обосновании статистических свойств датчиков случайных последовательностей на основе фильтрующих генераторов (их автоматная модель изложена, например, в [11]). При этом особое практическое значение имеет выбор пар (f, L) , при которых одновременно обеспечивается биективность отображения $B_{f,L}$ и максимальность периода отображения δ_L . В этой связи отметим: если функция L обратной связи регистра сдвига длины n выбрана так, что соответствующая подстановка δ_L обладает циклом длины $2^n - 1$, то имеется в точности $2^{t+1}(1 - 2^{-n})$, где $t = 2^n - 1$, булевых функций f от n переменных, при которых отображение $B_{f,L}$ является биективным [12, следствие 1].

Биективные отображения $B_{f,L}$ возникают также при исследовании классов регистров сдвига, обладающих одинаковой цикловой структурой. Действительно, как следует из результатов работы [12], если $B_{f,L}$ — биекция на двоичных векторах длины n , то регистры сдвига с функциями обратной связи $L(x)$ и $\varphi(x) = f((\delta_L)^n B_{f,L}^{-1}(x))$ имеют одинаковую цикловую структуру. Тем самым для получения явного вида функции обратной связи $\varphi(x)$ необходимо знать аналитический вид координатных функций отображения $B_{f,L}^{-1}$. В этой связи отметим, что в работе [7] получены оценки для степени нелинейности координатных функций (и их линейных комбинаций) отображения $B_{f,L}^{-1}$ для случая функции f от трёх переменных.

ЛИТЕРАТУРА

1. Лидл Р., Нидеррайтер Г. Конечные поля: в 2-х т. М.: Мир, 1988. 822 с.
2. Рожков М. И. К вопросу построения ортогональных систем двоичных функций с использованием регистра сдвига // Лесной вестник. 2011. Вып. 3. С. 180–185.
3. Huffman D. A. Canonical forms for information loss less finite state logical mashines // IRE Trans. Circuit Theory. 1959. V. 6, spec. suppl. P. 41–59.
4. Сумароков С. Н. Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обозрение прикл. и промышл. матем. Сер. дискретн. матем. 1994. Т. 1. Вып. 1. С. 33–35.
5. Логачев О. А., Смышляев С. В., Яценко В. В. Новые методы изучения совершенно уравновешенных булевых функций // Дискретная математика. 2009. Т. 21. № 2. С. 51–74.
6. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра: учебник. В 2-х т. Т. 2. М.: Гелиос АРВ, 2003. 416 с.
7. Саранцев А. В. Построение регулярных систем однотипных двоичных функций с использованием регистра сдвига // Лесной вестник. 2004. № 1(32). С. 164–169.
8. Рожков М. И. Некоторые алгоритмические вопросы идентификации конечных автоматов по распределению выходных m -грамм. Ч. 2 // Обозрение прикл. и промышл. матем. Сер. дискретн. матем. 2008. Т. 15. Вып. 5. С. 785–806.

9. *Рожков М. И.* Некоторые алгоритмические вопросы идентификации конечных автоматов по распределению выходных m -грамм. Ч. 3 // Обозрение прикл. и промышл. матем. Сер. дискретн. матем. 2009. Т. 16. Вып. 1. С. 35–60.
10. *Михайлов В. Г., Чистяков В. П.* О задачах теории конечных автоматов, связанных с числом прообразов выходной последовательности // Обозрение прикл. и промышл. матем. Сер. дискретн. матем. 1994. Т. 1. Вып. 1. С. 7–32.
11. *Фомичев В. М.* Дискретная математика и криптология. Курс лекций / под общ. ред. Н. Д. Подуфалова. М.: ДИАЛОГ-МИФИ, 2003. 400 с.
12. *Рожков М. И.* О некоторых классах нелинейных регистров сдвига, обладающих одинаковой цикловой структурой // Дискретная математика. 2010. Т. 22. № 2. С. 96–119.

ПОИСК ОПТИМАЛЬНОГО ЛИНЕЙНОГО ПРИБЛИЖЕНИЯ СЕТЕЙ ФЕЙСТЕЛЯ

Г. И. Шушуев

Новосибирский государственный университет, г. Новосибирск, Россия

E-mail: g.shushuev@gmail.com

Предлагается подход к нахождению линейных приближений сети Фейстеля, математическая постановка задачи о линейном приближении и алгоритм, позволяющий находить оптимальное линейное приближение обобщённой сети Фейстеля.

Ключевые слова: *линейный криптоанализ, сеть Фейстеля.*

Введение

Для применения линейного криптоанализа к итеративному блочному шифру требуется найти линейное приближение на определённое число раундов. Если известно лучшее приближение, то можно определить минимальную трудоёмкость линейного криптоанализа шифра, т. е. оценить криптографическую стойкость шифра. Таким образом, задача оценки криптографической стойкости сводится к поиску линейных приближений и нахождению среди них лучшего. В связи с этим возникает ряд проблем, так как помимо того, что нужно исследовать раундовую функцию, необходимо правильно согласовывать приближения раундов. Как правило, при проведении линейного криптоанализа выбирается некоторое найденное линейное приближение без доказательства того, что оно является лучшим.

Для поиска лучшего приближения можно перебирать всевозможные линейные соотношения, но на это может потребоваться больше времени, чем на составление словаря, поэтому необходимо придумывать другие способы.

В работе предлагается подход к нахождению линейных приближений сети Фейстеля, математическая постановка задачи о линейном приближении и алгоритм, позволяющий находить оптимальное линейное приближение обобщённой сети Фейстеля.

В п. 1 приведено описание обобщённой сети Фейстеля, вводятся линейные приближения, замечаются некоторые их свойства, вводится понятие раундового преобладания, используемое для сравнения приближений раундов. В п. 2 даётся математическая постановка задачи о линейном приближении, вводится понятие дерева шаблонов, рассматриваются его свойства и предлагается алгоритм поиска оптимального пути в дереве шаблонов, что является оптимальным линейным приближением для некоторой сети Фейстеля.

1. Линейные приближения обобщённой сети Фейстеля

Линейный криптоанализ использует линейное приближение шифра, в которое входят биты открытого текста, шифртекста и ключа. Линейное приближение шифра характеризуется вероятностью, с которой оно выполняется, и чем она выше, тем линейное приближение лучше, так как криптоанализ на его основе будет менее трудоёмок.

Рассмотрим процедуру построения линейного приближения шифра.

1.1. Обобщённая сеть Фейстеля

Обобщённая сеть Фейстеля — один из методов построения блочных шифров. Алгоритм шифрования реализуется несколькими итерациями преобразования сети с использованием ключа MK . Ценность метода заключается в том, что преобразование сети Фейстеля обратимо.

Обобщённая сеть Фейстеля характерна тем, что входное слово разбивается на два или более подслов, часть из которых на каждом раунде преобразуется по определённому закону. Если длины подслов совпадают, то такую сеть называют *сбалансированной*.

Приведём схему сбалансированной обобщённой сети Фейстеля с r раундами (рис. 1). Открытый текст P , шифртекст C имеют длину N бит, ключ MK — M бит. Открытый текст представляется как n m -битных подслов $P = X^0 = (X_1^0, X_2^0, X_3^0, \dots, X_n^0)$, X^i — промежуточный шифртекст после i -го раунда, где $i = 1, 2, \dots, r$; $F : (\mathbb{Z}_2^m)^n \rightarrow \mathbb{Z}_2^m$ — нелинейная раундовая функция. Раундовые подключи K^i длины k бит однозначно задаются ключом MK .

Процесс шифрования осуществляется следующим образом.

1. Входной открытый текст $P = X^0 = (X_1^0, X_2^0, X_3^0, \dots, X_n^0)$.

2. Для i от 1 до r

$$X_n^i = X_1^{i-1} \oplus F(K^i, X_2^{i-1}, X_3^{i-1}, \dots, X_n^{i-1}),$$

$$X^i = (X_1^i, X_2^i, \dots, X_n^i) = (X_2^{i-1}, X_3^{i-1}, \dots, X_n^{i-1}, X_1^{i-1} \oplus F(K^i, X_2^{i-1}, X_3^{i-1}, \dots, X_n^{i-1})).$$

3. Выходной шифртекст $C = X^r = (X_1^r, X_2^r, X_3^r, \dots, X_n^r)$.

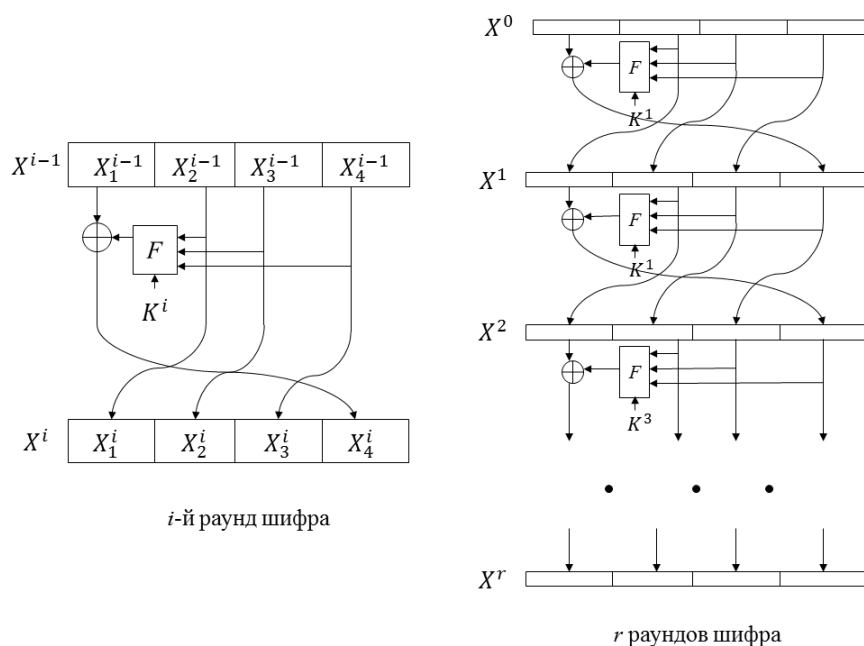


Рис. 1. Обобщённая сеть Фейстеля на примере SMS4 [1]

1.2. Описание и история линейного криптоанализа

Линейный криптоанализ — статистический метод, предложенный в 1992–1993 гг. японским криптографом Мицуру Мацуи. Сначала он вместе с А. Ямагиши исследовал этот метод для блочного шифра FEAL [2], а позднее применил его к шифру DES [3] и провёл экспериментальный криптоанализ полных его 16-ти раундов [4]. Линейный криптоанализ заключается в исследовании линейного приближения шифра на парах

«открытый текст — шифртекст» для получения информации о ключе. М. Мацуи предложил два алгоритма линейного криптоанализа, первый для нахождения линейного соотношения, выполняющегося на битах ключа, второй для нахождения части ключа.

Для проведения криптоанализа необходимо знание структуры шифра, а также достаточный объём выборки, состоящей из пар открытого текста и шифртекста, полученных на одном и том же *неизвестном* криптоаналитику ключе.

Большое число работ посвящено обобщениям и применениям линейного криптоанализа. Детальное исследование этого метода провела К. Ньюберг [5]. Для повышения эффективности метода в [6] предложено для одной комбинации битов ключа рассматривать одновременно несколько линейных приближений. Авторы [7] привели способ улучшения метода, предложив учитывать при приближении вероятностное поведение битов вместо их фиксированных значений. Общий метод уменьшения временной сложности линейного криптоанализа блочных шифров (в том числе SP-сетей и сетей Фейстеля) за счёт использования быстрых преобразований Фурье описывается в [8]. В [9] предложены идеи по использованию в линейном криптоанализе квадратичных соотношений специального вида.

1.3. Приближение раундовой функции

Линейные приближения раундовой функции находятся путём анализа конструкции конкретного шифра. Рассмотрим некоторые свойства линейных приближений и введём ряд определений для работы с ними.

Определение 1. *Раундовая функция* — функция вида $F : (\mathbb{Z}_2^m)^n \rightarrow \mathbb{Z}_2^m$. Пусть $F(X_1, X_2, \dots, X_n) = Y$, где $Y, X_i \in \mathbb{Z}_2^m, i = 1, 2, \dots, n$.

Как правило, раундовая функция обобщённой сети Фейстеля удовлетворяет некоторым ограничениям, например является простой (применяется в SMS4 [1]) или псевдопростой (DES [10], TEA [11]).

Определение 2. Раундовая функция F называется *простой*, если

$$F(X_1, X_2, \dots, X_n) = G(X_1 \oplus X_2 \oplus \dots \oplus X_n)$$

для некоторой функции $G : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$.

Определение 3. Раундовая функция F называется *псевдопростой*, если

$$F(X_1, X_2, \dots, X_n) = G(L_1(X_1) \oplus L_2(X_2) \oplus \dots \oplus L_n(X_n))$$

для некоторых функции $G : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$ и набора функций $L_1, \dots, L_n$, где $L_i : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^m$ не тождественно нулевые.

Определение 4. *Скалярное произведение* векторов $X, Y \in \mathbb{Z}_2^m$, где $X = (x_1, x_2, \dots, x_m)$, $Y = (y_1, y_2, \dots, y_m)$, $x_j, y_j \in \mathbb{Z}_2$, вычисляется следующим образом:

$$X \cdot Y = x_1 y_1 \oplus x_2 y_2 \oplus \dots \oplus x_m y_m.$$

Определение 5. *Линейной комбинацией* битов вектора $X \in \mathbb{Z}_2^m$ называется скалярное произведение X и некоторого вектора $b \in \mathbb{Z}_2^m$. Вектор b назовём *маской* для вектора X .

Линейной комбинацией битов X_i является

$$b_i \cdot X_i = b_{i1} x_{i1} \oplus b_{i2} x_{i2} \oplus \dots \oplus b_{im} x_{im},$$

где $b_i = (b_{i1}, b_{i2}, \dots, b_{im})$; $X_i = (x_{i1}, x_{i2}, \dots, x_{im})$; $b_{ij}, x_{ij} \in \mathbb{Z}_2, j = 1, \dots, m, i = 1, \dots, n$.

Определение 6. *Линейным приближением функции F называется соотношение*

$$b_1 \cdot X_1 \oplus b_2 \cdot X_2 \oplus \dots \oplus b_n \cdot X_n = a \cdot F(X_1, \dots, X_n), \quad (1)$$

выполняющееся с вероятностью $1/2 + \varepsilon$ при случайном равновероятном выборе X_i , где $|\varepsilon| \leq 1/2$; $a, b_i \in \mathbb{Z}_2^m$, $i = 1, 2, \dots, n$. Величину ε назовём *линейным преобладанием*, или просто *преобладанием*.

Пример линейного приближения раундовой функции изображён на рис. 2.

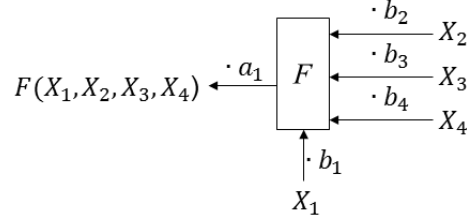


Рис. 2. Линейное приближение раундовой функции F , случай $n = 4$

Определим функцию $R_F : (\mathbb{Z}_2^m)^{n+1} \rightarrow \mathbb{R}$, действующую на масках $b_1, \dots, b_n, a$, следующим образом:

$$R_F(b_1, \dots, b_n, a) = \frac{1}{2} + \varepsilon.$$

Функция R_F на масках $b_1, \dots, b_n, a$ принимает значение вероятности, с которой выполняется соответствующее линейное приближение (1). Несложно доказать следующую вспомогательную лемму.

Лемма 1. Пусть $X \in \mathbb{Z}_2^l$, $y \in \mathbb{Z}_2$ — независимые случайные величины. Тогда равенство $f(X) \oplus y = 0$, где $f : \mathbb{Z}_2^l \rightarrow \mathbb{Z}_2$, выполняется с вероятностью $1/2$ для любого натурального $l > 0$.

Доказательство. Пусть $f(X) = 0$ в $(2^{l-1} + p)$ случаях и $f(X) = 1$ в $(2^{l-1} - p)$ случаях, $p \in \{0, 1, \dots, 2^{l-1}\}$. Покажем, что при любом значении p равенства $f(X) \oplus y = 0$ и $f(X) \oplus y = 1$ выполняются одинаково часто (в 2^l случаях).

Так как X не зависит от y , то пусть X пробегает все значения при фиксированном $y = 0$, тогда $f(X) \oplus y$ принимает значения 0 и 1 в $(2^{l-1} + p)$ и $(2^{l-1} - p)$ случаях соответственно. При $y = 1$ ситуация обратная, т. е. $f(X) \oplus y$ принимает значения 0 и 1 в $(2^{l-1} - p)$ и $(2^{l-1} + p)$ случаях соответственно. Значит, $f(X) \oplus y = 0$ в 2^l случаях и $f(X) \oplus y = 1$ в 2^l случаях, т. е. $f(X) \oplus y = 0$ с вероятностью $1/2$. ■

Утверждение 1. Если раундовая функция F является простой и $R_F(b_1, \dots, b_n, a) = 1/2 + \varepsilon$, где $|\varepsilon| > 0$, то $b_1 = b_2 = \dots = b_n$.

Доказательство. Пусть $b_1 = b$, $b_2 = b \oplus b'_2$, $\dots$, $b_n = b \oplus b'_n$. Тогда соотношение (1) можно представить в виде $b \cdot X_1 \oplus b \cdot X_2 \oplus b'_2 \cdot X_2 \oplus \dots \oplus b \cdot X_n \oplus b'_n \cdot X_n = a \cdot G(X_1 \oplus \dots \oplus X_n)$. После группировки слагаемых получим

$$b \cdot (X_1 \oplus \dots \oplus X_n) \oplus (b'_2 \cdot X_2 \oplus \dots \oplus b'_n \cdot X_n) = a \cdot G(X_1 \oplus \dots \oplus X_n). \quad (2)$$

Положим $X_1 \oplus \dots \oplus X_n = X$ и заметим, что векторы X и $X_2 \oplus \dots \oplus X_n$ независимы. Действительно, так как X_1 не зависит от $X_2 \oplus \dots \oplus X_n$, то и X принимает всевозможные значения независимо от $X_2 \oplus \dots \oplus X_n$.

Предположим, что $b'_i \neq 0$ для некоторого $i \in \{2, \dots, n\}$. Тогда линейная функция $l(X_2, \dots, X_n) = b'_2 \cdot X_2 \oplus \dots \oplus b'_n \cdot X_n$ не является тождественно нулевой и, следовательно, принимает значения 0 и 1 одинаковое число раз. Перепишем соотношение (2) в введённых обозначениях, перенеся всё в левую часть:

$$b \cdot X \oplus l(X_2, \dots, X_n) \oplus a \cdot G(X) = 0. \quad (3)$$

По лемме 1 получаем, что вероятность выполнения равенства (3) равна $1/2$, следовательно, $R_F(b_1, \dots, b_n, a) = 1/2$, что противоречит условию. ■

Следствие 1. Пусть F является псевдопростой, $F(X_1, X_2, \dots, X_n) = G(L_1(X_1) \oplus \dots \oplus L_n(X_n))$ и $R_F(b_1, \dots, b_n, a) = 1/2 + \varepsilon$, где $|\varepsilon| > 0$ для некоторых фиксированных $b_1, \dots, b_n, a$. Пусть функции $l_1, \dots, l_n$ выбраны так, что $b_i \cdot X_i = l_i(b_i) \cdot L_i(X_i)$ для любого $X_i \in \mathbb{Z}_2^m$. Тогда выполняется $l_1(b_1) = l_2(b_2) = \dots = l_n(b_n)$, причём если одна из масок b_i нулевая, то $b_1 = \dots = b_n = 0$.

Доказательство. Линейное приближение (1) можно переписать в виде

$$l_1(b_1) \cdot L_1(X_1) \oplus \dots \oplus l_n(b_n) \cdot L_n(X_n) = a \cdot G(L_1(X_1) \oplus \dots \oplus L_n(X_n)).$$

По утверждению 1 получим, что $l_1(b_1) = l_2(b_2) = \dots = l_n(b_n)$, так как $R_F(b_1, \dots, b_n, a) = R_G(l_1(b_1), \dots, l_n(b_n), a) = 1/2 + \varepsilon$, где $|\varepsilon| > 0$.

Если $b_i = 0$, то $b_i \cdot X_i = l_i(b_i) \cdot L_i(X_i) = 0$, значит, $l_i(b_i) = 0$. Обратное тоже верно: если $l_i(b_i) = 0$, то $b_i = 0$. Получаем, что $l_1(b_1) = l_2(b_2) = \dots = l_n(b_n) = b_1 = \dots = b_n = 0$, если $b_i = 0$. ■

Следствие 2. Если F является псевдопростой и хотя бы одна из масок $b_1, b_2, \dots, b_n, a$ является нулевой, то

$$R_F(b_1, \dots, b_n, a) = \begin{cases} 1, & \text{если } b_1 = b_2 = \dots = b_n = a = 0, \\ 1/2 & \text{иначе.} \end{cases}$$

Доказательство. Если $b_1 = b_2 = \dots = b_n = a = 0$, то $R_F(b_1, \dots, b_n, a) = 1$, так как в этом случае линейное приближение (1) функции F выглядит так: $0 = 0$. Если нулевой является одна из масок $b_1, \dots, b_n$, то, по следствию 1, выполняется либо $b_1 = \dots = b_n = 0$, либо $R_F(b_1, \dots, b_n, a) = 1/2$. Осталось рассмотреть два случая:

- маска a является нулевой, маски $b_1, \dots, b_n$ не все одновременно нулевые;
- маски $b_1, \dots, b_n$ все одновременно нулевые, маска a ненулевая.

Оба случая соответствуют ситуации, когда линейное приближение (1) есть некоторая линейная комбинация битов равная нулю. Так как линейная комбинация является сбалансированной булевой функцией, то на всевозможных наборах она принимает значение 0 и 1 одинаковое количество раз, а значит, $R_F(b_1, \dots, b_n, a) = 1/2$. ■

1.4. Раундовое приближение

Рассмотрим, как с помощью линейного приближения псевдопростой раундовой функции построить линейное приближение для одного раунда шифра. Промежуточный шифртекст до r -го раунда обозначим через $X^{r-1} = (X_1^{r-1}, X_2^{r-1}, \dots, X_n^{r-1})$, после r -го раунда — $X^r = (X_1^r, X_2^r, \dots, X_n^r)$, где $X^{r-1}, X^r \in (\mathbb{Z}_2^m)^n$; $X_j^r \in \mathbb{Z}_2^m$. На r -м раунде используется ключ $K^r \in \mathbb{Z}_2^m$.

Определение 7. *Линейным приближением раунда r называется соотношение*

$$a^{r-1} \cdot X^{r-1} \oplus a^r \cdot X^r \oplus \alpha^r = d^r \cdot K^r, \quad (4)$$

выполняющееся с вероятностью $1/2 + \varepsilon_r$, где $\varepsilon_r > 0$; $\alpha^r \in \mathbb{Z}_2$; $a^{r-1}, a^r \in (\mathbb{Z}_2^m)^n$; $d^r \in \mathbb{Z}_2^m$; a^{r-1}, a^r — маски входа и выхода раунда соответственно.

Пример линейного приближения раунда изображён на рис. 3.

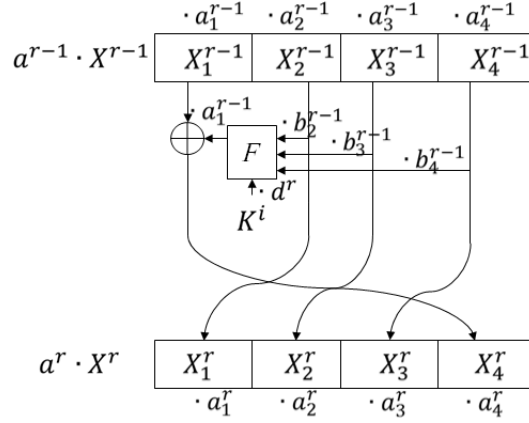


Рис. 3. Линейное приближение r -го раунда, случай $n = 4$

Поскольку шифртексты X^r и X^{r-1} находятся в зависимости

$$X^r = (X_1^r, X_2^r, \dots, X_n^r) = (X_2^{r-1}, X_3^{r-1}, \dots, X_n^{r-1}, F(K^r, X_2^{r-1}, X_3^{r-1}, \dots, X_n^{r-1})),$$

которую можно представить как

$$\begin{cases} X_i^r = X_{i+1}^{r-1}, & i = 1, \dots, n-1, \\ X_n^r = F(K^r, X_2^{r-1}, \dots, X_n^{r-1}), \end{cases}$$

приближение (1) раундовой функции в данном случае выглядит так:

$$d^r \cdot K^r \oplus b_2^{r-1} \cdot X_2^{r-1} \oplus \dots \oplus b_n^{r-1} \cdot X_n^{r-1} = a_1^{r-1} \cdot F(K^r, X_2^{r-1}, \dots, X_n^{r-1}).$$

Получаем, что маски $a^r = (a_1^r, \dots, a_n^r)$ и $a^{r-1} = (a_1^{r-1}, \dots, a_n^{r-1})$ связаны следующим образом:

$$\begin{cases} a_i^r = a_{i+1}^{r-1} \oplus b_{i+1}^{r-1}, & i = 1, \dots, n-1, \\ a_n^r = a_1^{r-1}, \end{cases}$$

где ввиду $R_F(d^r, b_2^{r-1}, \dots, b_n^{r-1}, a_1^{r-1}) \neq 1/2$ по следствию 1 маски $b_2^{r-1}, \dots, b_n^{r-1}$ однозначно определяются по d^r . Значение ε_r совпадает с модулем ε , вычисленным по приближению раундовой функции $R_F(d^r, b_2^{r-1}, \dots, b_n^{r-1}, a_1^{r-1}) = 1/2 + \varepsilon$, а α^r подбирается так, чтобы $\varepsilon_r > 0$ (если $\varepsilon > 0$, то $\alpha^r = 0$; если $\varepsilon < 0$, то $\alpha^r = 1$).

Если хотя бы одна из масок $d^r, b_2^{r-1}, \dots, b_n^{r-1}, a_1^{r-1}$ является нулевой, то по следствию 2, для того чтобы выполнялось $R_F(d^r, b_2^{r-1}, \dots, b_n^{r-1}, a_1^{r-1}) \neq 1/2$, все они должны быть нулевыми; значит, соотношение (4) упрощается:

$$a^{r-1} \cdot X^{r-1} \oplus a^r \cdot X^r = 0$$

и выполняется с вероятностью 1, а маски $a^r = (a_1^r, \dots, a_n^r)$ и $a^{r-1} = (a_1^{r-1}, \dots, a_n^{r-1})$ связаны следующим образом:

$$\begin{cases} a_i^r = a_{i+1}^{r-1}, & i = 1, \dots, n-1, \\ a_n^r = a_1^{r-1} = 0. \end{cases} \quad (5)$$

Пример 1. Рассмотрим приближение одного раунда некоторого шифра с $n = 2$ и $m = 6$. Пусть имеется приближение раундовой функции $b_1 \cdot X_1 \oplus b_2 \cdot X_2 = a \cdot F(X_1, X_2)$, выполняющееся с вероятностью $1/2 + \varepsilon$, в котором $\varepsilon = -1/8$, $b_1 = (1, 0, 1, 0, 1, 0)$, $b_2 = (0, 1, 0, 1, 0, 1)$, $a = (0, 0, 1, 1, 0, 0)$. Функция R_F в данном случае примет вид $R_F(b_1, b_2, a) = 1/2 - 1/8$.

Составим линейное приближение первого раунда, построенное из имеющегося приближения раундовой функции. Шифртекст $X^1 = (X_1^1, X_2^1)$ вычисляется по $X^0 = (X_1^0, X_2^0)$ как $X^1 = (X_1^1, X_2^1) = (X_2^0, F(K^1, X_2^0))$; тогда имеющееся приближение раундовой функции F представимо в виде $d^1 \cdot K^1 \oplus b_2^0 \cdot X_2^0 = a_1^0 \cdot F(K^1, X_2^0)$. Получаем $R_F(d^1, b_2^0, a_1^0) = 1/2 - 1/8$. Осталось определить $a^0 = (a_1^0, a_2^0)$ и $a^1 = (a_1^1, a_2^1)$. Часть a^0 , а именно $a_1^0 = (0, 0, 1, 1, 0, 0)$, уже зафиксирована приближением раундовой функции; a_2^0 может быть любым вектором длины 6, допустим $(0, 1, 0, 0, 0, 0)$. Из следующей системы находится a^1 :

$$\begin{cases} a_1^1 = a_2^0 + b_2^0, \\ a_2^1 = a_1^0. \end{cases}$$

Подставим известные значения a_2^0, b_2^0, a_1^0 и получим

$$a_1^1 = (0, 1, 0, 0, 0, 0) \oplus (0, 1, 0, 1, 0, 1) = (0, 0, 0, 1, 0, 1), \quad a_2^1 = (0, 0, 1, 1, 0, 0).$$

В итоге линейным приближением первого раунда является соотношение

$$a^0 \cdot X^0 \oplus a^1 \cdot X^1 \oplus \alpha^1 = d^1 \cdot K^1,$$

выполняющееся с вероятностью $1/2 + 1/8$. Его можно представить в виде

$$x_{1,3}^0 \oplus x_{1,4}^0 \oplus x_{2,2}^0 \oplus x_{1,4}^1 \oplus x_{1,6}^1 \oplus x_{2,3}^1 \oplus x_{2,4}^1 \oplus 1 = k_1^1 \oplus k_3^1 \oplus k_5^1.$$

Заметим, что таким образом мы получаем некую информацию о битах ключа, а именно о битах k_1^1 , k_3^1 и k_5^1 .

1.5. Схема согласования раундовых приближений

Определение 8. *Схемой согласования раундовых приближений порядка p называется система, состоящая из уравнений вида (4)*

$$\begin{cases} a^0 \cdot X^0 \oplus a^1 \cdot X^1 \oplus \alpha^1 = d^1 \cdot K^1, \\ a^1 \cdot X^1 \oplus a^2 \cdot X^2 \oplus \alpha^2 = d^2 \cdot K^2, \\ \dots \\ a^{r-1} \cdot X^{r-1} \oplus a^r \cdot X^r \oplus \alpha^r = d^r \cdot K^r, \\ \dots \\ a^{p-1} \cdot X^{p-1} \oplus a^p \cdot X^p \oplus \alpha^p = d^p \cdot K^p, \end{cases} \quad (6)$$

в которой определены маски a^0, a^r, d^r , биты α^r и преобладания ε_r , $r = 1, \dots, p$. Маски a^0 и a^p назовём *начальной* и *конечной* масками соответственно.

На рис. 4 изображён пример схемы согласования раундов.

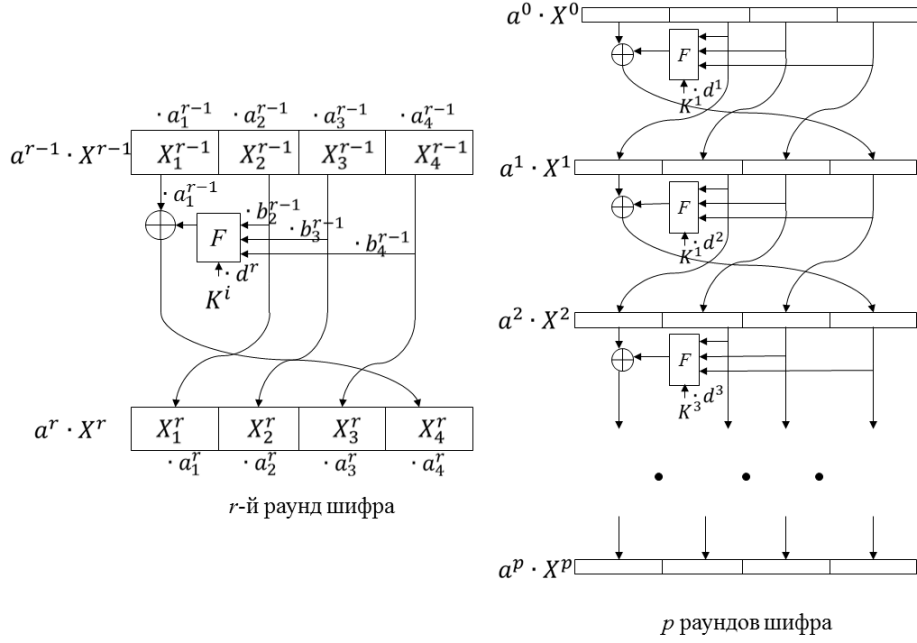


Рис. 4. Схема согласования раундовых приближений, случай $n = 4$

Схема согласования раундовых приближений порядка p порождает *линейное приближение p раундов шифра*. Заметим, что если сложить по модулю два все уравнения, то останутся только биты X^0, X^p и раундовых ключей.

Определение 9. *Линейным приближением p раундов шифра* называется соотношение

$$a^0 \cdot X^0 \oplus a^p \cdot X^p \oplus \alpha = d^1 \cdot K^1 \oplus \dots \oplus d^p \cdot K^p, \quad (7)$$

выполняющееся с вероятностью $1/2 + \varepsilon$, где $\varepsilon > 0$.

Бит α находится как $\alpha = \alpha^1 \oplus \alpha^2 \oplus \dots \oplus \alpha^p$. Вероятность выполнения линейного приближения, полученного из схемы (6), вычисляется с помощью известной леммы Мацуи [3].

Лемма 2 (Мацуи). Пусть ξ_i ($1 \leq i \leq n$) — независимые случайные величины, каждая из которых принимает значение 0 с вероятностью $1/2 + \varepsilon_i$ и значение 1 — с вероятностью $1/2 - \varepsilon_i$ ($-1/2 \leq \varepsilon_i \leq 1/2$). Тогда случайная величина $\xi_1 \oplus \xi_2 \oplus \dots \oplus \xi_n$ принимает значение 0 с вероятностью $1/2 + \varepsilon$ и значение 1 — с вероятностью $1/2 - \varepsilon$, где $\varepsilon = 2^{n-1} \prod_{i=1}^n \varepsilon_i$.

Таким образом получаем преобладание, с которым выполняется соотношение (7), равное $\varepsilon = 2^{p-1} \prod_{r=1}^p \varepsilon_r$, где ε_r взяты из схемы согласования.

Если начальная и конечная маски совпадают, то схема согласования раундовых приближений (6) называется *замкнутой*. Линейное приближение (7), порождённое замкнутой схемой согласования, называется *замкнутым* и имеет вид

$$a^0 \cdot X^0 \oplus a^p \cdot X^p \oplus \alpha = d^1 \cdot K^1 \oplus \dots \oplus d^p \cdot K^p.$$

Замкнутые приближения хороши тем, что их можно применять последовательно, получая тем самым линейное приближение на произвольное количество раундов.

Пусть $(a^i)_1, (b^i)_1, (\alpha^i)_1$ и $(a^i)_2, (b^i)_2, (\alpha^i)_2$ — параметры двух схем согласования. Введём отношение эквивалентности среди замкнутых схем согласования раундов.

Определение 10. Две замкнутые схемы согласования p раундов являются *эквивалентными*, если для каждого $i = 0, 1, \dots, p$ выполнено $(a^i)_1 = (a^i)_2, (d^i)_1 = (d^i)_2, (\alpha^i)_1 = (\alpha^i)_2$, где $j = (i + t) \pmod{p}$ для некоторого $t \in \{0, \dots, p-1\}$.

Замкнутые линейные приближения, порождённые эквивалентными схемами согласования раундов, называются *эквивалентными*. Нетрудно заметить, что преобразования эквивалентных замкнутых линейных приближений совпадают. Маски α и β называются *эквивалентными*, если существуют эквивалентные замкнутые схемы согласования, у которых эти маски являются начальными. Будем писать $\alpha \sim \beta$.

Утверждение 2. Маски α и β являются эквивалентными, если и только если существует замкнутая схема согласования p раундов с начальной маской $\alpha = a^0$ и для некоторого $t, 0 \leq t \leq p-1$, выполнено $\beta = a^t$.

Доказательство. Необходимость. Пусть $\alpha \sim \beta$. Рассмотрим эквивалентные замкнутые схемы согласования с начальными масками $\alpha = (a^0)_1$ и $\beta = (a^0)_2$. По определению эквивалентных замкнутых схем согласования, для некоторого $t \in \{0, \dots, p-1\}$ выполнено $\beta = (a^0)_2 = (a^t)_1 = a^t$. Необходимость доказана.

Достаточность. Замкнутая схема согласования с начальной маской $\alpha = a^0 = (a^0)_1$ эквивалентна замкнутой схеме согласования с начальной маской $\beta = a^t = (a^t)_1 = (a^0)_2$, в которой $(\alpha^j)_1 = (\alpha^i)_2$, где $j = (i + t) \pmod{p}$. ■

Утверждение 3 (о спуске). Если в одном из уравнений системы (6) маска входа $a^r = (a_1^r, a_2^r, \dots, a_m^r)$ раунда $r+1$ такая, что $a_i^r = 0$, где $i = 1, \dots, q, q < m$, то можно произвести спуск на q раундов, т. е. получить линейное соотношение $a^r \cdot X^r \oplus a^{r+q} \cdot X^{r+q} = 0$, выполняющееся с вероятностью 1. Маска a^{r+q} при этом будет иметь следующий вид: $a^{r+q} = (a_{q+1}^r, a_{q+2}^r, \dots, a_m^r, a_1^r, a_2^r, \dots, a_q^r) = (a_{q+1}^r, a_{q+2}^r, \dots, a_m^r, 0, 0, \dots, 0)$.

Доказательство. Так как $a_1^r = 0$, то по следствию 2 маска $a^{r+1} = (a_1^{r+1}, a_2^{r+1}, \dots, a_m^{r+1})$ находится из системы (5), а именно $a_1^{r+1} = a_2^r, a_2^{r+1} = a_3^r, \dots, a_{m-1}^{r+1} = a_m^r, a_m^{r+1} = a_1^r = 0$, и соотношение $a^r \cdot X^r \oplus a^{r+1} \cdot X^{r+1} = 0$ выполняется с вероятностью 1. Теперь, если a_2^r нулевая маска, то a_1^{r+1} тоже нулевая и a^{r+2} находится аналогичным способом. Таким образом находим маски $a^{r+1}, a^{r+2}, \dots, a^{r+q}$. В итоге получаем $a^{r+q} = (a_{q+1}^r, a_{q+2}^r, \dots, a_m^r, a_1^r, a_2^r, \dots, a_q^r) = (a_{q+1}^r, a_{q+2}^r, \dots, a_m^r, 0, 0, \dots, 0)$ и систему, описывающую q раундов:

$$\begin{cases} a^r \cdot X^r \oplus a^{r+1} \cdot X^{r+1} = 0, \\ a^{r+1} \cdot X^{r+1} \oplus a^{r+2} \cdot X^{r+2} = 0, \\ \dots \\ a^{r+q-1} \cdot X^{r+q-1} \oplus a^{r+q} \cdot X^{r+q} = 0, \end{cases}$$

т. е. подсистему системы (6), в которой $d^r = d^{r+1} = \dots = d^{r+q} = 0$ и $\alpha^1 = \alpha^2 = \dots = \alpha^{r+p} = 0$. Так как все уравнения в системе выполняются с вероятностью 1, то, если сложим их, по лемме 2 получим, что приближение $a^r \cdot X^r \oplus a^{r+p} \cdot X^{r+p} = 0$ выполняется с вероятностью 1. ■

1.6. Раундовое преобладание

Для применения линейного криптоанализа требуется найти линейное приближение на конкретное число раундов. Очевидно, что лучшим считается то, преобладание которого максимально. Как правило, число раундов довольно большое, а линейное

приближение получается последовательным применением некоторого замкнутого линейного приближения и, если требуется, анализом ещё нескольких раундов. Таким образом, для нахождения лучшего линейного приближения на шифр нужно найти лучшее замкнутое линейное приближение, а для этого нужно научиться их сравнивать. Критерием сравнения линейных приближений является раундовое преобладание.

Определение 11. *Раундовым преобладанием* линейного приближения p раундов назовём величину

$$\tilde{\varepsilon} = (\varepsilon \cdot 2^{1-p})^{1/p},$$

где ε является преобладанием линейного приближения p раундов.

С помощью раундового преобладания можно сравнивать замкнутые линейные приближения на различное количество раундов и определять оптимальное.

Будем говорить, что замкнутое раундовое приближение L_1 *лучше* замкнутого раундового приближения L_2 , если раундовое преобладание приближения L_1 больше раундового преобладания приближения L_2 . *Оптимальным линейным приближением раундов* называется замкнутое линейное приближение, раундовое преобладание которого максимально.

Преобладание линейного приближения, построенного путём последовательного применения замкнутого линейного приближения, вычисляется по лемме 2. Поэтому из оптимального линейного приближения получается линейное приближение, требуемое для линейного криптоанализа шифра, с максимальным преобладанием. Имея такое линейное приближение, можно говорить о стойкости шифра к линейному криптоанализу, о минимальном количестве пар статистики, требуемом для определения ключа.

2. Математическая постановка задачи о линейном приближении

2.1. Дерево шаблонов

Для нахождения оптимального линейного приближения строится бинарное дерево, корень которого фиксирован и каждая вершина имеет двух сыновей, левого и правого. Назовём такое дерево *деревом шаблонов*. Вершины дерева шаблонов будем обозначать v , каждой вершине в таком дереве соответствует некоторый набор означиваний.

Пусть $a_1, a_2, \dots, a_m$ здесь и далее принимают произвольные значения из $\mathbb{Z}_2^n$. Определим функции

$$\begin{aligned} left &: \{(a_1, a_2, a_3, \dots, a_m) : a_1 = 0\} \rightarrow (\mathbb{Z}_2^n)^m, \\ right &: \{(a_1, a_2, a_3, \dots, a_m) : a_1 \neq 0\} \rightarrow \mathcal{P}((\mathbb{Z}_2^n)^m) \end{aligned}$$

следующим образом:

$$\begin{aligned} left((0, a_2, a_3, \dots, a_m)) &= (a_2, a_3, \dots, a_m, 0), \\ right((a_0, \dots, a_m)) &= \\ &= \{(a_2 \oplus b_2, \dots, a_m \oplus b_m, a_1) : R_F(b_1, b_2, \dots, b_m, a_1) \neq 1/2; b_1, b_2, \dots, b_m \in \mathbb{Z}_2^n\}. \end{aligned}$$

Пусть V — это множество вершин, v — вершина. *Означенной вершиной* $\bar{v}$ назовём вектор из $(\mathbb{Z}_2^n)^m$. *Функция означивания* f — это многозначная функция, действующая из V в $(\mathbb{Z}_2^n)^m$, т. е. $\bar{v} = (a_1, a_2, a_3, \dots, a_m) \in f(v)$, где $a_1, \dots, a_m \in \mathbb{Z}_2^n$.

Определим функцию означивания следующим образом. Если v — корень, то $f(v) = (\mathbb{Z}_2^n)^m$. Пусть v_l и v_r — соответственно левый и правый сыновья вершины v_r ,

тогда

$$f(v_l) = \{left(\bar{v}) : \bar{v} \in \text{dom}(left) \cap f(v_p)\},$$

$$f(v_r) = \bigcup_{\bar{v} \in \text{dom}(right) \cap f(v)} right(\bar{v}).$$

Шаблон пути l — это упорядоченный набор вершин $(v_0, v_1, v_2, \dots, v_r)$, где каждая пара (v_i, v_{i+1}) является ребром в дереве шаблонов. Если v_0 — корень дерева, то шаблон пути от корня до вершины v_r обозначим $l(v_r)$, заметим, что $l(v_r)$ единственный. Если v_0 не является корнем, то шаблон пути от v_0 до v_r будем обозначать $l(v_0, v_r)$.

Означенным ребром назовём упорядоченную пару означенных вершин $(\bar{v}, \bar{w})$, для которых выполнено либо $\bar{w} = left(\bar{v})$, либо $\bar{w} \in right(\bar{v})$. *Путь* L — это упорядоченный набор означенных вершин $(\bar{v}_0, \bar{v}_1, \bar{v}_2, \dots, \bar{v}_r)$, где каждая пара $(\bar{v}_i, \bar{v}_{i+1})$ является означенным ребром. Путь L от $\bar{v}_0$ до $\bar{v}_r$ будем обозначать $L(\bar{v}_0, \bar{v}_r)$.

Длиной пути L назовём количество рёбер, входящих в путь L . Длину пути L будем обозначать $|L|$. Аналогично, длину шаблона пути l будем обозначать $|l|$. Заметим, что означенное ребро является путём длины один.

2.2. Поиск итерлируемого пути в дереве

Каждому означенному ребру $(\bar{v}_i, \bar{v}_j)$ ставится в соответствие значение функции ε . Функция действует из множества путей на отрезок $[0, 1/2]$. Путь $L(\bar{v}_0, \bar{v}_r) = (\bar{v}_0, \bar{v}_1, \bar{v}_2, \dots, \bar{v}_r)$ можно задать также и рёбрами $((\bar{v}_0, \bar{v}_1), (\bar{v}_1, \bar{v}_2), \dots, (\bar{v}_{r-1}, \bar{v}_r))$. Пусть действие функции ε определено на означенных рёбрах. Определим действие функции ε на пути следующим образом:

$$\varepsilon(L(\bar{v}_0, \bar{v}_r)) = \frac{1}{2^r} \prod_{i=1}^r \varepsilon(\bar{v}_{i-1}, \bar{v}_i) = \frac{1}{2^r} \prod_{i=1}^r \varepsilon_i, \quad (8)$$

где $\varepsilon(\bar{v}_{i-1}, \bar{v}_i) = \varepsilon_i$.

Определим функцию $\tilde{\varepsilon}$. Функция действует из множества путей на отрезок $[0, 1/2]$. Пусть L — некоторый путь, $\varepsilon = \varepsilon(L)$, $r = |L|$, тогда

$$\tilde{\varepsilon}(L) = (\varepsilon \cdot 2^{1-r})^{1/r}. \quad (9)$$

Будем говорить, что L_1 *лучше*, чем L_2 , и писать $L_1 > L_2$, если $\tilde{\varepsilon}(L_1) > \tilde{\varepsilon}(L_2)$; будем писать $L_1 \geq L_2$, если $\tilde{\varepsilon}(L_1) \geq \tilde{\varepsilon}(L_2)$.

Итерлируемым путём назовём путь $L(\bar{v}_0, \bar{v}_r)$, такой, что $\bar{v}_0 = \bar{v}_r$. Введём отношение эквивалентности на итерлируемых путях. Два итерлируемых пути $L(\bar{v}_0, \bar{v}_r)$ и $L(\bar{w}_0, \bar{w}_r)$ назовём *эквивалентными с параметром* t и будем писать $L(\bar{v}_0, \bar{v}_r) \sim L(\bar{w}_0, \bar{w}_r)$, если для каждого i верно $\bar{v}_i = \bar{w}_j$, где $j = (i + t) \bmod r$ для некоторого t . Означенная вершина $\bar{w}_r$ определяется однозначно, так как $\bar{w}_r = \bar{w}_0$.

Проверим, что введённое отношение действительно является отношением эквивалентности. Рефлексивность выполняется при $t = 0$. Симметричность: если $L_1 \sim L_2$ с параметром t_1 , то $L_2 \sim L_1$ с параметром $t_2 = -t_1$. Транзитивность: если $L_1 \sim L_2$ с параметром t_1 , $L_2 \sim L_3$ с параметром t_2 , то $L_1 \sim L_3$ с параметром $t_3 = t_1 + t_2$.

Оптимальным путём назовём итерлируемый путь L_1 , такой, что для любого итерлируемого пути L_2 выполнено $L_1 \geq L_2$.

Утверждение 4. Пусть L_1 — некоторый путь. Тогда если существует итерлируемый путь L_2 , такой, что $L_2 > L_1$ и $|L_2| > |L_1|$, то L_2 либо его эквивалент содержит подпуть L_3 , такой, что $|L_3| = |L_1|$ и $L_3 > L_1$.

Доказательство. Пусть $\tilde{\varepsilon}_1 = \tilde{\varepsilon}_1(L_1)$, $\tilde{\varepsilon}_2 = \tilde{\varepsilon}_2(L_2)$. Поскольку $L_2 > L_1$, то $\tilde{\varepsilon}_2 > \tilde{\varepsilon}_1$. Пусть $|L_1| = r_1$, $|L_2| = r_2$, тогда по формуле (8) выполняется $(\varepsilon_2 \cdot 2^{1-r_2})^{1/r_2} > (\varepsilon_1 \cdot 2^{1-r_1})^{1/r_1}$; преобразуем далее по формуле (9) и получим

$$\left(\left(2^{r_2-1} \prod_{i=1}^{r_2} \varepsilon_{2_i} \right) 2^{1-r_2} \right)^{1/r_2} > \left(\left(2^{r_1-1} \prod_{i=1}^{r_1} \varepsilon_{1_i} \right) 2^{1-r_1} \right)^{1/r_1},$$

что то же самое, что и $\left(\prod_{i=1}^{r_2} \varepsilon_{2_i} \right)^{1/r_2} > \left(\prod_{i=1}^{r_1} \varepsilon_{1_i} \right)^{1/r_1}$. Для того чтобы нашёлся требуемый подпуть L_3 , такой, что $|L_3| = |L_1| = r_1$ и $L_3 > L_1$, нужно, чтобы нашёлся такой номер j , $1 \leq j \leq r_2$, что $\left(\prod_{i=j+1}^{j+r_1} \varepsilon_{2_i} \right)^{1/r_1} > \left(\prod_{i=1}^{r_1} \varepsilon_{1_i} \right)^{1/r_1}$, где суммы $j+1$ и $j+r_1$ берутся по модулю r_2 .

Заметим, что $\tilde{\varepsilon}_2 = \left(\prod_{i=1}^{r_2} \varepsilon_{2_i} \right)^{1/r_2} = (\varepsilon_{2_1} \varepsilon_{2_2} \cdot \dots \cdot \varepsilon_{2_{r_2}})^{1/r_2} = ((\varepsilon_{2_1} \varepsilon_{2_2} \cdot \dots \cdot \varepsilon_{1_{r_1}})(\varepsilon_{2_2} \varepsilon_{2_3} \times \dots \times \varepsilon_{1_{r_1+1}}) \cdot \dots \cdot (\varepsilon_{1_{r_2}} \varepsilon_{2_1} \cdot \dots \cdot \varepsilon_{1_{r_1-1}}))^{1/(r_1 r_2)} = ((\varepsilon_{2_1} \varepsilon_{2_2} \cdot \dots \cdot \varepsilon_{2_{r_1}})^{1/r_1} (\varepsilon_{2_2} \varepsilon_{2_3} \cdot \dots \cdot \varepsilon_{2_{r_1+1}})^{1/r_1} \cdot \dots \times (\varepsilon_{2_{r_2}} \varepsilon_{2_1} \cdot \dots \cdot \varepsilon_{2_{r_1-1}})^{1/r_1})^{1/r_2}$, т.е. $\tilde{\varepsilon}_2$ представимо в виде среднего геометрического слагаемых вида $(\varepsilon_{2_{j+1}} \varepsilon_{2_{j+2}} \cdot \dots \cdot \varepsilon_{2_{j+r_1}})^{1/r_1}$, где суммы $j+1, j+2, \dots, j+r_1$ рассматриваются по модулю r_2 , $j = 0, \dots, r_2 - 1$. Очевидно, что среднее геометрическое неотрицательных чисел не может превосходить все эти числа, значит, найдётся хотя бы один такой номер j , что $(\varepsilon_{2_{j+1}} \varepsilon_{2_{j+2}} \cdot \dots \cdot \varepsilon_{2_{j+r_1}})^{1/r_1} \geq \tilde{\varepsilon}_2$. Таким образом, так как $0 \leq \varepsilon_{2_i} \leq 1/2$, $r_1 \geq 1$, получаем $\left(\prod_{i=j+1}^{j+r_1} \varepsilon_{2_i} \right)^{1/r_1} = (\varepsilon_{2_{j+1}} \varepsilon_{2_{j+1}} \cdot \dots \cdot \varepsilon_{2_{j+r_1}})^{1/r_1} \geq \tilde{\varepsilon}_2 > \tilde{\varepsilon}_1 = \left(\prod_{i=1}^{r_1} \varepsilon_{1_i} \right)^{1/r_1}$ ■

Теорема 1. Если существует итерируемый путь L_1 , такой, что среди вершин на глубине, не большей $|L_1|$, нет таких, что означивание пути от корня до них даёт путь лучше, чем L_1 , то путь L_1 является оптимальным.

Доказательство. Допустим, что существует итерируемый путь L_2 , такой, что $L_2 > L_1$. Тогда по условию $|L_2| > |L_1|$. По утверждению 4 итерируемый путь L_2 либо его эквивалент содержит подпуть L_3 , такой, что $|L_3| = |L_1|$ и $L_3 > L_1$. Найдём путь в дереве от корня, эквивалентный L_1 . Поскольку $|L_3| = |L_1|$ и $L_3 > L_1$, то это значит, что на глубине $|L_1|$ нашлась вершина, которая порождает путь, лучше чем L_1 , противоречие. ■

Замечание 1. В доказательстве используется отсутствие итерируемых путей L_2 , таких, что $L_2 > L_1$, поэтому посылку теоремы можно ослабить и требовать отсутствие *итерируемых* путей, лучших чем L_1 , на глубине меньшей $|L_1|$. На глубине $|L_1|$ отсутствие путей, лучших чем L_1 , категорично.

Следствие 3. Пусть вершина $\bar{v}_1$ такова, что $L(\bar{v}_1)$ итерируем и

- 1) не существует вершины $\bar{v}_2$, такой, что $L(\bar{v}_2)$ итерируем и $|L(\bar{v}_2)| < |L(\bar{v}_1)|$;
- 2) для любой вершины $\bar{v}_3$, такой, что $|L(\bar{v}_3)| = |L(\bar{v}_1)|$, выполнено $L(\bar{v}_1) \geq L(\bar{v}_3)$.

Тогда путь $L(\bar{v}_1)$ является оптимальным.

Другими словами, самая первая вершина (если искать её в дереве по ярусам, увеличивая глубину), дающая итерируемый путь, который является лучшим среди всех путей на этой глубине, даёт оптимальный путь.

Следствие 4. Пусть вершина $\bar{v}_1$ такова, что $L(\bar{v}_1)$ итерируем и

- 1) не существует вершины $\bar{v}_2$, такой, что $L(\bar{v}_2)$ итерируем и $|L(\bar{v}_2)| < |L(\bar{v}_1)|$;
- 2) $\bar{w}_1, \dots, \bar{w}_m$ — все вершины, такие, что $|L(\bar{w}_i)| = |L(\bar{v}_1)|$ и $L(\bar{w}_i) \geq L(\bar{v}_1)$.

Тогда любой итерируемый путь $L(\bar{w})$, лучший, чем $L(\bar{v}_1)$, содержит одну из вершин $\bar{w}_1, \dots, \bar{w}_m$.

2.3. Алгоритм

Сложность поиска оптимального пути в том, что дерево может быть бесконечно. Не ясно, когда завершить поиск, как понять, что дальнейший поиск бесперспективен. Опишем алгоритм поиска оптимального пути, который имеет конкретное условие остановки и рассматривает меньше означиваний, чем исчерпывающий поиск; он основан на следующем утверждении.

Утверждение 5. Пусть $L(\bar{v}_1)$ — некоторый путь. Тогда для любой вершины $\bar{v}_2$, такой, что $L(\bar{v}_1) \geq L(\bar{v}_2)$ и $|L(\bar{v}_1)| \leq |L(\bar{v}_2)|$, верно, что если она принадлежит некоторому итерируемому пути $L(\bar{w}_2)$, лучшему, чем $L(\bar{v}_1)$, то у $L(\bar{w}_2)$ найдётся эквивалент с подпутём $L(\bar{v}')$, таким, что $|L(\bar{v}_2)| = |L(\bar{v}')|$ и $L(\bar{v}') > L(\bar{v}_1)$.

Доказательство. Допустим, что у вершины $\bar{v}_2$ нашёлся потомок $\bar{w}_2$, такой, что $L(\bar{w}_2)$ итерируем и $L(\bar{w}_2) > L(\bar{v}_1)$. Тогда, раз $L(\bar{w}_2) > L(\bar{v}_1) \geq L(\bar{v}_2)$, то $L(\bar{w}_2) > L(\bar{v}_2)$ и по утверждению 4 эквивалент пути $L(\bar{w}_2)$ — некоторый путь $L(\bar{w}_3)$ — содержит подпуть $L(\bar{v}_3)$, такой, что $|L(\bar{v}_3)| = |L(\bar{v}_2)|$ и $L(\bar{v}_3) > L(\bar{v}_2)$. Если $L(\bar{v}_3) > L(\bar{v}_1)$, то $L(\bar{v}_3)$ — искомый подпуть. Если же $L(\bar{v}_3) \leq L(\bar{v}_1)$, то $L(\bar{w}_3) = L(\bar{w}_2) > L(\bar{v}_1) \geq L(\bar{v}_3)$, т. е. $L(\bar{w}_3) > L(\bar{v}_3)$ и по утверждению 4 эквивалент пути $L(\bar{w}_3)$ содержит подпуть, лучший, чем $L(\bar{v}_3)$ и той же длины. Если он лучше $L(\bar{v}_1)$, то он искомый, иначе применяем утверждение 4 дальше, пока не найдём $L(\bar{v}')$, который будет лучше $L(\bar{v}_1)$.

Пусть $L(\bar{v}_i)$ — произвольный подпуть длины $|L(\bar{v}_2)|$ пути, эквивалентного $L(\bar{w}_2)$. Покажем, что $L(\bar{v}')$ обязательно найдётся. Действительно, если он не найдётся, т. е. для всех $L(\bar{v}_i)$ выполнено $L(\bar{v}_i) \leq L(\bar{v}_1)$, то пусть среди них $L(\bar{v}_m)$ — самый лучший, т. е. такой, что $L(\bar{v}_m) \geq L(\bar{v}_i)$ для всех $L(\bar{v}_i)$. Путь $L(\bar{v}_m)$ является подпутём $L(\bar{w}_m)$, который эквивалентен $L(\bar{w}_2)$, значит, $L(\bar{w}_m) = L(\bar{w}_2) > L(\bar{v}_1) \geq L(\bar{v}_m)$, т. е. $L(\bar{w}_m) > L(\bar{v}_m)$ и по утверждению 4 эквивалент пути $L(\bar{w}_m)$ содержит подпуть длины $|L(\bar{v}_2)|$, лучший, чем $L(\bar{v}_m)$, противоречие. ■

Замечание 2 (о корректности алгоритма). Если алгоритм останавливается, то он даёт оптимальный путь L_c . При работе алгоритма учитываются все кандидаты на оптимальный путь, не отбрасывается ничего нужного. Из утверждения 5 следует, что каждое новое заполнение множества кандидатов C содержит все пути, которые могут дать пути, лучшие, чем уже найденные. Если таких нет, то найденный путь является лучшим.

Алгоритм является алгоритмом поиска оптимального линейного приближения обобщённой сети Фейстеля, т. е. найденный оптимальный путь является оптимальным линейным приближением.

Каждое новое заполнение множества C даёт линейное приближение, лучшее, чем предыдущее, и соответствует рассмотрению ещё одного раунда; обобщённая сеть Фейстеля состоит из конечного числа раундов (пусть r). Отсюда следует, что если алгоритм не остановился за r перезаполнений, то лучшим приближением для r раундов будет лучшее приближение из последнего заполнения множества кандидатов C .

Алгоритм 1. Поиск оптимального пути**Вход:** функции $left$, $right$; корень v_0 **Выход:** оптимальный путь L_c

```

1:  $C := \{L(\bar{v}, \bar{v}), \bar{v} \in f(v_0)\}$ ,  $NC := \emptyset$ .
2: Пока  $C$  не пусто
3:   Для  $L(\bar{v}_0, \bar{v}) \in C$ 
4:     Для  $\bar{w} \in right(\bar{v}) \cup \{left(\bar{v})\}$ 
5:       Если  $\bar{w} = \bar{v}_0$ , то
6:         Если  $L_c$  не определён, то
7:            $L_c := L(\bar{v}_0, \bar{w})$ ;
8:         иначе
9:           Если  $L(\bar{v}_0, \bar{w}) > L_c$ , то
10:             $L_c := L(\bar{v}_0, \bar{w})$ .
11:     Для  $\bar{w} \in right(\bar{v}) \cup \{left(\bar{v})\}$ 
12:       Если  $L_c$  определён, то
13:         Если  $L(\bar{v}_0, \bar{w}) > L_c$ , то
14:           добавляем  $L(\bar{v}_0, \bar{w})$  в  $NC$ ;
15:       иначе
16:         добавляем  $L(\bar{v}_0, \bar{w})$  в  $NC$ .
17:    $C := NC$ ,  $NC := \emptyset$ .
```

Заключение

В работе получены следующие результаты:

- предложен общий подход к нахождению линейных приближений обобщённой сети Фейстеля;
- дана математическая постановка задачи о линейном приближении;
- разработан алгоритм поиска оптимального линейного приближения обобщённой сети Фейстеля.

Результаты работы могут быть применены при проведении линейного криптоанализа блочных шифров, построенных на основе сети Фейстеля, а также при получении оценок стойкости таких шифров к линейному криптоанализу.

ЛИТЕРАТУРА

1. Diffie W. SMS4 encryption algorithm for wireless networks // Cryptology ePrint Archive. Report 2008/329, 2008. <http://eprint.iacr.org/2008/329>
2. Matsui M. and Yamagishi A. A new method for known plaintext attack of FEAL cipher // EUROCRYPT'92. LNCS. 1993. V. 658. P. 81–91.
3. Matsui M. Linear cryptanalysis method for DES cipher // EUROCRYPT'93. LNCS. 1993. V. 765. P. 386–397.
4. Matsui M. The first experimental cryptanalysis of the Data Encryption Standard // CRYPTO'94. LNCS. 1994. V. 839. P. 1–11.
5. Nyberg K. Linear approximation of block ciphers // EUROCRYPT'94. LNCS. 1995. V. 950. P. 439–444.
6. Kaliski B. and Robshaw M. Linear cryptanalysis using multiple approximations // CRYPTO'94. LNCS. 1994. V. 839. P. 26–39.

7. *Sakurai K. and Furuya S.* Improving linear cryptanalysis of LOKI91 by probabilistic counting method // FSE'97. LNCS. 1997. V 1267. P. 114–133.
8. *Collard B., Standaert F.-X., and Quisquater J.-J.* Improving the time complexity of Matsui's linear cryptanalysis // ICISC'2007. LNCS. 2007. V. 4817. P. 77–88.
9. *Токарева Н. Н.* О квадратичных аппроксимациях в блочных шифрах // Проблемы передачи информации. 2008. Т. 44. № 3. С. 105–127.
10. *Алфёров А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2005.
11. *Wheeler D. J. and Needham R. M.* TEA, a tiny encryption algorithm // LNCS. 1994. V. 1008. P. 363–366.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

DOI 10.17223/20710410/23/6

УДК 519.7

МЕТОД ОБНАРУЖЕНИЯ АТАК ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ» НА WEB-ПРИЛОЖЕНИЯ

С. Н. Сорокин

*Московский институт электроники и математики Национального исследовательского
университета «Высшая школа экономики», г. Москва, Россия*

E-mail: sergey-dcm@yandex.ru

Рассматривается метод обнаружения атак типа «отказ в обслуживании» на web-приложения, основанный на использовании многослойного персептрона. Описаны основные вопросы, связанные с использованием нейронной сети: процесс сбора и подготовки статистических данных, особенности формирования показателей, описывающих состояние web-приложения, а также вопросы обучения и оценки качества работы нейронной сети.

Ключевые слова: обнаружение атак, отказ в обслуживании, DoS, web-приложение.

Введение

За сравнительно небольшой промежуток времени в сети Интернет возникло большое количество web-приложений, предоставляющих пользователям различную информацию или оказывающих услуги. В Интернет постепенно переносятся традиционные приложения, что обеспечивает возможность удобного взаимодействия с ними с помощью различных устройств и практически в любом месте. В связи с этим происходит постоянный рост числа пользователей web-приложений и возникает проблема обеспечения надежного функционирования таких систем.

Современные web-приложения являются достаточно сложным программным обеспечением, которое может обрабатывать большие объёмы данных и формировать ответы на запросы пользователей. Сложность функционирования web-приложений приводит к возникновению высоких нагрузок на аппаратные ресурсы, а большое количество пользователей делает такие приложения интересной мишенью для компьютерных атак. Атаки на web-приложения могут проводиться с разными целями, например с целью кражи персональной информации или информации о кредитных картах пользователей.

Одним из популярных типов атак на web-приложения является «отказ в обслуживании». Количество атак данного типа в 2013 г. увеличилось на 32,4 % по сравнению с 2012 г. [1]. Цель атак типа «отказ в обслуживании» — полный или частичный вывод из строя web-приложения, что лишает пользователей возможности в полной мере его использовать. «Отказ в обслуживании» web-приложения может достигаться с помощью атак, направленных на его инфраструктуру, либо может проводиться на прикладном уровне, при этом осуществляется взаимодействие с приложением по протоколу HTTP.

Атаки, направленные на инфраструктуру web-приложения, достаточно хорошо изучены; существует большое количество методов обнаружения таких атак:

- отклонение параметров данных;
- изменение вероятностных параметров данных;
- обнаружение с помощью извлечения данных;
- восстановление пути по сигнатурам;
- метод разметки пакетов;
- генерация служебных пакетов и др.

Данные методы плохо применимы для анализа атак на web-приложения, проводимых на прикладном уровне. Это связано с тем, что различные компоненты современных web-приложений сильно отличаются частотой использования и потреблением аппаратных ресурсов, а также с тем, что в современных web-приложениях происходит постоянный рост количества доступных для просмотра страниц.

На прикладном уровне к «отказу в обслуживании» web-приложения могут приводить эксплуатация различных уязвимостей в web-приложении и превышение допустимого количества запросов, которые могут быть одновременно обработаны web-приложением.

Увеличение количества запросов, находящихся одновременно на обработке в web-приложении, может происходить:

- за счёт увеличения интенсивности потока запросов;
- в процессе атак, использующих уязвимости в протоколе HTTP (например, `slow HTTP POST` [2]).

В работе рассматриваются атаки «отказ в обслуживании», возникающие вследствие увеличения интенсивности потока поступающих запросов, вызванного путем имитации действий пользователей автоматическими программами (ботами). Данный вид атак в 2013 г. составил 86 % от общего количества атак типа «отказ в обслуживании» на web-приложения, проводимых на прикладном уровне [1].

В настоящее время не существует общепринятых классификаций и эффективных методов обнаружения данного вида атак. На прикладном уровне известен метод обнаружения атак типа «отказ в обслуживании» на основе оценки вероятности потерь заявок, однако он применим только в случае низкоактивных атак [3]. В связи с этим задача создания метода обнаружения атак типа «отказ в обслуживании» на web-приложения, функционирующего на прикладном уровне, является актуальной.

1. Общая схема метода обнаружения атак типа «отказ в обслуживании» на web-приложения

Существует два основных подхода к обнаружению атак: обнаружение аномалий и обнаружение злоупотреблений [4]. При обнаружении аномалий составляется профиль нормального состояния системы, отклонение текущего состояния системы от профиля считается аномалией и делается заключение о возможной атаке. При обнаружении злоупотреблений задача состоит в том, чтобы описать профили системы в состоянии различных атак, чтобы в дальнейшем распознавать различные виды атакующих воздействий.

Для построения метода использован подход, связанный с обнаружением злоупотреблений с помощью нейронных сетей. Данный подход позволяет гибко адаптировать средство обнаружения атак к особенностям конкретного web-приложения (производить автоматическую настройку допустимых значений параметров), он успешно

используется для решения ряда смежных задач и обнаружения некоторых классов атак [5–7].

В качестве используемой нейронной сети целесообразно использовать сеть многослойного персептрона ввиду следующих особенностей [8]:

- эффективность решения задач аппроксимации;
- возможность работы с нелинейно-разделимыми входными показателями;
- простота реализации;
- высокая скорость работы сети — это делает возможным использование данного типа нейронной сети для обнаружения атак типа «отказ в обслуживании» в реальном времени.

Общая схема метода обнаружения атак типа «отказ в обслуживании» представлена на рис. 1.

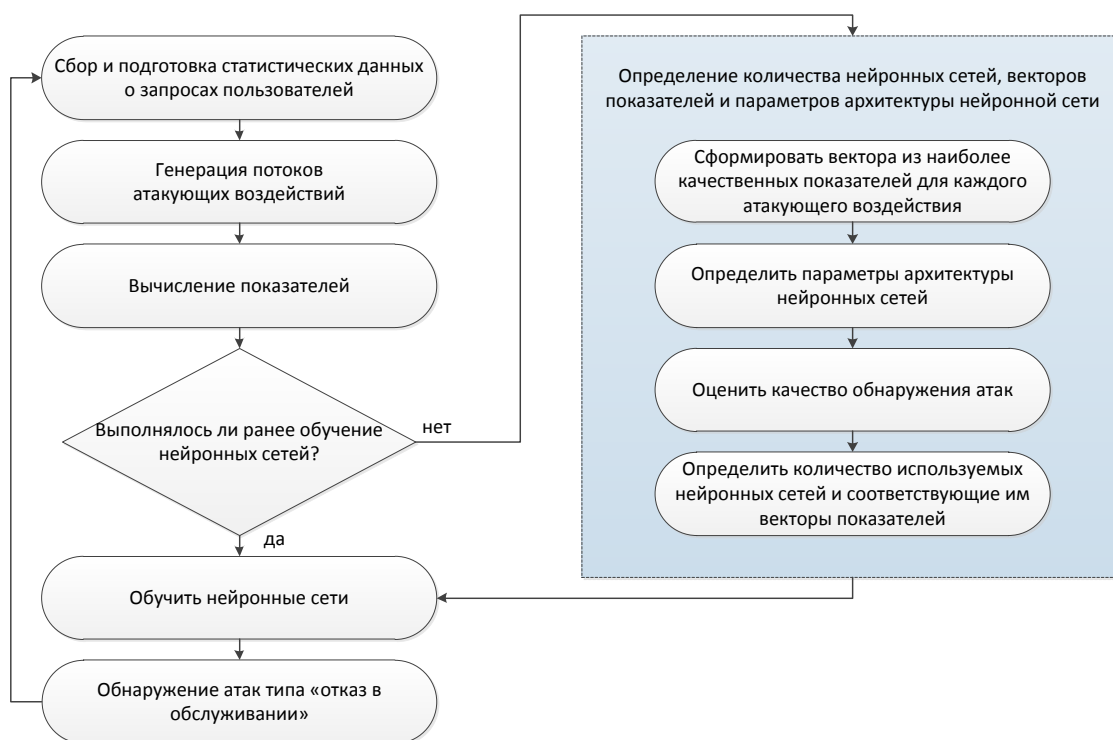


Рис. 1. Общая схема функционирования метода обнаружения атак типа «отказ в обслуживании» на web-приложения

Метод заключается в следующем:

- 1) подготовить статистическую информацию о поведении пользователей;
- 2) произвести генерацию статистической информации о различных видах атакующих воздействий, приводящих к «отказу в обслуживании»;
- 3) вычислить в рассматриваемом временном периоде (не меньше недели) значения показателей (и соответствующих показателям статистических структур);
- 4) провести оценку применимости показателей и сформировать множества показателей, наиболее подходящих для определения различных видов атак;

- 5) определить наилучшие параметры архитектуры нейронных сетей для различных видов атак и качество обнаружения атак;
- 6) сгруппировать различные виды атак в классы атакующих воздействий с целью уменьшения количества используемых нейронных сетей;
- 7) произвести обучение нейронных сетей;
- 8) использовать нейронные сети для обнаружения атак типа «отказ в обслуживании»;
- 9) по необходимости производить переобучение нейронных сетей на новых статистических данных.

2. Сбор статистических данных

Для описания запроса пользователя к web-приложению разработан следующий формат векторов данных:

$$(Time_i, SessionID_i, IsSessionStart_i, URL_i, Parameters_i, IP_i, Referer_i, UserAgent_i, Latency_i, DocSize_i, Memory_i, CpuTime_i),$$

где

- i — порядковый номер запроса к web-приложению;
- $Time_i$ — время запроса, выраженное в формате `timestamp`;
- $SessionID_i$ — идентификатор сеанса;
- $IsSessionStart_i$ — индикатор начала сеанса;
- URL_i — URL-адрес запроса;
- $Parameters_i$ — GET-параметры запроса;
- IP_i — IP-адрес, с которого был сделан запрос;
- $Referer_i$ — адрес предыдущей посещенной страницы;
- $UserAgent_i$ — идентификационная строка клиентской программы пользователя;
- $Latency_i$ — время отклика сервера при обработке данного запроса;
- $DocSize_i$ — объём данных, которые были загружены пользователем в ответ на запрос;
- $Memory_i$ — количество оперативной памяти сервера, потраченное на обработку запроса;
- $CpuTime_i$ — процессорное время, потраченное на выполнение запроса.

Порядок подготовки статистических данных о запросах пользователей представлен на рис. 2.

После сбора статистики в предложенном формате необходимо произвести преобразование URL-запросов к каноническому виду с помощью правил преобразования адреса, удаления и задания порядка параметров запросов.

Введём следующие обозначения:

- URL — строка URL [9];
- $ScriptURL$ — строка URL без строки запроса (начальный фрагмент URL до символа «?»);
- n — максимально возможное количество параметров в запросе;
- s — количество всех возможных параметров в web-системе;
- $\{parameter_1, \dots, parameter_s\}$ — множество всех возможных параметров в web-системе;
- $parameter_i^j$ — некоторый j -й параметр в запросе, $j \in \{1, \dots, n\}$, $i \in \{1, \dots, s\}$;
- $parameters = parameter_{i_1}^1 \& \dots \& parameter_{i_k}^k$ — строка параметров, содержащая $k \in \{1, \dots, n\}$ параметров, $i_k \in \{1, \dots, s\}$;

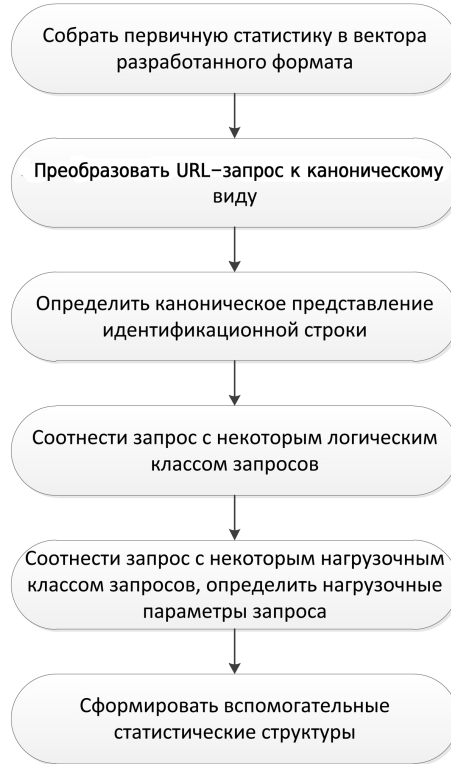


Рис. 2. Порядок подготовки статистических данных

- $URLFilter(ScriptURL)$ — функция, описывающая алгоритм формирования пути к ресурсу на сервере, не содержащего специальных конструкций;
- $ParametersSequence(parameter_{i_1}, \dots, parameter_{i_k})$ — функция, описывающая применение правил формирования последовательности параметров к некоторой последовательности параметров $parameter_{i_1}, \dots, parameter_{i_k}$, $i_j \in \{1, \dots, s\}$, $j \in \{1, \dots, k\}$, $k \in \{1, \dots, n\}$, результат работы функции не зависит от порядка следования аргументов;
- $ParameterPresence(parameter_i)$ — функция, описывающая применение правил удаления параметров к некоторому параметру $parameter_i$, $i \in \{1, \dots, s\}$;
- $.$ — операция «склейки» строк.

Во введённых обозначениях URL можно представить [9] как

$$URL = ScriptURL.?.parameters.$$

Канонической формой запроса для некоторого запроса URL называется запрос следующего вида:

$$CanonicalURL(URL) = URLFilter(ScriptURL).?.ParametersSequence \left(\begin{array}{c} ParameterPresence(parameter_{i_1}^1), \\ \dots \\ ParameterPresence(parameter_{i_k}^k) \end{array} \right).$$

Алгоритм формирования пути $URLFilter(ScriptURL)$ может быть описан следующим образом: удалить из части строки $ScriptURL$, следующей за названием домена и портом, в следующей последовательности:

- 1) конструкции вида «//» из строки $ScriptURL$;

- 2) конструкции вида «./» из строки *ScriptURL*;
- 3) конструкции вида «/text/./», где *text* — произвольная строка, не содержащая символов «/».

Каноническое представление идентификационной строки необходимо для анализа строки *User – Agent*. Анализ исходных данных *User – Agent* затруднён, поскольку существует большое количество браузеров, а эти строки могут существенно различаться даже у различных версий одного браузера. Поэтому необходимо выделить из строк *User – Agent* значимые параметры и привести их строковую запись к единому виду. Этот процесс аналогичен получению канонического вида строк URL-запросов: необходимо сформировать правила удаления и упорядочивания параметров строки *User – Agent*.

В дальнейшем необходимо разбить все запросы по логическому и нагрузочному типу страниц.

В основе **кластеризации по логическому типу страницы** лежат следующие предположения:

- пользователям свойственно совершение некоторых последовательностей действий, которые имеют схожую смысловую нагрузку: например, просмотр новостей обычно подразумевает просмотр ленты новостей, чередующийся с просмотром страниц конкретных новостей;
- схожие действия пользователей (например, просмотр новости или профиля) приводят к возникновению схожих нагрузок на сервере.

Разбиение по логическому типу страниц производится в два этапа:

- выделение крупных логических разделов на множестве страниц web-приложения (например, форум, чат, новостная лента и т. п.);
- выделение различных типовых действий пользователей внутри логических разделов (например, для форума: чтение списка форумов, чтение списка тем, чтение темы и т. п.).

При **кластеризации по нагрузочным показателям** в один класс помещаются запросы, создающие на сервере сходные нагрузки на различные ресурсы. Кластеризация по нагрузочным характеристикам неинформативна для описания поведения пользователей, поскольку сходные по нагрузке запросы могут быть совершенно различными, не связанными между собой действиями пользователя web-приложения. Поэтому целесообразно использовать комбинированный подход, при котором сначала производится разбиение запросов по логическому типу, а потом запросы из одного логического класса ещё раз разбиваются на классы по нагрузочным показателям.

Для разбиения по нагрузочным характеристикам можно использовать алгоритм построения минимального остовного дерева [10].

Для формирования показателей, учитывающих зависимости между запросами пользователей, необходимо сформировать дополнительные статистические структуры, описывающие различные свойства поведения пользователей. В рамках исследования автором выделены следующие направления анализа зависимостей:

- зависимость появления запроса от предыдущего запроса;
- зависимость появления запроса от его расположения в пользовательских сеансах;
- зависимость появления запроса от последовательности предыдущих запросов.

Для учёта каждой из этих зависимостей предложено использовать следующие статистические структуры:

- матрица зависимостей от предыдущих запросов;

- матрица зависимостей от номера запроса в сеансе;
- лес сеансовых деревьев.

3. Формирование множества показателей, описывающих состояние web-приложения

Предлагается подход к формированию показателей для обучения нейронной сети, которые учитывают изменения посещаемости web-приложения в различное время суток, в разные дни недели. Данный подход позволяет также учесть естественные изменения популярности web-приложения.

Пусть:

- u — количество показателей, подаваемых на вход нейронной сети;
- K_g — некоторый показатель, подаваемый на вход нейронной сети, $g \in \{1, \dots, u\}$;
- $K_{g,i,t,h}$ — некоторый показатель, подаваемый на вход нейронной сети, вычисленный i дней назад во время t за временной интервал h , $g \in \{1, \dots, u\}$;
- $\bar{K} = (K_1, \dots, K_u)$ — вектор длины u , характеризующий набор показателей, подающихся на вход нейронной сети.

В зависимости от значения длины временного интервала h сутки можно разбить на различное количество временных интервалов. Обозначим N_h — количество временных интервалов при выбранном значении h . Тогда $N_h = 86400/h$; 86400 — это длина суток, выраженная в секундах.

3.1. Учёт времени суток при работе с нейронной сетью

Пусть натуральное число $n_{t,h} \in \{1, \dots, N_h\}$ — порядковый номер временного интервала, соответствующего времени t в текущих сутках, вычисляемый по формуле $n_{t,h} = \lfloor t \bmod 86400/h \rfloor$.

Для учёта изменений поведения пользователей в различное время суток необходимо добавить в векторы входных показателей нейронной сети $(K_1, \dots, K_u)$ специальный показатель $n_{t,h}$.

3.2. Учёт дня недели и изменения популярности web-приложения

Для учёта данных изменений при расчёте показателей необходимо использовать результаты вычисления показателей в прошлом и специальный поправочный множитель (множитель популярности), характеризующий тенденцию изменения популярности web-приложения.

Схема вычисления прогнозного значения представлена на рис. 3.

Цифрами обозначены дни недели, отсчитанные от текущего дня в прошлое. Для прогнозирования текущего значения берётся прошлое значение и корректируется с помощью множителя популярности. Пример показателя, сформированного по данной схеме, представлен формулой (1).

Для формирования множества показателей можно использовать следующие классы показателей (классификация проведена по типу оцениваемых характеристик web-приложения):

- частотные показатели учитывают частотные свойства потока запросов к web-приложению;
- нагрузочные показатели основаны на изменениях нагрузочных характеристик запросов;
- структурные показатели учитывают структурные изменения в потоке запросов к web-приложению.

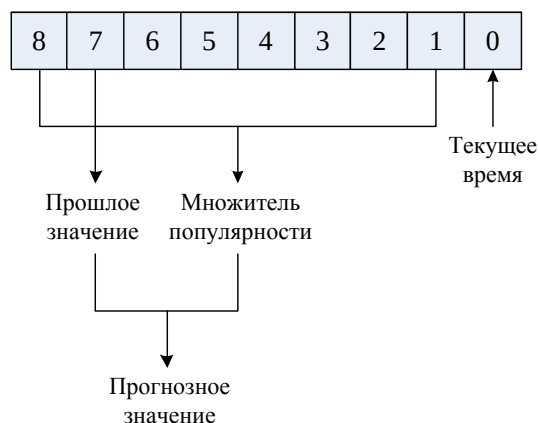


Рис. 3. Схема вычисления прогнозного значения показателя

Пример частотного показателя «Отношение посещаемости», отражающего, насколько текущая посещаемость отличается от прогнозной:

$$SessionsRatio_{0,t,h} = \frac{Sessions_{0,t,h}}{Sessions_{7,t,h} \cdot \frac{Sessions_{1,t,h}}{Sessions_{8,t,h}}}, \quad (1)$$

где $Sessions_{i,t,h}$ — количество сеансов пользователей, работавших с web-приложением i дней назад, рассчитанное во время t за временной интервал h .

4. Генерация атакующих воздействий

В процессе исследований рассмотрены модель поведения пользователей web-приложения и классификация основных типов автоматических программ, действия которых могут приводить к «отказу в обслуживании». Выделены следующие основные классы автоматических программ:

- поисковые;
- выгружающие содержимое страниц web-приложения;
- взаимодействующие с поисковой выдачей web-приложения;
- связанные с конкретными HTML-формами;
- собирающие информацию о web-приложении;
- атакующие.

На основании данной классификации можно сформировать статистические данные о запросах для различных типов атакующих воздействий. Более подробно вопросы классификации и имитации различных классов автоматических программ будут рассмотрены в других работах автора.

5. Обучение, определение параметров архитектуры и оценка качества работы нейронной сети

Обучение многослойного персептрона проводится с помощью алгоритма обратного распространения ошибки. Для обучения можно использовать следующий критерий останова [8]:

- ошибка обучения перестаёт уменьшаться (либо интенсивность уменьшения ошибки достигает порогового значения);

- ошибка достигает некоторого порогового значения;
- количество обучающих итераций достигает порогового значения (при этом не гарантируется правильность обучения многослойного персептрона).

Для определения параметров архитектуры необходимо провести последовательность тестов с увеличением количества слоёв нейронов и нейронов в одном слое. В результате тестов определяются параметры, когда минимальны

- средняя ошибка обучения на момент останова обучения;
- среднее количество обучающих эпох.

Для оценки качества работы нейронной сети используются следующие показатели:

- доля правильных ответов;
- доля ошибок первого рода;
- доля ошибок второго рода;
- доля неопределённых ответов.

6. Формирование векторов показателей для обучения нейронной сети

На первом этапе для формирования векторов показателей необходимо определить наиболее подходящие показатели для определения различных типов атакующих воздействий. Для этого используется методика оценки применимости показателей, основанная на вычислении следующих характеристик:

- амплитуды (разброса значений показателя);
- цикличности (степени различий между значениями показателя в различные дни недели);
- дифференциации (степени различий средних значений показателя на статистике нормального поведения пользователей и статистике атак).

На основании разработанной методики производится отбор наиболее подходящих для обнаружения различных видов атакующих воздействий показателей.

При таком подходе для обнаружения различных видов атакующих воздействий используются разные нейронные сети. Для ускорения работы метода предложена методика объединения различных типов атакующих воздействий в классы атак, что позволило использовать общий вектор показателей и одну нейронную сеть для атакующих воздействий, находящихся в одном классе атак.

Подробнее методики оценки качества показателей и формирования векторов показателей будут рассмотрены в других работах автора.

Заключение

Рассматривается метод, позволяющий производить обнаружение атак типа «отказ в обслуживании» на web-приложения на прикладном уровне. Данный метод был успешно протестирован и планируется к использованию при построении и внедрении систем обнаружения атак на web-приложения в органах государственной власти РФ.

Описанный подход к построению множества показателей позволяет обеспечить работоспособность метода с учётом изменения посещаемости web-приложения с течением времени суток, в различные дни недели и с учётом естественных изменений популярности web-приложений.

Методики оценки показателей и формирования векторов показателей и классов атак позволяют повысить производительность метода за счёт уменьшения количества используемых нейронных сетей и векторов показателей. Это позволяет использовать метод в реальном времени.

ЛИТЕРАТУРА

1. <http://www.prolexic.com/knowledge-center-ddos-attack-report-2013-q4.html> — Q4 2013 Global DDoS Attack Report. 2014.
2. <https://community.qualys.com/blogs/securitylabs/2012/01/05/slow-read> — Are you ready for slow reading? 2012.
3. *Щерба М. В.* Обнаружение низкоактивных распределенных атак типа «отказ в обслуживании» в компьютерных сетях: дис. ... канд. техн. наук. Омск, 2007. 130 с.
4. *Гамаюнов Д. Ю.* Обнаружение компьютерных атак на основе поведения сетевых объектов: дис. ... канд. физ.-мат. наук. М., 2007. 89 с.
5. *Жульков Е. В.* Построение нейронных сетей для обнаружения классов сетевых атак: дис. ... канд. техн. наук. СПб., 2007. 155 с.
6. *Александров И. С.* Разработка системы защиты web-приложений от автоматизированного копирования информации: дис. ... канд. техн. наук. М., 2003. 127 с.
7. *Хафизов А. Ф.* Нейросетевая система обнаружения атак на www-сервер: дис. ... канд. техн. наук. Уфа, 2004. 172 с.
8. *Хайкин С.* Нейронные сети: полный курс. 2-е изд., испр. М.: ООО «И.Д. Вильямс», 2006. 1104 с.
9. <http://tools.ietf.org/html/rfc1738#section-3.3> — Uniform Resource Locators (URL). 1994.
10. *Menasce D. A. and Almeida V. A. F.* Capacity Planning for Web Services. Metrics, Models, and Methods. New Jersey: Prentice Hall PTR, 2001. 608 p.

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

DOI 10.17223/20710410/23/7

УДК 519.7

О ВЕСОВЫХ СПЕКТРАХ ОДНОГО КЛАССА ЛИНЕЙНЫХ КОДОВ

А. В. Покровский

Институт проблем информационной безопасности Московского государственного университета им. М. В. Ломоносова, г. Москва, Россия

E-mail: AlexPokrovskiy@yandex.ru

Рассматривается класс линейных кодов, являющихся подкодами кода Рида — Маллера. Для данного класса кодов рассчитываются их весовые спектры.

Ключевые слова: код Рида — Маллера, весовой спектр, булевы функции, вес булевой функции.

Введение

Проблема описания весового спектра кода Рида — Маллера тесным образом связана с задачей классификации булевых функций относительно группы аффинных или линейных преобразований, действующих на её аргументах. Для квадратичных булевых функций она была решена с помощью аппарата симплектических форм и теоремы Диксона [1, 2], что позволило описать весовой спектр кода Рида — Маллера второго порядка. Иначе обстоит дело с классификацией булевых функций более высоких степеней. Начиная уже с кубических форм, нет их полной классификации, хотя исследования в этом направлении проводятся довольно давно. В этой связи следует отметить работу [3], в которой получено существенное продвижение в данном вопросе. Аналогичная ситуация складывается и при описании весового спектра кодов Рида — Маллера более высоких порядков. Существенными результатами в области описания этой характеристики кодов являются формула Касами — Токуры [2] для числа кодовых слов, вес которых лежит в определённом диапазоне, и теорема, описывающая весовой спектр произвольного кода с максимальным расстоянием [4]. В настоящей работе рассматривается один из подкодов кода Рида — Маллера произвольного порядка и описывается его весовой спектр.

1. Основные обозначения и определения

Символом $\mathcal{F}_n$, $n \in \mathbb{N}$, будем обозначать множество булевых функций от n переменных, $\mathbb{F}_q$ — поле из q элементов. Для веса булевой функции и степени её полинома Жегалкина используем запись $\text{wt}(f)$ и $\deg(f)$ соответственно.

Определение 1. *Линейным кодом над $\mathbb{F}_q$ называется подпространство $\mathcal{C}$ векторного пространства $\mathbb{F}_q^n$. Размерность $\mathcal{C}$ называется *размерностью кода*. Если она равна k , то такой код называется (n, k) -кодом. *Кодовым расстоянием $\mathcal{C}$* называется минимальный вес Хемминга ненулевого элемента $c \in \mathcal{C}$. Если кодовое расстояние $\mathcal{C}$ равно d , то такой код называется (n, k, d) -кодом.*

Для любого линейного (n, k, d) -кода справедлива оценка Синглтона [1, 2, 4]

$$d \leq n - k + 1.$$

Определение 2. Любой код с кодовым расстоянием, удовлетворяющим равенству $d = n - k + 1$, называется *кодом с максимальным расстоянием*.

Определение 3. *Весовым спектром* (n, k) -кода $\mathcal{C}$ называется совокупность чисел $A_0, A_1, \dots, A_n$, где $A_i = |\{c \in \mathcal{C} : \text{wt}(c) = i\}|$, $i = 0, 1, \dots, n$.

Весовой спектр кодов с максимальным расстоянием описывает следующая теорема.

Теорема 1 [4]. Распределение весов (n, k, d) -кода над $\mathbb{F}_q$ с максимальным расстоянием определяется формулами $A_0 = 1$, $A_l = 0$ при $l = 1, \dots, d - 1$ и

$$A_l = \binom{n}{l} (q - 1) \sum_{j=0}^{l-d} (-1)^j \binom{l-1}{j} q^{l-d-j} \quad \text{при } l \geq d.$$

Практически важным классом линейных кодов является код Рида — Маллера, который определяется через булевы функции заданной степени. Обозначим Ω_f вектор значений функции $f \in \mathcal{F}_n$:

$$\Omega_f = (f(u_0), f(u_1), \dots, f(u_{2^n-1})), \quad u_i \in \mathbb{F}_2^n, \quad i = 0, \dots, 2^n - 1.$$

Определение 4. Для произвольных $n, r \in \mathbb{N}$, $0 \leq r \leq n$, *кодом Рида — Маллера* $\text{RM}(r, n)$ порядка r и длины 2^n называется множество всех строк Ω_f булевых функций $f \in \mathcal{F}_n$, удовлетворяющих условию $\deg(f) \leq r$.

На данный момент полностью описан весовой спектр кода $\text{RM}(2, n)$. Эту задачу удалось решить, используя полученную классификацию квадратичных форм. Обозначим AGL группу аффинных преобразований на $\mathbb{F}_2^n$.

Определение 5. Функции $f_1, f_2 \in \mathcal{F}_n$ называются *аффинно эквивалентными*, если существует пара $(A, \gamma) \in \text{AGL}$, такая, что $f_1(xA \oplus \gamma) = f_2(x)$ для любого $x \in \mathbb{F}_2^n$, где A — невырожденная матрица размера $n \times n$ над $\mathbb{F}_2$; γ — вектор из $\mathbb{F}_2^n$.

В дальнейшем обозначать аффинную эквивалентность функций будем символом $f_1 \sim_{\text{AGL}} f_2$. Как известно [1, 2], любая квадратичная форма аффинной заменой переменных может быть приведена к одному и только одному каноническому виду:

$$\begin{aligned} q_1^k(x_1, \dots, x_n) &= x_1 x_2 \oplus \dots \oplus x_{2k-1} x_{2k}; \\ q_2^k(x_1, \dots, x_n) &= x_1 x_2 \oplus \dots \oplus x_{2k-1} x_{2k} \oplus 1; \\ q_3^k(x_1, \dots, x_n) &= x_1 x_2 \oplus \dots \oplus x_{2k-1} x_{2k} \oplus x_{2k+1}. \end{aligned}$$

Число k называется *рангом квадратичной формы* и может изменяться в интервале от 1 до $\lfloor n/2 \rfloor$. Канонические формы q_1^k , q_2^k , q_3^k имеют вес $2^{n-t-1} - 2^{n-t-k-1}$, $2^{n-t-1} + 2^{n-t-k-1}$, 2^{n-t-1} соответственно и лежат на разных орбитах.

Обозначим $O_{q_i}(k)$, $i = 1, 2, 3$, мощность орбиты, на которой лежит i -я каноническая форма ранга k . Аффинные функции в этом смысле могут трактоваться как квадратичные формы ранга 0. Тогда всё множество аффинных функций от n переменных разбивается на три орбиты:

$$\begin{aligned} O_{q_1}(0) &= |\{0\}| = 1, \\ O_{q_2}(0) &= |\{1\}| = 1, \\ O_{q_3}(0) &= |\{a_1 x_1 \oplus \dots \oplus a_n x_n \oplus \varepsilon, \quad a_i, \varepsilon \in \mathbb{F}_2, \quad i = 1, \dots, n, \quad (a_1, \dots, a_n) \neq \bar{0}\}| = 2^{n+1} - 2. \end{aligned}$$

Совершенно иначе обстоит дело с описанием весового спектра кода $\text{RM}(r, n)$ при $r \geq 3$. Уже при $r = 3$ его весовой спектр не известен для произвольного n . На данный

момент наиболее исчерпывающий ответ на этот вопрос даёт формула Касами — Токуры, которая позволяет подсчитать количество слов, вес которых лежит в диапазоне $2^{n-r} \leq \text{wt}(f) < 2^{n-r+1}$, $\Omega_f \in \text{RM}(r, n)$. Позже эта формула была обобщена на случай $2^{n-r} \leq \text{wt}(f) \leq 2,5 \cdot 2^{n-r}$.

2. Весовой спектр одного подкода кода Рида — Маллера

Рассмотрим множество $\mathcal{C}_t \subset \mathcal{F}_n$, $t = 1, \dots, n-1$, определяемое следующим образом:

$$\mathcal{C}_t = \left\{ g(x_{n-t+1}, \dots, x_n) \oplus \bigoplus_{1 \leq i < j \leq n-t} a_{ij} x_i x_j \oplus \bigoplus_{k=n-t+1}^n x_k l_k(x_1, \dots, x_{n-t}) \oplus \right. \\ \left. \oplus l(x_1, \dots, x_{n-t}) \oplus \varepsilon, \text{ где } g \in \mathcal{F}_t, a_{ij}, \varepsilon \in \{0, 1\}, \right. \\ \left. l(x_1, \dots, x_{n-t}), l_k(x_1, \dots, x_{n-t}) \text{ — линейные функции} \right\}.$$

Очевидно следующее утверждение.

Утверждение 1. Множество векторов значений Ω_f , $f \in \mathcal{C}_t$, является подкодом кода $\text{RM}(\max\{t, 2\}, n)$ размерности $2^t + \binom{n-t}{2} + (n-t)(t+1)$.

Наиболее интересен этот код при $t \geq 3$, так как при этих значениях параметра получаем подкод кода Рида — Маллера третьего или более высокого порядка. В случае $t = 3$ это подкод кода $\text{RM}(3, n)$, включающий в себя функции третьей степени нелинейности, содержащие лишь один кубический моном. Весовой спектр этого кода рассчитан в [5]. В данной работе предлагается обобщение этого результата для произвольного значения t из указанного интервала.

Имеет место следующая теорема.

Теорема 2. Весовой спектр кода $\mathcal{C}_t$ в случае нечётного $(n-t)$ представлен в табл. 1, где $i = 0, \dots, 2^{t-r}$; $r = 0, \dots, \min\{t, n-t-2k\}$; $k = 0, \dots, [(n-t)/2]$; в случае чётного $(n-t)$ — в табл. 2, где $i = 0, \dots, 2^{t-r}$; $j = 0, \dots, 2^t$; $r = 0, \dots, \min\{t, n-t-2k\}$; $k = 0, \dots, (n-t)/2 - 1$;

$$N(t, n-t-2k, r) = \begin{cases} 0, & \text{если } r > \min\{t, n-t-2k\}, \\ 1, & \text{если } r = 0, \\ (2^{n-t-2k})(2^t - 1), & \text{если } r = 1, \\ N(t-1, n-t-2k, r-1) \times \\ \quad \times (2^{n-t-2k} - 2^{r-1}) + \\ \quad + N(t-1, n-t-2k, r)2^r, & \text{если } 2 \leq r \leq \min\{t, n-t-2k\}; \end{cases}$$

$$M(t, n-t-2k, r) = \begin{cases} 0, & \text{если } r > \min\{t, n-t-2k\} \text{ или } r = 0, \\ 2^t - 1, & \text{если } r = 1, \\ N(t, n-t-2k, r) - \\ \quad - N(t, n-t-2k-1, r)2^r, & \text{если } 2 \leq r \leq \min\{t, n-t-2k\}. \end{cases}$$

Т а б л и ц а 1

Весовой спектр кода $\mathcal{C}_t$ в случае нечётного $(n - t)$

Количество функций	Вес
$O_{q_3}(k)2^{2^t+2kt}\left(2^{t(n-t-2k)} - \sum_{r=1}^{\min\{t, n-t-2k\}} M(t, n-t-2k, r)\right)$	2^{n-1}
$\binom{2^{t-r}}{i} O_{q_3}(k)M(t, n-t-2k, r)2^{2^t-2^{t-r}+2kt}$	$i \text{ wt}(q_1^k) + (2^{t-r} - i) \text{ wt}(q_2^k) +$ $+(2^t - 2^{t-r}) \text{ wt}(q_3^k)$
$\binom{2^{t-r}}{i} O_{q_1}(k)N(t, n-t-2k, r)2^{2^t-2^{t-r}+2kt}$	$i \text{ wt}(q_1^k) + (2^{t-r} - i) \text{ wt}(q_2^k) +$ $+(2^t - 2^{t-r}) \text{ wt}(q_3^k)$
$\binom{2^{t-r}}{i} O_{q_2}(k)N(t, n-t-2k, r)2^{2^t-2^{t-r}+2kt}$	$i \text{ wt}(q_2^k) + (2^{t-r} - i) \text{ wt}(q_1^k) +$ $+(2^t - 2^{t-r}) \text{ wt}(q_3^k)$

Т а б л и ц а 2

Весовой спектр кода $\mathcal{C}_t$ в случае чётного $(n - t)$

Количество функций	Вес
$O_{q_3}(k)2^{2^t+2kt}\left(2^{t(n-t-2k)} - \sum_{r=1}^{\min\{t, n-t-2k\}} M(t, n-t-2k, r)\right)$	2^{n-1}
$\binom{2^{t-r}}{i} O_{q_3}(k)M(t, n-t-2k, r)2^{2^t-2^{t-r}+2kt}$	$i \text{ wt}(q_1^k) + (2^{t-r} - i) \text{ wt}(q_2^k) +$ $+(2^t - 2^{t-r}) \text{ wt}(q_3^k)$
$\binom{2^{t-r}}{i} O_{q_1}(k)N(t, n-t-2k, r)2^{2^t-2^{t-r}+2kt}$	$i \text{ wt}(q_1^k) + (2^{t-r} - i) \text{ wt}(q_2^k) +$ $+(2^t - 2^{t-r}) \text{ wt}(q_3^k)$
$\binom{2^{t-r}}{i} O_{q_2}(k)N(t, n-t-2k, r)2^{2^t-2^{t-r}+2kt}$	$i \text{ wt}(q_2^k) + (2^{t-r} - i) \text{ wt}(q_1^k) +$ $+(2^t - 2^{t-r}) \text{ wt}(q_3^k)$
$O_{q_1}\left(\frac{n-t}{2}\right)\binom{2^t}{j}2^{t(n-t)}$	$j \text{ wt}\left(q_1^{(n-t)/2}\right) + (2^t - j) \text{ wt}\left(q_2^{(n-t)/2}\right)$
$O_{q_2}\left(\frac{n-t}{2}\right)\binom{2^t}{j}2^{t(n-t)}$	$j \text{ wt}\left(q_2^{(n-t)/2}\right) + (2^t - j) \text{ wt}\left(q_1^{(n-t)/2}\right)$

Доказательство. Для фиксированной функции из $\mathcal{C}_t$ возможен лишь один из трёх случаев:

$$\begin{aligned}
& \bigoplus_{1 \leq i < j \leq n-t} a_{ij}x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_1^k(x_1, \dots, x_{n-t}); \\
& \bigoplus_{1 \leq i < j \leq n-t} a_{ij}x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_2^k(x_1, \dots, x_{n-t}); \\
& \bigoplus_{1 \leq i < j \leq n-t} a_{ij}x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_3^k(x_1, \dots, x_{n-t}).
\end{aligned}$$

Пусть $(A, \gamma) \in \text{AGL}$ — преобразование, приводящее квадратичную форму

$$\bigoplus_{1 \leq i < j \leq n-t} a_{ij}x_i x_j \oplus l(x_1, \dots, x_{n-t})$$

к одному из канонических видов. Применим это преобразование к произвольной функции $f \in \mathcal{C}_t$ и будем рассматривать вес функции $f(xA \oplus \gamma) = \hat{f}(x)$. Функция $\hat{f}$ может

быть лишь одного из трёх видов:

$$\begin{aligned} &g(x_{n-t+1}, \dots, x_n) \oplus q_1^k(x_1, \dots, x_{n-t}) \oplus \bigoplus_{i=n-t+1}^n x_i l^{(i)}(x_1, \dots, x_{n-t}) \oplus \varepsilon'; \\ &g(x_{n-t+1}, \dots, x_n) \oplus q_2^k(x_1, \dots, x_{n-t}) \oplus \bigoplus_{i=n-t+1}^n x_i l^{(i)}(x_1, \dots, x_{n-t}) \oplus \varepsilon'; \\ &g(x_{n-t+1}, \dots, x_n) \oplus q_3^k(x_1, \dots, x_{n-t}) \oplus \bigoplus_{i=n-t+1}^n x_i l^{(i)}(x_1, \dots, x_{n-t}) \oplus \varepsilon'. \end{aligned}$$

Вес функции $\widehat{f}$ равен $\text{wt}(\widehat{f}) = \sum_{(i_{n-t+1}, \dots, i_n) \in \mathbb{F}^t} \text{wt}(\widehat{f}_{n-t+1, \dots, n}^{i_{n-t+1}, \dots, i_n})$, где $\widehat{f}_{n-t+1, \dots, n}^{i_{n-t+1}, \dots, i_n}$ — подфункция функции $\widehat{f}$, полученная фиксацией переменных с номерами $n-t+1, \dots, n$ константами $i_{n-t+1}, \dots, i_n$ соответственно.

Рассмотрим $t \times (n-t)$ -матрицу $\mathcal{L}$, состоящую из коэффициентов линейных функций $l^{(i)}(x_1, \dots, x_{n-t})$, $i = n-t+1, \dots, n$:

$$\mathcal{L} = \begin{pmatrix} l_1^{(1)} & \dots & l_{n-t}^{(1)} \\ l_1^{(2)} & \dots & l_{n-t}^{(2)} \\ & \ddots & \\ l_1^{(t)} & \dots & l_{n-t}^{(t)} \end{pmatrix}.$$

Разобьём матрицу $\mathcal{L}$ на две подматрицы

$$\mathcal{L} = (\mathcal{L}'_{t \times 2k} | \mathcal{L}''_{t \times (n-t-2k)}),$$

и пусть $\text{rang}(\mathcal{L}'') = r$, $r = 0, \dots, \min\{t, n-t-2k\}$. Для сокращения записи обозначим число $t \times (n-t-2k)$ -матриц ранга r через $N(t, n-t-2k, r)$:

$$N(t, n-t-2k, r) = \begin{cases} 0, & \text{если } r > \min\{t, n-t-2k\}, \\ 1, & \text{если } r = 0, \\ (2^{n-t-2k} - 1)(2^t - 1), & \text{если } r = 1, \\ N(t-1, n-t-2k, r-1) \times \\ \quad \times (2^{n-t-2k} - 2^{r-1}) + \\ + N(t-1, n-t-2k, r) 2^r, & \text{если } 2 \leq r \leq \min\{t, n-t-2k\}. \end{cases}$$

Пусть

$$\bigoplus_{1 \leq i < j \leq n-t} a_{ij} x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_1^k(x_1, \dots, x_{n-t})$$

и $\text{rang}(\mathcal{L}'') = r$. Тогда система

$$(x_{n-t+1}, \dots, x_n) \mathcal{L}'' = 0 \tag{1}$$

имеет 2^{t-r} решений. Если $(x_{n-t+1}, \dots, x_n) \in \mathbb{F}^t$ является решением системы, то $\text{wt}(\widehat{f}_{n-t+1, \dots, n}^{x_{n-t+1}, \dots, x_n})$ равен $\text{wt}(q_1^k)$, если $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon' = 0$, и равен $\text{wt}(q_2^k)$, если $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon' = 1$. Поскольку $g(x_{n-t+1}, \dots, x_n)$, а следовательно и $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon'$, пробегает всё множество $\mathcal{F}_t$, то при любой фиксации переменных $x_{n-t+1}, \dots, x_n$ значение функции $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon'$ может быть произвольным.

В противном случае (когда $(x_{n-t+1}, \dots, x_n)$ не является решением системы (1)) выполняется равенство $\text{wt}(\widehat{f}_{n-t+1, \dots, n}^{x_{n-t+1}, \dots, x_n}) = \text{wt}(q_3^k)$.

Далее рассмотрим два случая:

- 1) $(n - t)$ нечётно и $0 \leq k \leq [(n - t)/2]$ или $(n - t)$ чётно и $0 \leq k \leq (n - t)/2 - 1$;
- 2) $(n - t)$ чётно и $k = (n - t)/2$.

Из сказанного выше следует, что в первом случае ровно

$$\binom{2^{t-r}}{i} N(t, n - t - 2k, r) O_{q_1}(k) 2^{2^t - 2^{t-r} + 2kt}$$

функций имеют вес

$$i \operatorname{wt}(q_1^k) + (2^{t-r} - i) \operatorname{wt}(q_2^k) + (2^t - 2^{t-r}) \operatorname{wt}(q_3^k),$$

где $r = 0, \dots, \min\{n - t - 2k, t\}$, $i = 0, \dots, 2^{t-r}$.

Для случая

$$\bigoplus_{1 \leq i < j \leq n-t} a_{ij} x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_2^k(x_1, \dots, x_{n-t})$$

рассуждения проводятся аналогичным образом, заменяя q_1^k на q_2^k и наоборот. Получим, что

$$\binom{2^{t-r}}{i} N(t, n - t - 2k, r) O_{q_2}(k) 2^{2^t - 2^{t-r} + 2kt}$$

функций имеют вес

$$i \operatorname{wt}(q_2^k) + (2^{t-r} - i) \operatorname{wt}(q_1^k) + (2^t - 2^{t-r}) \operatorname{wt}(q_3^k),$$

где $r = 0, \dots, \min\{n - t - 2k, t\}$; $i = 0, \dots, 2^{t-r}$.

Теперь рассмотрим случай, когда $(n - t)$ чётно и $k = (n - t)/2$ при условии, что

$$\bigoplus_{1 \leq i < j \leq n-t} a_{ij} x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_1^k(x_1, \dots, x_{n-t}).$$

В этом случае $\mathcal{L} = \mathcal{L}'$, и при любой фиксации $x_{n-t+1}, \dots, x_n$ прибавление к q_1^k линейной комбинации $\bigoplus_{i=n-t+1}^n x_i l^{(i)}(x_1, \dots, x_t)$ либо оставляет её на орбите, содержащей q_1^k , либо переводит на орбиту, содержащую q_2^k . В конечном итоге вес $\widehat{f}_{n-t+1, \dots, n}^{x_{n-t+1}, \dots, x_n}$ будет определяться лишь значением функции $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon'$, которое может быть произвольным.

Зафиксируем в $\mathbb{F}^t$ j векторов, на которых функция $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon'$ принимает такие значения, что выполняется условие $\operatorname{wt}(\widehat{f}_{n-t+1, \dots, n}^{x_{n-t+1}, \dots, x_n}) = \operatorname{wt}(q_1^k)$, а на оставшихся $(2^t - j)$ векторах $\operatorname{wt}(\widehat{f}_{n-t+1, \dots, n}^{x_{n-t+1}, \dots, x_n}) = \operatorname{wt}(q_2^k)$. Тогда вес функции $\operatorname{wt}(\widehat{f})$ равен

$$j \operatorname{wt}\left(q_1^{(n-t)/2}\right) + (2^t - j) \operatorname{wt}\left(q_2^{(n-t)/2}\right).$$

Поскольку при указанных условиях $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon'$ однозначно определяется, то функций указанного веса будет ровно

$$O_{q_1}\left(\frac{n-t}{2}\right) \binom{2^t}{j} 2^{t(n-t)}, \quad j = 0, \dots, 2^t.$$

Случай, когда $(n - t)$ чётно и $k = (n - t)/2$ при условии, что

$$\bigoplus_{1 \leq i < j \leq n-t} a_{ij} x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_2^k(x_1, \dots, x_{n-t}),$$

рассматривается аналогично предыдущему.

Опишем теперь последний из возможных случаев, когда

$$\bigoplus_{1 \leq i < j \leq n-t} a_{ij} x_i x_j \oplus l(x_1, \dots, x_{n-t})_{\text{AGL}} q_3^k(x_1, \dots, x_{n-t}).$$

Рассмотрим систему

$$(x_{n-t+1}, \dots, x_n) \mathcal{L}'' = (1, 0, \dots, 0). \quad (2)$$

Если вектор $(x_{n-t+1}, \dots, x_n) \in \mathbb{F}^t$ является её решением, то $\text{wt}(q_3^k(x_1, \dots, x_{n-t}) \oplus \bigoplus_{i=n-t+1}^n x_i l^{(i)}(x_1, \dots, x_{n-t}))$ равен $\text{wt}(q_1^k)$, если $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon' = 0$, и $\text{wt}(q_2^k)$ в противном случае.

Для всех остальных векторов α , для которых система

$$(x_{n-t+1}, \dots, x_n) \mathcal{L}'' = \alpha$$

совместна и вектор $(x_{n-t+1}, \dots, x_n)$ лежит в множестве её решений, выполняется равенство

$$\text{wt} \left(q_3^k(x_1, \dots, x_{n-t}) \oplus \bigoplus_{i=1}^{n-t} x_i l^{(i)}(x_1, \dots, x_{n-t}) \right) = 2^{n-t-1}.$$

Число $t \times (n-t-2k)$ -матриц ранга r , для которых система (2) совместна, обозначим $M(t, n-t-2k, r)$. Поскольку система совместна тогда и только тогда, когда $\text{rang}(\mathcal{L}'')^T = \text{rang}((\mathcal{L}'')^T | \beta^T)$, где $\beta = (1, 0, \dots, 0)$, то имеет место рекуррентная формула

$$M(t, n-t-2k, r) = \begin{cases} 0, & \text{если } r > \min\{t, n-t-2k\} \text{ или } r = 0, \\ 2^t - 1, & \text{если } r = 1, \\ N(t, n-t-2k, r) - \\ - N(t, n-t-2k-1, r) 2^r, & \text{если } 2 \leq r \leq \min\{t, n-t-2k\}. \end{cases}$$

Из этого следует, что $t \times (n-t-2k)$ -матриц ранга r , для которых система (2) несовместна, ровно

$$2^{t(n-t-2k)} - \sum_{r=1}^{\min\{t, n-t-2k\}} M(t, n-t-2k, r).$$

Поэтому в исследуемом коде содержится

$$O_{q_3}(k) \left(2^{t(n-t-2k)} - \sum_{r=1}^{\min\{t, n-t-2k\}} M(t, n-t-2k, r) \right) 2^{2^t+2kt}$$

функций веса

$$\text{wt}(q_3^k) 2^t = 2^t 2^{n-t-1} = 2^{n-1}$$

и

$$\binom{2^{t-r}}{i} O_{q_3}(k) M(t, n-t-2k, r) 2^{2^t-2^{t-r}+2kt}$$

функций веса

$$i \text{wt}(q_1^k) + (2^{t-r} - i) \text{wt}(q_2^k) + 2^{2^t-2^{t-r}} \text{wt}(q_3^k),$$

где $i = 0, \dots, 2^{t-r}$, $r = 1, \dots, \min\{t, n-t-2k\}$, $k = 1, \dots, [(n-t)/2]$. ■

ЛИТЕРАТУРА

1. *Логачев О. А., Сальников А. А., Яценко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 469 с.
2. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
3. *Черемушкин А. В.* Методы аффинной и линейной классификации булевых функций // Труды по дискретной математике. 2001. Т. 4. С. 273–314.
4. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986. 576 с.
5. *Покровский А. В., Никифоров М. С.* Весовой спектр одного подкода кода $RM(3, n)$ // XIV Междунар. конф. «Проблемы теоретической кибернетики». Пенза: ПГУ, 2006. Ч. 2. С. 68–70.

О РАНГАХ ПОДМНОЖЕСТВ ПРОСТРАНСТВА ДВОИЧНЫХ ВЕКТОРОВ, ДОПУСКАЮЩИХ ВСТРАИВАНИЕ СИСТЕМЫ ШТЕЙНЕРА $S(2, 4, v)^1$

Ю. В. Таранников

Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

E-mail: taran@butovo.com

Получена оценка ранга подмножества X пространства $\mathbb{F}_2^n$ через радиус покрытия кода, лежащего в подпространстве линейных зависимостей векторов из X . Получена верхняя оценка радиуса покрытия кода, порождённого матрицей инцидентности системы Штейнера $S(2, 4, v)$. Получены верхняя точная и асимптотическая оценки ранга подмножества X пространства $\mathbb{F}_2^n$, допускающего встраивание системы Штейнера $S(2, 4, v)$.

Ключевые слова: ранг, аффинный ранг, оценки, линейное подпространство, линейный код, радиус покрытия, система Штейнера, булевы функции, носитель спектра.

Пусть $X \subseteq \mathbb{F}_2^n$. Рангом множества X называется размерность $\dim\langle X \rangle$ его линейной оболочки $\langle X \rangle$. Аффинным рангом множества X называется наименьшая размерность класса смежности линейного подпространства в $\mathbb{F}_2^n$, содержащего X . Пусть μ_X — взаимно-однозначное отображение векторов из X в компоненты пространства $\mathbb{F}_2^{|X|}$. Отображение μ_X индуцирует взаимно-однозначное сопоставление каждому подмножеству $A \subseteq X$ характеристического вектора $a = (a_1, \dots, a_{|X|}) = \xi_X(A)$ в $\mathbb{F}_2^{|X|}$, такого, что $a_i = 1$, если $\mu_X^{-1}(i) \in A$, и $a_i = 0$, если $\mu_X^{-1}(i) \notin A$, $i = 1, \dots, |X|$. Пусть $\mathcal{B}_X = \{B^1, \dots, B^s\}$ — совокупность всех таких подмножеств $B^i = \{x^{i_1}, \dots, x^{i_{k_i}}\}$ множества X , что $\sum_{j=1}^{k_i} x^{ij} = (0, \dots, 0)$. Тогда множество векторов $\xi_X(\mathcal{B}_X) = \{\xi_X(B^1), \dots, \xi_X(B^s)\}$, очевидно, является линейным подпространством в $\mathbb{F}_2^{|X|}$.

Лемма 1. Имеет место равенство $\dim\langle X \rangle = |X| - \dim \xi_X(\mathcal{B}_X)$.

Доказательство леммы 1 практически очевидно, потому что если $\dim \xi_X(\mathcal{B}_X) = r$, то в X найдется подмножество X' из $|X| - r$ линейно независимых векторов, а все векторы из $X \setminus X'$ могут быть выражены как линейные комбинации векторов из X' .

Из леммы 1 получаем

Следствие 1. Пусть $C \subseteq \xi_X(\mathcal{B}_X)$. Тогда

$$\dim\langle X \rangle \leq |X| - \dim\langle C \rangle.$$

Произвольное множество C , $C \subseteq \mathbb{F}_2^m$, называется кодом. Если C — линейное пространство в $\mathbb{F}_2^m$, то C называется линейным кодом. Расстоянием (Хэмминга) $d(a, b)$ между векторами a и b из $\mathbb{F}_2^m$ называется число компонент, в которых a и b различаются. Радиусом покрытия $R = R(C)$ кода C , $C \subseteq \mathbb{F}_2^m$, называется величина

¹Работа поддержана грантом РФФИ, проект №13-01-00183-а.

$R = R(C) = \max_{a \in \mathbb{F}_2^m} \min_{b \in C} d(a, b)$. Радиусу покрытия и связанным с ним вопросам теории кодирования посвящена монография [1]. Из определения радиуса покрытия сразу следует, что мощность кода C , $C \subseteq \mathbb{F}_2^m$, оценивается через его радиус покрытия $R(C)$ как

$$|C| \geq 2^m / \sum_{i=0}^{R(C)} \binom{m}{i}.$$

Отсюда, если C — линейный код, то

$$\dim C \geq m - \log_2 \sum_{i=0}^{R(C)} \binom{m}{i}. \quad (1)$$

Из (1) и следствия 1 получаем следующую теорему.

Теорема 1. Пусть $C \subseteq \xi_X(\mathcal{B}_X)$. Тогда

$$\dim \langle X \rangle \leq \log_2 \sum_{i=0}^{R(C)} \binom{|X|}{i}.$$

Системой Штейнера $S(t, k, v)$ называется пара $(V, \mathcal{B})$, где V — множество мощности v , а $\mathcal{B}$ — семейство k -элементных подмножеств V , называемых *блоками*, таких, что любое t -элементное подмножество V целиком принадлежит ровно одному блоку.

Будем говорить, что пара $(V, \mathcal{B})$, являющаяся системой Штейнера $S(t, k, v)$, *встраивается* во множество X , $X \subseteq \mathbb{F}_2^n$, если существует биекция $\varphi : V \rightarrow X$, такая, что для любого блока B , $B \in \mathcal{B}$, выполнено соотношение $\sum_{x \in B} \varphi(x) = (0, \dots, 0)$. Саму биекцию φ будем при этом называть *встраиванием*.

Заметим, что если такое встраивание существует, то семейство блоков $\mathcal{B} = \{B^1, \dots, B^b\}$ перейдёт в семейство $\varphi(\mathcal{B}) = \{\varphi(B^1), \dots, \varphi(B^b)\}$ подмножеств множества $\mathcal{B}_X$, которое, в свою очередь, соответствует множеству двоичных векторов $\xi_X(\varphi(\mathcal{B}))$, лежащему в $\xi_X(\mathcal{B}_X)$.

Следующая теорема справедлива, даже если биекция φ не обязательно является встраиванием. Фактически теорема устанавливает верхнюю оценку радиуса покрытия кода, порождённого матрицей инцидентности системы Штейнера $S(2, 4, v)$.

Теорема 2. Пусть $X \subseteq \mathbb{F}_2^n$, $|X| = v$; $(V, \mathcal{B})$ — система Штейнера $S(2, 4, v)$; φ — взаимно-однозначное отображение $V \rightarrow X$. Тогда для радиуса покрытия R линейного кода $C = \langle \xi_X(\varphi(\mathcal{B})) \rangle$ в $\mathbb{F}_2^v$ справедливо неравенство $R(C) \leq \sqrt{v}$.

Доказательство. Пусть a — произвольный вектор из $\mathbb{F}_2^v$. Надо доказать, что найдётся вектор u из $\langle \xi_X(\varphi(\mathcal{B})) \rangle$, для которого $d(a, u) \leq \sqrt{v}$. Для этого покажем, что если $|a| > \sqrt{v}$, где $|a|$ — вес вектора a , т. е. число ненулевых компонент в a , то найдётся вектор u^1 из $\langle \xi_X(\varphi(\mathcal{B})) \rangle$, такой, что $|a + u^1| < |a|$. Если $|a + u^1| > \sqrt{v}$, то применим эти же рассуждения к вектору $a + u^1$ и т. д. В силу конечности веса вектора a получим множество наборов $u^1, \dots, u^s$ из $\langle \xi_X(\varphi(\mathcal{B})) \rangle$, что $|a + u^1 + \dots + u^s| \leq \sqrt{v}$, т. е. $d(a, u^1 + \dots + u^s) \leq \sqrt{v}$, где $(u^1 + \dots + u^s) \in \langle \xi_X(\varphi(\mathcal{B})) \rangle$, что и требуется.

Итак, предположим, что $|a| > \sqrt{v}$. Напомним, что все векторы из $\xi_X(\varphi(\mathcal{B}))$ имеют вес 4. Выделим две достаточные для доказательства ситуации:

а) Если найдётся вектор u из $\xi_X(\varphi(\mathcal{B}))$, имеющий с набором a не менее трёх общих единиц, то, очевидно, $|a| < |a + u|$.

б) Если найдутся векторы u^1 и u^2 из $\xi_X(\varphi(\mathcal{B}))$, имеющие одну общую единицу между собой (но не более в силу определения системы Штейнера), причём в компоненте,

где в наборе a нуль, и каждый из них не менее двух общих единиц с набором a , то, очевидно, $|a| < |a + (u^1 + u^2)|$.

Обозначим за I множество всех компонент пространства $\mathbb{F}_2^v$, в которых вектор a имеет единицы. Для любых $i, j \in I$, $i \neq j$, в силу того, что $(V, \mathcal{B})$ — система Штейнера $S(2, 4, v)$, существует вектор $u^{(i,j)}$ из $\xi_X(\varphi(\mathcal{B}))$, имеющий единицы в компонентах i и j . Если $u^{(i,j)}$ имеет ещё хотя бы одну единицу в компоненте из I , то имеет место ситуация «а». Если для разных пар (i, j) и (i', j') векторы $u^{(i,j)}$ и $u^{(i',j')}$ имеют общую единицу в компоненте не из I , то имеет место ситуация «б». Поэтому все векторы $u^{(i,j)}$, $i, j \in I$, $i \neq j$, разные и никакие два из них не имеют общих единиц в компонентах не из I . Следовательно, число компонент не из I , равное $v - |a|$, оценивается как $v - |a| \geq 2|a|(|a| - 1)/2$. Отсюда $|a| \leq \sqrt{v}$, что доказывает теорему. ■

Объединяя утверждения теорем 1 и 2, получаем следующую теорему.

Теорема 3. Пусть $X \subseteq \mathbb{F}_2^n$ и существует встраивание системы Штейнера $S(2, 4, |X|)$ в X . Тогда

$$\dim \langle X \rangle \leq \min \left\{ n, \log_2 \sum_{i=0}^{\lfloor \sqrt{|X|} \rfloor} \binom{|X|}{i} \right\}.$$

Из теоремы 3 вытекает асимптотическая оценка.

Следствие 2. Пусть существует последовательность подмножеств $X \subseteq \mathbb{F}_2^n$, $n \rightarrow \infty$, $|X| \rightarrow \infty$, для каждого из которых существует встраивание системы Штейнера $S(2, 4, |X|)$ в X . Тогда

$$\dim \langle X \rangle \leq \frac{1}{2} \sqrt{|X|} \log_2 |X| (1 + o(1)).$$

Для доказательства следствия 2 достаточно воспользоваться неравенством $\sum_{k=0}^t \binom{n}{k} \leq 2^{nH(t/n)}$ при $1 \leq t \leq n/2$, где $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ — двоичная энтропия (см., например, [2, с. 37]).

Параметры линейных кодов, порождённых системами Штейнера $S(t, k, v)$, достаточно активно изучаются при $k = t + 1$ [3, 4]. Обсудим, почему нами выбраны именно системы Штейнера $S(2, 4, v)$. Это связано с исследованиями ранга и аффинного ранга носителей спектра булевых функций.

Булева функция от n переменных — это отображение из $\mathbb{F}_2^n$ в $\mathbb{F}_2$. *Преобразованием Уолша* булевой функции f называется целочисленная функция над $\mathbb{F}_2^n$, определяемая как $W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \langle u, x \rangle}$. Для каждого $u \in \mathbb{F}_2^n$ значение $W_f(u)$ называется *коэффициентом Уолша*. Коэффициенты Уолша называются *спектральными коэффициентами*, а совокупность всех 2^n коэффициентов Уолша — *спектром* булевой функции. Множество S_f всех наборов u , таких, что $W_f(u) \neq 0$, называется *носителем спектра* функции f .

Для коэффициентов Уолша булевой функции f над $\mathbb{F}_2^n$ справедлива теорема Титсворта (см., например, [5, с. 135]): для любого ненулевого $s \in \mathbb{F}_2^n$ выполнено равенство $\sum_{x \in \mathbb{F}_2^n} W_f(x) W_f(x + s) = 0$. Отсюда следует, что если носителю спектра S_f принадлежат наборы x и $x + s$, то в S_f должна лежать ещё хотя бы одна пара наборов, отличающаяся на s , скажем, y и $y + s$. Но тогда $x + (x + s) + y + (y + s) = (0, \dots, 0)$,

т. е. $\{x, x + s, y, y + s\}$ — четвёрка наборов, удовлетворяющая условию на встраивание. Конечно, система Штейнера $S(2, 4, v)$ — это достаточно специфический комбинаторный объект, существующий не при всех v . Известно [6], что система Штейнера $S(2, 4, v)$ существует тогда и только тогда, когда $v \equiv 1, 4 \pmod{12}$. Однако этому условию удовлетворяет мощность носителя спектра платовидной функции. Булева функция называется *платовидной*, если её коэффициенты Уолша принимают ровно три возможных значения: 0 и $\pm 2^h$ для некоторого h . Платовидные функции представляют большой интерес для изучения бент-функций (например, потому, что при разложении бент-функций по переменной возникают две платовидные функции), а также потому, что многие криптографически важные функции являются платовидными (например, m -устойчивые функции с максимально возможной для них нелинейностью $2^{n-1} - 2^{m+1}$). Возможные значения аффинного ранга платовидных функций исследовались в [7]. Из равенства Парсеваля $\sum_{u \in \mathbb{F}_2^n} W_f^2(u) = 4^n$ сразу следует, что мощность носителя спектра равна $|S_f| = 4^{n-h} \equiv 4 \pmod{12}$. Кроме того, из теоремы Титсворта видно, что для любого ненулевого $s \in \mathbb{F}_2^n$ носитель спектра платовидной функции содержит чётное число пар наборов, отличающихся на s , что даёт надежду сгруппировать наборы в совокупность четвёрок, являющихся встраиванием системы Штейнера $S(2, 4, v)$. В [8] построены бесконечные последовательности платовидных функций с растущей мощностью носителей спектров, как допускающих, так и не допускающих встраивание системы Штейнера $S(2, 4, v)$.

ЛИТЕРАТУРА

1. Cohen G., Honkala I., Litsyn S., and Lobstein A. Covering codes. Elsevier Science, 1997.
2. Чашкин А. В. Дискретная математика. М.: Академия, 2012.
3. Зиновьев В. А., Зиновьев Д. В. Системы Штейнера $S(v, k, k - 1)$: компоненты и ранг // Проблемы передачи информации. 2011. Т. 47. № 2. С. 52–71.
4. Ковалевская Д. И., Соловьева Ф. И. Системы четверок Штейнера малых рангов и расширенные совершенные двоичные коды // Дискретный анализ и исследование операций. 2013. Т. 20. Вып. 4. С. 46–64.
5. Таранников Ю. В. Комбинаторные свойства дискретных структур и приложения к криптологии. М.: МЦНМО, 2011.
6. Reid C. and Rosa A. Steiner systems $S(2, 4, v)$ — a survey // Electron. J. Combinator. 2010. DS18.
7. Таранников Ю. В. О значениях аффинного ранга носителя спектра платовидной функции // Дискретная математика. 2006. Т. 18. Вып. 3. С. 120–137.
8. Урбанович Т. А. О дизайнах специального вида на подмножествах булева куба: дипломная работа / механико-математический факультет МГУ им. М. В. Ломоносова. М., 2012.

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

DOI 10.17223/20710410/23/9

УДК 519.6

УТОЧНЁННЫЕ ОЦЕНКИ ЭКСПОНЕНТОВ ПЕРЕМЕШИВАЮЩИХ
ГРАФОВ БИЕКТИВНЫХ РЕГИСТРОВ СДВИГА
НАД МНОЖЕСТВОМ ДВОИЧНЫХ ВЕКТОРОВ

А. М. Дорохова*, В. М. Фомичев**

*Национальный исследовательский ядерный университет (МИФИ), г. Москва, Россия,

**Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия

E-mail: alisa.koreneva@gmail.com, fomichev@nm.ru

Для перемешивающего графа Γ подстановочного преобразования регистра сдвига длины n над множеством r -мерных двоичных векторов получены новые оценки длин простых путей и циклов, доказаны достаточные условия примитивности графа Γ , понижена полученная ранее верхняя оценка значения экспонента.

Ключевые слова: перемешивающий граф преобразования, диаметр графа, экспонент графа.

Введение

Раундовая подстановка алгоритмов шифрования, использующих конструкцию Фейстеля, построена на основе подстановки регистра сдвига длины 2 над множеством V_r двоичных r -мерных векторов. В [1] в порядке обобщения рассмотрена подстановка φ регистра сдвига длины $n \geq 2$ над V_r , получены в различных условиях верхние оценки диаметра и экспонента перемешивающего графа $\Gamma(\varphi)$ подстановки φ . В настоящей работе получены новые достаточные условия примитивности перемешивающего графа $\Gamma(\varphi)$, улучшена оценка [1, теорема 3] экспонента графа $\Gamma(\varphi)$.

1. Определяющие свойства перемешивающего графа

Используем обозначения работы [1]. Обозначим φ подстановку множества V_{rn} , реализующую регистром сдвига длины $n > 1$ над пространством V_r двоичных r -мерных векторов, где $r > 1$ — длина в битах двоичных слов, записанных в ячейках регистра сдвига. Состояние регистра в текущий момент времени представим двоичной матрицей размера $r \times n$, считая при этом, что $(k+1)$ -й столбец матрицы, обозначаемый $y_{k+1} = (x_{1+rk}, \dots, x_{r+rk})^T$, записан в k -й ячейке регистра сдвига, $k = 0, 1, \dots, n-1$.

Пусть подстановка φ определена равенством

$$\varphi(y_1, \dots, y_n) = (y_2, \dots, y_n, y_1 \oplus \psi(y_2, \dots, y_n)), \quad (1)$$

где $\oplus$ — операция XOR в пространстве V_r и функция $\psi : V_{r(n-1)} \rightarrow V_r$ отлична от константы. Условие $\psi \neq \text{const}$ означает, что подстановка φ не есть циклический сдвиг столбцов двоичной матрицы размера $r \times n$.

Подстановка φ задается системой rn булевых координатных функций

$$\{\varphi_1(x_1, \dots, x_{rn}), \dots, \varphi_{rn}(x_1, \dots, x_{rn})\},$$

где функция $\varphi_{v+rk}(x_1, \dots, x_{rn})$ вычисляет v -й бит x_{v+rk} вектора y_{k+1} , $v = 1, \dots, r$, $k = 0, 1, \dots, n-1$.

Обозначим $S(\varphi_j)$ множество номеров существенных булевых переменных функции $\varphi_j(x_1, \dots, x_{rn})$, $j = 1, \dots, rn$. Отметим свойства множеств $S(\varphi_j)$, вытекающие из (1):

- а) $S(\varphi_{v+rk}(x_1, \dots, x_{rn})) = \{v + r(k+1)\}$, $k = 0, 1, \dots, n-2$, $v = 1, \dots, r$;
- б) $v \in S(\varphi_{u+r(n-1)}(x_1, \dots, x_{rn}))$, где $u, v \in \{1, \dots, r\}$, если и только если $u = v$;
- в) $(S(\varphi_{1+r(n-1)}(x_1, \dots, x_{rn})) \cup \dots \cup S(\varphi_{r+r(n-1)}(x_1, \dots, x_{rn}))) \setminus \{1, \dots, r\} \neq \emptyset$.

Множество $S(\varphi_{u+r(n-1)}(x_1, \dots, x_{rn}))$ зададим таблицей T_u , состоящей из r строк, где v -я строка состоит из номеров существенных переменных функции $\varphi_{u+r(n-1)}(x_1, \dots, x_{rn})$, взятых из множества $\{x_v, x_{v+r}, \dots, x_{v+r(n-1)}\}$; наибольшее из чисел v -й строки таблицы T_u обозначим $m(v, u)$, $v, u = 1, \dots, r$.

Перемешивающий граф $\Gamma(\varphi)$ подстановки φ есть rn -вершинный орграф, в котором есть дуга (i, j) тогда и только тогда, когда $i \in S(\varphi_j)$, $i, j \in \{1, \dots, rn\}$. При рассмотрении диаметра графа расстояние от i до j положим равным длине кратчайшего из циклов, проходящих через вершину i .

Обозначим ϑ функцию отождествления вершин графа $\Gamma(\varphi)$: для любого $v = 1, \dots, r$ положим $\vartheta(v + rk) = v$, $k = 0, 1, \dots, n-1$. Функция ϑ индуцирует функцию Θ , отображающую rn -вершинный орграф $\Gamma(\varphi)$ в r -вершинный орграф $\Gamma(\psi)$, где пара (v, u) образует дугу графа $\Gamma(\psi)$ тогда и только тогда, когда функция $\varphi_{u+r(n-1)}$ зависит существенно хотя бы от одной из переменных множества $\{x_v, x_{v+r}, \dots, x_{v+r(n-1)}\}$, $v, u \in \{1, \dots, r\}$ (записывается $\Theta(\Gamma(\varphi)) = \Gamma(\psi)$).

Отметим свойства орграфов $\Gamma(\varphi)$ и $\Gamma(\psi)$, некоторые из них приведены в [1].

1) В силу свойств а и б множеств $S(\varphi_j)$ орграф $\Gamma(\varphi)$ содержит r независимых циклов $C_1, \dots, C_r$ длины n , где $C_v = (v + r(n-1), v + r(n-2), \dots, v + r, v)$, $v = 1, \dots, r$.

2) Вершина j достижима из вершины i в орграфе $\Gamma(\psi)$, если и только если в орграфе $\Gamma(\varphi)$ любая вершина, принадлежащая циклу C_j , достижима из любой вершины, принадлежащей циклу C_i при $i \neq j$, где $i, j \in \{1, \dots, r\}$.

3) Орграф $\Gamma(\varphi)$ сильносвязный, если и только если орграф $\Gamma(\psi)$ сильносвязный.

4) Простой путь из вершины $v + ri$ в вершину $v + rj$ в цикле C_v (обозначим его $[i, j]_v$) имеет длину $L(i, j)$, где $L(i, j) = i - j$, если $i \geq j$, и $L(i, j) = n - j + i$, если $i < j$.

На рис. 1 изображена часть перемешивающего графа $\Gamma(\varphi)$ подстановки φ , содержащая циклы C_v и C_u , которая при отождествлении вершин преобразуется в дугу (v, u) орграфа $\Gamma(\psi)$. Здесь координатная функция $\varphi_{u+r(n-1)}$ подстановки φ зависит существенно от некоторых переменных множества $\{x_v, x_{v+r}, \dots, x_{v+r(n-1)}\}$.

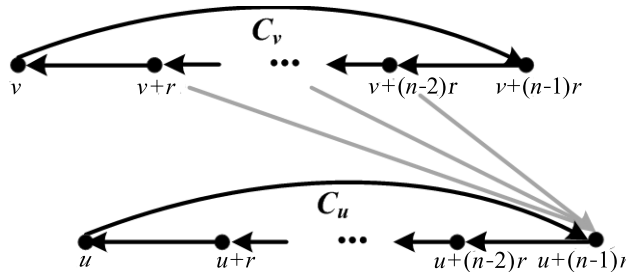


Рис. 1. Часть орграфа $\Gamma(\varphi)$

2. Простые пути и циклы в перемешивающем графе

Функция Θ отображает путь $z = (i_0, \dots, i_t)$ длины t в графе $\Gamma(\varphi)$ в путь $\Theta(z)$ длины $\tau \leq t$ в графе $\Gamma(\psi)$, который получается с помощью замены числом i в последовательности $(\vartheta(i_0), \dots, \vartheta(i_t))$ каждой серии $i, \dots, i$ одинаковых чисел.

Функция Θ определяет отношение эквивалентности $\cong$ на множестве путей (циклов) графа $\Gamma(\varphi)$: если z и z' — пути в графе $\Gamma(\varphi)$, то $z \cong z'$, если и только если $\Theta(z) = \Theta(z')$. Класс эквивалентных путей (циклов) z в графе $\Gamma(\varphi)$, которым при отождествлении вершин соответствует путь (цикл) w в графе $\Gamma(\psi)$, то есть $\Theta(z) = w$, обозначим $[w]$.

Для последовательности из $m > 1$ путей определена операция конкатенации (обозначим символом $\cdot$), если конечная вершина предыдущего пути совпадает с начальной вершиной следующего пути; записывается $z = z_0 \cdot z_1 \cdot \dots \cdot z_m$.

Теорема 1.

а) Если путь z в графе $\Gamma(\varphi)$, начинающийся с вершины $v_0 + r(n-1)$ (цикл z , проходящий через вершину $v_0 + r(n-1)$), простой, где $v_0 \in \{1, \dots, r\}$, то и путь (цикл) $\Theta(z)$ в графе $\Gamma(\psi)$ простой.

б) Для любого простого пути w длины $\tau > 0$ (цикла w длины $\tau > 1$) в графе $\Gamma(\psi)$ класс $[w]$ содержит непустое множество простых путей (простых циклов) графа $\Gamma(\varphi)$.

Доказательство.

а) Простой путь (цикл) z не содержит одинаковых вершин, в частности, не содержит более одного раза вершину $v_0 + (n-1)r$. Если путь (цикл) z целиком состоит из вершин цикла C_{v_0} , то $\Theta(z)$ есть путь (цикл длины 1), состоящий из единственной вершины v_0 , то есть $\Theta(z)$ простой.

В противном случае путь (цикл) z представляется с помощью конкатенации путей, составленной из вершин различных циклов $C_{v_0}, \dots, C_{v_\tau}$, где $\tau \geq 1$, при этом путь z и цикл z имеют соответствующий вид:

- $z = z_0 \cdot \delta_0 \cdot z_1 \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-1} \cdot z'_\tau$ — путь,
- $z = z_0 \cdot \delta_0 \cdot z_1 \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-1} \cdot z_\tau \cdot \delta_\tau$ — цикл,

где z_j — путь в цикле C_{v_j} с начальной вершиной $v_j + r(n-1)$ и с конечной вершиной $v_j + rk_j$, взятой из строки с номером v_j таблицы $T_{v_{j+1}}$; $v_{\tau+1} = v_0$ (длина пути z_j не более n , иначе путь z не простой); z'_τ — путь в цикле C_{v_τ} длины менее n с начальной вершиной $v_\tau + r(n-1)$; $\delta_j = (v_j + rk_j, v_{j+1} + r(n-1))$ — дуги графа $\Gamma(\varphi)$, $j = 0, \dots, \tau$.

Осталось заметить, что $\Theta(z) = (v_0, v_1, \dots, v_\tau)$ и числа $v_0, v_1, \dots, v_\tau$ попарно различные. Действительно, если $v_i = v_j$, где $i, j \in \{0, 1, \dots, \tau\}$, $i \neq j$, то совпадают начальные вершины путей z_i и z_j (z_i и z'_τ), это противоречит тому, что путь (цикл) z простой.

б) Дадим конструктивное описание всех эквивалентных простых путей (циклов) в графе $\Gamma(\varphi)$, которым в графе $\Gamma(\psi)$ соответствует простой путь (цикл) $\Theta(z)$, а именно: если $w = (v_0, v_1, \dots, v_\tau)$ — простой путь (цикл) в графе $\Gamma(\psi)$, то простой путь (цикл) z в графе $\Gamma(\varphi)$, для которого $\Theta(z) = w$, является конкатенацией путей

$$z = z_0 \cdot \delta_0 \cdot z_1 \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-1} \cdot z'_\tau \quad (z = z_0 \cdot \delta_0 \cdot z_1 \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-1} \cdot z_\tau \cdot \delta_\tau).$$

Перебирая все возможные комбинации вершин в строках с номерами v_j таблиц $T_{v_{j+1}}$, $j = 0, \dots, \tau$, получаем требуемое множество эквивалентных путей из класса $[w]$. ■

Обозначим: $L_\psi(w)$ — длина пути w в графе $\Gamma(\psi)$; $L_\varphi(z)$ — длина пути z в графе $\Gamma(\varphi)$.

Теорема 2.

а) Если в графе $\Gamma(\psi)$ имеется простой путь $w = (v_0, v_1, \dots, v_\tau)$ длины $\tau > 0$, то при любых $\lambda, \mu \in \{0, \dots, n-1\}$ в графе $\Gamma(\varphi)$ имеется принадлежащий классу $[w]$ простой

путь $z(w, \lambda, \mu)$ из вершины $v_0 + r\lambda$ в вершину $v_\tau + r\mu$, длина которого

$$L_\varphi(z(w, \lambda, \mu)) = n\tau + L(\lambda, m(v_0, v_1)) - m(v_1, v_2) - \dots - m(v_{\tau-1}, v_\tau) - \mu.$$

б) Если в графе $\Gamma(\psi)$ имеется простой цикл $w = (v_0, v_1, \dots, v_{\tau-1})$ длины $\tau > 1$, то в $\Gamma(\varphi)$ имеется принадлежащий классу $[w]$ простой цикл $z(w)$, длина которого

$$L_\varphi(z(w)) = n\tau + L(\lambda, m(v_0, v_1)) - m(v_1, v_2) - \dots - m(v_{\tau-1}, v_\tau).$$

Доказательство.

а) В соответствии с теоремой 1б путь $z(w, \lambda, \mu) \in [w]$ имеет вид (номера существенных переменных в строках таблиц T_u взяты наибольшие)

$$z(w, \lambda, \mu) = [\lambda, m(v_0, v_1)]_{v_0} \cdot \delta_0 \cdot [n-1, m(v_1, v_2)]_{v_1} \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-1} \cdot [n-1, \mu]_{v_\tau}.$$

Длины путей $[\lambda, m(v_0, v_1)]_{v_0}$, $[n-1, m(v_s, v_{s+1})]_{v_s}$ и $[n-1, \mu]_{v_\tau}$ в соответствии со свойством 4 равны соответственно $L(\lambda, m(v_0, v_1))$, $n-1-m(v_s, v_{s+1})$ и $n-1-\mu$, $s = 1, \dots, \tau-1$. В пути $z(w, \lambda, \mu)$ имеются также дуги $\delta_0, \dots, \delta_{\tau-1}$. Следовательно,

$$L_\varphi(z(w, \lambda, \mu)) = L(\lambda, m(v_0, v_1)) + (\tau-1)(n-1) - m(v_1, v_2) - \dots - m(v_{\tau-1}, v_\tau) + (n-1) - \mu + \tau = n\tau + L(\lambda, m(v_0, v_1)) - m(v_1, v_2) - \dots - m(v_{\tau-1}, v_\tau) - \mu.$$

б) В соответствии с теоремой 1б проходящий через вершину $v_0 + r(n-1)$ цикл $z(w) \in [w]$ имеет вид

$$z(w) = [n-1, m(v_0, v_1)]_{v_0} \cdot \delta_0 \cdot [n-1, m(v_1, v_2)]_{v_1} \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-2} \cdot [n-1, m(v_{\tau-1}, v_0)]_{v_{\tau-1}} \cdot \delta_{\tau-1}.$$

В соответствии со свойством 4 длины путей $[n-1, m(v_s, v_{s+1})]$ равны $n-1-m(v_s, v_{s+1})$, $s = 0, \dots, \tau-1$, $v_\tau = v_0$. В цикле $z(w)$ имеются также дуги $\delta_0, \dots, \delta_{\tau-1}$. Следовательно,

$$\begin{aligned} L_\varphi(z(w)) &= \tau(n-1) - m(v_0, v_1) - \dots - m(v_{\tau-2}, v_{\tau-1}) - m(v_{\tau-1}, v_0) + \tau = \\ &= n\tau - m(v_0, v_1) - \dots - m(v_{\tau-2}, v_{\tau-1}) - m(v_{\tau-1}, v_0). \end{aligned}$$

Теорема доказана. ■

Следствие 1. В условиях теоремы имеют место следующие неравенства:

$$\text{а) } \tau \leq L_\varphi(z(w, \lambda, \mu)) \leq n\tau + n - \tau;$$

$$\text{б) } \tau \leq L_\varphi(z(w)) \leq n\tau - \tau.$$

Доказательство. Вытекает из оценок $1 \leq m(v_1, v_2) \leq n-1, \dots, 1 \leq m(v_{\tau-1}, v_\tau) \leq n-1$, $0 \leq L(\lambda, m(v_0, v_1)) \leq n-1$, $0 \leq \mu \leq n-1$. ■

Обозначим через d_ψ и d_φ диаметры графов $\Gamma(\varphi)$ и $\Gamma(\psi)$ соответственно.

Теорема 3. Для сильносвязного графа $\Gamma(\psi)$ с диаметром $d_\psi > 1$ верны оценки

$$d_\psi - 1 + n \leq d_\varphi \leq (n-1) \min\{d_\psi, r-1\} + n.$$

Доказательство. Верхняя оценка доказана в [1, теорема 3.1]. Докажем нижнюю оценку. При $r > 1$ в сильносвязном графе $\Gamma(\psi)$ с диаметром $d_\psi > 1$ имеется пара различных вершин (v_0, v_τ) , для которых кратчайший путь $w = (v_0, \dots, v_\tau)$ имеет длину $\tau = d_\psi - 1$. Тогда по теореме 2а в $\Gamma(\varphi)$ при $\lambda = \mu = 0$ и $m(v_{j-1}, v_j) = n-1$, $j = 2, \dots, \tau$, имеется кратчайший путь $z(w, 0, 0) \in [w]$ из вершины v_0 в вершину v_τ вида

$$z(w, 0, 0) = [0, m(v_0, v_1)]_{v_0} \cdot \delta_0 \cdot \delta_1 \cdot \dots \cdot \delta_{\tau-1} \cdot [n-1, 0]_{v_\tau},$$

где $\delta_j = (v_j + r(n-1), v_{j+1} + r(n-1))$ — дуги графа $\Gamma(\varphi)$, $j = 0, \dots, \tau-1$. С учётом оценок $L(0, m(v_0, v_1)) \geq 1$ и $L(n-1, 0) = n-1$ получаем отсюда длину пути $z(w, 0, 0)$ равную $\tau + n$. Длина пути $z(w, 0, 0)$ является нижней оценкой для d_φ , так как пути w и $z(w, 0, 0)$ кратчайшие. ■

3. Примитивность и экспонент перемешивающего графа

Пусть U_ψ — множество дуг (v, u) графа $\Gamma(\psi)$, таких, что координатная функция $\varphi_{u+(n-1)r}$ подстановки φ зависит существенно от переменных x_{v+tr} не менее чем при двух различных значениях t , где $t \in \{1, \dots, n-1\}$ (в v -й строке таблицы T_u записано не менее двух вершин).

Теорема 4 (достаточное условие примитивности сильносвязного орграфа $\Gamma(\varphi)$). Пусть $(v, u) \in U_\psi$ и координатная функция $\varphi_{u+(n-1)r}$ зависит существенно от переменных с номерами $v + r(t - d_j^{(v,u)})$, $j = 0, \dots, h_{v,u}$, где

$$h_{v,u} > 0, \quad 0 = d_0^{(v,u)} < \dots < d_{h_{v,u}}^{(v,u)} \leq n-2, \quad t \in \{d_{h_{v,u}}^{(v,u)} + 1, \dots, n-1\}.$$

Тогда граф $\Gamma(\varphi)$ примитивен, если $(n, \vartheta) = 1$, где

$$\vartheta = \text{НОД}\{\vartheta_{v,u} : (v, u) \in U_\psi\}, \quad \vartheta_{v,u} = \left(d_1^{(v,u)}, \dots, d_{h_{v,u}}^{(v,u)}\right).$$

Доказательство. По условию граф $\Gamma(\varphi)$ сильносвязный, тогда и $\Gamma(\psi)$ сильносвязный. Обозначим w простой цикл длины $\tau > 1$ в графе $\Gamma(\psi)$, проходящий через дугу (v, u) . Без ограничения общности можно считать, что $w = (1, 2, \dots, \tau)$, $v = \tau$ и $u = 1$, то есть функция $\varphi_{1+(n-1)r}$ зависит существенно от переменных с номерами $\tau + r(t - d_j^{(\tau,1)})$, $j = 0, \dots, h_{\tau,1}$. Следовательно, в сильносвязном графе $\Gamma(\varphi)$ существует простой цикл $z(w)$, проходящий через вершину с номером $\tau + rt$ (в этом случае $j = 0$ и $d_0^{(\tau,1)} = 0$) и представимый конкатенацией следующих путей (при $t = m(\tau, 1)$ данный цикл совпадает с циклом, рассмотренным при доказательстве теоремы 2б):

$$z(w) = [n-1, m(1, 2)]_1 \cdot \delta_1 \cdot \dots \cdot [n-1, m(\tau-1, \tau)]_{\tau-1} \cdot \delta_{\tau-1} \cdot [n-1, t]_\tau \cdot \delta_\tau,$$

где $\delta_\tau = (\tau + rt, 1 + r(n-1))$ и $\delta_s = (s + rm(s, s+1), s+1 + r(n-1))$, $s = 1, \dots, \tau-1$.

Так как при $j = 1, \dots, h_{\tau,1}$ переменные с номерами $\tau + r(t - d_j^{(\tau,1)})$ также являются существенными для координатной функции $\varphi_{1+(n-1)r}$, то в сильносвязном графе $\Gamma(\varphi)$ существуют простые циклы $z_j(w)$, каждый из которых проходит через все вершины цикла $z(w)$ и содержит новую вершину с номером $\tau + r(t - d_j^{(\tau,1)})$:

$$\begin{aligned} z_1(w) &= [n-1, m(1, 2)]_1 \cdot \delta_1 \cdot \dots \cdot [n-1, m(\tau-1, \tau)]_{\tau-1} \cdot \delta_{\tau-1} \cdot [n-1, t - d_1^{(\tau,1)}]_\tau \cdot \delta_\tau^1, \dots, \\ z_{h_{\tau,1}}(w) &= [n-1, m(1, 2)]_1 \cdot \delta_1 \cdot \dots \cdot [n-1, m(\tau-1, \tau)]_{\tau-1} \cdot \delta_{\tau-1} \cdot [n-1, t - d_{h_{\tau,1}}^{(\tau,1)}]_\tau \cdot \delta_\tau^{h_{\tau,1}}, \end{aligned}$$

где $\delta_\tau^j = (\tau + r(t - d_j^{(\tau,1)}), 1 + r(n-1))$.

При фиксированных τ и t длины циклов $z(w)$, $z_1(w)$, $\dots$, $z_{h_{\tau,1}}(w)$ равны

$$\begin{aligned} L_\varphi(z(w)) &= n\tau - m(1, 2) - m(2, 3) - \dots - m(\tau-1, \tau) - t, \\ L_\varphi(z_1(w)) &= L_\varphi(z(w)) + d_1^{(\tau,1)}, \quad \dots, \quad L_\varphi(z_{h_{\tau,1}}(w)) = L_\varphi(z(w)) + d_{h_{\tau,1}}^{(\tau,1)}. \end{aligned}$$

Таким образом, если для рассмотренной дуги $(\tau, 1)$ обозначить $L_\varphi(z(w)) = \lambda_{\tau,1}$ и распространить аналогичные рассуждения на произвольную дугу $(v, u) \in U_\psi$, то получим, что для любой дуги в графе $\Gamma(\varphi)$ имеются простые циклы длины n , $\lambda_{v,u}$, $\lambda_{v,u} + d_1^{(v,u)}$, $\dots$, $\lambda_{v,u} + d_{h_{v,u}}^{(v,u)}$ при некотором натуральном числе $\lambda_{v,u}$. Если все эти числа имеют делитель $\mu > 1$, то μ делит не только число n , но и разность любой пары из этих чисел, в частности делит числа $d_1^{(v,u)}$, $\dots$, $d_{h_{v,u}}^{(v,u)}$. Отсюда μ делит числа $\vartheta_{v,u}$ для

любой дуги $(v, u) \in U_\psi$ и, следовательно, μ делит ϑ . Имеем противоречие с условием $(n, \vartheta) = 1$. Тогда длины указанных простых циклов взаимно просты, и в соответствии с [2, с. 226] граф $\Gamma(\varphi)$ примитивный. ■

В качестве следствия уточним оценку экспонента, полученную в [1, теорема 3.3].

Следствие 2.

а) Если w — простой цикл длины $\tau > 1$ в примитивном графе $\Gamma(\psi)$, то

$$\exp \Gamma(\varphi) \leq nr + \min\{n, L_\varphi(z(w))\}(nr - 2).$$

б) Пусть $\tau_{v,u}$ — длина простого цикла $w_{v,u}$ в графе $\Gamma(\psi)$, проходящего через дугу (v, u) , где $\tau_{v,u} > 1$, и функция $\varphi_{u+r(n-1)}$ зависит существенно от x_{v+rt} и $x_{v+r(t-1)}$, $t \in \{2, \dots, n-1\}$. Тогда граф $\Gamma(\varphi)$ примитивный и

$$\exp \Gamma(\varphi) \leq (\lambda_{v,u})^2 - 2\lambda_{v,u} + 2nr - 1,$$

где $\lambda_{v,u}$ — длина простого цикла $z(w_{v,u})$ в графе $\Gamma(\varphi)$, проходящего через дугу $(v + rt, u + (n-1)r)$.

в) Если в графе $\Gamma(\varphi)$ имеется простой цикл H длины L , проходящий через дугу $(v + tr, u + (n-1)r)$, где $(L, n) = 1$, то

$$\exp \Gamma(\varphi) \leq n(L + 2r) - t - L - 2 \min\{L, n\}.$$

Доказательство.

а) Оценка экспонента следует из теоремы [2, с. 227]: для примитивного m -вершинного графа Γ выполняется $\exp \Gamma \leq m + \lambda(m - 2)$, где λ — длина кратчайшего цикла.

б) Граф $\Gamma(\varphi)$ содержит простые циклы $z(w_{v,u})$ и $z_1(w_{v,u})$, их длины равны соответственно $\lambda_{v,u}$ и $\lambda_{v,u} + 1$, отсюда $(\lambda_{v,u}, \lambda_{v,u} + 1) = 1$ и граф $\Gamma(\varphi)$ примитивный. Тогда в соответствии с [3, теорема 1б] для экспонента графа $\Gamma(\varphi)$ верна оценка $\exp \Gamma(\varphi) \leq (\lambda_{v,u})^2 - 2\lambda_{v,u} + 2nr - 1$.

в) Граф $\Gamma(\varphi)$ содержит независимые простые циклы $C_1, \dots, C_r$ длины n . Если $(L, n) = 1$, то граф $\Gamma(\varphi)$ примитивный. По условию цикл H в графе $\Gamma(\varphi)$ проходит через дугу $(v + tr, u + (n-1)r)$, следовательно, он проходит через вершины $v + (n-1)r, v + (n-2)r, \dots, v + tr$, то есть цикл H имеет $n - t$ общих вершин с циклом C_v .

Оценим экспонент графа $\Gamma(\varphi)$. Используя формулу теоремы 1б [3] при $n < L$, получим

$$\exp \Gamma(\varphi) \leq Ln - L - 3n + n - t + 2nr = n(L + 2r) - t - L - 2n,$$

используя формулу теоремы 1б [3] при $L < n$, имеем

$$\exp \Gamma(\varphi) \leq nL - n - 3L + n - t + 2nr = n(L + 2r) - t - L - 2L.$$

Таким образом, в обоих случаях верна оценка

$$\exp \Gamma(\varphi) \leq n(L + 2r) - t - L - 2 \min\{L, n\}.$$

Следствие доказано. ■

Замечание. Оценка следствия а лучше оценки теоремы 3.3 [1] при $L_\varphi(z(w)) < n$, необходимое условие этого $\tau < n$.

Оценка следствия б лучше оценки теоремы 3.3 [1] при $\lambda_{v,u} < \sqrt{n^2r - n(r-2)}$.

Оценка следствия в лучше оценки теоремы 3.3 [1] при $L < r(n-1)$.

Заключение

Для подстановок φ регистров сдвига длины n над множеством r -мерных двоичных векторов с сильносвязным перемешивающим графом $\Gamma(\varphi)$:

- описаны множества простых путей и циклов графа $\Gamma(\varphi)$, оценены их длины;
- получены новые достаточные условия примитивности графа $\Gamma(\varphi)$;
- уточнены верхние оценки экспонента графа $\Gamma(\varphi)$.

ЛИТЕРАТУРА

1. Коренева А. М., Фомичев В. М. Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика. 2012. № 3 (17). С. 34–40.
2. Сачков В. Н., Тараканов В. Е. Комбинаторика неотрицательных матриц. М.: ТВП, 2000.
3. Фомичев В. М. Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2 (12). С. 101–112.

**СТРУКТУРА ФУНКЦИОНАЛЬНЫХ ГРАФОВ ДЛЯ ЦИРКУЛЯНТОВ
С ЛИНЕЙНЫМИ БУЛЕВЫМИ ФУНКЦИЯМИ В ВЕРШИНАХ¹**

А. С. Корниенко

*Институт математики СО РАН, г. Новосибирск, Россия***E-mail:** anastasia.s.kornienko@gmail.com

Исследуется функциональный граф дискретной динамической системы, заданной на циркулянте с линейной булевой функцией от трёх аргументов в вершинах сети. Получено описание структуры деревьев и циклов функционального графа.

Ключевые слова: *дискретная динамическая система, циркулянт, генная сеть, регуляторный контур, функциональный граф.*

Введение

Генные сети служат основой для моделирования процессов, протекающих в клетке: поддерживают в организме устойчивые состояния, характеризующиеся постоянством концентрации веществ (стационарные состояния); обеспечивают периодические нутухающие колебания концентрации определённых групп веществ (контурь); контролируют необратимые процессы развития и роста [1].

Контурь с положительными и отрицательными обратными связями обеспечивают управление генной сетью. Некоторые структурные особенности строения регуляторных контуров естественно формулируются в терминах ориентированных графов и дискретных моделей регуляторных контуров.

В работе рассматривается дискретная динамическая система, которая является одной из таких моделей регуляторного контура генной сети. Функционирование контура определяется сменой его состояний и полностью характеризуется структурой функционального графа заданного преобразования $A_{f,2}: F_2^n \rightarrow F_2^n$. Метки вершин задают уровень концентрации веществ (гены, белки и др.), сопоставляемых этим вершинам [2–4]. В отличие от [2–4], где функции в вершинах являются пороговыми, в настоящей работе исследуется случай линейных функций.

Для характеристики функционального графа с заданной линейной функцией в вершинах используются циклические коды и техника их порождения с помощью полиномов [5]. Описывается структура деревьев функционального графа и изучаются его контурь: неподвижные точки, длины контуров. Рассматривается некоторое обобщение преобразования $A_{f,2}$.

В основе данной работы лежит защищённая магистерская диссертация [6].

1. Постановка задачи

Используем основные определения и понятия из работы [5], необходимые для постановки задачи.

Пусть даны $n \geq 3$, $1 \leq k \leq n$, $\{d_1, d_2, \dots, d_k\} \subseteq \{0, 1, \dots, n-1\}$ и ориентированный граф $G_{n;d_1, d_2, \dots, d_k}$ с множествами вершин $\{0, 1, \dots, n-1\}$ и дуг $\{(i, j) : (j-i) \equiv$

¹Работа поддержана грантом РФФИ №14-01-00507 и междисциплинарным интеграционным проектом СО РАН №80.

$\equiv d_r \pmod{n}$, $r = 1, 2, \dots, k$. Матрица смежности таких графов называется циркулянтом. Эти графы также принято называть *циркулянтами* [7].

Рассмотрим следующую дискретную динамическую систему. В каждый момент времени вершины циркулянта $G_{n;d_1,d_2,\dots,d_k}$ помечены элементами $v_0, v_1, \dots, v_{n-1}$ из конечного поля F_q порядка q . Набор $\tilde{v} = (v_0, v_1, \dots, v_{n-1}) \in F_q^n$ назовём *состоянием системы*. В следующий момент времени (такт работы системы) состояние системы меняется и динамика его изменения определяется отображением

$$A_{f,q}: F_q^n \rightarrow F_q^n,$$

где $f = (f_0, f_1, \dots, f_{n-1})$ и новая метка каждой вершины $i \in \{0, 1, \dots, n-1\}$ является значением функции $f_i: F_q^k \rightarrow F_q$, аргументы которой принимают значения старых меток в тех вершинах, дуги из которых входят в вершину i .

Функциональным графом $G_{f,q}$ называется ориентированный граф, вершинами которого являются элементы F_q^n , причём дуга из вершины $\tilde{v}$ идёт в вершину $\tilde{u}$ тогда и только тогда, когда $A_{f,q}(\tilde{v}) = \tilde{u}$. Известно, что функциональный граф любого преобразования конечного множества состоит из нескольких (быть может, одной) компонент связности. Каждая компонента содержит единственный контур (в частности, петлю, соответствующую неподвижной точке отображения). Некоторые вершины контура являются корнями деревьев, все дуги которых ориентированы к корню [8].

В работе исследуется структура функционального графа в случае, когда $q = 2$ (то есть действия происходят над полем F_2), все функции f_i равны между собой и линейны и отображение $A_{f,2}$ действует следующим образом:

$$\begin{aligned} A_{f,2}(v_0, v_1, \dots, v_{n-1}) &= (u_0, u_1, \dots, u_{n-1}), \\ u_i &= v_{i-1} + v_i + v_{i+1}, \quad i = 0, 1, \dots, n-1, \end{aligned} \quad (1)$$

где $v_{-1} = v_{n-1}, v_n = v_0$.

2. Структура деревьев в функциональном графе

Линейное подпространство C векторного пространства F_2^n называется *циклическим кодом длины n* над F_2^n , если из $(v_0, v_1, \dots, v_{n-1}) \in C$ следует $(v_1, \dots, v_{n-1}, v_0) \in C$ [9].

Каждому набору $\tilde{v} = (v_0, v_1, \dots, v_{n-1})$ из F_2^n поставим в соответствие многочлен $v(x) = v_0 + v_1x + \dots + v_{n-1}x^{n-1}$ из кольца многочленов $F_2[x]$ над полем F_2 . Известно [9], что при таком соответствии действие отображения $A_{f,2}(\tilde{v}) = \tilde{u}$, определяемое линейной рекуррентностью (1), можно записать в следующем виде.

Предложение 1 [9]. $A_{f,2}(\tilde{v}) = \tilde{u}$ тогда и только тогда, когда

$$v(x)(x^{n-1} + x + 1) \equiv u(x) \pmod{x^n - 1}.$$

Теперь в качестве состояний системы будем рассматривать элементы фактор-кольца $F_2[x]/(x^n - 1)$, а изменение состояния определяется умножением в этом фактор-кольце на многочлен

$$A(x) = x^{n-1} + x + 1.$$

Такую динамическую систему обозначим через $(n, 2, A(x))$ и далее будем называть *моделью*.

Известно [9], что если $C \subseteq F_2^n$ является циклическим кодом, то соответствующее ему подпространство (обозначать будем той же буквой C) фактор-кольца $F_2[x]/(x^n - 1)$

является идеалом. Порождающий многочлен $g(x)$ этого идеала называют *порождающим* кода C . Тогда если $\deg g(x) = r$, то $C = \{g(x)f(x) : f(x) \in F_2[x], \deg f(x) < n-r\}$. Многочлен $h(x)$, заданный соотношением $g(x)h(x) = x^n - 1$, является *проверочным* циклического кода C . Таким образом, $c(x) \in C$ тогда и только тогда, когда $c(x)h(x) = 0$ в $F_2[x]/(x^n - 1)$.

Утверждение 1 [5, следствие 1]. Если $A(x)$ и $x^n - 1$ взаимно просты в кольце $F_2[x]$, то отображение $A_{f,2}$ обратимо и функциональный граф $G_{f,2}$ является дизъюнктивным объединением простых контуров.

Предложение 2. При n не кратном 3 отображение $A_{f,2}$ обратимо и функциональный граф $G_{f,2}$ является дизъюнктивным объединением простых контуров.

Доказательство. По утверждению 1 достаточно показать, что если n не кратно 3, то $(A(x), x^n - 1) = 1$ над полем F_2 . Действительно, по алгоритму Евклида имеем

$$\begin{aligned} (A(x), x^n - 1) &= (x^{n-1} + x + 1, x^n - 1) = (x^{n-1} + x + 1, (x^{n-1} + x + 1)x + x^2 + x + 1) = \\ &= (x^{n-1} + x + 1, x^2 + x + 1). \end{aligned}$$

Из разложения $x^{n-1} + x + 1 = (x^2 + x + 1)(x^{n-3} + x^{n-4}) + x^{(n-1)-3} + x + 1$ следует сравнение $x^{n-1} + x + 1 \equiv x^{(n-1)-3} + x + 1 \pmod{x^2 + x + 1}$. Продолжая аналогичные рассуждения, видим что $x^{n-1} + x + 1 \equiv x^{(n-1) \bmod 3} + x + 1 \pmod{x^2 + x + 1}$. Таким образом, получаем

$$\begin{aligned} n \equiv 0 \pmod{3} &\Rightarrow x^{n-1} + x + 1 \equiv 0 \pmod{x^2 + x + 1}, \\ n \equiv 1 \pmod{3} &\Rightarrow x^{n-1} + x + 1 \equiv x \pmod{x^2 + x + 1}, \\ n \equiv 2 \pmod{3} &\Rightarrow x^{n-1} + x + 1 \equiv 1 \pmod{x^2 + x + 1}. \end{aligned}$$

Предложение доказано. ■

На рис. 1 изображён функциональный граф модели $(5, 2, A(x))$, который представляет из себя дизъюнктивное объединение простых контуров. Здесь двоичные наборы длины 5, соответствующие вершинам, записаны их десятичными представлениями.

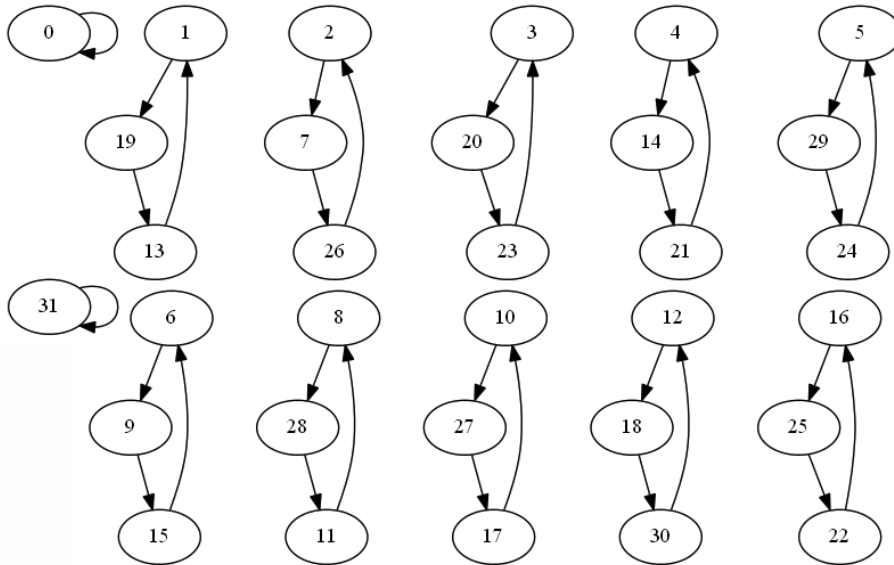


Рис. 1. Функциональный граф $G_{f,2}$ при $n = 5$

Пусть $(A(x), x^n - 1) \neq 1$, т. е. n кратно 3 по предложению 2. Рассмотрим, как в [5], последовательность циклических кодов $C_0 = F_2[x]/(x^n - 1)$, $C_1, C_2, \dots, C_t$, таких, что

код C_i имеет порождающий и проверочный многочлены $g_i(x)$ и $h_i(x)$, $i = 1, 2, \dots, t$, соответственно, где

$$g_1(x) = (A(x), x^n - 1), \quad h_1(x) = (x^n - 1)/g_1(x), \\ g_i(x) = g_{i-1}(x)(g_1(x), h_{i-1}(x)), \quad h_i(x) = (x^n - 1)/g_i(x), \quad i = 2, 3, \dots, t,$$

и t — такое минимальное число, что $(g_1(x), h_t(x)) = 1$.

Пусть $S_i = C_i \setminus C_{i+1}$, $i = 0, 1, \dots, t-1$, и $S_t = C_t$.

Утверждение 2 [5, теорема 2]. В функциональном графе $G_{f,2}$ вершины, принадлежащие контурам, образуют множество S_t . Множество вершин, принадлежащих деревьям, разбивается на t уровней $S_0, S_1, \dots, S_{t-1}$, таких, что S_0 — множество листьев, а вершины из S_i находятся на расстоянии i от вершин из S_0 , $1 \leq i \leq t-1$.

Теорема 1. При $n = 3 \cdot 2^k(2m+1)$, где $k, m \geq 0$, в функциональном графе $G_{f,2}$ множество вершин, принадлежащих деревьям, разбивается на 2^k уровней, причём каждая вершина дерева, кроме листьев, имеет ровно четырёх предков.

Доказательство. Из доказательства предложения 2 имеем $g_1(x) = x^2 + x + 1$. Используя неприводимость многочлена $g_1(x)$ над F_2 , получаем, что для всех $i = 2, 3, \dots, t$ порождающие многочлены $g_i(x) = g_{i-1}(x)(g_1(x), h_{i-1}(x))$ имеют вид $g_i(x) = g_{i-1}(x)g_1(x) = g_1^i(x) = (x^2 + x + 1)^i$, пока многочлен $x^n - 1$ делится на $(x^2 + x + 1)^i$, так как $h_i(x) = (x^n - 1)/g_i(x)$. Таким образом, $(g_1(x), h_t(x))$ впервые равен 1, когда t равно максимальной степени вхождения многочлена $x^2 + x + 1$ в разложение $x^n - 1$ на неприводимые множители над F_2 .

Сначала докажем индукцией по k , что множество вершин, принадлежащих деревьям, разбивается на 2^k уровней.

Пусть $k = 0$, т.е. $n = 3(2m+1)$. Покажем, что в этом случае $t = 1$. Допустим обратное, тогда $x^n - 1$ должно делиться без остатка на $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. Из представления $x^n - 1 = (x^4 + x^2 + 1)(x^{n-4} + x^{n-6}) + x^{n-6} - 1$ получаем, что $x^n - 1 \equiv x^{n-6} - 1 \equiv \dots \equiv x^{n \bmod 6} - 1 \equiv 0 \pmod{x^4 + x^2 + 1}$. Но $n = 3(2m+1) = 6m+3 \equiv 3 \pmod{6}$, противоречие. База индукции доказана.

Предположим, что для $n_k = 3 \cdot 2^k(2m+1)$ максимальная степень вхождения $x^2 + x + 1$ в разложение на неприводимые множители $x^{n_k} - 1$ над F_2 равна $t_k = 2^k$. Пусть теперь $n = 3 \cdot 2^{k+1}(2m+1)$. Из разложения $x^n - 1 = x^{2n_k} - 1 = (x^{n_k} - 1)(x^{n_k} + 1)$ и предположения индукции получаем, что $t = 2t_k = 2^{k+1}$. Таким образом, первая часть теоремы доказана.

Теперь, используя мощностные оценки, докажем, что каждая вершина в дереве, кроме листьев, имеет ровно четырёх предков.

Найдём мощность множества S_t вершин, принадлежащих контурам. Из утверждения 2 это множество совпадает с циклическим кодом C_t с порождающим многочленом $g_t(x)$. Из доказанного выше знаем, что при $n = 3 \cdot 2^k(2m+1)$ имеем $t = 2^k$ и $g_t(x) = (x^2 + x + 1)^t$. Степень порождающего многочлена равна $2t$, значит, циклический код C_t имеет мощность 2^{n-2t} .

Заметим, что уравнение $A_{f,2}(\tilde{v}) = \tilde{v}$ с неизвестным $\tilde{v}$ имеет не более четырёх решений. Действительно, из равенств (1) получаем, что решение $\tilde{v}$, если оно существует, можно представить в следующем рекуррентном виде:

$$v_i = u_{i-1} + v_{i-1} + v_{i-2}, \quad i = 2, 3, \dots, n-1,$$

если v_0, v_1 заданы. Так как v_0 и v_1 из F_2 , то начальное условие, которое полностью задаёт решение, можно выбрать четырьмя различными способами.

Другими словами, доказано, что каждая вершина функционального графа $G_{f,2}$ имеет не более четырёх прообразов. Корень каждого дерева имеет не более трёх предков в своём дереве, так как он уже является образом некоторой вершины из контура. Оставшиеся вершины дерева, кроме листьев, имеют не более четырёх предков. Тогда весь функциональный граф имеет вершин не более, чем

$$\begin{aligned} 2^{n-2t} + \sum_{l=0}^{t-1} 4^l \cdot 3 \cdot 2^{n-2t} &= 2^{n-2t} + 3 \cdot 2^{n-2t} \sum_{l=0}^{t-1} 4^l = \\ &= 2^{n-2t} + 3 \cdot 2^{n-2t} \cdot \frac{4^t - 1}{3} = 2^{n-2t} + 2^{n-2t} \cdot 4^t - 2^{n-2t} = 2^{n-2t} \cdot 2^{2t} = 2^n. \end{aligned}$$

Но именно столько элементов в пространстве F_2^n . Значит, каждая вершина функционального графа, не являющаяся листом, имеет ровно четыре прообраза, и теорема полностью доказана. ■

На рис. 2 изображено дерево, притягиваемое вершиной $\tilde{v} = (0, 0, \dots, 0)$, в функциональном графе $G_{f,2}$ при $n = 6$. Двоичные наборы длины 6, соответствующие вершинам, записаны их десятичными представлениями.

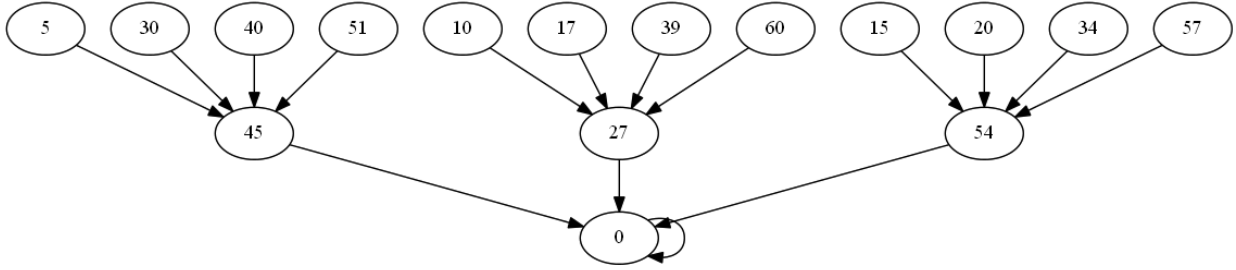


Рис. 2. Дерево, притягиваемое вершиной $\tilde{v} = (0, 0, \dots, 0)$, в функциональном графе $G_{f,2}$ при $n = 6$

3. Контур в функциональном графе

Рассмотрим неподвижные точки и длины контуров в функциональном графе $G_{f,2}$.

Утверждение 3 [5, следствие 4]. Неподвижные точки функционального графа $G_{f,2}$ образуют циклический код с проверочным многочленом $(A(x) - 1, x^n - 1)$. Если степень этого многочлена равна r , то число неподвижных точек равно 2^r .

Предложение 3. При чётном n функциональный граф $G_{f,2}$ содержит четыре неподвижные точки, в противном случае — две.

Доказательство. По утверждению 3 для того, чтобы найти неподвижные точки функционального графа, необходимо и достаточно найти проверочный многочлен $h(x) = (A(x) - 1, x^n - 1)$ циклического кода, состоящего из неподвижных точек функционального графа $G_{f,2}$. Используя алгоритм Евклида, получаем

$$\begin{aligned} (A(x) - 1, x^n - 1) &= (x^{n-1} + x, x^n - 1) = (x^{n-2} + 1, x^n - 1) = \\ &= (x^{n-2} + 1, (x^{n-2} + 1)x^2 + x^2 + 1) = (x^{n-2} + 1, x^2 + 1) = x^{2-n \bmod 2} + 1. \end{aligned}$$

В зависимости от чётности n имеем

$$\begin{aligned} n \equiv 0 \pmod{2} &\Rightarrow h(x) = (A(x) - 1, x^n - 1) = x^2 + 1, \\ n \equiv 1 \pmod{2} &\Rightarrow h(x) = (A(x) - 1, x^n - 1) = x + 1. \end{aligned}$$

Рассмотрим каждый вариант по отдельности.

В первом случае проверочный многочлен циклического кода $h(x) = x^2 + 1$. По определению $g(x)h(x) = x^n - 1$, значит, порождающий многочлен $g(x) = x^{n-2} + x^{n-4} + \dots + 1$, и порождающая матрица циклического кода, состоящего из неподвижных точек функционального графа $G_{f,2}$, имеет вид

$$\begin{pmatrix} 1 & 0 & 1 & 0 & \dots & 1 & 0 \\ 0 & 1 & 0 & 1 & \dots & 0 & 1 \end{pmatrix}.$$

Таким образом, имеем четыре неподвижные точки: 0 , $x^{n-2} + x^{n-4} + \dots + 1$, $x^{n-1} + x^{n-3} + \dots + x$, $x^{n-1} + x^{n-2} + \dots + 1$. В F_2^n неподвижные точки соответствуют элементам $(0, 0, \dots, 0)$, $(1, 0, \dots, 1, 0)$, $(0, 1, \dots, 0, 1)$, $(1, 1, \dots, 1)$.

Во втором случае $h(x) = x + 1$ и порождающий многочлен $g(x) = x^{n-1} + x^{n-2} + \dots + 1$. Существуют всего две неподвижные точки: 0 и $x^{n-1} + x^{n-2} + \dots + 1$. В F_2^n неподвижные точки соответствуют элементам $(0, 0, \dots, 0)$ и $(1, 1, \dots, 1)$. ■

Утверждение 4 [5, теорема 3]. Для любого целого положительного l все вершины функционального графа, принадлежащие контурам длины, делящей l , образуют циклический код с проверочным многочленом $(A^l(x) - 1, x^n - 1)$.

Утверждение 5 [5, теорема 4]. Если наибольшая длина контура функционального графа модели $(n, 2, A(x))$ равна l и $h_t(x)$ является порождающим многочленом циклического кода, образованного вершинами всех контуров, то максимальная длина контура функционального графа модели $(2n, 2, A(x))$ не изменится тогда и только тогда, когда $h_t^2(x)$ делит $A^l(x) - 1$. В противном случае наибольшая длина контура удвоится.

Теорема 2. Если $n = 2^k(2m + 1)$, где $k, m \geq 0$, то все длины контуров функционального графа $G_{f,2}$ являются делителями $2^k(2^s - 1)$, где

$$s = \min\{j : j > 0, 2^j \equiv 1 \pmod{2m+1} \text{ или } 2^j \equiv -1 \pmod{2m+1}\}.$$

Доказательство. Пусть n — нечётное число. Положим $l = 2^s - 1$, где

$$s = \min\{j : j > 0, 2^j \equiv 1 \pmod{n} \text{ или } 2^j \equiv -1 \pmod{n}\}.$$

Так как сложение происходит по модулю 2, то имеем следующие сравнения:

$$\begin{aligned} A^{2^s}(x) &= (x^{n-1} + x + 1)^{2^s} = x^{2^s(n-1)} + x^{2^s} + 1 \equiv x^{n-1} + x + 1 = A(x) \pmod{x^n - 1}, \\ A(x)(A(x)^{2^s-1} - 1) &\equiv 0 \pmod{x^n - 1}, \\ A(x)(A^l(x) - 1) &\equiv 0 \pmod{x^n - 1}. \end{aligned}$$

Так как по предположению 2 выполняется $(A(x), x^n - 1) = 1$ при n , не кратном 3, то

$$A^l(x) - 1 \equiv 0 \pmod{x^n - 1}, \text{ то есть } (A^l(x) - 1, x^n - 1) = x^n - 1 = h_t(x).$$

В случае же, когда n делится на 3, имеем

$$\begin{aligned} (A(x), x^n - 1) &= x^2 + x + 1, \\ (A^l(x) - 1, x^n - 1) &= \frac{x^n - 1}{x^2 + x + 1} = h_t(x). \end{aligned}$$

По утверждению 4 получаем, что для нечётного n теорема доказана. Из утверждения 5 следует истинность и для чётного n . ■

Утверждение 6 [5, следствие 6]. Если в модели $(n, 2, A(x))$ наибольшая длина контура чётна, то в модели $(2n, 2, A(x))$ наибольшая длина контура равна $2l$.

Теорема 3. Пусть в модели $(n, 2, A(x))$ наибольшая длина контура равна l , тогда в модели $(2n, 2, A(x))$ наибольшая длина контура не изменится, если $n \in \{1, 3\}$, в противном случае она удвоится.

Доказательство. Пусть n нечётное. По теореме 2 и утверждению 5, если длина контура в модели $(2n, 2, A(x))$ не удваивается, то $h_t^2(x)$ должен делить $A^l(x) - 1$ и $A^{2^s-1}(x) - 1$, поскольку l — делитель числа $2^s - 1$ по теореме 2, где s удовлетворяет сравнению

$$\begin{aligned} 2^s &\equiv \pm 1 \pmod{n}, \text{ так как } n \text{ нечётное,} \\ 2^s &\equiv n \pm 1 \pmod{2n}. \end{aligned}$$

Рассмотрим при $n \neq 1$ в модели $(2n, 2, A(x))$ более подробно разность

$$\begin{aligned} A^{2^s}(x) - A(x) &= (x^{2^s \cdot (2n-1)} + x^{2^s} + 1) - (x^{2n-1} + x + 1) \equiv \\ &\equiv x^{(n-1)(2n-1)} + x^{n-1} - x^{2n-1} - x \equiv x^{n+1} + x^{n-1} - x^{2n-1} - x \equiv \\ &\equiv x^{2n-2} + x^n + x^{n-2} + 1 \pmod{x^{2n} - 1}, \text{ если } 2^s \equiv n - 1 \pmod{2n}; \\ A^{2^s}(x) - A(x) &= (x^{2^s \cdot (2n-1)} + x^{2^s} + 1) - (x^{2n-1} + x + 1) \equiv \\ &\equiv x^{(n+1)(2n-1)} + x^{n+1} - x^{2n-1} - x \equiv x^{n-1} + x^{n+1} - x^{2n-1} - x \equiv \\ &\equiv x^{2n-2} + x^n + x^{n-2} + 1 \pmod{x^{2n} - 1}, \text{ если } 2^s \equiv n + 1 \pmod{2n}. \end{aligned}$$

Для n , не кратного 3, порождающий многочлен циклического кода, образованного вершинами всех контуров функционального графа модели $(n, 2, A(x))$, равен $h_t(x) = x^n - 1$, и

$$\begin{aligned} A^{2^s-1}(x) - 1 &\equiv 0 \pmod{x^{2n} - 1}, \\ A^{2^s}(x) - A(x) &\equiv 0 \pmod{x^{2n} - 1}, \\ x^{2n-2} + x^n + x^{n-2} + 1 &\equiv 0 \pmod{x^{2n} - 1}, \\ (x^{n-2} + 1)(x^n + 1) &\equiv 0 \pmod{(x^n - 1)(x^n + 1)}, \\ x^{n-2} + 1 &\equiv 0 \pmod{x^n - 1} \Rightarrow x^{n-2} + 1 = 0. \end{aligned}$$

Равенство верно только при $n = 2$. Для n , кратного 3, порождающий многочлен равен $h_t(x) = (x^n - 1)/(x^2 + x + 1)$, $(A(x), x^{2n} - 1) = x^2 + x + 1$, и

$$\begin{aligned} A^{2^s-1}(x) - 1 &\equiv 0 \pmod{(x^{2n} - 1)/(x^2 + x + 1)^2}, \\ (A^{2^s-1}(x) - 1)(x^2 + x + 1)^2 &\equiv 0 \pmod{x^{2n} - 1}, \\ (A^{2^s-1}(x) - 1)(x^2 + x + 1)^2 A(x) &\equiv 0 \pmod{x^{2n} - 1}, \\ (A^{2^s}(x) - A(x))(x^2 + x + 1) &\equiv 0 \pmod{x^{2n} - 1}, \\ (x^{2n-2} + x^n + x^{n-2} + 1)(x^2 + x + 1) &\equiv 0 \pmod{x^{2n} - 1}, \\ (x^{n-2} + 1)(x^n + 1)(x^2 + x + 1) &\equiv 0 \pmod{(x^n - 1)(x^n + 1)}, \\ (x^{n-2} + 1)(x^2 + x + 1) &\equiv 0 \pmod{x^n - 1}, \\ x^n + x^{n-1} + x^{n-2} + x^2 + x + 1 &\equiv 0 \pmod{x^n - 1}, \\ x^{n-1} + x^{n-2} + x^2 + x &\equiv 0 \pmod{x^n - 1} \Rightarrow (x^{n-3} + 1)(x + 1)x = 0. \end{aligned}$$

Равенство верно только при $n = 3$.

Легко проверить, что у моделей $(1, 2, A(x))$ и $(2, 2, A(x))$, как и у моделей $(3, 2, A(x))$ и $(6, 2, A(x))$, максимальные длины контуров одинаковы и равны 1. А у моделей $(4, 2, A(x))$ и $(12, 2, A(x))$ максимальные длины контуров равны 2.

Таким образом, теорема доказана для нечётного l . Для чётного l истинность следует из утверждения 6. ■

Утверждение 7 [5, следствие 5]. Наибольшая длина контура в функциональном графе равна минимальному l , для которого

$$(A^l(x) - 1, x^n - 1) = h_t(x).$$

Следствие 1. Если $n = 2^k(2^m \pm 1)$, $k \geq 0$ и $m > 2$, то наибольшая длина контура в $G_{f,2}$ равна $2^k(2^m - 1)$.

Доказательство. Следует из теорем 2, 3 и утверждения 7. ■

Предложение 4. Если $n \neq 3$ — простое число, то все контуры в $G_{f,2}$, кроме двух неподвижных точек, имеют одинаковую длину.

Доказательство. Допустим, что существует контур, длина l которого отлична от максимальной длины всех контуров. Тогда по утверждению 7 должно выполняться

$$(A^l(x) - 1, x^n - 1) \neq h_t(x), \text{ то есть } (A^l(x) - 1, x^n - 1) \neq x^n - 1,$$

для простого $n \neq 3$ проверочный многочлен $h_t(x) = x^n - 1$. Разложим на множители $x^n - 1 = (x - 1)(x^{n-1} + \dots + x + 1)$. Известно [10], что многочлен $x^{n-1} + \dots + x + 1$ является неприводимым над полем F_2 . Таким образом, получаем, что $(A^l(x) - 1, x^n - 1) = x - 1$, так как

$$\begin{aligned} A(x) &= x^{n-1} + x + 1 \equiv 1 \pmod{x - 1}, \\ A^l(x) - 1 &\equiv 0 \pmod{x - 1}. \end{aligned}$$

Но $x - 1$ — это проверочный многочлен для циклического кода, состоящего из неподвижных точек функционального графа $G_{f,2}$. Тем самым предложение доказано. ■

4. Сместённое преобразование

Отображение $A_{f,2}: F_2^n \rightarrow F_2^n$, определённое равенством (1), можно записать в следующем виде: $A_{f,2} = I_n + L_n + R_n$, где I_n , L_n и R_n — тождественный оператор, операторы левого и правого сдвигов пространства F_2^n соответственно.

Рассмотрим отображения $A_{f_L,2} = L_n \cdot A_{f,2}$ и $A_{f_R,2} = R_n \cdot A_{f,2}$ и назовём их *сместёнными влево* и *вправо* относительно отображения $A_{f,2}$ соответственно. В силу симметрии структуры функциональных графов этих отображений совпадают, поэтому достаточно изучить структуру функционального графа только одного преобразования, например $A_{f_R,2}$.

4.1. Структура деревьев

Отображение $A_{f_R,2}: F_2^n \rightarrow F_2^n$, действующее следующим образом:

$$\begin{aligned} A_{f_R,2}(v_0, v_1, \dots, v_{n-1}) &= (u_0, u_1, \dots, u_{n-1}), \\ u_i &= v_{i-2} + v_{i-1} + v_i, \quad i = 0, 1, \dots, n-1, \\ v_{-2} &= v_{n-2}, v_{-1} = v_{n-1}, \end{aligned}$$

в фактор-кольце $F_2[x]/(x^n - 1)$ определяется как умножение элементов фактор-кольца на многочлен $A_R(x) = x^2 + x + 1$. Значит, порождающие $g_i(x)$ и проверочные $h_i(x)$ многочлены отображений $A_{f_R,2}$ и $A_{f,2}$ совпадают. Таким образом, можем описать структуру деревьев функционального графа отображения $A_{f_R,2}$.

Предложение 5. При n , не кратном 3, отображение $A_{f_R,2}$ обратимо и функциональный граф $G_{f_R,2}$ является дизъюнктивным объединением простых контуров.

Предложение 6. При $n = 3 \cdot 2^k(2m + 1)$, где $k, m \geq 0$, в функциональном графе $G_{f_R,2}$ множество вершин, принадлежащих деревьям, разбивается на 2^k уровней, причём каждая вершина дерева, кроме листьев, имеет ровно четырёх предков.

4.2. Контур ы

В отличие от структур деревьев функциональных графов преобразований $A_{f_R,2}(x)$ и $A_{f,2}(x)$, которые совпадают, структуры контуров имеют различия.

Предложение 7. Функциональный граф $G_{f_R,2}$ содержит две неподвижные точки.

Доказательство. По утверждению 3, для того, чтобы найти неподвижные точки функционального графа, необходимо и достаточно найти проверочный многочлен $h(x)$:

$$h(x) = (A_R(x) - 1, x^n - 1) = (x^2 + x, x^n - 1) = (x + 1, x^n - 1) = x + 1.$$

По определению $g(x)h(x) = x^n - 1$, значит, порождающий многочлен циклического кода, состоящего из неподвижных точек функционального графа $G_{f_R,2}$, равен $g(x) = x^{n-1} + x^{n-2} + \dots + 1$. Таким образом, имеем две неподвижные точки: 0 и $x^{n-1} + x^{n-2} + \dots + 1$, которые в F_2^n соответствуют элементам $(0, 0, \dots, 0)$ и $(1, 1, \dots, 1)$. ■

Предложение 8. Если $n = 2^k(2m + 1)$, $k, m \geq 0$, то все длины контуров функционального графа $G_{f_R,2}$ являются делителями $2^k(2^s - 1)$, где

$$s = \min\{j : j > 0, \quad 2^j \equiv 1 \pmod{2m + 1}\}.$$

Доказательство. Пусть n — нечётное число. Положим $l = 2^s - 1$, где

$$s = \min\{j : j > 0, \quad 2^j \equiv 1 \pmod{n}\}.$$

Так как сложение происходит по модулю 2, то имеем следующие сравнения:

$$A_R^{2^s}(x) = (x^2 + x + 1)^{2^s} = x^{2 \cdot 2^s} + x^{2^s} + 1 \equiv x^2 + x + 1 = A_R(x) \pmod{x^n - 1},$$

$$A_R(x)(A_R(x)^{2^s-1} - 1) \equiv 0 \pmod{x^n - 1},$$

$$A_R(x)(A_R^l(x) - 1) \equiv 0 \pmod{x^n - 1}.$$

Так как $(A_R(x), x^n - 1) = 1$ при n , не кратном 3, то

$$A_R^l(x) - 1 \equiv 0 \pmod{x^n - 1},$$

$$(A_R(x)^l - 1, x^n - 1) = x^n - 1 = h_t(x).$$

В случае же, когда n делится на 3, имеем

$$(A_R(x), x^n - 1) = x^2 + x + 1,$$

$$(A_R(x)^l - 1, x^n - 1) = \frac{x^n - 1}{x^2 + x + 1} = h_t(x).$$

По утверждению 4 получаем, что для нечётного n предложение доказано. Из утверждения 5 следует истинность и для чётного n . ■

Предложение 9. Наибольшая длина контура в модели $(2n, 2, A_R(x))$ в 2 раза больше, чем в модели $(n, 2, A_R(x))$.

Доказательство. Пусть n нечётное. По предложению 8 и утверждению 5, если длина контура в модели $(2n, 2, A_R(x))$ не удваивается, то $h_t^2(x)$ должен делить $A_R^l - 1$ и $A_R^{2^s-1} - 1$, поскольку l — делитель числа $2^s - 1$ по предложению 8, где s удовлетворяет сравнению

$$\begin{aligned} 2^s &\equiv 1 \pmod{n}, \text{ так как } n \text{ нечётное,} \\ 2^s &\equiv n + 1 \pmod{2n}. \end{aligned}$$

Рассмотрим более подробно разность

$$\begin{aligned} A_R^{2^s}(x) - A_R(x) &= (x^{2 \cdot 2^s} + x^{2^s} + 1) - (x^2 + x + 1) \equiv \\ &\equiv x^{2(n+1)} + x^{n+1} - x^2 - x \equiv x^2 + x^{n+1} - x^2 - x \equiv x^n + 1 \pmod{x^{2n} - 1}. \end{aligned}$$

Для n , не кратного 3, получаем, что $h_t(x) = x^n - 1$ и

$$\begin{aligned} A_R^{2^s-1}(x) - 1 &\equiv 0 \pmod{x^{2n} - 1}, \\ A_R^{2^s}(x) - A_R(x) &\equiv 0 \pmod{x^{2n} - 1}, \\ x^n + 1 &\equiv 0 \pmod{x^{2n} - 1}. \end{aligned}$$

Для n , кратного 3, получаем, что $h_t(x) = (x^n - 1)/(x^2 + x + 1)$ и

$$\begin{aligned} (A_R^{2^s-1}(x) - 1)(x^2 + x + 1)^2 &\equiv 0 \pmod{x^{2n} - 1}, \\ (A_R^{2^s}(x) - A_R(x))(x^2 + x + 1) &\equiv 0 \pmod{x^{2n} - 1}, \\ (x^n + 1)(x^2 + x + 1) &\equiv 0 \pmod{x^{2n} - 1}, \\ x^{n+2} + x^{n+1} + x^n + x^2 + x + 1 &\equiv 0 \pmod{x^{2n} - 1}. \end{aligned}$$

В обоих случаях полученные сравнения не верны для любого n .

Таким образом, предложение доказано для нечётного l . Для чётного l предложение следует из утверждения 6. ■

Следствие 2. Если $n = 2^k(2^m - 1)$, $k, m \geq 0$ и $m \neq 2$, то наибольшая длина контура в $G_{f_R,2}$ равна n .

Доказательство. Следует из предложений 8, 9 и утверждения 7. ■

Предложение 10. Если $n \neq 3$ — простое число, то все контуры в $G_{f_R,2}$, кроме двух неподвижных точек, имеют одинаковую длину.

Доказательство. Допустим, что существует контур, длина l которого отлична от максимальной длины всех контуров. Тогда по утверждению 7 должно выполняться

$$\begin{aligned} (A_R^l(x) - 1, x^n - 1) &\neq h_t(x), \text{ то есть} \\ (A_R^l(x) - 1, x^n - 1) &\neq x^n - 1, \end{aligned}$$

для простого $n \neq 3$ проверочный многочлен $h_t(x) = x^n - 1$. Разложим на множители $x^n - 1 = (x - 1)(x^{n-1} + \dots + x + 1)$. Как было замечено ранее, многочлен $x^{n-1} + \dots + x + 1$ неприводим над полем F_2 . Таким образом, $(A_R^l(x) - 1, x^n - 1) = x - 1$, так как

$$\begin{aligned} A_R &= x^2 + x + 1 \equiv 1 \pmod{x - 1}, \\ A_R^l(x) - 1 &\equiv 0 \pmod{x - 1}. \end{aligned}$$

Но $x - 1$ — это проверочный многочлен циклического кода, состоящего из неподвижных точек функционального графа $G_{f_R,2}$. Тем самым предложение доказано. ■

Предложение 11. Функциональный граф $G_{fR,2}$ содержит контур длины 2, причём только один, тогда и только тогда, когда n чётное.

Доказательство. По утверждению 4 все вершины функционального графа, принадлежащие контурам длины, делящей 2, образуют циклический код с проверочным многочленом

$$\begin{aligned} (A_R^2(x) - 1, x^n - 1) &= ((x^2 + x + 1)^2 - 1, x^n - 1) = \\ &= (x^4 + x^2, x^n - 1) = (x^2 + 1, x^n - 1) = x^{2-n \bmod 2} - 1. \end{aligned}$$

В случае нечётного n проверочный многочлен равен $x - 1$ и является проверочным для кода, состоящего из неподвижных точек. В случае чётного n имеем $x^2 - 1$, и такой проверочный многочлен образует циклический код из четырёх элементов, два и только два из которых — неподвижные точки. Значит, оставшиеся два элемента образуют один цикл длины 2. ■

5. Некоторое обобщение

Отображение $A_{f,2}: F_2^n \rightarrow F_2^n$ можно записать в виде $A_{f,2} = I_n + L_n + R_n$.

Рассмотрим отображение более общего вида $A_{f,2}(k) = I_n + L_n^k + R_n^k$.

Теорема 4. Пусть $(n, k) = 1$. Тогда $A_{f,2}(k)$ является алгебраическим сопряжением к $A_{f,2}$.

Доказательство. Пусть $\tilde{v} = (v_0, v_1, \dots, v_{n-1}) \in F_2^n$. Определим отображение $\sigma: F_2^n \rightarrow F_2^n$ следующим образом:

$$\sigma(\tilde{v}) = (v_{\pi(0)}, v_{\pi(1)}, \dots, v_{\pi(n-1)}), \text{ где } \pi(jk \bmod n) = j, j = 0, \dots, n-1.$$

Так как $(n, k) = 1$, π является перестановкой $(0, 1, \dots, n-1)$, а $\pi^{-1}(j) = jk \bmod n$ — обратная к ней перестановка. Таким образом, имеем

$$\begin{aligned} (A_{f,2}(k)\sigma(\tilde{v}))_{jk \bmod n} &= v_j + v_{j+1} + v_{j-1}, \\ (\sigma^{-1}A_{f,2}(k)\sigma(\tilde{v}))_j &= v_j + v_{j+1} + v_{j-1}, \text{ где } v_{-1} = v_{n-1}, v_n = v_0. \end{aligned}$$

Отсюда получаем $\sigma^{-1}A_{f,2}(k)\sigma = A_{f,2}$, что и требовалось доказать. ■

Следствие 3. При $(n, k) = 1$ структура функционального графа отображения $A_{f,2}(k)$ совпадает со структурой функционального графа отображения $A_{f,2}$.

Заключение

В работе рассмотрена дискретная динамическая система, являющаяся моделью регуляторного контура генной сети, функционирование которого определяется сменой его состояний и полностью характеризуется структурой функционального графа $G_{f,2}$ заданного преобразования $A_{f,2}: F_2^n \rightarrow F_2^n$.

Для характеристики функционального графа $G_{f,2}$ с заданной линейной функцией в вершинах использованы циклические коды и техника их порождения с помощью полиномов. Описана структура деревьев функционального графа и изучены некоторые свойства контуров: найдены неподвижные точки; найдено число, делителями которого являются все длины контуров функционального графа; для некоторого вида n найдена максимальная длина контуров. Данные результаты удалось распространить на более общий вид преобразования $A_{f,2}$.

Доказаны также аналогичные свойства деревьев и контуров функциональных графов преобразований, смещённых относительно $A_{f,2}$.

ЛИТЕРАТУРА

1. *Лихошвай В. А., Матушкин Ю. Г., Фадеев С. И.* Задачи теории функционирования генных сетей // Сиб. журн. индустр. математики. 2003. Т. 6. № 2 (14). С. 64–80.
2. *Григоренко Е. Д., Евдокимов А. А., Лихошвай В. А., Лобарева И. А.* Неподвижные точки и циклы автоматных отображений, моделирующих функционирование генных сетей // Вестник ТГУ. 2005. Приложение № 14. С. 206–212.
3. *Евдокимов А. А.* Дискретные модели генных сетей: анализ и сложность функционирования // Вычислительные технологии. 2008. Т. 13. № 3. С. 31–37.
4. *Евдокимов А. А., Лиховидова Е. О.* Дискретная модель генной сети циркулянтного типа с пороговыми функциями // Вестник ТГУ. Управление, вычислительная техника и информатика. 2008. № 2. С. 18–21.
5. *Евдокимов А. А., Пережогин А. Л.* Дискретные динамические системы циркулянтного типа с линейными функциями в вершинах сети // Дискретный анализ и исследование операций. 2011. Т. 18. № 3. С. 39–48.
6. *Корниенко А. С.* Структура функциональных графов для циркулянтов с линейными булевыми функциями в вершинах: магистерская диссертация / Новосибирский государственный университет. Новосибирск, 2013. 22 с.
7. *Харари Ф.* Теория графов. М.: УРСС, 2003. 300 с.
8. *Оре О.* Теория графов. М.: Наука, 1980. 336 с.
9. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
10. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1. М.: Мир, 1988. 430 с.

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

DOI 10.17223/20710410/23/11

УДК 519.1, 519.8

ОБ АСИМПТОТИЧЕСКИ ОПТИМАЛЬНОМ ПЕРЕЧИСЛЕНИИ НЕПРИВОДИМЫХ ПОКРЫТИЙ БУЛЕВОЙ МАТРИЦЫ¹

Е. В. Дюкова^{*,**}, П. А. Прокофьев^{*}^{*}Вычислительный центр им. А. А. Дородницына, г. Москва, Россия^{**}Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия**E-mail:** edjukova@mail.ru, p_prok@mail.ru

Рассматривается задача перечисления неприводимых покрытий булевой матрицы, известная как задача дуализации. Эффективность алгоритма дуализации принято оценивать сложностью шага алгоритма (построения очередного неприводимого покрытия). Рассматривается подход к построению алгоритма дуализации, эффективного в «типичном случае». Подход основан на понятии асимптотически оптимального алгоритма с полиномиальной задержкой. Строятся две модификации предложенного ранее алгоритма АО2, позволяющие существенно сократить временные затраты в экспериментах со случайными булевыми матрицами.

Ключевые слова: булева матрица, перечисление неприводимых покрытий, асимптотически оптимальный алгоритм дуализации, нормальная форма монотонной булевой функции, минимальное вершинное покрытие гиперграфа.

Введение

Пусть $L = \|a_{ij}\|_{m \times n}$ — булева матрица и H — набор столбцов матрицы L . Набор H называется *покрытием* матрицы L , если каждая строка матрицы L в пересечении хотя бы с одним столбцом из H даёт 1. Покрытие H называется *неприводимым*, если любое собственное подмножество H не является покрытием L .

Через $\mathcal{P}(L)$ обозначается множество всех неприводимых покрытий матрицы L . Рассматривается задача перечисления элементов множества $\mathcal{P}(L)$, называемая *дуализацией*.

Задача дуализации может быть также переформулирована с использованием понятий теории булевых функций и теории графов и гиперграфов. Приведём эти формулировки:

- 1) Дана конъюнктивная нормальная форма из m элементарных дизъюнкций, реализующая монотонную булеву функцию F от n переменных. Требуется построить (перечислить) все максимальные конъюнкции функции F .
- 2) Дан гиперграф G с n вершинами и m ребрами. Требуется найти все минимальные вершинные покрытия гиперграфа G .

Двойственной к 2 является задача поиска максимальных независимых подмножеств вершин гиперграфа G .

¹Работа частично поддержана грантом РФФИ №13-01-00787-а и грантом президента РФ НШ-4652.2012.1.

В большинстве случаев мощность множества $\mathcal{P}(L)$ экспоненциально растёт с ростом размера матрицы L . Эффективность алгоритмов перечисления неприводимых покрытий принято оценивать сложностью получения очередного решения (сложностью шага алгоритма) [1]. Различают алгоритмы, эффективные в «худшем случае», и алгоритмы, эффективные в «типичном случае». К алгоритмам, эффективным в худшем случае, относят, в частности, алгоритмы с (квази)полиномиальными задержками [1, 2] и инкрементальные (квази)полиномиальные алгоритмы [3–6].

Говорят, что алгоритм работает с (квази)полиномиальной задержкой, если каждый его шаг (построение очередного неприводимого покрытия) осуществляется за (квази)полиномиальное время от размера задачи. В общем случае алгоритм, находящий на каждом шаге неприводимое покрытие за (квази)полиномиальное время, до сих пор не построен, и неизвестно, существует ли он. Для некоторых частных случаев построены алгоритмы с (квази)полиномиальной задержкой. Например, в [1] с полиномиальной задержкой перечисляются максимальные независимые наборы вершин графа, что соответствует случаю, когда матрица L в каждой строке имеет не более двух единичных элементов.

Для построения алгоритмов, эффективных в типичном случае, используется подход, основанный на понятии *асимптотически оптимального алгоритма с полиномиальной задержкой*, который впервые предложен в [7] и развит в последующих работах [8–10]. В отличие от «точного» алгоритма с полиномиальной задержкой, асимптотически оптимальному алгоритму разрешено делать «лишние» полиномиальные шаги, но число таких шагов для почти всех матриц размера $m \times n$ должно иметь более низкий порядок роста, чем число всех шагов алгоритма, с ростом m и n .

К настоящему моменту для случая, когда $\log m \leq (1 - \varepsilon) \log n$, при $0 < \varepsilon < 1$, построен ряд асимптотически оптимальных алгоритмов дуализации [7–9]. В этих алгоритмах встречаются лишние шаги двух типов: 1) построение набора столбцов, не являющегося покрытием, и 2) нахождение неприводимого покрытия, которое было построено на предыдущих шагах. Среди построенных алгоритмов есть такие, в которых присутствуют лишние шаги обоих типов, например алгоритм АО1 [7], и есть алгоритмы с лишними шагами только одного вида, например алгоритм АО2 [8]. Обзор в области синтеза асимптотически оптимальных алгоритмов перечисления неприводимых покрытий можно найти в [9].

В настоящей работе получены следующие результаты. Описана схема построения алгоритма типа АО2. Приведено описание алгоритма АО2 в рамках предложенной схемы. Показано, что для ответа на вопрос, является ли очередной шаг алгоритма типа АО2 лишним, необходимо решить NP-полную задачу. Предложены две модификации алгоритма АО2, названные АО2К и АО2М. Проведено тестирование алгоритмов АО2, АО2К и АО2М на случайных булевых матрицах.

1. Основные понятия и обозначения

Введём обозначение $E(L) = \{(i, j) : a_{ij} = 1, i \in \{1, \dots, m\}, j \in \{1, \dots, n\}\}$.

Два элемента (i, j) и (t, l) из $E(L)$ называются *совместимыми*, если $a_{il} = 0$, $a_{tj} = 0$. Набор $Q \subseteq E(L)$ называется *совместимым*, если любые два различных элемента (i, j) и (t, l) из Q совместимы. Пусть $B \subseteq E(L)$. Через $H(B)$ обозначается множество столбцов с номерами из множества $\{j : \exists i ((i, j) \in B)\}$.

Строка с номером i матрицы L называется *покрытой* совместимым набором Q , если эта строка в пересечении с хотя бы одним столбцом из $H(Q)$ даёт 1. Совместимый

набор Q называется *покрывающим*, если все строки L покрыты Q . Очевидно следующее утверждение.

Утверждение 1. Набор столбцов H является неприводимым покрытием тогда и только тогда, когда найдётся покрывающий набор Q , для которого $H(Q) = H$.

Следовательно, перечисляя все покрывающие наборы, можно построить множество $\mathcal{P}(L)$.

Покрывающий набор $Q = \{(i_1, j_1), \dots, (i_r, j_r)\}$ называется *верхним*, если для любого покрывающего набора $Q' = \{(t_1, j_1), \dots, (t_r, j_r)\}$ верны неравенства $t_u \geq i_u$, $u \in \{1, \dots, r\}$. Очевидно следующее утверждение.

Утверждение 2. Для любого неприводимого покрытия H существует единственный верхний набор Q , такой, что $H(Q) = H$.

Таким образом, задача перечисления неприводимых покрытий матрицы L может быть сведена к перечислению верхних наборов для матрицы L .

Алгоритм АО2 на каждом шаге строит очередной покрывающий набор Q . В случае, когда Q является верхним, происходит пополнение множества найденных неприводимых покрытий матрицы L набором столбцов $H(Q)$. В противном случае шаг считается лишним. Будем говорить, что алгоритм A имеет *тип АО2*, если A для поиска неприводимых покрытий перечисляет покрывающие наборы и выбирает среди них верхние наборы.

2. Общая схема построения алгоритмов типа АО2

Совместимый набор Q называется *правильным относительно* $B \subseteq E(L)$, если существует покрывающий набор $Q' \supseteq Q$, такой, что $Q' \setminus Q \subseteq B$.

Элемент $(i, j) \in B$ называется *запрещённым для* Q *относительно* B , если набор $Q' = Q \cup \{(i, j)\}$ либо не является совместимым, либо не является правильным относительно B . Обозначим через $\Delta(B, Q)$ множество запрещённых для Q относительно B элементов.

Конечная последовательность пар $\alpha = \{(B_1, Q_1), \dots, (B_l, Q_l)\}$ называется *траекторией*, если:

- 1) набор Q_t , $1 \leq t \leq l$, является правильным относительно $B_t \subseteq E(L)$;
- 2.1) либо B_t , $1 < t \leq l$, получается удалением одного или нескольких элементов из B_{t-1} , а Q_{t-1} не меняется, то есть $(B_t, Q_t) = (B_{t-1} \setminus A_t, Q_{t-1})$ для некоторого $A_t \neq \emptyset$, $A_t \subseteq B_{t-1}$;
- 2.2) либо Q_t , $1 < t \leq l$, получается добавлением к Q_{t-1} некоторого незапрещённого для Q_{t-1} относительно B_{t-1} элемента (i_t, j_t) , а набор B_t получается удалением из B_{t-1} элемента (i_t, j_t) , то есть $(B_t, Q_t) = (B_{t-1} \setminus \{(i_t, j_t)\}, Q_{t-1} \cup \{(i_t, j_t)\})$, где элемент $(i_t, j_t) \in B_{t-1} \setminus \Delta(B_{t-1}, Q_{t-1})$.

Траектория $\alpha = \{(B_1, Q_1), \dots, (B_l, Q_l)\}$ называется *законченной*, если $B_l = \emptyset$. При этом набор Q_l является покрывающим и называется *результатом* законченной траектории α .

Ясно, что для любого покрывающего набора Q можно построить хотя бы одну законченную траекторию, результат которой равен Q . То есть, перечисляя всевозможные законченные траектории, можно найти все покрывающие наборы. Однако число траекторий, как правило, значительно больше числа покрывающих наборов. Поэтому желательно исключить перечисление траекторий, приводящих к одним и тем же покрывающим наборам, но при этом не пропустить ни одного покрывающего набора.

Пусть последовательность $\alpha = \{(B_1, Q_1), \dots, (B_l, Q_l)\}$ является траекторией. Последовательность $\alpha_t^* = \{(B_1, Q_1), \dots, (B_{t-1}, Q_{t-1}), (B_t, Q_{t-1})\}$, $t \in \{2, \dots, l-1\}$, являющаяся траекторией, но не совпадающая с началом α , называется *альтернативной* траекторией для α . Последовательность α_t^* альтернативна для α в том и только в том случае, когда набор Q_{t-1} является правильным относительно B_t , и $Q_{t-1} \neq Q_t$.

Для α может не существовать ни одной альтернативной траектории. В случае, когда есть хотя бы одна альтернативная траектория для α , самая длинная из них называется *соседней* траекторией для α . Легко доказывается следующее полезное свойство соседних траекторий.

Утверждение 3. Пусть $\alpha_1, \dots, \alpha_r$ — упорядоченное семейство законченных траекторий, такое, что началом траектории α_u , $u \in \{2, \dots, r\}$, является соседняя траектория для α_{u-1} . Тогда результаты всех траекторий семейства различны.

Законченная траектория $\alpha = \{(B_1, Q_1), \dots, (B_l, Q_l)\}$ называется *реализацией*, если для всех $t \in \{2, \dots, l\}$ либо $Q_{t-1} \neq Q_t$, либо $(B_{t-1} \setminus B_t) \subseteq \Delta(B_{t-1}, Q_{t-1})$.

Алгоритм типа АО2 (общая схема)

Вход: L — булева матрица.

Н а ш а г е 1 проверить, является ли набор $\emptyset$ правильным относительно $E(L)$. Если не является, то закончить работу и вернуть результат $\mathcal{P}(L) = \emptyset$. В противном случае построить реализацию α_1 , начинающуюся с $(E(L), \emptyset)$. В случае, когда результат реализации α_1 — набор $Q^{(1)}$ — является верхним, пополнить множество решений неприводимым покрытием $H(Q^{(1)})$. В противном случае множество решений не пополняется. Перейти к шагу 2.

Пусть на шаге t построена траектория α_t .

Н а ш а г е $t+1$, $t \geq 1$ проверить, существует ли соседняя траектория для α_t . Если не существует, то закончить работу алгоритма. В противном случае взять соседнюю для α_t траекторию α^* . Построить реализацию α' , первый элемент которой совпадает с последним элементом α^* . Удалить из α^* последний элемент и добавить к ней элементы реализации α' . Полученная траектория α_{t+1} является законченной. В случае, когда результат реализации α_{t+1} — набор $Q^{(t+1)}$ — является верхним, пополнить множество решений неприводимым покрытием $H(Q^{(t+1)})$. В противном случае множество решений не пополняется. Перейти к шагу $t+2$.

Для обоснования корректности алгоритма, построенного по описанной схеме, достаточно показать, что каждый покрывающий набор строится на каком-либо шаге алгоритма и при этом один и тот же набор не строится на разных шагах.

Заметим, что реализация отличается от законченной траектории тем, что если при переходе от (B_{t-1}, Q_{t-1}) к (B_t, Q_t) набор Q_{t-1} не пополняется, то из B_{t-1} удаляются только запрещённые для Q_{t-1} относительно B_{t-1} элементы. Это свойство позволяет гарантировать, что ни один покрывающий набор не будет пропущен алгоритмом. Отсутствие повторов следует из утверждения 3.

Число шагов алгоритма равно числу покрывающих наборов матрицы L . Сложность шага складывается из сложности поиска соседней траектории и сложности построения реализации с заданным началом. Согласно [8], алгоритм, решающий указанные подзадачи на каждом шаге за полиномиальное время, является асимптотически оптимальным с полиномиальной задержкой для случая, когда размер входа удовлетворяет ограничению $\log m \leq (1 - \varepsilon) \log n$, $0 < \varepsilon < 1$.

Приведём описание асимптотически оптимального алгоритма АО2 в рамках предложенной схемы.

3. Алгоритм АО2

Пусть $B \subseteq E(L)$ и $(i, j) \in E(L)$. Обозначим через $\Delta_{ij}(B)$ набор элементов из B , не совместимых с (i, j) . Очевидно, если $(i, j) \in Q$, то $\Delta_{ij}(B) \subseteq \Delta(B, Q)$.

Пусть H — набор столбцов матрицы L . Строка с номером i называется *охватывающей* для строки с номером t относительно H , если для любого столбца из H с номером j выполняется неравенство $a_{ij} \geq a_{tj}$.

Пусть $B \subseteq E(L)$ и пусть не покрытая совместимым набором Q строка с номером i охватывает не покрытую Q строку с номером t относительно $H(B)$. Элемент $(i, j) \in B$, для которого $a_{tj} = 0$, является запрещённым для Q относительно B . Обозначим множество таких элементов через $\Delta^*(B, Q)$.

Процедура построения реализации в алгоритме АО2

Вход: (B_1, Q_1) — начало траектории.

Выполнить в цикле следующие шаги.

Шаг 1. Пусть построена траектория длины $t \geq 1$. Если $B_t = \emptyset$, то закончить цикл.

Шаг 2. Если $\Delta^*(B_t, Q_t) \neq \emptyset$, то построить $(B_{t+1}, Q_{t+1}) = (B_t \setminus \Delta^*(B_t, Q_t), Q_t)$ и продолжить цикл.

Шаг 3. Взять элемент (i, j) из B_t с наименьшим порядковым номером $m(j-1) + i$. Построить пару $(B_{t+1}, Q_{t+1}) = (B_t \setminus \{(i, j)\}, Q_t \cup \{(i, j)\})$.

Шаг 4. Если $\Delta_{ij}(B_{t+1}) \neq \emptyset$, то построить пару $(B_{t+2}, Q_{t+2}) = (B_{t+1} \setminus \Delta_{ij}(B_{t+1}), Q_{t+1})$. Продолжить цикл.

Процедура поиска соседней траектории в алгоритме АО2

Вход: $\alpha = \{(B_1, Q_1), \dots, (B_l, Q_l)\}$ — траектория.

Выполнить в цикле следующие шаги.

Шаг 1. Пусть текущая длина α равна t . Если $t \leq 1$, то вернуть ответ, что соседней траектории не существует.

Шаг 2. Если $t > 1$ и $Q_t = Q_{t-1}$, то удалить из α последний элемент и продолжить цикл.

Шаг 3. Проверить, что для любой не покрытой Q_{t-1} строки с номером i есть хотя бы один элемент $(i, j) \in B_t$. Если условие выполняется, то заменить в α последний элемент на пару (B_t, Q_{t-1}) и вернуть α . В противном случае удалить из α последний элемент и продолжить цикл.

Проведём анализ временной сложности шага алгоритма АО2. При поиске элементов множества $\Delta_{ij}(B)$ максимальное число просматриваемых элементов матрицы не превосходит mn . При поиске элементов множества $\Delta^*(B, Q)$ максимальное число просматриваемых элементов матрицы не превосходит m^2n (поиск охватывающих строк). Длина любой траектории не превосходит $3q$, где $q = \min\{m, n\}$. Поэтому время работы процедуры построения реализации равно $O(qm^2n)$. Время работы процедуры поиска соседней траектории равно $O(qmn)$. Проверка того, что покрывающий набор Q является верхним, осуществляется за $O(mn)$. Итак, временная сложность шага алгоритма АО2 составляет $O(qm^2n)$.

Проведём анализ затрат памяти алгоритма АО2. Прежде всего отметим, что алгоритм АО2 так же, как любой алгоритм, построенный по описанной выше схеме, относится к типу «построил и забыл». Это означает, что для работы алгоритма нет необходимости хранить все найденные ранее покрывающие наборы или неприводимые покрытия. Каждая траектория $\alpha = \{(B_1, Q_1), \dots, (B_l, Q_l)\}$ обладает свойством

$B_1 \supset \dots \supset B_l$ и $Q_1 \subseteq \dots \subseteq Q_l$. Поэтому α может быть закодирована в одной целочисленной матрице $D_\alpha = \|d_{ij}\|_{m \times n}$, элементы которой определяются следующим образом: $d_{ij} = 0$, $(i, j) \notin E(L)$; $d_{ij} = 0$, $(i, j) \in B_l$; $d_{ij} = -t$, $(i, j) \in Q_{t+1} \setminus Q_t$; $d_{ij} = t$, $(i, j) \in B_t \setminus B_{t+1}$. При таком представлении затраты памяти составляют $O(mn \log q)$ бит.

4. О перечислении верхних наборов

Строка матрицы L с номером t называется *конкурентной* для совместимого набора Q , если существует совместимый набор Q' , такой, что $H(Q) = H(Q')$, и для $(t, j) \in Q'$ и $(i, j) \in Q$ выполняется неравенство $i > t$. Ясно, что верхний набор Q не может иметь конкурентных строк.

Правильный относительно B набор Q называется *верным относительно B* , если существует верхний набор $Q' \supseteq Q$, такой, что $Q' \setminus Q \subseteq B$.

Привлекательной является идея строить при поиске покрывающего набора такую траекторию $\alpha = \{(B_1, Q_1), \dots, (B_l, Q_l)\}$, что набор Q_t , $t \in \{1, \dots, l\}$, является верным относительно B_t . Тогда при $B_l = \emptyset$ набор Q_l является верхним. Алгоритм, строящий такую траекторию за полиномиальное время от m и n , возвращал бы на каждом шаге очередное неприводимое покрытие с полиномиальной задержкой. Это эквивалентно тому, что исходя из траектории, построенной на текущем шаге, можно за полиномиальное время определить, является ли очередной шаг алгоритма лишним. Однако справедлива следующая теорема.

Теорема 1. Задача проверки того, является ли набор $Q \neq \emptyset$ верным относительно $E(L)$, NP-полна.

Доказательство. Пусть булева функция $f(x_1, \dots, x_N)$ задана конъюнктивной нормальной формой (КНФ) $C_1 \wedge \dots \wedge C_M$, где $C_1, \dots, C_M$ — элементарные дизъюнкции от переменных $x_1, \dots, x_N$.

Построим граф $G = (V, E)$, где множество V состоит из вершин $1, \emptyset, C_1, \dots, C_M, x_1, \dots, x_N, \bar{x}_1, \dots, \bar{x}_N$, и множество E состоит из рёбер четырёх типов:

- 1) рёбра для конъюнкций $\{1, C_1\}, \dots, \{1, C_M\}$;
- 2) вспомогательное ребро $\{1, \emptyset\}$;
- 3) рёбра для переменных $\{x_1, \bar{x}_1\}, \dots, \{x_N, \bar{x}_N\}$;
- 4) рёбра для вхождений переменных в конъюнкции: $\{C_i, x_j\}$, если x_j входит в C_i , и $\{C_i, \bar{x}_j\}$, если $\bar{x}_j$ входит в C_i .

Пусть L — матрица инцидентности графа G и столбцы с номерами $1, \dots, M+2$ соответствуют вершинам $1, \emptyset, C_1, \dots, C_M$, а строки с номерами $1, \dots, M, M+1$ — рёбрам $\{1, C_1\}, \dots, \{1, C_M\}, \{1, \emptyset\}$.

Набор $Q = \{(M+1, 1)\}$ является правильным относительно $E(L)$. Требуется определить, является ли Q верным относительно $E(L)$.

Набор Q покрывает строки с номерами $1, \dots, M, M+1$, при этом строки с номерами $1, \dots, M$ являются конкурентными. Поэтому если верхний набор Q' содержит Q , то в $H(Q')$ должны входить столбцы с номерами $3, \dots, 2+M$, чтобы строки с номерами $1, \dots, M$ не были конкурентными для Q' . Из этого следует, что $Q' \supset \{(i_1, 3), \dots, (i_M, 2+M)\}$, где для любого $l \in \{1, \dots, M\}$ строка с номером i_l соответствует либо ребру $\{C_l, x_{s_l}\}$, либо ребру $\{C_l, \bar{x}_{s_l}\}$.

При этом Q' покрывает соответствующие рёбрам $\{x_1, \bar{x}_1\}, \dots, \{x_N, \bar{x}_N\}$ строки тогда и только тогда, когда среди номеров строк $i_1, \dots, i_M$ нет двух таких i_u, i_v , что строка с номером i_u соответствует ребру $\{C_u, x_{s_u}\}$, а строка с номером i_v — ребру $\{C_v, \bar{x}_{s_v}\}$, и $s_u = s_v$.

Таким образом, существование верхнего набора $Q' \supset Q$ равносильно существованию набора значений переменных $x_1, \dots, x_N$, для которого истинны все элементарные дизъюнкции $C_1, \dots, C_M$, а следовательно, выполнима функция $f(x_1, \dots, x_N)$.

В результате задача проверки выполнимости функции, заданной КНФ, полиномиально сведена к задаче проверки верности правильного набора Q относительно $E(L)$. Как известно, задача проверки выполнимости КНФ NP-полна. ■

Обозначим $E_t(L)$, $t \in \{1, \dots, m\}$, множество элементов $\{(i, j) \in E(L) : a_{ij} = a_{tj} = 1\}$.

Повысить эффективность алгоритма АО2 позволяет осуществление при построении реализации проверки выполнения следующего необходимого условия верности набора.

Утверждение 4. Пусть Q — верный относительно $B \subseteq E(L)$ набор. Тогда для каждой не покрытой Q или конкурентной для Q строки с номером t выполняется $E_t(L) \cap B \neq \emptyset$.

Теперь, если в процедуре построения реализации в алгоритме АО2 всякий раз останавливаться, как только в траекторию была добавлена пара (B_t, Q_t) , не удовлетворяющая необходимому условию утверждения 4, то, во-первых, часть траекторий будет короче, а во-вторых, число шагов алгоритма будет меньше. Эксперименты показали, что, как правило, снижение числа шагов, а следовательно, и времени выполнения алгоритма довольно существенно.

5. Модификации алгоритма АО2

Опишем две модификации алгоритма АО2, названные АО2К и АО2М. Алгоритмы АО2К и АО2М полностью вписываются в общую схему построения алгоритма типа АО2. Отличия от АО2 появляются только в процедуре построения реализации.

Процедура построения реализации в алгоритме АО2К

Вход: (B_1, Q_1) — начало траектории.

Выполнить в цикле следующие шаги.

Шаг 1. Пусть построена траектория длины $t \geq 1$. Если $B_t = \emptyset$, то закончить цикл.

Шаг 2. Если пара (B_t, Q_t) не удовлетворяет необходимому условию утверждения 4, то закончить цикл.

Шаг 3. Если $\Delta^*(B_t, Q_t) \neq \emptyset$, то построить $(B_{t+1}, Q_{t+1}) = (B_t \setminus \Delta^*(B_t, Q_t), Q_t)$ и продолжить цикл.

Шаг 4. Если у набора Q_t есть хотя бы одна конкурентная строка, то найти конкурентную строку с наименьшим номером r и взять элемент (i, j) из $E_r(L) \cap B_t$ с наименьшим порядковым номером $m(j-1) + i$. В противном случае взять элемент (i, j) из B_t с наименьшим порядковым номером $m(j-1) + i$. Построить пару $(B_{t+1}, Q_{t+1}) = (B_t \setminus \{(i, j)\}, Q_t \cup \{(i, j)\})$.

Шаг 5. Если $\Delta_{ij}(B_{t+1}) \neq \emptyset$, то построить $(B_{t+2}, Q_{t+2}) = (B_{t+1} \setminus \Delta_{ij}(B_{t+1}), Q_{t+1})$. Продолжить цикл.

Предположим, что на вход процедуре построения реализации в алгоритме АО2К поступает набор Q_1 , не являющийся верным относительно B_1 . Чем раньше при построении реализации предпринимаются попытки покрыть конкурентные строки, тем быстрее обнаруживается, что набор Q_1 не является верным относительно B_1 . Стратегия алгоритма АО2К характеризуется как «борьба с конкурентными строками».

Процедура построения реализации в алгоритме АО2М

Вход: (B_1, Q_1) — начало траектории.

Выполнить в цикле следующие шаги.

Шаги 1–3 и 5 не отличаются от соответствующих шагов процедуры построения реализации в алгоритме АО2К.

Шаг 4. Найти номер r не покрытой Q_t или конкурентной для Q_t строки с наименьшим числом элементов в пересечении $E_r(L) \cap B_t$. Взять элемент (i, j) из $E_r(L) \cap B_t$ с наименьшим порядковым номером $m(j-1) + i$. Построить $(B_{t+1}, Q_{t+1}) = (B_t \setminus \{(i, j)\}, Q_t \cup \{(i, j)\})$.

Набор $Q_{t+1} = Q_t \cup \{(i, j)\}$ покрывает строку с номером r , только если $(i, j) \in E_r(L) \cap B_t$. На качественном уровне понятно, что чем меньше множество $E_r(L) \cap B_t$, тем «сложнее» строка с номером r для покрытия наборами строящейся реализации. Стратегия алгоритма АО2М характеризуется как «от сложного к простому». Оправдана эта стратегия тем, что результат реализации должен покрывать все, в том числе и «сложные» строки, а покрыть «простые» строки, вероятнее всего, получится и позднее, даже тогда, когда в множестве B_t будет меньше элементов.

В количественном отношении выигрыш алгоритма АО2М по сравнению с алгоритмами АО2 и АО2К проявляется следующим образом. Представим естественным образом каждую траекторию в виде простой цепи. Объединим все простые цепи траекторий, построенных алгоритмом, в один граф. Полученный граф, очевидно, является деревом и далее называется деревом решений алгоритма. Эксперименты показали, что число вершин и рёбер дерева решений, строящегося алгоритмом АО2М при дуализации матрицы L , как правило, меньше, чем соответственно число вершин и рёбер дерева решений, строящегося алгоритмом АО2 или АО2К при дуализации той же матрицы L .

6. Результаты экспериментов

Проведено тестирование алгоритмов АО2, АО2К и АО2М на случайных матрицах, для которых выполняется $50 \leq mn \leq 500$. Для каждой матрицы и каждого алгоритма измерялись:

- 1) T — время перечисления всех неприводимых покрытий;
- 2) $\delta_{\max}$ — максимальное время получения очередного неприводимого покрытия;
- 3) N — число узлов дерева решений;
- 4) N_0 — число лишних шагов алгоритма.

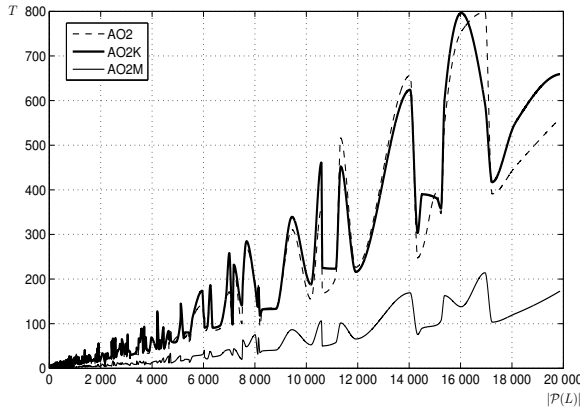
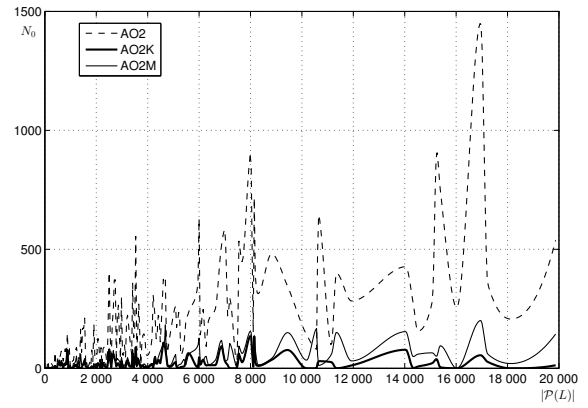
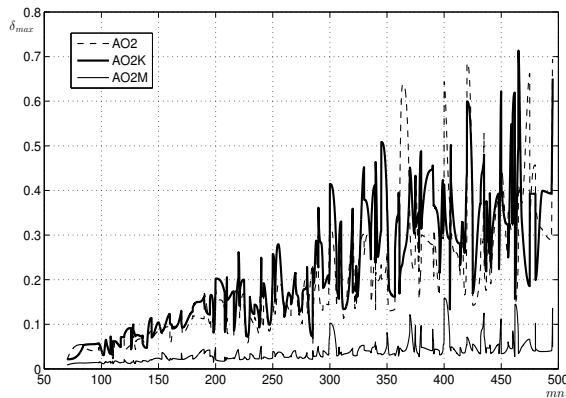
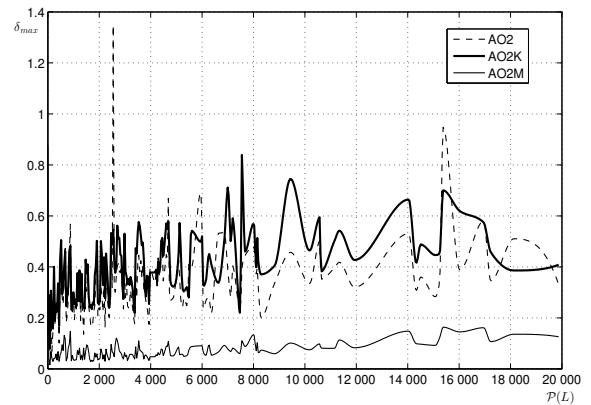
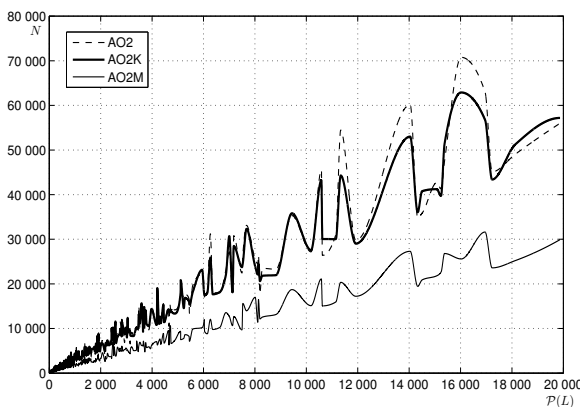
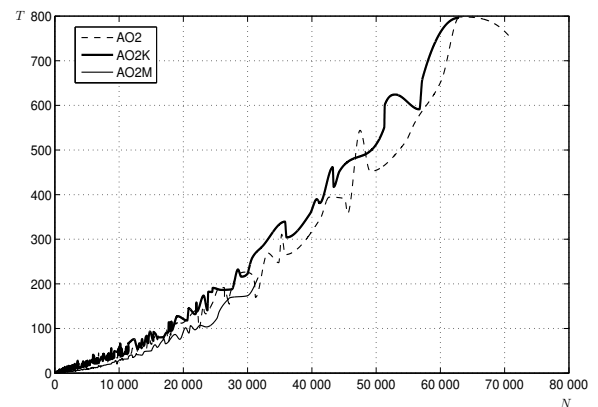
Результаты счёта приведены на рис. 1–6.

На рис. 1 видно, что алгоритм АО2М работает быстрее алгоритмов АО2 и АО2К. В среднем скорость АО2М в 4 раза больше скорости АО2. По показателю $\delta_{\max}$ алгоритм АО2М также лидирует (рис. 3 и 4). Скорость работы АО2К сравнима со скоростью АО2.

Анализ числа лишних шагов показывает, что алгоритмы АО2К и АО2М почти всегда делают меньше лишних шагов, чем алгоритм АО2 (рис. 2). Однако наименьшее значение этого показателя у модификации АО2К.

Заметим, что зависимости полного времени дуализации от числа узлов дерева решений у алгоритмов АО, АО2К и АО2М имеют довольно схожий характер (рис. 6). Число узлов дерева решений при росте числа неприводимых покрытий медленней всего увеличивается у алгоритма АО2М (рис. 5). По-видимому, число узлов дерева решений в большей степени влияет на время работы алгоритма, нежели число лишних шагов алгоритма.

Полученные выводы разнятся с первоначальными представлениями о факторах, влияющих на производительность алгоритма АО2. Предполагалось, что построенные модификации позволят снизить временные затраты на дуализацию за счёт уменьшения числа лишних шагов алгоритма. Однако оказалось, что значительное увеличение скорости дуализации достигается именно за счёт сокращения числа узлов дерева решений.

Рис. 1. Зависимость T от $|P(L)|$ Рис. 2. Зависимость N_0 от $|P(L)|$ Рис. 3. Зависимость $\delta_{\max}$ от mn Рис. 4. Зависимость $\delta_{\max}$ от $|P(L)|$ Рис. 5. Зависимость N от $|P(L)|$ Рис. 6. Зависимость T от N

Заключение

В работе используется подход к построению алгоритмов дуализации, эффективных в «типичном случае», в основе которого лежит понятие асимптотически оптимального алгоритма с полиномиальной задержкой.

В качестве отправной точки рассматривается асимптотически оптимальный алгоритм АО2, который на каждом шаге за полиномиальное время строит неприводимое покрытие, но построенное покрытие может совпадать с найденными на предыдущих шагах. Фактически, в алгоритме АО2 перечисление неприводимых покрытий сводится к перечислению покрывающих наборов единичных элементов матрицы. Каждому неприводимому покрытию соответствует единственный верхний покрывающий набор. Шаг, результат которого не является верхним набором, считается лишним.

Покрывающий набор строится последовательным добавлением единичных элементов матрицы. Алгоритм АО2 добавляет элементы в порядке возрастания их порядковых номеров. Предложены две модификации данного алгоритма, основное отличие которых от АО2 в стратегии выбора очередного добавляемого единичного элемента. Тестирование алгоритмов АО2, АО2К и АО2М показало, что внесённые в первоначальный алгоритм изменения позволяют снизить временные затраты дуализации за счёт уменьшения числа узлов дерева решений.

ЛИТЕРАТУРА

1. Johnson D., Yannakakis M., and Papadimitriou C. On generating all maximal independent sets // Inform. Process. Lett. 1988. V.27. No.3. P.119–123. URL: <http://www.sciencedirect.com/science/article/pii/0020019088900658>.
2. Eiter T., Gottlob G., and Makino K. New results on monotone dualization and generating hypergraph transversals // SIAM J. Comput. 2003. V.32. No.2. P.514–537.
3. Boros E. and Elbassioni K. Generating maximal independent sets for hypergraphs with bounded edge-intersections // LATIN 2004: Theoretical Informatics. Berlin; Heidelberg: Springer, 2004. P.488–498. URL: <http://www.springerlink.com/index/b9t9wx6ue9t9hvw3.pdf>.
4. Boros E., Gurvich V., Elbassioni K., and Khachiyan L. An efficient incremental algorithm for generating all maximal independent sets in hypergraphs of bounded dimension // Parallel Process. Lett. 2000. V.10. No.4. P.253–266. URL: <http://www.worldscientific.com/doi/abs/10.1142/S0129626400000251>.
5. Fredman M. L. and Khachiyan L. On the complexity of dualization of monotone disjunctive normal forms // J. Algorithms. 1996. V.21. P.618–628.
6. Khachiyan L., Boros E., Elbassioni K., and Gurvich V. An efficient implementation of a quasi-polynomial algorithm for generating hypergraph transversals and its application in joint generation // Discr. Appl. Math. 2006. V.154. No.16. P.2350–2372. URL: <http://linkinghub.elsevier.com/retrieve/pii/S0166218X06001910>.
7. Дюкова Е. В. Об асимптотически оптимальном алгоритме построения тупиковых тестов // ДАН СССР. 1977. Т.233. №4. С.527–530.
8. Дюкова Е. В. О сложности реализации дискретных (логических) процедур распознавания // Журн. вычисл. матем. и матем. физики. 2004. Т.44. №3. С.562–572.
9. Дюкова Е. В., Инякин А. С. Асимптотически оптимальное построение тупиковых покрытий целочисленной матрицы // Математические вопросы кибернетики. 2008. Т.17. С.235–246.
10. Дюкова Е. В., Сотнезов Р. М. О сложности задачи дуализации // Журн. вычисл. матем. и матем. физ. 2012. Т.52. №10. С.1926–1935.

PIPELINING COMBINATIONAL CIRCUITS

Yu. V. Pottosin, S. N. Kardash

*United Institute of Informatics Problems of NAS of Belarus, Minsk, Belarus***E-mail:** pott@newman.bas-net.by

For a multilevel combinatorial circuit, the problem of increasing its performance is considered. The problem is to divide the circuit into a given number of cascades and to connect them via registers providing pipeline-wise development of incoming signals. The frequency of incoming signals is established in the process of dividing the circuit. This frequency must be as high as possible. To solve this problem a model based on the representation of the circuit in the form of a directed graph is used.

Keywords: *combinational circuit, pipelining, directed graph.*

Introduction

Increasing throughput of information processing systems attracts the great attention of specialists in appropriate fields. One of the ways to increase the throughput is application of the pipeline structure [1]. Such a system is formed by several independent processors connected between each other so that the output from one processor is an input for another one. The processors form an information pipeline. The output processor produces results after short time intervals, but the real time for passing the information flow through the pipeline can be rather long.

The principle of pipelining is used effectively when the nature of information processing is a sequence of operations each of which consists of a sequence of stages [2, 3]. To start execution of the next operation one should not wait for finish of the whole previous operation. It is enough to finish only the first stage of the previous operation. In the pipeline with r successive stages, if the i -th operation passes the s -th stage, then $(i + k)$ -th operation can pass the $(s - k)$ -th stage where $1 \leq s$, $s - k \leq r$.

In constructing the systems of digital signal processing in real-time mode, the systolic principle of computing had been widely extended [4, 5]. One unified VLSI element is developed, and an array of elements of that type is built. The elements act concurrently fulfilling the base operation. After fulfilling that operation, output data are passed synchronously from one element to its neighbors through all the local connections.

In this paper, we try to find out the way to increase the throughput of a multilevel combinational circuit by pipelining.

1. Statement of the problem

In a multilevel combinational circuit, the delay is summed up of delays of elements in the longest chain. Let a sequence of p sets of binary signals is put at the input of a combinational circuit. If T is the delay time of the circuit, then the time period of changing input signals cannot be less than T . So, the response of the circuit to this sequence will appear at least in pT times. Let us partition the circuit into k cascades $C_1, C_2, \dots, C_k$. If τ_C is the delay time of the most slow cascade, then $T \leq k\tau_C$. Let us put memory elements (triggers of D type) at the outputs of every cascade that transmit signals from the cascades by a clock signal. The same clock signal determines the time period of the signal change at the input of the circuit. This time period, τ_{clock} , cannot be less than the sum of two delay

times: τ_C and delay time τ_D of the memory element ($\tau_{\text{clock}} \geq \tau_C + \tau_D$). Now, the time of the response to the mentioned sequence of length p is $(k + p)\tau_{\text{clock}}$.

Figure 1 shows an example of partitioning a circuit into three cascades. The borders between cascades are indicated by hatches. The modules used in the circuit at Fig. 1 are in the library of CMOS cells for custom VLSI design [6].

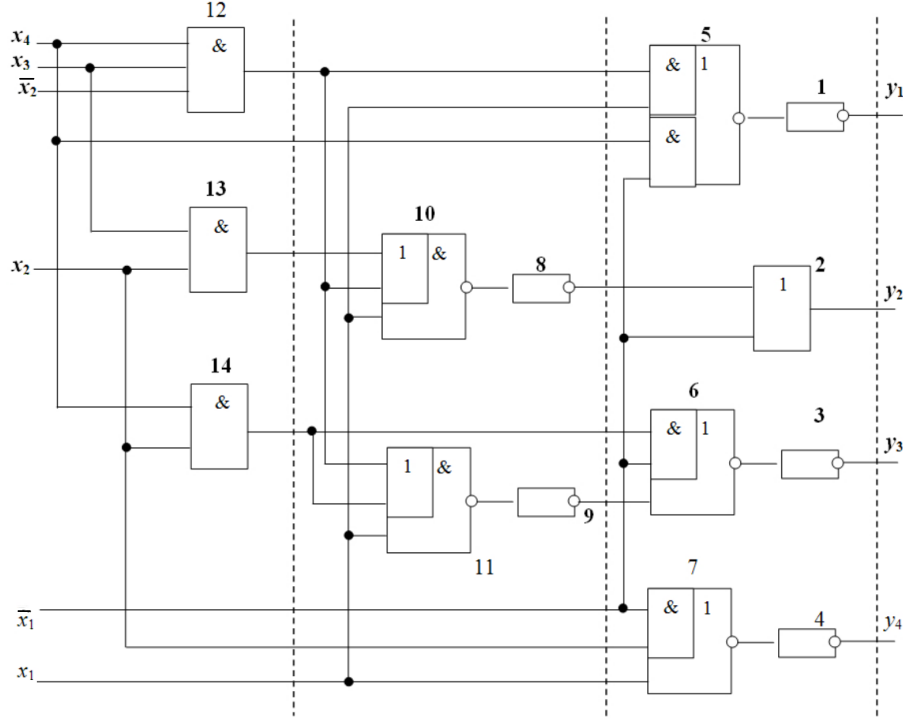


Fig. 1. Circuit with indicated cascades.

The lower bound of the length p of the sequence of binary signals sets at the input of the circuit, at which the signal processing accelerates, is defined by inequality

$$(k + p)\tau_{\text{clock}} < pT, \quad (1)$$

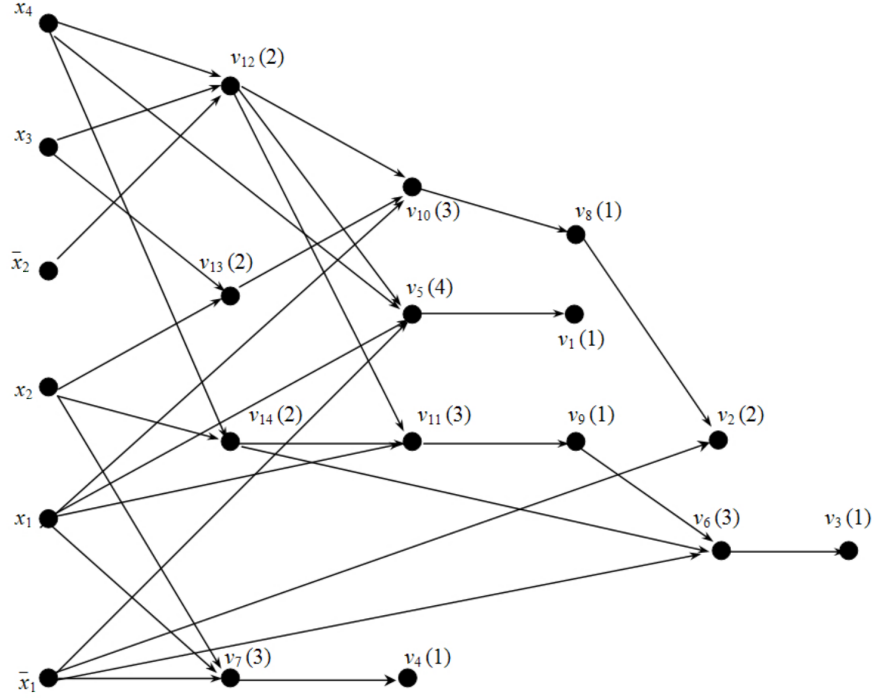
where T is the delay time of the initial circuit. Taking into consideration that $\tau_{\text{clock}} \geq \tau_C + \tau_D$, we have

$$p > \frac{k\tau_{\text{clock}}}{T - \tau_{\text{clock}}} \geq \frac{k(\tau_C + \tau_D)}{T - \tau_C - \tau_D}. \quad (2)$$

So, the given circuit should be partitioned into a demanded number k of cascades in order to provide maximum throughput at the described pipeline mode.

2. Model of a combinational circuit

To represent a combinational circuit, it is convenient to use, as a model, a directed graph (digraph) $G = (V, A)$ with the set V of vertices and the set A of arcs. The vertices of the digraph correspond to the logical elements and input pins of the circuit, and the arcs indicate directions of signals from outputs of certain elements to inputs of other ones. Figure 2 shows the model of the circuit at Fig. 1. The indices at the vertices at Fig. 2 coincide with the numbers of correspondent elements of the circuit at Fig. 1.

Fig. 2. Digraph G .

The digraph G has no circles. Its every vertex $v \in V$ is assigned with the weight $\tau(v)$ that is the delay of the corresponding element. The weights may be integers proportional to element delay times. The vertices corresponding to the circuit input pins have the weight equalled zero. The weights of vertices of G at Fig. 2 are indicated by the numbers in parentheses. Here, we consider that the more complicated the Boolean function implemented by an element, the longer delay that the element has.

3. Partitioning a circuit into layers

Let us construct the sequence of layers, $L_1, L_2, \dots, L_m$, being an ordered partition of the set V in the digraph G with the property that if a vertex v is in the semi-neighborhood of outcome $N^+(u)$ of a vertex u , then v and u are in different layers, and the layer containing u precedes (not necessary directly) the layer containing v . If the path lengths from the circuit input to its outputs are different, then this partition is not unique. The variant of partitioning the circuit into layers should be selected so that the sum of weights of all layers would be as small as possible. The weight of a layer means the maximum vertex weight in the layer.

Two types of vertices of the digraph G can be distinguished. The vertices of one type lie on the longest paths of G . They are distributed strictly among the layers and cannot change their positions. We call such a vertex *immovable*. The positions of the vertices of the other type called *movable* can change within the certain bounds; say from a layer L_l to a layer L_r ($l < r$). These bounds are rather easy to establish. It is enough to execute Algorithm 1 below for the given digraph G and for the digraph G^c obtained from G by reversing the directions of all the arcs and to change the order of the layers for inverse one in the sequence obtained for G^c . The following designations are accepted in Algorithm 1: $N^-(v)$ and $N^+(v)$ are, correspondingly, semi-neighborhood of income and semi-neighborhood of outcome of a vertex v ; L_i is the i -th layer, m is the number of layers.

Algorithm 1

- 1) $L_1 := \{v : N^-(v) = \emptyset\}$, $i := 1$;
- 2) $i := i + 1$, $L_i := \bigcup_{v \in L_{i-1}} N^+(v)$. If $L_i \neq \emptyset$, go to 2, otherwise $j := i$, $m := i := i - 1$;
- 3) $i := j := j - 1$. If $j = 1$, go to 5, otherwise
- 4) $i := i - 1$. If $i = 1$, go to 3, otherwise $L_i := L_i \setminus L_j$, go to 4;
- 5) End.

Each immovable vertex will be in the same layer of the sequences for G and G^c . For a movable vertex, the “left” layer L_l is that obtained by executing Algorithm 1 over digraph G and the “right” layer L_r is that obtained by executing Algorithm 1 over digraph G^c .

The distributions of vertices among layers being the results of applying Algorithm 1 to digraph G and to digraph G^c are shown in Fig. 2 and in Fig. 3, correspondingly. The layers are represented in these figures by vertical rows of vertices. The layers $L_1 = \{x_1, \bar{x}_1, x_2, \bar{x}_2, x_3, x_4\}$, $L_2 = \{v_7, v_{12}, v_{13}, v_{14}\}$, $L_3 = \{v_4, v_5, v_{10}, v_{11}\}$, $L_4 = \{v_1, v_8, v_9\}$, $L_5 = \{v_2, v_6\}$, $L_6 = \{v_3\}$ are obtained for digraph G , and $L_1 = \{x_2, \bar{x}_2, x_3, x_4\}$, $L_2 = \{x_1, v_{12}, v_{14}\}$, $L_3 = \{v_{11}, v_{13}\}$, $L_4 = \{\bar{x}_1, v_9, v_{10}\}$, $L_5 = \{v_5, v_6, v_7, v_8\}$, $L_6 = \{v_1, v_2, v_3, v_4\}$ for digraph G^c . The vertices $\bar{x}_2, x_2, x_3, x_4, v_3, v_6, v_9, v_{11}, v_{12}$ and v_{14} are immovable. They form sublayers $L'_1 = \{x_2, \bar{x}_2, x_3, x_4\}$, $L'_2 = \{v_{12}, v_{14}\}$, $L'_3 = \{v_{11}\}$, $L'_4 = \{v_9\}$, $L'_5 = \{v_6\}$ and $L'_6 = \{v_3\}$ with weights 0, 2, 3, 1, 3 and 1, correspondingly.

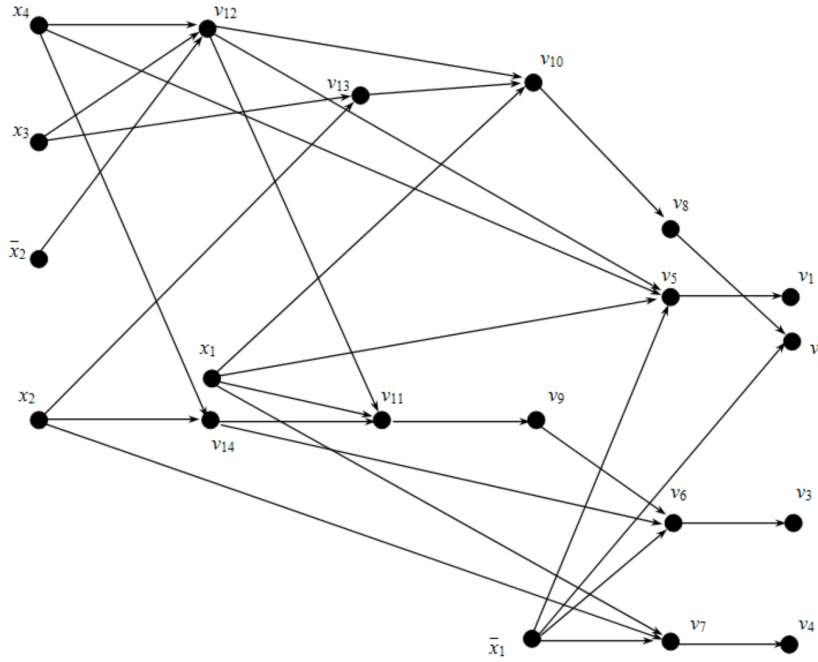


Fig. 3. Distribution of vertices among layers obtained by applying Algorithm 1 to G^c .

The rest of vertices ($x_1, \bar{x}_1, v_1, v_2, v_4, v_5, v_7, v_8, v_{10}, v_{13}$) are movable, and as it is shown above for each of them there exists the nonempty set of layers where the vertex can be. Vertex x_1 can be in layers L_1 and L_2 ; $\bar{x}_1$ in L_1, L_2, L_3 and L_4 ; v_1 in L_4, L_5 and L_6 ; v_2 in L_5 and L_6 ; v_4 in L_3, L_4, L_5 and L_6 ; v_5 in L_3, L_4 and L_5 ; v_7 in L_2, L_3, L_4 and L_5 ; v_8 in L_4 and L_5 ; v_{10} in L_3 and L_4 ; v_{13} in L_2 and L_3 . But the positions of some vertices may depend on the positions of other ones. In particular, the vertices connected with an arc cannot be in the same layer.

We suggest the following technique to distribute the vertices among layers so that the sum of the layer weights becomes possibly minimal. Having removed the immovable vertices and their incident arcs from G , we obtain digraph H where we choose a vertex of maximum

weight in each component of H . We put this vertex v in one of the layers of maximum weight that is acceptable for v . After this, the bounds of the vertex positions will change, and some movable vertices will become immovable. The further distribution of the vertices among the layers can be made for each component of H in the same way.

Figure 4 shows the digraph H with one component from the example on consideration. The vertices x_1 and $\bar{x}_1$ with zero weights can be put in any layer. According to the above technique, we put the vertex v_5 of maximum weight in the layer L_3 . Finally, we obtain $L_1 = \{x_1, \bar{x}_1, x_2, \bar{x}_2, x_3, x_4\}$, $L_2 = \{v_{12}, v_{13}, v_{14}\}$, $L_3 = \{v_5, v_7, v_{10}, v_{11}\}$, $L_4 = \{v_1, v_4, v_8, v_9\}$, $L_5 = \{v_2, v_6\}$ and $L_6 = \{v_3\}$.

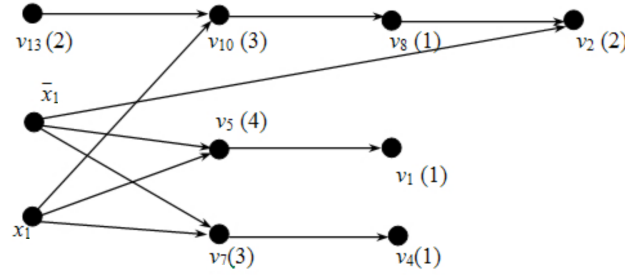


Fig. 4. Digraph H .

4. Equalization of paths in a digraph

Let us make all the lengths of paths in a digraph be equal by adding new vertices of zero weight. As a result, the initial digraph $G = (V, A)$ is transformed into digraph $G' = (V', A')$. New vertices are added to layers in G so that $N^+(v) \subseteq L_{i+1}$ for any $v \in L_i$, $i = 1, 2, \dots, m-1$, the vertex accessibility being kept. Here the vertex accessibility means that in any path from any vertex $v \in V$ to $u \in V$ in digraph G' , the sequence of vertices from V is the same as the sequence of vertices in the corresponding path in G . The new vertices are assigned with zero weight. To do it, Algorithm 2 is used. The digraph G' obtained from G in such a way is shown in Fig. 5 where the new vertices are indicated by light circles.

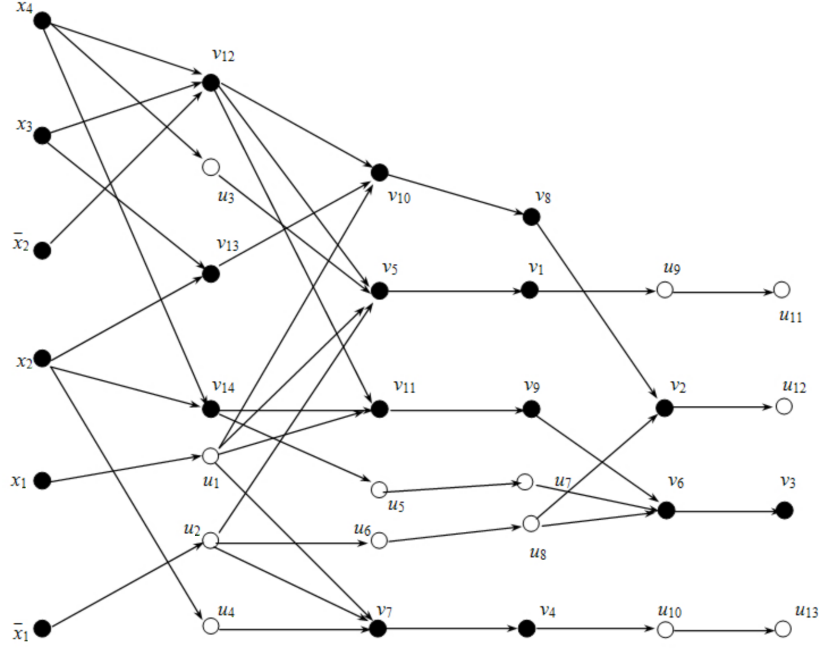
Algorithm 2

- 1) $i := 0, j := 0; U := \emptyset;$
- 2) $i := i + 1$. If $i = m$, go to 4, otherwise $L := L_i$;
- 3) If $L = \emptyset$, go to 2, otherwise choose $v \in L$, $L := L \setminus \{v\}$, $A := N^+(v) \setminus L_{i+1}$.
If $A = \emptyset$, go to 3, otherwise $j := j + 1$, $U := U \cup \{u_j\}$, $N^+(v) := (N^+(v) \cap L_{i+1}) \cup \{u_j\}$,
 $N^+(u_j) := A$, $L_{i+1} := L_{i+1} \cup \{u_j\}$, go to 3;
- 4) End.

5. Partitioning a circuit into cascades

Every layer of a circuit has a set of weights assigned to vertices belonging to the layer. The maximum weight in the layer is the delay of passing signal through it. A given combinational circuit must be partitioned into a fixed number k of *cascades*, the delay in the slowest cascade being minimal as possible. Each cascade is an ordered set of layers. The following problem arises. A similar problem is considered in [7].

A sequence $(a_1, a_2, \dots, a_n)$ of positive numbers is given. A part of it in the form $(a_p, a_{p+1}, \dots, a_q)$ where $1 \leq p < q \leq n$ is called segment. A given sequence must be partitioned into a fixed number k of segments $B_1, B_2, \dots, B_k$ where $B_i = (a_{n_{i-1}+1}, \dots, a_{n_i})$, $i = 1, 2, \dots, k$, $n_0 = 0$, $n_k = n$, with the following properties. Segments $B_1, B_2, \dots, B_k$ correspond to $S_1, S_2, \dots, S_k$ where $S_i = \sum_{a_j \in B_i} a_j$, and $\max\{S_1, S_2, \dots, S_k\}$ must be minimal.


 Fig. 5. Digraph G' with equalized paths.

The elements $S_1, S_2, \dots, S_k$ correspond to the desired cascades of the given circuit, and each of them is proportional to the delay of the corresponding cascade.

We suggest the following method to obtain a solution for this task next to optimal.

First, the lower bound of the largest delay in a cascade is determined as $b = \left(\sum_{j=1}^n a_j \right) / k$.

The current i -th segment is formed by accumulation of the sum $S_i = \sum_{a_j \in B_i} a_j$ comparing it with the bound b . When $S_i > b$ after adding next a_j to the sum S_i , the rightmost element in B_i is a_j if $b - (S_i - a_j) > S_i - b$, and a_{j-1} otherwise. The procedure is repeated for the rest of the sequence $(a_1, a_2, \dots, a_n)$.

Below, Algorithm 3 is given. It solves this problem when $\left(\sum_{j=1}^k S_j \right) / k > a_i$ for any $i = 1, 2, \dots, n$. The sequence $n_1, n_2, \dots, n_k$ represents a solution of the problem where n_i is the number of the rightmost element of i -th segment. In Algorithm 3, the symbols τ , S and B denote the maximal delay in a cascade, average value of S_i and the current value of S_i , correspondingly.

Algorithm 3

- 1) $i := 0, R := 0, \tau := 0, l := k, n_k := n$;
- 2) If $i = n$, go to 3, otherwise $i := i + 1, R := R + a_i$, go to 2;
- 3) $S := R/l, i := 0, B := 0, j := 1$;
- 4) $i := i + 1$. If $i = n$, go to 6,
 otherwise $C := B, B := B + a_i$. If $S > B$, go to 4,
 otherwise $D := S - C, E := B - S$.
 If $D < E$, then $j := j + 1, n_j := i - 1, B := a_i$, go to 5,
 otherwise $j := j + 1, n_j := i, C := B, B := 0$;
- 5) $l := l - 1, R := R - C, S := R/l$. If $\tau < C$, then $\tau := C$, go to 4,
 otherwise go to 4;
- 6) End.

In the considered example, the sequence of numbers (0, 2, 4, 1, 3, 1) represents the delays in the layers. Suppose this sequence must be partitioned into three segments ($k = 3$, $n = 6$). The result of execution of Algorithm 3 is the sequence $(n_1, n_2, n_3) = (2, 3, 6)$, and the maximal cascade delay is 5.

The triggers must be in the circuit after the second, third and sixth layers at each of the rightmost element of every cascade. The digraph transformed appropriately is shown in Fig. 6 where the vertices corresponding to triggers are marked with d_i . The vertices representing fictive elements with zero delay must be removed from the digraph.

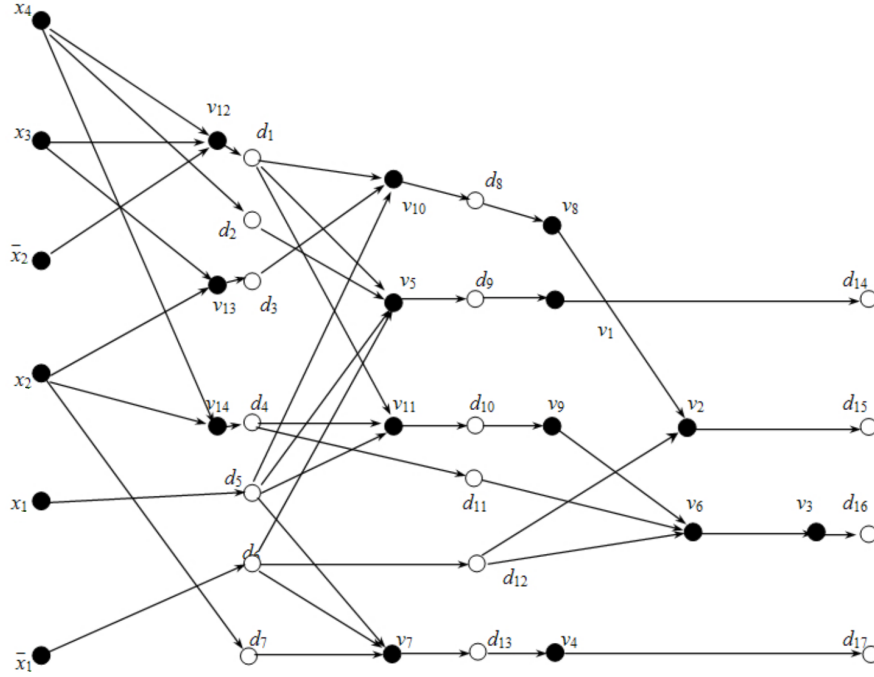


Fig. 6. Digraph with vertices corresponding to triggers.

Figure 7 shows the circuit working in the pipeline mode as a result of transformation of the circuit at Fig. 1. The inverse outputs of triggers are used instead of invertors in Fig. 7.

Suppose, the trigger delay is four conventional units of time that are used for estimate of cascade delay in the circuit from the considered example. The delay of the slowest cascade is equal to 5. So, the clock time period must be at least 9. According to the formula (2) the acceleration of signal processing can be reached when the length of the input sequence is at least 14. The complete reaction of the initial circuit to such a sequence will be after 154 conventional units of time, while the pipelined circuit will produce the reaction after 153 units. It is seen from the formula (1) that the difference between these values will increase if the length of input sequence increases.

Conclusion

The suggested approach to increasing the throughput of a combinational circuit is intended for its application to ready circuits, and it solves this task at the level of circuit technology. Perhaps, the more effect can be reached at the functional level. But in this case, it is necessary to design the circuit from the start, having its functional description.

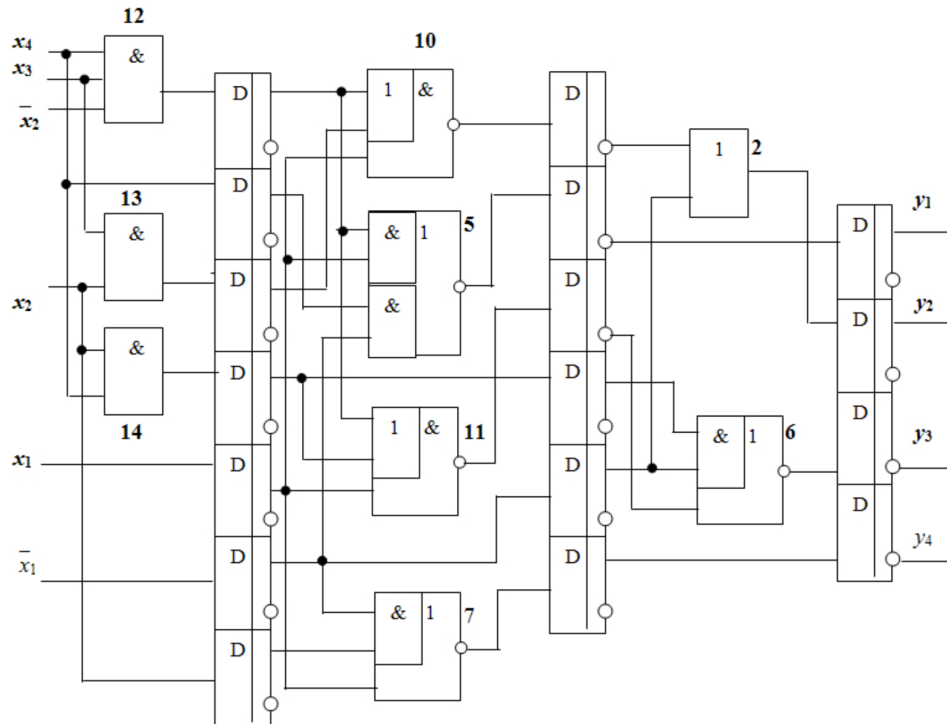


Fig. 7. Circuit working in pipeline mode.

BIBLIOGRAPHY

1. Kagan B. M. and Kanevskij M. M. Digital Computers and Systems. Moscow: Energiya, 1973. 680 p. (in Russian).
2. Voevodin V. B. Mathematical Models and Methods in Concurrent Processes. Moscow: Nauka, 1986. 296 p. (in Russian).
3. Kapitonova Yu. V. and Letichevskij A. A. Mathematical Theory of Computing System Design. Moscow: Nauka, 1988. 296 p. (in Russian).
4. Kukharev G. A., Tropchenko A. Yu., and Shmerko V. P. Systolic Processors for Signal Processing. Minsk: Belarus, 1988. 127 p. (in Russian).
5. Kukharev G. A., Shmerko V. P., and Zaitseva E. N. Algorithms and Systolic Processors for Multivalued Data Processing. Minsk: Navuka i Tekhnika, 1990. 296 p. (in Russian).
6. Lukoshko G. and Konnov E. CMOS-base array chips of K1574 series // Radiolyubitel. 1997. No. 9. P. 39–40 (in Russian).
7. Agibalov G. P. and Belyaev V. A. Technique for Solving Combinatorial Logical Tasks by the Method of Shortcut Bypassing of a Search Tree. Tomsk: TSU, 1981. 126 p. (in Russian).

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

DOI 10.17223/20710410/23/13

УДК 519.17

ПРИМЕНЕНИЕ КА-МОДЕЛИ ДЛЯ ИССЛЕДОВАНИЯ ВЛИЯНИЯ
ЗАГРЯЗНЕНИЙ НА ДИНАМИКУ ПОПУЛЯЦИЙ ГОЛОМЯНОК
И МАКРОГЕКТОПУСА В ОЗЕРЕ БАЙКАЛ¹

И. В. Афанасьев

*Институт вычислительной математики и математической геофизики, г. Новосибирск,
Россия***E-mail:** ivafanas@gmail.com

Предложенная ранее клеточно-автоматная модель динамики численности организмов озера Байкал скорректирована и дополнена учётом пространственной специфики моделируемой области, сезонности рождаемости и перемещения организмов под действием водных течений. Модель верифицирована по критериям отношения продукции к среднегодовой биомассе и относительной частоте встречаемости организмов. Приведены результаты применения модели для исследования влияния загрязнений. Получены оценки минимального загрязнения, достаточного для полного вымирания организмов, и максимального, влияние которого не заметно на фоне естественных процессов.

Ключевые слова: *самоорганизация, дискретное моделирование, клеточный автомат, композиционные модели, хищник — жертва.*

Введение

Длительное время исследования динамики популяций проводились с помощью систем дифференциальных уравнений [1, 2]. В используемых моделях исследовалось не более трёх групп организмов, а параметры особей были усреднены по пространству моделирования. В работе [3], где предложена модель восьми групп организмов, базирующаяся на системе обыкновенных дифференциальных уравнений, с помощью методов численного моделирования было снято первое ограничение.

В [4] предложена клеточно-автоматная модель (КА-модель) динамики численности восьми групп организмов озера Байкал, позволяющая учитывать пространственное распределение особей и возможные локальные загрязнения. В этой модели область моделирования является квадратной, и не учитываются влияние водных течений и сезонные изменения.

В данной работе КА-модель [4] модифицирована. Добавлено соответствие области моделирования пространственной структуре озера Байкал, учтено влияние сезонных изменений на динамику численности и перемещений организмов под действием водных течений. Скорректирован метод учёта влияния локальных загрязнений. Представлены результаты верификации модели. Приведены оценки минимальной интенсивности

¹Исследование выполнено по Программе фундаментальных исследований Президиума РАН, проект № 15.9 (2012 г.), а также при частичной финансовой поддержке РФФИ в рамках научного проекта № 11-01-00567а.

загрязнения, достаточной для полного вымирания организмов, и максимальной, при которой влияние загрязнения не заметно на фоне естественных процессов. Данные о популяции взяты из работы [3].

1. Композиционная КА-модель

Рассмотрим три вида организмов: макрогектопус (*macrohectopus*), малую (*comerphorus dybovski*) и большую (*comerphorus baikalensis*) голомянок.

Каждый из видов разделён на возрастные группы (вид будем обозначать буквой из $\{m, d, b\}$, возрастную группу — цифрой из $\{1, 2, 3\}$):

- макрогектопус — неполовозрелые m_1 , половозрелые m_2 ;
- малая голомянка — однолетки d_1 , неполовозрелые d_2 , половозрелые d_3 ;
- большая голомянка — однолетки b_1 , неполовозрелые b_2 , половозрелые b_3 .

Между группами определены взаимоотношения хищник — жертва и демографические взаимоотношения.

КА-модель динамики популяций организмов озера Байкал определяется четвёркой понятий

$$\aleph = \langle \Sigma, M, F, \rho \rangle,$$

где Σ — алфавит состояний клеток; M — множество имён клеток; F — глобальный оператор перехода; ρ — режим функционирования.

Модель — параллельная композиция [5] восьми КА, каждый из которых предназначен для моделирования численности конкретной группы организмов.

Пусть Q — квадратная сетка, покрывающая озеро Байкал. Множество имён клеток M — объединение восьми попарно непересекающихся множеств M_i^α :

$$M = M_1^m \cup M_2^m \cup M_1^d \cup M_2^d \cup M_3^d \cup M_1^b \cup M_2^b \cup M_3^b.$$

Предполагается, что каждой ячейке из Q соответствует восемь имён клеток — по одной из каждого из множеств M_i^α , т. е. для всех i и α существует биекция ψ_i^α между множеством M_i^α и множеством ячеек сетки Q :

$$\psi_i^\alpha : Q \rightarrow M_i^\alpha.$$

Клеткой называется элемент множества $M \times \Sigma$. *Состояния клетки* — элементы множества Σ (целые числа) — обозначают модельную плотность организмов в клетке.

Конечный набор

$$S(c) = \langle (\varphi_1(c), n_1), \dots, (\varphi_k(c), n_k) \rangle$$

называется *локальной конфигурацией*, где $n_i \in \Sigma$ — состояния клеток; $\varphi_i : M \rightarrow M$ — *именующие функции*, т. е. функции, определяющие для клетки с именем c имена клеток, с ней взаимодействующих.

В общем случае локальный оператор перехода $f : \{S(c)\} \rightarrow \{S(c)\}$ принимает на вход локальную конфигурацию $S(c)$. Его результат — локальная конфигурация $f(S(c))$, в которой изменены состояния клеток (возможно, не всех) из $S(c)$. *Итерация*, или *применение глобального оператора* F — применение локального оператора f ко всем клеткам. В модели глобальный оператор F является последовательной композицией двух операторов [5]

$$F = F_1 \circ F_2,$$

где F_1 предназначен для моделирования перемещения организмов, F_2 — для моделирования процессов поедания, вымирания и роста. Оператор перемещения F_1 , в свою

очередь, является последовательной композицией оператора собственного перемещения F_d и оператора перемещения под действием течений F_s :

$$F_1 = F_d \circ F_s.$$

Известны два основных режима применения глобального оператора: *синхронный* и *асинхронный*. Синхронный режим предполагает, что сначала вычисляются новые состояния клеток согласно локальному оператору перехода, а затем все клетки одновременно изменяют свои старые состояния на новые. В асинхронном режиме случайно выбирается клетка, вычисляется ее новое состояние и старое состояние клетки сразу заменяется на новое [6].

В предложенной КА-модели используются оба режима. Сначала асинхронно применяется F_1 , затем синхронно применяется F_2 .

1.1. Собственное перемещение организмов

Пусть f_z и F_z — локальный и глобальный операторы целочисленной диффузии, предложенной в работе [7],

$$f_z : \{S_1(c)\} \rightarrow \{S_1(c)\},$$

где $S_1(c)$ — набор соседей клетки с именем c , включая саму эту клетку. *Соседями* назовем клетки с именами $c_i^\alpha, c_i^{\alpha'} \in M_i^\alpha$, соответствующими соседним ячейкам сетки Q . Клетки с именами из разных подмножеств M_i^α соседями не являются, т. е. если $c_i^\alpha \in M_i^\alpha$ и $c_j^\beta \in M_j^\beta$ — соседи, то $i = j$, $\alpha = \beta$.

Применение f_z к клетке (c, n) выполняется по следующему алгоритму:

- 1) Пусть $(c_1, n_1), \dots, (c_k, n_k)$ — соседи клетки (c, n) , $k \leq 4$.
Случайно равновероятно выбирается (c_i, n_i) .
- 2) Новые состояния n' и n'_i вычисляются по формулам

$$n' = n - [\sigma n] + [\sigma n_i], \quad n'_i = n_i + [\sigma n] - [\sigma n_i],$$

где σ — коэффициент целочисленной диффузии, $0 \leq \sigma \leq 1$.

Оператор F_z применяется в асинхронном режиме.

Оператор F_d определяется следующим образом. Пусть l — физический размер квадратной ячейки, v_{cr} — крейсерская скорость организмов вида α возраста i , Δt — физическое время, соответствующее одной глобальной итерации КА. Тогда максимальное число ячеек, пройденное организмом за время Δt , может быть вычислено как

$$K_i^\alpha = \frac{v_{cr} \Delta t}{l}.$$

Так как применение f_z перемещает организм только на одну клетку, то перемещение с крейсерской скоростью достигается K_i^α -кратным применением оператора F_z на множестве M_i^α :

$$F_d|_{M_i^\alpha} = (F_z)^{K_i^\alpha}.$$

1.2. Перемещение под действием течений

Пусть $stream(c) : M \rightarrow \mathbb{R}^2$ — карта течений — отображение множества имён клеток M в пространство двумерных вещественных векторов.

Вектор $stream(c) = (v_x, v_y)$ — физическая скорость течения в клетке с именем c ; x соответствует направлению запад — восток, направление y — юг — север.

Локальный оператор f_s моделирует перемещение организмов вдоль траектории течения. Алгоритм применения f_s к клетке с именем c рекурсивен. Сначала просматривается клетка с именем c , затем её соседи, в которые течение переносит организмы, затем соседи соседей и так далее. Рекурсия обрывается на расстоянии, дальше которого течение не может перенести организмы за время, соответствующее одной итерации.

Пусть l — физический размер ячейки, Δt — физическое время, соответствующее одной итерации.

Алгоритм применения f_s к клетке с именем c :

- 1) Найти c_x^k и c_y^k — имена соседей клетки с именем c^k в направлении v_x^k и v_y^k , где k — уровень вложенности рекурсии; c^k — имя просматриваемой клетки. На первом уровне рекурсии просматривается клетка с именем c ($c^1 = c$). На втором уровне просматриваются две клетки — соседи клетки с именем c^1 , в которые попадает течение ($c^2 \in \{c_x^1, c_y^1\}$). На k -м уровне просматривается не более 2^k клеток, $(v_x^k, v_y^k) = stream(c^k)$ — вектор течения в клетке с именем c^k .
- 2) Вычислить n_x^k, n_y^k — число организмов клетки с именем c^k , перемещаемых течением в клетки с именами c_x^k и c_y^k соответственно:

$$n_x^k = \begin{cases} n^k \frac{v_x^k}{|v_x^k| + |v_y^k|}, & \text{если } s_x^k > 1, \\ n^k \frac{v_x^k}{|v_x^k| + |v_y^k|} s_x^k, & \text{если } s_x^k \leq 1, \end{cases} \quad n_y^k = \begin{cases} n^k \frac{v_y^k}{|v_x^k| + |v_y^k|}, & \text{если } s_y^k > 1, \\ n^k \frac{v_y^k}{|v_x^k| + |v_y^k|} s_y^k, & \text{если } s_y^k \leq 1, \end{cases}$$

где n^k — модельное число перемещаемых организмов клетки с именем c^k . Число n^k при $k > 1$ вычисляется на $(k - 1)$ -м уровне рекурсии на шаге 3; n^1 — состояние клетки с именем c , т. е. на первом уровне вложенности под действием течения перемещаются все особи, находящиеся в клетке с именем c ; s_x^k, s_y^k — модельные расстояния, преодолеваемые течением за время τ^k , в количестве клеток:

$$s_x^k = \frac{\tau^k v_x^k}{l}, \quad s_y^k = \frac{\tau^k v_y^k}{l};$$

τ^k — физическое время, оставшееся для перемещения организмов под действием водных течений в течение одной итерации с учётом времени, затраченного на предыдущих уровнях рекурсии:

$$\tau^1 = \Delta t, \quad \tau^k = \tau^{k-1} - \Delta \tau^{k-1};$$

$\Delta \tau^{k-1}$ — физическое время, затраченное течением на преодоление клетки на $(k - 1)$ -м уровне вложенности рекурсии:

$$\Delta \tau^{k-1} = \frac{l}{v_x^{k-1}} \quad \text{или} \quad \Delta \tau^{k-1} = \frac{l}{v_y^{k-1}}.$$

- 3) Если $s_x^k > 1$ (т. е. течение за время τ^k может пересечь более одной клетки в направлении x), то алгоритм рекурсивно выполняется для клетки $c^{k+1} = c_x^k$ с числом перемещаемых организмов $n^{k+1} = n_x^k$ и временем, затраченным на перемещение, $\Delta \tau^k = \frac{l}{v_x^k}$. Аналогичная проверка выполняется в направлении y .

Чтобы учесть влияние замерзания озера на скорость течений, физическая скорость водных течений в период замерзания считается равной половине от физической скорости в период, когда озеро свободно ото льда.

1.3. Оператор изменения численности

Пусть f_2 — локальный оператор изменения численности:

$$f_2 : \{S_2(c)\} \rightarrow \{S_2(c)\},$$

где $S_2(c)$ — набор клеток-близнецов (рис. 1). Клетки с именами $c_i^\alpha \in M_i^\alpha$ и $c_j^\beta \in M_j^\beta$ называются *близнецами*, если они соответствуют одной и той же ячейке из Q , т. е. $(\psi_i^\alpha)^{-1}(c_i^\alpha) = (\psi_j^\beta)^{-1}(c_j^\beta)$. Таким образом, для $c \in M_i^\alpha$ и $q = (\psi_i^\alpha)^{-1}(c) \in Q$

$$S_2(c) = \langle \psi_1^m(q), \psi_2^m(q), \psi_1^d(q), \psi_2^d(q), \psi_3^d(q), \psi_1^b(q), \psi_2^b(q), \psi_3^b(q) \rangle.$$

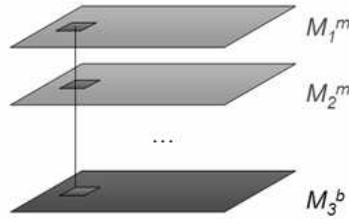


Рис. 1. Клетки-близнецы $S_2(c)$

Локальный оператор f_2 применяется синхронно. Новое состояние клетки с именем $c_i^\alpha \in M_i^\alpha$ вычисляется по формуле

$$(n_i^\alpha)' = n_i^\alpha + (\rho_i^\alpha n_j^\alpha - \lambda_i^\alpha n_i^\alpha - \theta_i^\alpha n_i^\alpha) \Delta t,$$

где j — возрастная группа особей, порождающих особей возраста i ; Δt — физическое время, соответствующее одной итерации КА; $\rho_i^\alpha n_j^\alpha$ — приток в группу за счёт рождаемости или старения предыдущей группы; $\lambda_i^\alpha n_i^\alpha$ — отток из группы за счёт смертности; $\theta_i^\alpha n_i^\alpha$ — отток из группы за счёт старения.

Коэффициенты рождаемости ρ_i^α , смертности λ_i^α и старения θ_i^α взяты из работы [3]:

- 1) коэффициенты старения θ_i^α постоянны;
- 2) коэффициенты смертности $\lambda_2^d, \lambda_3^d, \lambda_2^b, \lambda_3^b$ постоянны;
- 3) коэффициенты смертности $\lambda_1^m, \lambda_2^m, \lambda_1^d, \lambda_1^b$ имеют вид

$$\lambda_i^\alpha = a_i^\alpha + b_i^\alpha(n_2^d + n_3^d) + d_i^\alpha(n_2^b + n_3^b), \quad (1)$$

где $a_i^\alpha, b_i^\alpha, d_i^\alpha$ — постоянные величины; b_i^α и d_i^α характеризуют смертность от выедания хищниками (малыми и большими голомянками) и зависят от вкусовых предпочтений хищников; a_i^α характеризует смертность от остальных причин;

- 4) коэффициент рождаемости ρ_1^m постоянен;
- 5) коэффициенты рождаемости ρ_1^d, ρ_1^b имеют вид

$$\rho_1^\alpha = \mu^\alpha(n_1^m + n_2^m) + \nu^\alpha(n_1^d + n_1^b),$$

где постоянные коэффициенты μ^α и ν^α зависят от рациона хищников.

Чтобы учесть зависимость рождаемости от сезонов, в КА-модели коэффициенты рождаемости ρ_1^d и ρ_1^b умножаются на периодические функции $season_d : \mathbb{R} \rightarrow \mathbb{R}$ и $season_b : \mathbb{R} \rightarrow \mathbb{R}$, графики которых приведены на рис. 2. Период функций $season_d(t)$ и $season_b(t)$ равен одному году: $season_b(t+1) = season_b(t)$, $season_d(t+1) = season_d(t)$.

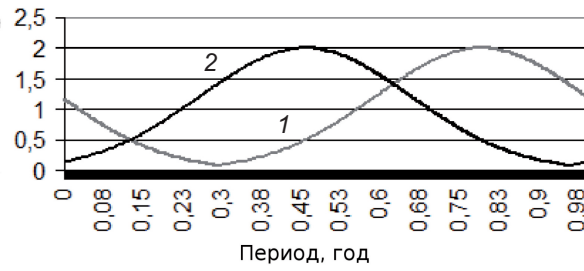


Рис. 2. Графики функций $season_b(t)$ (кр. 1) и $season_d(t)$ (кр. 2). По оси абсцисс отложен один год. Ноль соответствует 1 января

2. Верификация модели

Верификация проводится по трём видам организмов (суммарно по возрастным группам) и следующим критериям:

- P_α/B_α — отношение годовой продукции к среднегодовой биомассе организма α . Годовая продукция P_α — положительный прирост биомассы организма вида $\alpha \in \{m, d, b\}$ за год. В это значение входят массы родившихся организмов и прирост массы организмом во время взросления;
- N_α/N_β — отношение числа организмов вида α к числу организмов вида β ; N_α — усредненная по пространству среднегодовая численность;

$$\begin{aligned} P_m &= P_m^1 + P_m^2, & B_m &= B_m^1 + B_m^2, & N_m &= N_m^1 + N_m^2, \\ P_d &= P_d^1 + P_d^2 + P_d^3, & B_d &= B_d^1 + B_d^2 + B_d^3, & N_d &= N_d^1 + N_d^2 + N_d^3, \\ P_b &= P_b^1 + P_b^2 + P_b^3, & B_b &= B_b^1 + B_b^2 + B_b^3, & N_b &= N_b^1 + N_b^2 + N_b^3. \end{aligned}$$

В [8] дана оценка биомассы макроректопуса B_m в 110000 тонн. Оценка продукции макроректопуса P_m варьируется от 330000 до 900000 тонн [8], т. е. коэффициент P_m/B_m должен находиться в пределах 3–8.

Оценка коэффициента $\frac{P_d + P_b}{B_d + B_b}$ взята из [9] и равна 1,24. Оценки коэффициентов $\frac{N_m}{N_d}$ и $\frac{N_m}{N_b}$ взяты из [3]. Результаты верификации представлены в таблице. Модельные оценки отличаются от оценок, приведённых в [3, 8, 9], не более чем на 20 %.

Результаты верификации модели

Оценки	$\frac{P_m}{B_m}$	$\frac{P_d + P_b}{B_d + B_b}$	$\frac{N_m}{N_d}$	$\frac{N_m}{N_b}$
В [3, 8, 9]	3–8	1,24	6,05	21,52
Модель	5,77	1,49	6,00	20,45

3. Влияние загрязнений

Модель позволяет исследовать влияние вероятного загрязнения.

Пусть $poll(c) : M \rightarrow \mathbb{R}_+$ — карта загрязнений — функционал, ставящий в соответствие имени клетки положительное число, характеризующее интенсивность загрязнения. Предполагается, что загрязнение влияет на смертность организмов.

Новые коэффициенты смертности для хищников $\lambda_2^d, \lambda_3^d, \lambda_2^b, \lambda_3^b$ вычисляются по формуле

$$(\lambda_i^\alpha(c))' = \lambda_i^\alpha + \lambda_i^\alpha poll(c).$$

Новые коэффициенты смертности для жертв $\lambda_1^m, \lambda_2^m, \lambda_1^d, \lambda_1^b$ вычисляются по формуле

$$(\lambda_i^\alpha(c))' = \lambda_i^\alpha + a_i^\alpha poll(c),$$

где a_i^α — постоянный коэффициент смертности из (1).

Разделение для коэффициентов на хищников $\lambda_2^d, \lambda_3^d, \lambda_2^b, \lambda_3^b$ и жертв $\lambda_1^m, \lambda_2^m, \lambda_1^d, \lambda_1^b$ при учёте загрязнений сделано для того, чтобы в множитель смертности от загрязнения не попала смертность от выедания хищниками из (1).

Карта загрязнений $poll(c)$, используемая в вычислительных экспериментах, имеет вид рис. 3. Функционал $poll(c)$ представляет собой плотность стандартного нормального распределения с центром в клетке с именем c_0 в южной части озера Байкал, умноженную на константу.

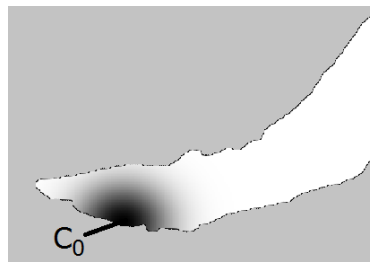


Рис. 3. Карта загрязнений: серый цвет — земля; белый — вода; более тёмный цвет означает большую интенсивность загрязнения

4. Применение модели для исследования влияния загрязнений

Для исследования влияния локальных загрязнений проведён вычислительный эксперимент. Начальное состояние — равномерное распределение особей по области моделирования, совпадающее по значению с устойчивым состоянием численностей, взятому из [3]. Значение $poll(c_0)$ в эксперименте равно 14.

Несколько итераций алгоритма для половозрелого макрогектопуса представлены на рис. 4. Вне области загрязнения наблюдается устойчивый образ из пятен. Неравномерное распределение обусловлено влиянием водных течений.

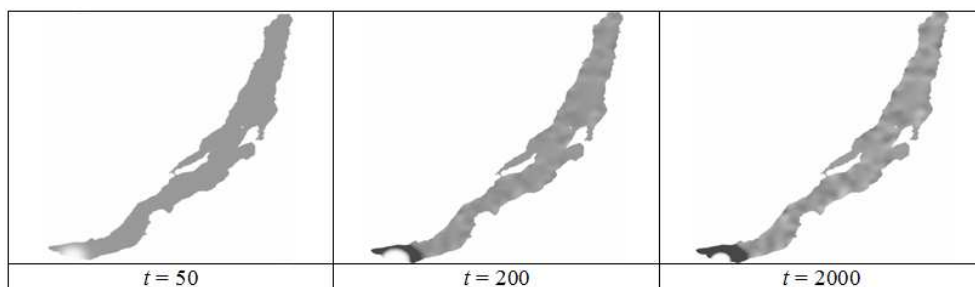


Рис. 4. Несколько итераций для половозрелого макрогектопуса. Более тёмный цвет означает большую плотность организмов

Динамика популяций в клетке на севере озера (рис. 5) стремится к устойчивому колебательному процессу с периодом колебаний 1 год. Годовые колебания — следствие сезонной зависимости коэффициентов рождаемости больших и малых голомянок.

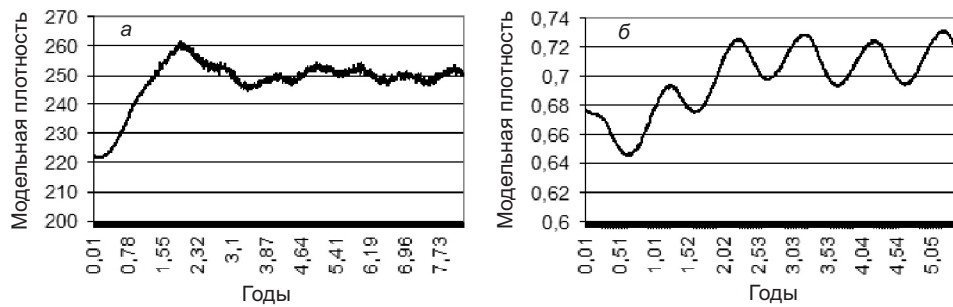


Рис. 5. Динамика модельной плотности в клетке на севере озера (без загрязнения) для неполовозрелого макрогектопуса (а) и неполовозрелой малой голомянки (б)

Динамика популяций в эпицентре загрязнения представлена на рис. 6. Значение $poll(c_0)$ загрязнения в эпицентре равно 14. Этого достаточно для того, чтобы все организмы погибли.

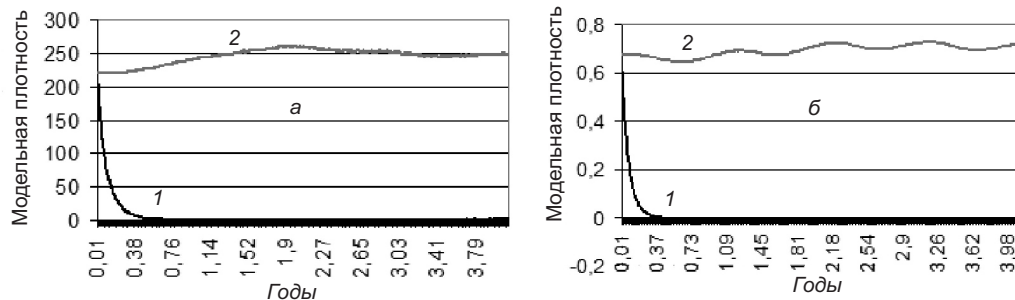


Рис. 6. Динамика модельной плотности в клетке в эпицентре загрязнения (кр. 1) для неполовозрелого макрогектопуса (а) и неполовозрелой малой голомянки (б); кр. 2 — аналогичная динамика в клетке без загрязнения

Динамика популяций в области загрязнения в клетке со значением интенсивности $poll = 2,3$ представлена на рис. 7. Численность жертв увеличилась, а численность хищников уменьшилась по сравнению со среднегодовым значением в области, где загрязнение не оказывает влияния.

Чтобы изучить зависимость среднегодовой плотности организмов от интенсивности загрязнения, были исследованы точки вдоль отрезка, показанного на рис. 8. Юго-восточный конец отрезка находится близ эпицентра загрязнения, северо-западный — в области, не подверженной загрязнению.

Распределение интенсивности загрязнения и изменение численности макрогектопуса на 2000-й итерации алгоритма вдоль отрезка с юго-востока на северо-запад представлены на рис. 9.

По результатам экспериментов можно сделать следующие выводы:

- при $poll(c) > 10$ плотность макрогектопуса на 2000-й итерации падает ниже 3 % от средней плотности в незагрязненной области, что позволяет говорить о практически полном вымирании организмов в загрязненной области;
- если $poll(c) \in (0,15, 5)$, то в этой области увеличено число жертв и уменьшено число хищников; степень различий зависит от значения $poll(m)$;

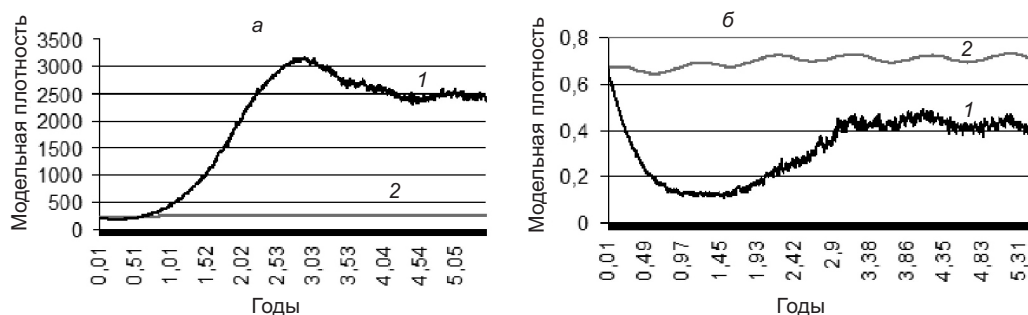


Рис. 7. Динамика модельной плотности в клетке со значением загрязнения $poll = 2,3$ (кр. 1) для неполовозрелого макрогектопуса (а) и неполовозрелой малой головянки (б); кр. 2 — аналогичная динамика в клетке без загрязнения



Рис. 8. Отрезок, вдоль которого исследовалась динамика модельной плотности

- если $poll(c) < 0,03$, то влияние загрязнения незаметно на фоне среднегодовых колебаний численности организмов.

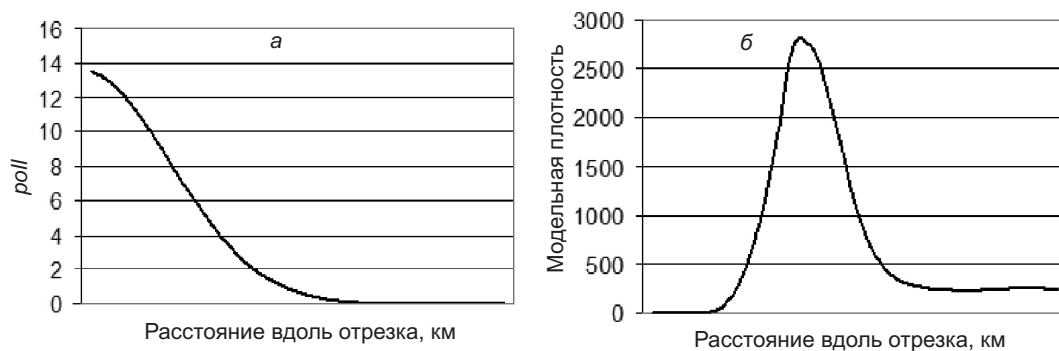


Рис. 9. Распределение интенсивности загрязнения вдоль исследуемого отрезка (а) и модельной плотности неполовозрелого макрогектопуса на 2000-й итерации (б). По оси абсцисс отложено расстояние на отрезке от эпицентра загрязнения, правая граница соответствует 11,5 км

Закключение

Предложенная ранее КА-модель динамики численности восьми групп организмов озера Байкал скорректирована и дополнена учётом пространственных особенностей области моделирования, зависимости взаимодействий между группами от времени года и перемещения особей под действием течений.

Модель верифицирована. Результаты верификации по критериям отношения продукции к биомассе и частот встречаемости отличаются от оценок, приведённых в работах [3, 8, 9], не более чем на 20 %.

Показано, что моделируемая динамика популяций — колебательный процесс с периодом в один год. Получена зависимость поведения модели от интенсивности загрязнения. Влияние загрязнения локально и не распространяется далеко за его пределы. Найдены предельные показатели интенсивности загрязнения: минимальное, при котором происходит вымирание организмов, и максимальное, влияние которого не заметно на фоне естественных годовых колебаний численности.

ЛИТЕРАТУРА

1. *Свирижев Ю. М., Логофет Д. О.* Устойчивость биологических сообществ. М.: Наука, 1978. 352 с.
2. *Базыкин А. Д.* Нелинейная динамика взаимодействующих популяций. Ижевск: ИКИ, 2003. 368 с.
3. *Зоркальцев В. И., Казаева А. В., Мокрый И. В.* Модель взаимодействия трех пелагических видов организмов озера Байкал // Современные технологии. Системный анализ. Моделирование. 2008 № 1. С. 182–193.
4. *Афанасьев И. В.* Клеточно-автоматная модель динамики численности организмов озера Байкал // Прикладная дискретная математика. 2012. № 1. С. 121–132.
5. *Bandman O. L.* Cellular automata composition techniques for spatial dynamics simulation // Simulating Complex Systems by Cellular Automata. Understanding complex Systems / eds. A. G. Hoekstra et al. Berlin, 2010. P. 81–115.
6. *Бандман О. Л.* Клеточно-автоматные модели пространственной динамики // Системная информатика. 2006. № 10. С. 58–113.
7. *Medvedev Y. G.* Multi-particle cellular automata models for diffusion simulation // Meth. Tools Parall. Program. Multicomp. 2011. V. 6083/2011. P. 204–211.
8. *Мазепова Г. Ф., Тимошкин О. А., Мельник Н. Г. и др.* Атлас и определитель пелагиобиев Байкала. Новосибирск: Наука, 1995. 693 с.
9. *Стариков Г. В.* Голомянки Байкала. Новосибирск: Наука, 1977. 94 с.

СВЕДЕНИЯ ОБ АВТОРАХ

АБОРНЕВ Александр Викторович — ООО «Центр сертификационных исследований», г. Москва. E-mail: abconf.c@gmail.com

АФАНАСЬЕВ Иван Владимирович — аспирант Института вычислительной математики и математической геофизики, г. Новосибирск. E-mail: ivafanas@gmail.com

ДОРОХОВА Алиса Михайловна — аспирантка кафедры криптологии и дискретной математики НИЯУ (МИФИ), г. Москва. E-mail: alisa.koreneva@gmail.com

ДЮКОВА Елена Всеволодовна — доктор физико-математических наук, доцент кафедры математических методов прогнозирования факультета вычислительной математики и кибернетики Московского государственного университета им. М. В. Ломоносова, главный научный сотрудник Вычислительного центра им. А. А. Дородницына, г. Москва. E-mail: edjukova@mail.ru

КАРДАШ Сергей Николаевич — кандидат технических наук, старший научный сотрудник Объединенного института проблем информатики НАН Беларуси, г. Минск.

КОРНИЕНКО Анастасия Сергеевна — аспирантка Института математики СО РАН, г. Новосибирск. E-mail: anastasia.s.kornienko@gmail.com

ПОКРОВСКИЙ Алексей Вячеславович — сотрудник математического отдела Института проблем информационной безопасности Московского государственного университета им. М. В. Ломоносова, г. Москва. E-mail: AlexPokrovskiy@yandex.ru

ПОТТОСИН Юрий Васильевич — доцент, кандидат физико-математических наук, ведущий научный сотрудник Объединенного института проблем информатики НАН Беларуси, г. Минск. E-mail: pott@newman.bas-net.by

ПРОКОФЬЕВ Петр Александрович — соискатель Вычислительного центра им. А. А. Дородницына, г. Москва. E-mail: p_prok@mail.ru

РОЖКОВ Михаил Иванович — доцент Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики», г. Москва. E-mail: rozhkov.m.i@yandex.ru

СОРОКИН Сергей Николаевич — старший преподаватель кафедры компьютерной безопасности Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики», г. Москва.

E-mail: sergey-dcm@yandex.ru

ТАРАННИКОВ Юрий Валерьевич — кандидат физико-математических наук, доцент Московского государственного университета им. М. В. Ломоносова, г. Москва. E-mail: taran@butovo.com

ФОМИЧЕВ Владимир Михайлович — доктор физико-математических наук, профессор, профессор Финансового университета при Правительстве Российской Федерации, г. Москва. E-mail: fomichev@nm.ru

ШУШУЕВ Георгий Иннокентьевич — магистрант Новосибирского государственного университета, г. Новосибирск. E-mail: g.shushuev@gmail.com

АННОТАЦИИ СТАТЕЙ НА АНГЛИЙСКОМ ЯЗЫКЕ

Abornev A. V. **PERMUTATIONS INDUCED BY DIGIT-PERMUTABLE TRANSFORMATIONS OF A MODULE OVER A GALOIS RING OF CHARACTERISTIC 4.** New classes of nonlinear permutations on a vector space that can be represented by linear transformations of a module over a Galois ring of characteristic 4 are constructed. The system of coordinate functions of such permutation is an orthogonal system of polynomials over the field. Orthogonal systems of two quadratic functions and diagonal quadratic functions are described.

Keywords: *digit-permutable matrix, DP-matrix, permutation, Galois ring.*

Fomichev V. M. **PRIMITIVE SETS OF NUMBERS BEING EQUIVALENT BY FROBENIUS.** Equivalence of primitive sets of natural numbers is investigated in connection with the Diophantine Frobenius problem. The equivalence is used for simplifying calculations of Frobenius number $g(a_1, \dots, a_k)$ and of the whole set of numbers that are not contained in the additive semigroup generated by a set $\{a_1, \dots, a_k\}$.

Keywords: *Frobenius number, primitive set, additive semigroup generated by set of numbers.*

Rozhkov M. I. **BIJECTIVE MAPPINGS GENERATED BY FILTERING GENERATOR.** The paper deals with the methods for constructing bijective mappings $B_{f,L}$ whose coordinate functions are defined by a great length shift register with a feedback function $L(x_1, x_2, \dots, x_n)$ and with an output (filtering) nonlinear function $f(x_1, x_2, \dots, x_k)$ depending on a small number k of its arguments ($k \ll n$). It is known that the orthogonality of the coordinate functions is equivalent to the bijectiveness of the mapping $B_{f,L}$. A method developed in the paper reduces the problem of bijectiveness of $B_{f,L}$ for any n to the case of bounded $n < n_0$. The method allows to build new infinite classes of bijective mappings $B_{f,L}$ for nonlinear functions f depending on four, five or six variables. Earlier, similar results were known for a function f depending on three arguments. The results can be useful for constructing and proving statistical properties of random sequences generated on the basis of filter generators.

Keywords: *orthogonal system of Boolean functions, feedback shift register, filter generator.*

Shushuev G. I. **FINDING THE OPTIMAL LINEAR APPROXIMATION OF FEISTEL NETWORK.** An approach to finding the linear approximation of Feistel network is presented. The mathematical formulation of the linear approximation problem and an algorithm for finding the optimal linear approximation of the generalized Feistel network are described.

Keywords: *linear cryptanalysis, Feistel network.*

Sorokin S. N. **INTRUSION DETECTION METHOD FOR DENIAL OF SERVICE ATTACKS ON THE WEB-APPLICATIONS.** The article describes the main issues related to multilayer perceptron used for “denial of service” attacks detection: statistical data collection and preparation, formation of indicators describing the state of a web-application, training and performance evaluation of neural network.

Keywords: *intrusion detection, denial of service, DoS, web-application.*

Pokrovskiy A. V. **ON THE WEIGHT SPECTRUM IN LINEAR CODES OF A CLASS.** A class of linear codes being subcodes of a Reed — Müller code is considered. The weight spectra of codes from this class are calculated.

Keywords: *Reed — Müller code, weight spectrum, Boolean functions, weight of Boolean function.*

Tarannikov Y. V. **ON RANKS OF SUBSETS IN THE SPACE OF BINARY VECTORS ADMITTING AN EMBEDDING OF A STEINER SYSTEM $S(2, 4, v)$.** A bound for the rank of a subset X in the vector space $\mathbb{F}_2^n$ is obtained via the covering radius of the code lying in the subspace of linear dependencies of vectors in X . Also, an upper bound for the covering radius of a code generated by the incidence matrix of a Steiner system $S(2, 4, v)$ is obtained. Precise and asymptotic bounds for the rank of a subset X in the vector space $\mathbb{F}_2^n$ admitting an embedding of a Steiner system $S(2, 4, v)$ are obtained too.

Keywords: *rank, affine rank, bounds, linear subspace, linear code, covering radius, Steiner system, Boolean functions, spectrum support.*

Dorokhova A. M., Fomichev V. M. **IMPROVEMENT OF EXPONENT ESTIMATES FOR MIXING GRAPHS OF BIJECTIVE SHIFT REGISTERS OVER A SET OF BINARY VECTORS.** This article presents new estimates for lengths of simple paths and cycles in the mixing graph G of a bijective shift register over a binary vectors set. Also, some sufficient conditions for primitiveness of G are obtained. An upper bound given earlier for the exponent of G is reduced.

Keywords: *mixing graph of transformation, graph diameter, graph exponent.*

Kornienko A. S. **STRUCTURE OF FUNCTIONAL GRAPHS FOR CIRCULANTS WITH LINEAR BOOLEAN FUNCTIONS AT THE VERTICES.** The functional graph of a discrete dynamic system which is given over circulant with linear Boolean functions of three arguments at the vertices is considered. Trees and loops structures of the functional graph are described.

Keywords: *discrete dynamical system, circulant, gene network, regulatory circuit, functional graph.*

Djukova E. V., Prokofjev P. A. **ON ASYMPTOTICALLY OPTIMAL ENUMERATION FOR IRREDUCIBLE COVERINGS OF BOOLEAN MATRIX.** Enumeration problem for irreducible coverings of Boolean matrix is considered. This problem is known as the problem of dualization. Efficiency of dualization algorithm is usually appreciated with the complexity of a step (creating a next irreducible covering). The algorithms being effective in typical case (for almost all matrices of fixed size) are built by using an approach based on the concept of an asymptotically optimal algorithm with a polynomial delay. Two faster modifications of the asymptotically optimal algorithm AO2 are built. Algorithms have been tested on random Boolean matrices.

Keywords: *Boolean matrix, enumeration of irreducible coverings, asymptotically optimal algorithm for the dualization, CNF and DNF of monotonic Boolean function, minimal transversal of hypergraph.*

Pottosin Yu. V., Kardash S. N. **PIPELINING COMBINATIONAL CIRCUITS.** For a multilevel combinational circuit, the problem of increasing its performance is considered. The problem is to divide the circuit into a given number of cascades and to connect them via registers providing pipeline-wise development of incoming signals. The frequency of incoming signals is established in the process of dividing the circuit. This frequency must

be as high as possible. To solve this problem a model based on the representation of the circuit in the form of a directed graph is used.

Keywords: *combinational circuit, pipelining, directed graph.*

Afanasyev I. V. **CELLULAR AUTOMATA MODEL APPLICATION FOR INVESTIGATION OF POLLUTION INFLUENCE ON POPULATION DYNAMICS OF COMEPHORUS AND MACROHECTOPUS IN LAKE BAIKAL.**

Cellular automata model was modified in order to take into account birthrates seasonal dependency and influence of water streams on movement of organisms. The model was verified within production-to-biomass and relative average quantity criteria and was used for investigation of pollution influence on population dynamic. Estimates of minimal pollution that leads to total death of organisms and of maximum pollution which influence is not observable within natural population dynamics are presented.

Keywords: *self-organization, cellular automata, composition, population dynamic model, prey — predator system.*

Журнал «Прикладная дискретная математика» включен в перечень ВАК рецензируемых российских журналов, в которых должны быть опубликованы основные результаты диссертаций, представляемых на соискание учёной степени кандидата и доктора наук, а также в перечень журналов, рекомендованных УМО в области информационной безопасности РФ в качестве учебной литературы по специальности «Компьютерная безопасность».

Журнал «Прикладная дискретная математика» распространяется по подписке; его подписной индекс 38696 в объединённом каталоге «Пресса России». Полнотекстовые электронные версии вышедших номеров журнала доступны на его сайте vestnik.tsu.ru/pdm и на Общероссийском математическом портале www.mathnet.ru. На сайте журнала можно найти также и правила подготовки рукописей статей в журнал.

Тематика публикаций журнала:

- *Теоретические основы прикладной дискретной математики*
- *Математические методы криптографии*
- *Математические методы стеганографии*
- *Математические основы компьютерной безопасности*
- *Математические основы надёжности вычислительных и управляющих систем*
- *Прикладная теория кодирования*
- *Прикладная теория автоматов*
- *Прикладная теория графов*
- *Логическое проектирование дискретных автоматов*
- *Математические основы информатики и программирования*
- *Вычислительные методы в дискретной математике*
- *Дискретные модели реальных процессов*
- *Математические основы интеллектуальных систем*
- *Исторические очерки по дискретной математике и её приложениям*