МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2012 №4(18)

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

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

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 10.12.2012.
Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 13,4. Уч.-изд. л. 15. Тираж 300 экз.

Издательство ТГУ. 634029, Томск, ул. Никитина, 4
Отпечатано в типографии ТПУ.

СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

ИСТОРИЧЕСКИЕ ОЧЕРКИ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЁ ПРИЛОЖЕНИЯМ

АНАЛИТИЧЕСКИЕ ОБЗОРЫ

CONTENTS

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/18/1

УДК 519.6

ПОЛОЖИТЕЛЬНЫЕ СВОЙСТВА НЕОТРИЦАТЕЛЬНЫХ МАТРИЦ

К. Г. Когос*, В. М. Фомичев**

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

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

E-mail: fomichev@nm.ru

Дан обзор результатов исследования примитивности графов (неотрицательных матриц) и некоторых направлений обобщения. Приведены оценки экспонентов различных классов графов и систем графов (матриц и систем матриц).

Ключевые слова: *примитивный граф, примитивная матрица, экспонент, субэкспонент.*

Одним из положительных криптографических свойств преобразований векторных пространств является хорошее перемешивание, то есть зависимость каждой координатной функции от всех переменных. Перемешивающие свойства преобразования g пространства P^n над полем P, заданного системой координатных функций $\{g_1(x_1,\dots,x_n),\dots,g_n(x_1,\dots,x_n)\}$, определяются системой множеств $\{S(g_1),\dots,S(g_n)\}$, где $S(g_j)$ — множество номеров существенных переменных координатной функции $g_j(x_1,\dots,x_n)$, $j=1,\dots,n$. Наилучшее перемешивание достигается, если каждая из координатных функций преобразования g зависит от всех переменных, то есть $S(g_j)=\{1,\dots,n\}$, $j=1,\dots,n$. Такие преобразования принято называть совершенными. Обобщениями свойства совершенности функций являются такие свойства, как строгий лавинный критерий, критерии распространения, свойство «бент».

Почти все преобразования векторного пространства P^n над конечным полем P являются совершенными при $n\to\infty$. Однако подобный вывод неприменим к функциям, используемым в криптографических системах, так как они выбираются не случайно, а из отображений с рядом заданных свойств. Поэтому изучение перемешивающих свойств криптографических функций — актуальная задача криптографического анализа.

Некоторые функции с полным перемешиванием обладают свойством распространения искажений входных данных, что позволяет использовать их в криптосистемах аутентификации. С другой стороны, к функциям шифрования с неполным перемешиванием входов применимы методы определения ключа типа последовательного опробования, что делает привлекательным использование в криптосистеме шифрования совершенных преобразований.

Аппаратная или программная реализация совершенных преобразований затруднена в связи с необходимостью реализации функций от большого числа переменных. Поэтому для хорошего перемешивания используются итерации (возведение в степень) преобразования с относительно слабыми перемешивающими свойствами. Показатель степени преобразования, при которой достигается хорошее перемешивание, является

важной криптографической характеристикой. В частности, показатель степени раундовой подстановки блочного шифра, при которой достигается хорошее перемешивание, является определяющим при выборе разработчиком числа циклов шифрования.

Матрицу A над полем действительных чисел называют положительной (неотрицательной), если положительны (неотрицательны) все её элементы, при этом пишут $A > 0$ ($A \geqslant 0$). Носителем неотрицательной матрицы $A = (a_{i,j})$ называется $0,1$-матрица $v(A) = (v(a_{i,j}))$, где $v(a_{i,j}) = 1$, если $a_{i,j} > 0$, и $v(a_{i,j}) = 0$, если $a_{i,j} = 0$, при всех допустимых i, j. Заметим, что v есть гомоморфизм мультипликативного моноида неотрицательных матриц над полем действительных чисел на мультипликативный моноид $0,1$-матриц, где $v(AB) = v(A) \cdot v(B)$.

Точное определение множества $\{S(g_1), \ldots, S(g_n)\}$ является во многих случаях сложной вычислительной задачей. Поэтому при исследовании перемешивающих свойств степеней преобразований применяется оценочный теоретико-графовый или матричный подход. Обозначим $\Gamma(g)$ перемешивающий n-вершинный орграф преобразования g, в котором пара (i, j) является дугой тогда и только тогда, когда $i \in S(g_j)$, $i, j \in \{1, \ldots, n\}$. Матрицу $M(g)$ смежности вершин графа $\Gamma(g)$ называют перемешивающей матрицей преобразования g. Суть оценочного подхода состоит в исследовании степеней матрицы $M(g)$ и определении наименьшего натурального числа t, такого, что $(M(g))^t > 0$. Корректность такого подхода вытекает, например, из следствия 2 теоремы 10.3 [1]: если матрица $(M(g))^t$ не положительна, то преобразование g^t не совершенно. Оценочный теоретико-графовый или матричный подход реализуется существенно проще с точки зрения сложности вычислений, чем точное вычисление множеств существенных переменных.

При исследовании перемешивающих свойств часто используется эпиморфизм φ мультипликативного моноида неотрицательных матриц порядка n на моноид n-вершинных орграфов, где умножение графов определено как умножение бинарных отношений. При эпиморфизме φ матрице M соответствует орграф Γ с множеством вершин $\{1, \ldots, n\}$ и множеством дуг U, где $(i, j) \in U \Leftrightarrow m_{i,j} > 0$. При эпиморфизме φ выполнено: $M > 0$, если и только если граф $\Gamma = \varphi(M)$ полный. Эпиморфизм φ всякой неотрицательной матрице A ставит в соответствие орграф $\Gamma = \varphi(A)$, матрица смежности вершин которого есть $v(A)$. В частности, $\varphi(M(g)) = \Gamma(g)$ для графа Γ. Следовательно, орграф $\Gamma = \varphi(A)$ полный в том и только в том случае, если $A > 0$. И вообще, система понятий, связанных с изучением перемешивающих свойств преобразований, применима как для неотрицательных матриц, так и для графов.

Ограничение эпиморфизма φ на подмоноид симметричных матриц (для них $m_{i,j} = m_{j,i}$ при всех допустимых i, j) есть эпиморфизм на подмоноид n-вершинных неориентированных графов.

Настоящий обзор посвящён положительным свойствам неотрицательных матриц, под которыми понимаются свойства, связанные со способностью порождения тем или иным способом положительной матрицы. Обзор содержит известные результаты по оценке таких характеристик систем неотрицательных матриц (графов и орграфов), как экспоненты, множественные экспоненты, субэкспоненты. Экспонент системы неотрицательных матриц Ω есть наименьшая длина записи положительной матрицы в системе образующих Ω мультипликативной полугруппы. Множественный экспонент определяет наименьшую длину произведений образующих матриц, при которой каждое произведение данной длины есть положительная матрица. Субэкспонент неотрицательной матрицы есть наименьшее число первых членов мультипликативной циклической полугруппы, порождённой данной матрицей, сумма которых положительна.

1. Примитивность неотрицательных матриц

Неотрицательную матрицу A называют примитивной, если $A^t > 0$ при некотором натуральном t, а наименьшее натуральное γ, при котором $A^\gamma > 0$, называют экспонентом или показателем примитивности матрицы A и обозначают как $\exp A$. Если такого t не существует, то $\exp A = \infty$.

Абсолютная оценка экспонента примитивной матрицы A порядка n дана Виландтом [2]:

$$\exp A \leqslant n^2 - 2n + 2. \tag{1}$$

В [3, с. 409] получены выражения экспонента примитивной матрицы через характеристики матрицы (в частности, через число положительных элементов на главной диагонали). Пусть A — примитивная матрица порядка n, а матрица A^h имеет не менее $d > 0$ положительных элементов на главной диагонали для любого $h \geqslant k$ при целом неотрицательном k. Тогда

$$\exp A \leqslant 2n - d + k - 1.$$

Отсюда следует, что если матрица A имеет не менее $d > 0$ положительных элементов на главной диагонали, то

$$\exp A \leqslant 2n - d - 1,$$

и если положительны все элементы на главной диагонали, то

$$\exp A \leqslant n - 1.$$

Пусть матрица A примитивна и матрица $A + \ldots + A^h$, $h \geqslant 1$, имеет не менее $d > 0$ положительных элементов на главной диагонали. Тогда [3, с. 409]

$$\exp A \leqslant n - d + h(n - 1).$$

Экспонент примитивной симметричной матрицы [3, с. 409] удовлетворяет оценке

$$\exp A \leqslant 2(n - 1).$$

Замечание 1 [4, с. 140]. В связи с абсолютной оценкой (1) отметим, что Далмейджем (Dulmage A. L.) и Мендельсоном (Mendelsohn N. S.) выделены «лакуны», то есть некоторые числа, не превышающие $n^2 - 2n + 2$ и не являющиеся показателями примитивности какой-либо матрицы порядка n. Таковы, например, числа из интервалов $(n^2 - 3n + 4, (n - 1)^2)$ и $(n^2 - 4n + 6, n^2 - 3n + 2)$. При чётном n «лакуной» является интервал $(n^2 - 4n + 6, (n - 1)^2)$, объединяющий оба предыдущих. В [5] данные результаты усилены. Показано, что для любых целых n, t не существует примитивной матрицы порядка n, экспонент которой удовлетворяет неравенствам

$$n^2 - tn + \frac{1}{4}(t + 1)^2 < \exp A < n^2 - (t - 1)n + t - 2.$$

Замечание 2 [2, с. 243]. При $n \to \infty$ случайная равновероятная 0, 1-матрица порядка n с вероятностью, стремящейся к единице, является примитивной и имеет экспонент равный двум.

Матрица A порядка n называется частично разложимой, если у нее есть нулевая подматрица размера $r \times s, r + s = n$. Матрица A вполне неразложима, если она не является частично разложимой.

Известно [3, с. 300], что вполне неразложимая матрица A примитивна и

$$\exp A \leqslant n - 1.$$

Критерий примитивности матрицы A дан ниже в связи с рассмотрением орграфа $\Gamma = \varphi(A)$.

2. Примитивность графов

Примитивность графа определяется естественным образом: граф Γ примитивен, если примитивна матрица смежности его вершин, то есть неотрицательная матрица A и орграф $\Gamma = \varphi(A)$ одновременно примитивны или не примитивны, в случае примитивности их экспоненты равны. При исследованиях примитивности матриц и графов применяется как матричный, так и теретико-графовый язык.

Связь между графами и неотрицательными матрицами устанавливает следующая теорема [6]: пусть M — матрица смежности вершин графа Γ и $M^t = (m_{ij}^{(t)})$, тогда число путей длины t из i в j в графе Γ равно $m_{ij}^{(t)}$, $i, j \in \{1, \ldots, n\}$.

Таким образом, примитивность графа и величина экспонента определяются свойствами путей в графе. В частности, любой примитивный орграф Γ является сильносвязным и $\exp\Gamma$ не меньше диаметра графа Γ.

Напомним, что абсолютная оценка диаметра сильносвязного n-вершинного орграфа Γ имеет вид

$$\operatorname{diam}\Gamma \leqslant n.$$

2.1. Свойства экспонентов ориентированных графов

В [7] указаны примитивные орграфы, на которых достигается абсолютная оценка (1). При $n > 2$ рассмотрим n-вершинный орграф Γ, состоящий из гамильтонова контура $C = (1, 2, \ldots, n)$, к которому добавлена дуга (i, j), где вершины i, j расположены на контуре C на расстоянии 2, $i, j \in \{1, \ldots, n\}$. Множество n-вершинных орграфов, изоморфных орграфу Γ, назовём n-вершинными графами Виландта и обозначим это множество $\Gamma_W(n)$. При любом $n > 2$ множество $\Gamma_W(n)$ состоит из $n!$ изоморфных графов; абсолютная оценка Виландта достигается на графах Виландта, и только на них.

Для остальных примитивных n-вершинных орграфов Γ при нечётном $n > 3$ верна достижимая оценка (в соответствии с известными «лакунами»)

$$\exp\Gamma \leqslant n^2 - 3n + 4.$$

Верхняя граница экспонента примитивного орграфа может быть понижена [3, с. 227], если в орграфе известна длина простого контура. Пусть Γ — примитивный орграф с n вершинами, l — длина кратчайшего простого контура в Γ, тогда

$$\exp\Gamma \leqslant n + l(n - 2). \tag{2}$$

В частности, если в примитивном орграфе имеется петля, то $\exp\Gamma \leqslant 2n - 2$.

Граница (2) экспонента примитивного орграфа может быть понижена [7], если в орграфе известны длины l и λ двух простых контуров, где $(l, \lambda) = 1$. Пусть в n-вершинном орграфе Γ имеются простые контуры C и C' длины соответственно l и λ, где $n > 2$, $1 < \lambda < l \leqslant n$ и $(l, \lambda) = 1$. Обозначим $C \cap C'$ пересечение множеств вершин контуров C и C'. Тогда

1) если $C \cap C' = \varnothing$, то $\exp\Gamma \leqslant l\lambda - 2l - 3\lambda + 3n$;
2) если $C \cap C' = H$, где $|H| = h > 0$, то $\exp\Gamma \leqslant l\lambda - l - 3\lambda + h + 2n$.

Отсюда следует, что для любого примитивного n-вершинного орграфа Γ при $n > 2$ верно:

1) если контуры C и C' не имеют общих вершин, то

$$\exp\Gamma \leqslant \left\lfloor \frac{n+1}{2} \right\rfloor \left\lceil \frac{n+1}{2} \right\rceil \leqslant \frac{n^2}{4} + \frac{n}{2} + \frac{1}{4};$$

2) если контуры C и C' имеют h общих вершин, где $1 \leqslant h \leqslant \lambda$, то

$$\exp\Gamma \leqslant \left\lfloor \frac{n+h+2}{2} \right\rfloor \left\lceil \frac{n+h+2}{2} \right\rceil - 2h - n \leqslant n^2 - 2n + 2.$$

В [8] получена оценка диаметра и экспонента nr-вершинного перемешивающего графа $\Gamma(\varphi)$ обратимого преобразования φ регистра сдвига длины n над множеством V_r двоичных r-мерных векторов, где n, r — натуральные (такие графы возникают при рассмотрении обобщения блочных шифров Фейстеля). Подстановка φ такого регистра сдвига имеет вид

$$\varphi(y_1, \ldots, y_n) = (y_2, \ldots, y_n, \psi(y_2, \ldots, y_n) \oplus y_1),$$

где $y_1, \ldots, y_n \in V_r$; $\psi(y_2, \ldots, y_n)$ называется функцией усложнения.

Пусть подстановка φ задается системой булевых координатных функций $\{\varphi_1(x_1, x_2, \ldots, x_{nr}), \varphi_2(x_1, x_2, \ldots, x_{nr}), \ldots, \varphi_{nr}(x_1, x_2, \ldots, x_{nr})\}$. Тогда функции усложнения $\psi(y_2, \ldots, y_n)$ соответствует r-вершинный граф Γ_ψ: пара (v, w) образует дугу тогда и только тогда, когда функция $\varphi_{(n-1)r+w}$ зависит существенно от некоторой переменной из множества $\{x_v, x_{r+v}, \ldots, x_{(n-1)r+v}\}$. Показано, что перемешивающий граф $\Gamma(\varphi)$ сильно связен тогда и только тогда, когда сильно связен граф Γ_ψ.

Получено, что если граф Γ_ψ сильносвязный и $\operatorname{diam}\Gamma_\psi \leqslant d$, то

1) $\operatorname{diam}\Gamma(\varphi) \leqslant (n-1) \cdot \min\{d, r-1\} + n$;
2) если граф $\Gamma(\varphi)$ примитивный и $\psi(y_2, \ldots, y_n) = \psi(y_n, \ldots, y_2)$ (в этом случае алгоритм блочного шифрования инволютивен), то $\operatorname{diam}\Gamma(\varphi) \leqslant n/2 \cdot \min\{d, r-1\} + n$;
3) если граф $\Gamma(\varphi)$ примитивный, то $\exp\Gamma(\varphi) \leqslant n^2 r + nr - 2n$.

В [3, с. 398] дана оценка экспонентов турнира, то есть ориентированного n-вершинного орграфа T_n без петель, в котором каждая пара i, j различных вершин соединена ровно одной дугой. Турнир T_n называется приводимым, если существует такое разбиение множества вершин на два подмножества, что в T_n присутствуют все дуги, направленные из первого блока разбиения во второй блок. В противном случае турнир называется неприводимым. Показано, что при $n \geqslant 4$ турнир T_n примитивен тогда и только тогда, когда он неприводим. Экспонент турнира T_n оценивается при $n \geqslant 5$ через его диаметр d:

$$d \leqslant \exp T_n \leqslant d + 3.$$

В общем случае

$$3 \leqslant \exp T_n \leqslant n - 1.$$

При $n \geqslant 6$ и $3 < \gamma < n+2$ существует неприводимый турнир T_n, экспонент которого равен γ.

Для вершины i ориентированного n-вершинного графа, $i = 1, \ldots, n$, обозначим через p_i число дуг, входящих в вершину i, и через q_i — число дуг, исходящих из вершины i (полустепень захода и полустепень исхода вершины i). Граф называется псевдосимметрическим, если $p_i = q_i$ при $i = 1, \ldots, n$ (дихотомическим при $p_i = q_i = 2$, $i = 1, \ldots, n$). В [9] получены верхние оценки экспонентов примитивных псевдосимметрических и дихотомических графов, при этом рассматриваемые графы классифицированы по длине обхвата (кратчайшего контура). Класс сильносвязных псевдосимметрических графов с n вершинами, каждая из которых имеет не менее k (в точности k) входящих и исходящих дуг, с обхватом не менее p (в точности p) обозначается $H(n, k, p)$ ($G(n, k, p)$). Класс

примитивных графов из $G(n,k,p)$ с обхватом в точности p обозначается $P(n,k,p)$. Справедлива цепочка включений

$$P(n,k,p) \subset G(n,k,p) \subset H(n,k,p).$$

В [9, § 3, ч. 3] описаны структурные свойства графов из множества $G(n,2,(n-1)/2)$. При нечётном $n > 12$ доказано, что $G(n,2,(n-1)/2) = P(n,2,(n-1)/2)$ и для любого $\Gamma \in P(n,2,(n-1)/2)$

$$\exp\Gamma \leqslant \frac{(n-1)^2}{4} + 5.$$

Верхние оценки экспонентов дихотомических графов получены в [9, § 4, ч. 3]. Для любого орграфа $\Gamma \in P(n,2,p)$, где $3 \leqslant p \leqslant \lceil n/2 \rceil$, доказано, что

$$\exp\Gamma \leqslant \frac{(p+1)n}{2p-1} + p(n-2) + 5.$$

В [9, § 5, ч. 3] получены верхние оценки экспонентов графов из классов $P(n,k,p)$ при $p = 1, 2$. В частности, для любого $\Gamma \in P(n,k,2)$, где $k > 2$, справедливо неравенство

$$\exp\Gamma \leqslant \begin{cases} \dfrac{1}{2}\left(29\dfrac{n-1}{k+1} - 5\right), & k > 6\dfrac{n-1}{n+1} - 1, \\ \\ n + \dfrac{1}{2}\left(\dfrac{11n-6}{k+1} - 3\right), & k \leqslant 6\dfrac{n-1}{n+1} - 1. \end{cases}$$

Для любого $\Gamma \in P(n,k,1)$, где $k > 2$, выполнено

$$\exp\Gamma \leqslant 3\left(\frac{n-1}{k+1} + \frac{n-2}{k}\right) - 2.$$

Универсальный критерий примитивности орграфа Γ [3, с. 226] определяется длинами его простых контуров. Если $C_1, \ldots, C_k$ есть все простые контуры орграфа Γ длин $l_1, \ldots, l_k$ соответственно, то сильносвязный орграф Γ примитивный, если и только если $(l_1, \ldots, l_k) = 1$.

Периодом вершины i орграфа называется наибольший общий делитель таких чисел k, что $a_{i,i}^{(k)} > 0$, $i = 1, \ldots, n$. Иными словами, период d вершины i равен наибольшему общему делителю длин всех контуров, проходящих через вершину i в орграфе Γ. Неотрицательная матрица $A = (a_{i,j})$ порядка $n > 1$ называется неразложимой (или неприводимой), если для всех $i, j = 1, \ldots, n$ существует $t \in N$, такое, что $a_{i,j}^{(t)} > 0$, где $A^t = (a_{i,j}^{(t)})$. Это означает, что орграф $\Gamma = \varphi(A)$ сильносвязный: в орграфе Γ для любой пары вершин (i,j), $i, j = 1, \ldots, n$, существует путь из i в j. Неразложимая матрица A называется периодической (или циклической), если период любой вершины орграфа Γ равен $d > 1$. Если $d = 1$ для некоторой вершины орграфа Γ, то матрица называется апериодической (или ациклической).

Универсальный критерий примитивности на матричном языке имеет вид [3, с. 392]: неотрицательная матрица A примитивна тогда и только тогда, когда A неразложима и апериодична.

Сумма неразложимой матрицы A и единичной матрицы I является примитивной матрицей (ей соответствует граф с n петлями), и $\exp(A+I) \leqslant n-1$.

Достаточные условия примитивности орграфа $\Gamma(\varphi)$ подстановки φ регистра сдвига длины n над множеством V_r двоичных r-мерных векторов получены в [8]. Сильносвязный граф $\Gamma(\varphi)$ примитивен, если выполнено любое из следующих условий:

1) координатная функция φ_m зависит существенно от переменной x_m при некотором $m \in \{(n-1)r+1, (n-1)r+2, \ldots, nr\}$, в этом случае $\exp\Gamma(\varphi) \leqslant 2nr-2$;
2) $\psi(y_2, \ldots, y_n) = \psi(y_n, \ldots, y_2)$ и при некоторых $m \in \{(n-1)r+1, (n-1)r+2, \ldots, nr\}$ и $\mu \in \{1, \ldots, r\}$ координатная функция φ_m зависит существенно от переменной $x_{jr+\mu}$ при $n-2j=1$, в этом случае $\exp\Gamma(\varphi) \leqslant (ln/2)^2 + n(r-l) - 2$, где l — длина кратчайшего цикла графа Γ_ψ, проходящего через дугу (μ, m).

В [10] исследован алгоритм «поиска в глубину», используемый для определения длин всех простых циклов сильносвязного n-вершинного орграфа. Вычислительная сложность алгоритма оценивается величиной порядка $\mathrm{O}(n^2 \log n)$, где элементарной операцией считается обращение к памяти и распознавание смежности двух вершин.

В [10] исследован также алгоритм распознавания примитивности n-вершинного орграфа и вычисления его экспонента, основанный на быстром возведении в степень матрицы смежности вершин. Алгоритм требует $\mathrm{O}(n^3 \log n)$ операций сложения и умножения в поле $\mathrm{GF}(2)$.

2.2. Свойства экспонентов неориентированных графов

В [7] сформулированы равносильные критерии примитивности неориентированных графов (далее просто графов) при условии, что ребро можно считать циклом длины 2:

1) связный n-вершинный граф G примитивен тогда и только тогда, когда в G имеется простой цикл нечётной длины;
2) связный n-вершинный граф G примитивен тогда и только тогда, когда G не является двудольным.

Универсальная оценка экспонента примитивного графа [3, с. 409] значительно ниже аналогичной оценки для примитивных орграфов. Если n-вершинный граф G примитивен, то

$$\exp G \leqslant 2(n-1). \tag{3}$$

Рассмотрим n-вершинный граф G. Обозначим при $i \neq j$, где $i, j \in \{1, \ldots, n\}$: $w(i,j)$ — путь из i в j; $[i,j]$ — кратчайший путь из i в j; $[i,i]$ — кратчайший цикл, проходящий через вершину i; $\mathrm{len}[i,j]$ — длина пути $[i,j]$, измеряемая числом рёбер графа G, составляющих путь.

Обозначим через $e(C)$ эксцентриситет цикла C в неориентированном графе G, т. е.

$$e(C) = \max_{i \notin C} \{\min_{j \in C} \mathrm{len}[i,j]\}.$$

Верхнюю границу (3) экспонента графа G при $n > 1$ можно уточнить [7]: если l — длина длиннейшего простого цикла C нечётной длины в примитивном n-вершинном графе G, $1 \leqslant l \leqslant n$, то

$$\exp\Gamma \leqslant 2e(C) + l - 1 \leqslant 2n - l - 1.$$

Если простые циклы нечётных длин покрывают множество вершин графа G, то $\exp\Gamma \leqslant n-1$.

Построено множество графов [7], на которых достигается верхняя граница неравенства (3). Обозначим через $\Gamma_P(n)$ множество примитивных n-вершинных графов, состоящих из гамильтонова пути и петли, инцидентной одной из концевых вершин. При любом $n > 1$ множество $\Gamma_P(n)$ состоит из $n!$ изоморфных графов; абсолютная оценка $\exp\Gamma = 2n-2$ достигается на графах G из множества $\Gamma_P(n)$, и только на них.

3. Оценки субэкспонентов и множественных экспонентов систем матриц

Неотрицательную матрицу A называют субпримитивной, если $A^{[1,t]} > 0$, где $t \in N$, $A^{[1,t]} = A + A^2 + \ldots + A^t$. Субэкспонентом матрицы A называется наименьшее $\sigma \in N$, такое, что $A^{[1,\sigma]} > 0$, и обозначается $\operatorname{sbxp} A$. Если матрица A не субпримитивна, то положим $\operatorname{sbxp} A = \infty$.

Понятия экспонента и субэкспонента могут быть обобщены на систему квадратных неотрицательных матриц $\Omega = \{M_1, \ldots, M_p\}$ одинакового размера. Пусть $N_p = \{1, \ldots, p\}$, N_p^* — множество всех слов в алфавите N_p. Слову $w = s_1 \ldots s_l$ из N_p^* при заданной системе матриц Ω соответствует матрица $M_{s_1} \ldots M_{s_l}$, являющаяся элементом мультипликативной полугруппы $\langle\Omega\rangle$ неотрицательных матриц, порождённой системой Ω. Обозначим $M_{s_1} \ldots M_{s_l} = M(w) = (m_{i,j}(w))$.

Экспонентом системы матриц Ω (обозначается $\exp \Omega$) называется наименьшая длина l слова $w \in N_p^*$, при котором $M(w) > 0$. Если такого слова не существует, то полагаем $\exp \Omega = \infty$.

Субэкспонентом системы матриц Ω (обозначается $\operatorname{sbxp} \Omega$) называется наименьшая длина l слова $w \in N_p^*$, при котором $M^{[1,l]}(w) > 0$, где $M^{[1,l]}(w) = M_{s_1} + M_{s_1} M_{s_2} + \ldots + M(w)$. Если такого слова не существует, то полагаем $\operatorname{sbxp} \Omega = \infty$.

Известно [11], что для любой системы Ω квадратных неотрицательных матриц одинакового размера справедливо

$$\operatorname{sbxp} \Omega \leqslant \exp \Omega.$$

Пусть G_s — орграф с множеством вершин $\{1, \ldots, n\}$, где все дуги помечены числом s, а $M_s = (m_{ij}(s))$ — матрица смежности вершин орграфа G_s, $s = 1, \ldots, p$. Тогда объединение графов $G^{(p)} = G_1 \cup \ldots \cup G_p$ есть либо орграф, либо мультиграф (в зависимости от множества объединяемых дуг), которому соответствует система матриц смежности $\Omega = \{M_1, \ldots, M_p\}$. При этом любой путь длины l в мультиграфе (графе) $G^{(p)}$ помечен словом в алфавите N_p^* длины l. Отсюда система неотрицательных матриц Ω и соответствующий ей мультиграф $G^{(p)}$ одновременно примитивны (субпримитивны) или не примитивны (не субпримитивны), в случае примитивности (субпримитивности) их экспоненты (субэкспоненты) равны.

Для любого мультиграфа $G^{(p)}$ справедливо [11]

$$\operatorname{diam} G^{(p)} \leqslant \operatorname{sbxp} \Omega,$$

причём если $G = G_1 = \ldots = G_p$, то $\operatorname{diam} G = \operatorname{sbxp} \Omega$.

В [11] показано, что мультиграф $G^{(p)}$ сильно связен тогда и только тогда, когда он субпримитивен. Если n-вершинный мультиграф $G^{(p)}$ сильно связен, то при $n \geqslant 4$

$$\operatorname{sbxp} \Omega \leqslant \frac{(n^2 - 2)(n - 1)}{2}.$$

Система квадратных неотрицательных матриц одинакового размера называется множественно примитивной, если существует натуральное l, такое, что для любого слова длины l в алфавите N_p^* имеет место неравенство $M(w) > 0$. Минимальное число k, обладающее таким свойством, называется множественным экспонентом системы матриц Ω.

В [12] доказано, что множество вполне неразложимых матриц порядка n является множественно примитивным и для множественного экспонента k имеет место оценка

$$k \leqslant n - 1.$$

Известна достижимая оценка множественного экспонента любой множественно примитивной системы Ω квадратных неотрицательных матриц порядка n: $k \leqslant 2^n - 2$.

Неотрицательная матрица A порядка n называется r-неразложимой, $0 \leqslant r \leqslant n$, если она не содержит нулевой подматрицы размера $p \times q$, $p + q = n - r + 1$, $0 < p$, $q \leqslant n - r$. Наибольшее из чисел r, при которых матрица A является r-неразложимой, называется индексом неразложимости A.

Пусть $\Omega = \{M_1, \ldots, M_p\}$ — система квадратных неотрицательных матриц порядка n, где индекс неразложимости каждой матрицы M_i, $i = 1, \ldots, p$, не меньше некоторого фиксированного числа r, $r \geqslant 1$. Тогда система Ω множественно примитивна [13], причём для множественного экспонента k системы Ω справедливо

$$k \leqslant \begin{cases} \dfrac{n-1}{r}, & (n-1) \bmod r = 0, \\ \left[\dfrac{n-1}{r}\right] + 1, & (n-1) \bmod r \neq 0. \end{cases}$$

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2009.
2. *Wielandt H.* Unzerlegbare nicht negative Matrizen // Math. Zeitschr. 1950. No. 52. S. 642–648.
3. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000.
4. *Носов В. А., Сачков В. Н., Тараканов В. Е.* Комбинаторный анализ. Неотрицательные матрицы, алгоритмические проблемы // Итоги науки и техники. Сер. теория вер., матем. статист., теорет. киберн. 1983. Т. 21. С. 120–178.
5. *Lewin M. and Vitek Y.* A system of gaps in the exponent set of primitive matrices // Illinois J. Math. 1981. Issue 1. No. 25. P. 87–98.
6. *Берж К.* Теория графов и её применение. М.: ИЛ, 1962.
7. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.
8. *Коренева А. М., Фомичев В. М.* Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика. 2012. № 3(17). С. 34–40.
9. *Князев А. В.* Оценки экстремальных значений основных метрических характеристик псевдосимметрических графов: дис. ... докт. физ.-мат. наук. М., 2002. 203 с.
10. *Кяжин С. Н., Фомичев В. М.* О примитивных наборах натуральных чисел // Прикладная дискретная математика. 2012. № 2(16). С. 5–14.
11. *Фомичев В. М.* Свойства путей в графах и мультиграфах // Прикладная дискретная математика. 2010. № 1(7). С. 118–124.
12. *Сачков В. Н.* Вероятностные преобразователи и правильные мультиграфы // Труды по дискретной математике. 1997. Т. 1. С. 227–250.
13. *Сачков В. Н., Ошкин И. Б.* Экспоненты классов неотрицательных матриц // Дискретная математика. 1993. Т. 5. Вып. 2. С. 150–159.

2012 Теоретические основы прикладной дискретной математики №4(18)

DOI 10.17223/20710410/18/2

УДК 519.214

ОЦЕНКИ СКОРОСТИ СХОДИМОСТИ В ПРЕДЕЛЬНЫХ ТЕОРЕМАХ ДЛЯ СОВМЕСТНЫХ РАСПРЕДЕЛЕНИЙ ЧАСТИ ХАРАКТЕРИСТИК СЛУЧАЙНЫХ ДВОИЧНЫХ ОТОБРАЖЕНИЙ

К. Н. Панков

Московский государственный технический университет радиотехники, электроники и автоматики, г. Москва, Россия

E-mail: k.n.pankov@gmail.com

Исследуется предельное распределение векторов, состоящих из части спектральных и автокорреляционных коэффициентов и весов подфункций линейных комбинаций координатных функций случайной двоичной вектор-функции. Получены теоремы об асимптотической нормальности этих векторов с оценкой скорости сходимости. Получены сравнения, которым должны удовлетворять координаты этих векторов.

Ключевые слова: *случайное двоичное отображение, локальная предельная теорема, закон больших чисел, автокорреляционные коэффициенты, спектральные коэффициенты, веса подфункций.*

Введение

Согласно [1], в устойчивости современных блочных и поточных шифрсистем к различным методам анализа значительную роль играют свойства используемых в них двоичных вектор-функций или S-box'ов. В работе [2] доказано, что многие важные свойства двоичного отображения f, такие, как максимальная нелинейность, корреляционная иммунность, устойчивость, сводятся к обладанию этими свойствами всеми ненулевыми линейными комбинациями координатных функций f, называемых в [3] компонентными функциями или компонентами. Свойства же компонент могут быть выражены в терминах их коэффициентов Фурье — Уолша — Адамара (спектральных коэффициентов), весов подфункций и автокорреляций.

Для произвольных подмножества $I = \{i_1, \ldots, i_{|I|}\}$ множества $\{1, \ldots, n\}$ и непустого подмножества $J = \{j_1, \ldots, j_{|J|}\}$ множества $\{1, \ldots, m\}$ через $w_I^J(f)$ обозначим вес $\left\| \left(f^J\right)^{1,\ldots,1}_{i_1,\ldots,i_{|I|}} \right\|$ подфункции $\left(f^J\right)^{1,\ldots,1}_{i_1,\ldots,i_{|I|}}$ компоненты $f^J = f_{j_1} \oplus \ldots \oplus f_{j_{|J|}}$ отображения $f = (f_1, \ldots, f_m) \in B_n^m$, получаемой, если у аргумента функции f^J значения координат с номерами $i_1, \ldots, i_{|I|}$ положить равными единице. Под $|I|$ понимается мощность множества I.

В таких же условиях для компоненты f^J можно определить спектральный коэффициент Фурье — Уолша — Адамара

$$F_I^J(f) = \frac{1}{2} \sum_{x \in V_n} (-1)^{f^J(x) \oplus x_{i_1} \oplus \ldots \oplus x_{i_{|I|}}}$$

и автокорреляционный коэффициент (автокорреляционную функцию, автокорреляцию)

$$r_I^J(f) = \sum_{x \in V_n} (-1)^{f^J(x) \oplus f^J(x \oplus e_I)},$$

где $e_I \in V_n$ — двоичный вектор веса $|I|$, в котором единицы стоят на $i_1, \ldots, i_{|I|}$ местах, $I \neq \varnothing$.

Многие свойства двоичных отображений зависят от того, чему равен вектор, состоящий из части определённых выше характеристик всех компонент или их части. В частности, двоичное отображение является корреляционно-иммунным порядка k, если вектор

$$\left(w_I^J(f) - 2^{n-|I|-1} : J \subset \{1,\ldots,m\}, J \neq \varnothing, I \subset \{1,\ldots,n\}, 1 \leqslant |I| \leqslant k\right)$$

или вектор

$$\left(F_I^J(f) : J \subset \{1,\ldots,m\}, J \neq \varnothing, I \subset \{1,\ldots,n\}, 1 \leqslant |I| \leqslant k\right)$$

состоят из одних нулей [4]. Кроме того, отображение подчиняется строгому лавинному критерию или критерию распространения степени 1, если состоит из нулей вектор $\left(r_{\{i\}}^{\{j\}}(f) : j \in \{1,\ldots,m\}, i \in \{1,\ldots,n\}\right)$ [1].

Изучению подобных векторов в случае одной компоненты или булевой функции посвящены работы [4–6]. Подробный обзор публикаций, в том числе и по этой тематике, содержится в [1].

Пусть функция f выбирается случайно и равновероятно из множества B_n^m всех m-мерных двоичных функций от n переменных. Это эквивалентно независимому равновероятному выбору её значений $f(\alpha)$ из множества V_m двоичных векторов размерности m для всех α из множества V_n. Можно рассматривать значение функции f как вектор длины m, состоящий из значений её координатных двоичных функций от n переменных:

$$f(\alpha) = (f_1(\alpha), f_2(\alpha), \ldots, f_m(\alpha)) : V_n \to V_m,$$

где $f_i(\alpha) : V_n \to \{0,1\}$ для всех $i \in \{1,\ldots,m\}$.

Тогда значения $f_i(\alpha)$ выбираются независимо и равновероятно из множества $\{0,1\}$ для всех α из множества V_n и для всех $i \in \{1,\ldots,m\}$.

В случае случайного выбора f векторы, состоящие из части характеристик компонент отображения, также являются случайными, и возникает вопрос об их распределении, в том числе и предельном.

В п. 1 данной работы доказаны отношения сравнимости, которым должны удовлетворять координаты векторов части характеристик. В п. 2 получены результаты о характере и скорости сходимости к нулю нормы вектора части спектральных коэффициентов компонент случайного двоичного отображения, а также показана асимптотическая нормальность этого вектора с оценкой скорости сходимости. В п. 3 и 4 при введении дополнительных условий аналогичные результаты получены для векторов части весов подфункций компонент и автокорреляционных коэффициентов.

Везде далее $\mathsf{E}\xi$ обозначает математическое ожидание случайной величины ξ.

1. Сравнения для характеристик компонент двоичного отображения

Для произвольного или случайного отображения f будем записывать далее

$$F_I^J(f) = F_I^J, \quad w_I^J(f) = w_I^J, \quad r_I^J(f) = r_I^J.$$

Формулы связи между спектральными и автокорреляционными коэффициентами широко известны (к примеру, теорема 65 в [7]).

В работе [4] доказаны формулы связи весов подфункций и спектральных коэффициентов для любых булевых функций:

$$F_I^J = \sum_{L \subset I} (-1)^{|L|} \left(2^{n-1} - 2^{|L|} w_L^J\right),$$
$$w_I^J - 2^{n-|I|-1} = 2^{-|I|} \sum_{L \subset I} (-1)^{|L|+1} F_L^J.$$

Последнее равенство, опубликованное О. В. Денисовым в начале 2000 г., является аналогом равенства Саркара для коэффициентов Уолша $W_I^J = 2F_I^J$, названного так в [8]. Из него легко выводится отношение сравнимости для спектральных коэффициентов, также представленное в [4]:

$$F_I^J \equiv \sum_{\substack{L \subset I, \\ L \neq I}} (-1)^{|I \setminus L|+1} F_L^J \pmod{2^{|I|}}.$$

Но это отношение верно для части спектральных коэффициентов, относящихся только к одной компоненте f^J функции f. Докажем следующее

Утверждение 1. Для любого непустого подмножества $J = \left\{j_1, \ldots, j_{|J|}\right\}$ множества $\{1, \ldots, m\}$ и произвольного подмножества $I = \left\{i_1, \ldots, i_{|I|}\right\}$ множества $\{1, \ldots, n\}$ имеет место

$$\sum_{\varnothing \neq S \subset J} (-1)^{|S|+1} w_I^S = 2^{|J|-1} \left\| \left(f_{j_1} \cdot \ldots \cdot f_{j_{|J|}}\right)_{i_1, \ldots, i_{|I|}}^{1, \ldots, 1} \right\|.$$

Доказательство. Очевидно, что $w_I^J = \sum_{\alpha \in V_n} \beta_I(\alpha) f^J(\alpha)$, где $\beta_I(\alpha) = \alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_{|I|}}$ (при $I = \varnothing$ считаем, что $\beta_I(\alpha) \equiv 1$). Получим

$$\sum_{\varnothing \neq S \subset J} (-1)^{|S|+1} w_I^S = \sum_{\varnothing \neq S \subset J} (-1)^{|S|+1} \sum_{\alpha \in V_n} \beta_I(\alpha) f^S(\alpha) =$$
$$= \sum_{\alpha \in V_n} \beta_I(\alpha) \sum_{\varnothing \neq S \subset J} (-1)^{|S|+1} \left(f_{s_1} \oplus \ldots \oplus f_{s_{|S|}}\right).$$

Известно, что $f_{j_1} \oplus \ldots \oplus f_{j_{|J|}} = \sum_{\varnothing \neq K \subset J} (-2)^{|K|-1} f_{k_1} \ldots f_{k_{|K|}}$, следовательно,

$$\sum_{\varnothing \neq S \subset J} (-1)^{|S|+1} \left(f_{s_1} \oplus \ldots \oplus f_{s_{|S|}}\right) = \sum_{\varnothing \neq S \subset J} (-1)^{|S|+1} \sum_{\varnothing \neq K \subset S} (-2)^{|K|-1} f_{k_1} \ldots f_{k_{|K|}} =$$
$$= \sum_{\varnothing \neq K \subset J} (-2)^{|K|-1} f_{k_1} \ldots f_{k_{|K|}} \sum_{S : K \subset S \subset J} (-1)^{|S|+1} =$$
$$= \sum_{\varnothing \neq K \subset J} 2^{|K|-1} f_{k_1} \ldots f_{k_{|K|}} I\{K = J\} = 2^{|J|-1} f_{j_1} \ldots f_{j_{|J|}},$$

где $I\{K = J\}$ — индикатор того, что множество K равно множеству J.

В итоге получаем

$$\sum_{\varnothing \neq S \subset J} (-1)^{|S|+1} w_I^S = \sum_{\alpha \in V_n} \beta_I(\alpha) \sum_{\varnothing \neq S \subset J} (-1)^{|S|+1} \left(f_{s_1} \oplus \ldots \oplus f_{s_{|S|}}\right) =$$
$$= 2^{|J|-1} \sum_{\alpha \in V_n} \beta_I(\alpha) f_{j_1} \ldots f_{j_{|J|}}.$$

Утверждение доказано. ■

Из последнего равенства легко выводится сравнение для весов подфункций.

Следствие 1. В условиях утверждения 1 выполняется сравнение

$$\sum_{\varnothing\neq S\subset J}(-1)^{|S|}w_I^S\equiv 0 \pmod{2^{|J|-1}}.$$

К отношению же из [4] добавляется новое сравнение для спектральных коэффициентов.

Следствие 2. В условиях утверждения 1 выполняются сравнения

$$\sum_{L\subset I}(-1)^{|L|}F_L^J\equiv 0 \pmod{2^{|I|}},$$
$$\sum_{\substack{\varnothing\neq S\subset J,\\ L\subset I}}(-1)^{|L|+|S|}F_L^S\equiv 0 \pmod{2^{|I|+|J|-1}}.$$

Доказательство. Первое сравнение очевидно. Рассмотрим

$$\sum_{\varnothing\neq S\subset J}(-1)^{|S|+1}\left(w_I^S-2^{n-|I|-1}\right)=\sum_{\varnothing\neq S\subset J}(-1)^{|S|+1}\left(2^{-|I|}\cdot\sum_{L\subset I}(-1)^{|L|+1}F_L^S\right),$$
$$\sum_{\varnothing\neq S\subset J}(-1)^{|S|+1}\left(w_I^S-2^{n-|I|-1}\right)=\left(\sum_{\varnothing\neq S\subset J}(-1)^{|S|+1}w_I^S\right)-2^{n-|I|-1}=$$
$$=2^{|J|-1}\left\|\left(f_{j_1}\cdot\ldots\cdot f_{j_{|J|}}\right)_{i_1,\ldots,i_{|I|}}^{1,\ldots,1}\right\|-2^{n-|I|-1},$$
$$\sum_{\varnothing\neq S\subset J}(-1)^{|S|+1}\left(2^{-|I|}\cdot\sum_{L\subset I}(-1)^{|L|+1}F_L^S\right)=2^{-|I|}\sum_{\varnothing\neq S\subset J}\sum_{L\subset I}(-1)^{|L|+|S|}F_L^S.$$

Следовательно, $2^{-|I|-|J|+1}\sum\limits_{\varnothing\neq S\subset J}\sum\limits_{L\subset I}(-1)^{|L|+|S|}F_L^S=\left\|\left(f_{j_1}\cdot\ldots\cdot f_{j_{|J|}}\right)_{i_1,\ldots,i_{|I|}}^{1,\ldots,1}\right\|-2^{n-|I|-|J|}$. ■

Теперь докажем два свойства, общих для автокорреляционных коэффициентов всех двоичных отображений.

Утверждение 2. Пусть $n\in\mathbb{N}$, $n\geqslant 2$, $f(x)\in B_n^m$ — произвольная функция, $I\subset\{1,\ldots,n\}$ и $J\subset\{1,\ldots,m\}$, где $I,J\neq\varnothing$. Тогда

$$r_I^J(f)\equiv 0 \pmod 4.$$

Доказательство. Пусть без ограничения общности $J=\{1\}$, $I=\{n-|I|+1,\ldots,n\}$. Обозначим $\overline{1}_n\in V_n$ двоичный вектор веса $|I|$, состоящий из единиц. Получим

$$r_I^J(f)=\sum_{x\in V_n}(-1)^{f^J(x)\oplus f^J(x\oplus e_I)}=\sum_{\alpha\in V_{n-|I|}}\sum_{\beta\in V_{|I|}}\left((-1)^{f_1(\alpha,\beta)\oplus f_1\left(\alpha,\beta\oplus\overline{1}_{|I|}\right)}\right)=$$
$$=\sum_{\alpha\in V_{n-|I|}}2\sum_{\gamma\in V_{|I|-1}}\left((-1)^{f_1(\alpha,0,\gamma)\oplus f_1\left(\alpha,1,\gamma\oplus\overline{1}_{|I|-1}\right)}\right)=$$
$$=2\sum_{\alpha\in V_{n-|I|}}\sum_{\gamma\in V_{|I|-1}}\left(1-2\left(I\left\{f_1(\alpha,0,\gamma)\oplus f_1\left(\alpha,1,\gamma\oplus\overline{e}_{|I|-1}\right)=1\right\}\right)\right)=$$
$$=4\left(2^{n-2}-\sum_{\alpha\in V_{n-|I|}}\left(\sum_{\gamma\in V_{|I|-1}}I\left\{f_1(\alpha,0,\gamma)\oplus f\left(\alpha,1,\gamma\oplus\overline{e}_{|I|-1}\right)=1\right\}\right)\right).$$

Утверждение доказано. ■

Утверждение 3. Пусть $I_1, I_2 \subset \{1,\dots,n\}$ и $J \subset \{1,\dots,m\}$, где $I_1, I_2, J \neq \varnothing$. Тогда

$$r^J_{I_1} - r^J_{I_2} \equiv 0 \pmod 8.$$

Доказательство. Если $I_1 = I_2$, то утверждение очевидно. Без ограничения общности считаем, что $J = \{1\}$, $I_1 \neq I_2$. Обозначим $e_{I_1} = \alpha$, $e_{I_2} = \beta$, $\alpha \neq \beta$. Тогда

$$r^J_{I_1} - r^J_{I_2} = \sum_{x \in V_n} (-1)^{f_1(x)} \left((-1)^{f_1(x\oplus\alpha)} - (-1)^{f_1(x\oplus\beta)} \right).$$

Будем говорить, что $y \in V_n$ эквивалентен $x \in V_n$, если $y = x \oplus \delta_1\alpha \oplus \delta_2\beta$ для некоторых $\delta_1, \delta_2 \in \{0,1\}$. Очевидно, что отношение эквивалентности введено корректно. Разобьём V_n на классы эквивалентности $V_n/\!\equiv$ по этому отношению и преобразуем разность $r^J_{I_1}(f) - r^J_{I_2}(f)$:

$$\begin{aligned} r^J_{I_1}(f) - r^J_{I_2}(f) = \sum_{x \in V_n/\equiv} \Big(& 2(-1)^{f_1(x\oplus\alpha)\oplus f_1(x)} + 2(-1)^{f_1(x\oplus\alpha\oplus\beta)\oplus f_1(x\oplus\alpha)} - \\ & -2(-1)^{f_1(x\oplus\beta)\oplus f_1(x)} - 2(-1)^{f_1(x\oplus\alpha\oplus\beta)\oplus f_1(x\oplus\beta)} \Big) = \\ = 2 \sum_{x \in V_n/\equiv} & \left((-1)^{f_1(x\oplus\alpha)} - (-1)^{f_1(x\oplus\beta)} \right) \left((-1)^{f_1(x)} + (-1)^{f_1(x\oplus\alpha\oplus\beta)} \right). \end{aligned}$$

Осталось заметить, что в сумме каждый из двух сомножителей делится на 2. ■

Полученные сравнения позволяют уточнить вопрос о возможных значениях, которые могут принимать координаты векторов, состоящие из части характеристик компонент случайного двоичного отображения.

2. Предельные теоремы для вектора, состоящего из части спектральных коэффициентов компонент случайного двоичного отображения

Пусть f — случайная функция из B^m_n. Рассмотрим вектор

$$S(f) = \left(F^{J_s}_{I_s}(f) : I_s \subset \{1,\dots,n\}, \varnothing \neq J_s \subset \{1,\dots,m\}, s \in \{1,\dots,r\} \right),$$

состоящий из r коэффициентов Фурье — Уолша — Адамара, где r — некоторое натуральное число, не превышающее $2^{n+m} - 2^n$, и наборы множеств $(J_1, I_1), \dots, (J_r, I_r)$ попарно различны.

Из определения спектральных коэффициентов легко видеть, что этот вектор равен сумме 2^n векторов

$$S(f) = \frac{1}{2} \sum_{\alpha \in V_n} \chi(\alpha) = \frac{1}{2} \sum_{\alpha \in V_n} \left((-1)^{f^{J_s}(\alpha)\oplus\alpha_{i_1}\oplus\dots\oplus\alpha_{i_{|I_s|}}} : s \in \{1,\dots,r\} \right).$$

Рассмотрим набор из 2^n независимых и одинаково распределённых случайных векторов $\chi(\alpha) = (\chi_1(\alpha), \dots, \chi_r(\alpha))$, $\alpha \in V_n$, координаты которых имеют математическое ожидание

$$\mathsf{E}\chi_s(\alpha) = \mathsf{E}(-1)^{f^{J_s}(\alpha)\oplus\alpha_{i_1}\oplus\dots\oplus\alpha_{i_{|I_s|}}} = 0$$

для всех $s \in \{1,\dots,r\}$.

Очевидно, что для любых $k, s \in \{1,\dots,r\}$ ковариация координат равна

$$\operatorname{cov}(\chi_s(\alpha), \chi_k(\alpha)) = \mathsf{E}(-1)^{f^{J_s}(\alpha)\oplus\alpha_{i_1}\oplus\dots\oplus\alpha_{i_{|I_s|}}\oplus f^{J_k}(\alpha)\oplus\alpha_{i_1}\oplus\dots\oplus\alpha_{i_{|I_k|}}} = I\{k = s\}.$$

Следовательно, $\chi(\alpha)$, $\alpha \in V_n$, — независимые одинаково распределённые в $\mathbb{R}^r$ случайные векторы с единичной ковариационной матрицей и нулевым средним.

Сумма векторов $\sum\limits_{\alpha \in V_n} \chi(\alpha)$ лежит в множестве $\mathbb{R}^r$, которое является евклидовым пространством со скалярным произведением $(\overrightarrow{x}, \overrightarrow{y}) = \sum\limits_{i=1}^{r} x_i y_i$, где $\overrightarrow{x} = (x_1 \dots x_r) \in \mathbb{R}^r$, $\overrightarrow{y} = (y_1 \dots y_r) \in \mathbb{R}^r$, и нормой $\|\overrightarrow{x}\| = \sqrt{(\overrightarrow{x}, \overrightarrow{x})}$.

Как легко видеть, $\|\chi(\alpha)\| = \sqrt{r}$, следовательно, верно, что $\mathsf{E}\left(\|\chi(\alpha)\|^{\beta}\right) = r^{\beta/2} < \infty$ при всех вещественных $\beta \in (0, 2)$. Таким образом, мы попадаем в условия основной теоремы [9], из которой следует, что верно

Утверждение 4. Пусть $n \to \infty$, m — произвольное натуральное число, $\beta \in \in (0, 2)$ — вещественное число. Тогда для любых попарно различных наборов множеств (J_1, I_1), …, (J_r, I_r), где $I_s \subset \{1, \dots, n\}$, $\varnothing \neq J_s \subset \{1, \dots, m\}$ для всех $s \in \{1, \dots, r\}$, $r \in \mathbb{N}$, верно, что норма вектора $2^{-n/\beta} S(f)$ сходится к нулю с вероятностью 1.

Данное утверждение при $\beta = 1$ является формулировкой усиленного закона больших чисел для случайных векторов $\chi(\alpha)$, $\alpha \in V_n$.

Очевидно, что выполняется и обычный закон больших чисел для случайных векторов, и возникает вопрос о скорости сходимости нормы вектора $2^{-n/\beta} S(f)$ к нулю.

Для случайных векторов с нулевыми математическими ожиданиями выполняется теорема 1 [10, с. 47], из которой следует

Утверждение 5. Пусть n, m — произвольные натуральные числа, $\beta \in (0, 2)$ — вещественное число. Тогда для любых попарно различных (J_1, I_1), …, (J_r, I_r), где $I_s \subset \{1, \dots, n\}$, $\varnothing \neq J_s \subset \{1, \dots, m\}$ для всех $s \in \{1, \dots, r\}$, $r \in \mathbb{N}$, для любого $\varepsilon > 0$ верно неравенство

$$\mathsf{P}\left\{\left\|2^{-n/\beta} S(f)\right\| \geqslant \varepsilon\right\} \leqslant \frac{4r}{\varepsilon^2} 2^{(\beta-2)n/\beta}.$$

Докажем теперь теорему о скорости сходимости распределения P_n вектора $2^{1-n/2} S(f)$ к распределению Φ стандартного r-мерного нормального закона.

Теорема 1. Пусть n, m — произвольные натуральные числа. Тогда для любых попарно различных $(J_1, I_1), \dots, (J_r, I_r)$, где $I_s \subset \{1, \dots, n\}$, $\varnothing \neq J_s \subset \{1, \dots, m\}$ для всех $s \in \{1, \dots, r\}$, $r \in \mathbb{N}$, и для любого выпуклого борелевского множества B справедливо неравенство $|P_n(B) - \Phi(B)| \leqslant 400 r^{7/4} 2^{-n/2}$.

Доказательство. Согласно основному результату [11], если $\xi^{(1)}, \xi^{(2)}, \dots$ — независимые одинаково распределённые в $\mathbb{R}^r$ случайные величины с единичной ковариационной матрицей и нулевым средним, μ — случайная величина со стандартным r-мерным нормальным распределением, $S_N = N^{-1/2} \sum\limits_{j=1}^{N} \xi^{(j)}$, то $\delta_N = \sup\limits_{A \in L} |P(S_N \in A) - P(\mu \in A)| \leqslant 400 r^{1/4} \mathsf{E}\left\|\xi^{(1)}\right\|^3 N^{-1/2}$, где L — класс выпуклых борелевских подмножеств $\mathbb{R}^r$.

Для векторов $\chi(\alpha)$, $\alpha \in V_n$, попадаем в условия этого результата при $\mathsf{E}\|\chi(\alpha)\|^3 = r^{3/2}$ и $N = 2^n$. ■

Данная теорема предлагает равномерные по r оценки расстояния между распределением вектора $2^{1-n/2} S(f)$ и многомерным стандартным нормальным распределением в обобщённой метрике полной вариации по классу выпуклых борелевских множеств и, следовательно, в равномерной метрике в терминах [12]. При $n \to \infty$ из этой тео-

ремы следует асимптотическая нормальность вектора и, следовательно, интегральная предельная теорема.

3. Предельные теоремы для вектора, состоящего из части весов подфункций компонент случайного двоичного отображения

Теперь рассмотрим вектор $W(f) = \left(2^{1+(|I_s|/2)}\left(w_{I_s}^{J_s}(f) - 2^{n-|I_s|-1}\right) : I_s \subset \{1,\dots,n\},\ \varnothing \neq J_s \subset \{1,\dots,m\}, s \in \{1,\dots,r\}\right)$, состоящий из r весов подфункций, где r — некоторое натуральное число, не превышающее $2^{n+m} - 2^n$, а пары множеств $(J_1, I_1), \dots, (J_r, I_r)$ — любые попарно различные.

Из определения $w_I^J(f)$ легко видеть, что этот вектор равен сумме векторов

$$W(f) = \sum_{\alpha \in V_n} \left(2^{\frac{|I_s|}{2}} \beta_{I_S}(\alpha)(-1)^{f^{J_s}(\alpha)\oplus 1} : s \in \{1,\dots,r\}\right) = \sum_{\alpha \in V_n} \tau(\alpha),$$

где $\beta_I(\alpha) = \alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_{|I|}}$(при $I = \varnothing$ считаем, что $\beta_I(\alpha) \equiv 1$).

Рассмотрим набор из 2^n независимых случайных векторов $\tau(\alpha)$, для всех координат которого $\tau_s(\alpha)$ верно равенство

$$\mathsf{E}\tau_s(\alpha) = 2^{\frac{|I_s|}{2}} \beta_{I_S}(\alpha)\,\mathsf{E}(-1)^{f^{J_s}(\alpha)\oplus 1} = 0.$$

Следовательно, $\tau(\alpha)$, $\alpha \in V_n$ — независимые не одинаково распределенные в $\mathbb{R}^r$ случайные величины с нулевым средним. Сумма векторов $\sum\limits_{\alpha \in V_n} \tau(\alpha)$ лежит в $\mathbb{R}^r$. Введём

Условия 1. Пусть выполняется следующее:

1) Зафиксировано некоторое натуральное $r \in \{1,\dots,2^m - 1\}$.
2) Зафиксирован набор непустых попарно различных подмножеств $J_1,\dots,J_r$ множества $\{1,\dots,m\}$.
3) Для любого $s \in \{1,\dots,r\}$ зафиксировано произвольное подмножество I_s множества $\{1,\dots,n\}$.

Обозначим $\delta = \sum\limits_{s=1}^{r} 2^{|I_s|}$.

Пусть выполняются условия 1. Тогда при фиксированном m выполняется неравенство $\mathsf{E}\|\tau(\alpha)\|^2 \leqslant \delta < +\infty$. Следовательно, попадаем в условия теоремы 4.2.1 [13], согласно которой верно следующее

Утверждение 6. Пусть $n \to \infty$, m — произвольное натуральное число. Тогда для любых попарно различных $(J_1, I_1), \dots, (J_r, I_r)$, удовлетворяющих условиям 1, норма вектора $2^{-n}W(f)$ сходится к нулю с вероятностью 1.

Данное утверждение является формулировкой усиленного закона больших чисел для случайных векторов $\tau(\alpha)$, $\alpha \in V_n$.

Рассмотрим вопрос о скорости сходимости нормы вектора $2^{-n}W(f)$ к нулю. Аналогично утверждению 5 можно легко доказать, что верно

Утверждение 7. Пусть n,m — произвольные натуральные числа. Тогда для любых попарно различных $(J_1, I_1), \dots, (J_r, I_r)$ и для любого $\varepsilon > 0$ верно неравенство

$$\mathsf{P}\left\{\left\|2^{-n}W(f)\right\| \geqslant \varepsilon\right\} \leqslant \varepsilon^{-2}2^{-n}\sum_{s=1}^{r} 2^{|I_s|}.$$

Определение 1 [14]. Пусть $\xi^{(1)},\dots,\xi^{(N)}$ есть N независимых не обязательно одинаково распределённых случайных векторов в $\mathbb{R}^r$ с ковариационными матрицами $\operatorname{cov}\left(\xi^{(j)}\right)$, $j\in\{1,\dots,N\}$. Тогда средней ковариационной матрицей случайных векторов $\xi^{(1)},\dots,\xi^{(N)}$ называется матрица $V=\dfrac{1}{N}\sum\limits_{j=1}^{N}\operatorname{cov}\left(\xi^{(j)}\right)$.

Теперь оценим скорость сходимости характеристической функции специальным образом преобразованного вектора, составленного из весов подфункций, к характеристической функции стандартного многомерного нормального закона соответствующей размерности.

Утверждение 8. Пусть n, m — произвольные натуральные числа. Дано случайное отображение $f=(f_1,f_2,\dots,f_m)\in B_n^m$ и выполняются условия 1. Тогда для всех $t\in\mathbb{R}^r$, таких, что $\|t\|\leqslant 2^{n/4-1}\delta^{-1/2}$, для характеристической функции $\varphi_{w_r}(t)$ случайного вектора

$$w_r=\left(2^{\frac{|I_s|}{2}+1-\frac{n}{2}}\left(w_{I_s}^{J_s}(f)-2^{n-|I_s|-1}\right):I_s\subset\{1,\dots,n\},\varnothing\neq J_s\subset\{1,\dots,m\},s\in\{1,\dots,r\}\right)$$

верно неравенство

$$\left|\varphi_{w_r}(t)-e^{-\frac{1}{2}\|t\|^2}\right|\leqslant 2^{-n-2}\|t\|^4\delta^2\left(\frac{7}{10}e^{-\frac{1}{2}\|t\|^4}+\delta\|t\|^2\left(\frac{9}{125}2^{-n}\delta\|t\|^2+\frac{1}{9}\right)e^{-\frac{383}{1000}\|t\|^2}\right).$$

Доказательство. Пусть f — случайная функция из B_n^m. Рассмотрим вектор

$$w_r=\left(2^{\frac{|I_s|}{2}+1-\frac{n}{2}}\left(w_{I_s}^{J_s}(f)-\mathsf{E}w_{I_s}^{J_s}(f)\right):s\in\{1,\dots,r\}\right),$$

где $\mathsf{E}w_{I_s}^{J_s}(f)=2^{n-|I_s|-1}$. Очевидно, что $w_r=2^{-n/2}\sum\limits_{\alpha\in V_n}\tau(\alpha)$.

Рассмотрим набор из 2^n независимых случайных векторов $\tau(\alpha)$, для всех координат которого $\tau_s(\alpha)$ выполняется свойство $\mathsf{E}\tau_s(\alpha)=0$.

Для любых $k,s\in\{1,\dots,r\}$ верно равенство

$$\operatorname{cov}\left(\tau_s(\alpha),\tau_k(\alpha)\right)=2^{\frac{|I_s|}{2}+\frac{|I_k|}{2}}\beta_{I_s}(\alpha)\beta_{I_k}(\alpha)\,\mathsf{E}(-1)^{f^{J_s}(\alpha)\oplus f^{J_k}(\alpha)}=2^{|I_s|}\beta_{I_s}(\alpha)\,I\{k=s\}.$$

Следовательно, средняя ковариационная матрица V, за исключением главной диагонали, заполнена нулями, а элементы главной диагонали равны

$$\frac{1}{2^n}\sum_{\alpha\in V_n}2^{|I_s|}\beta_{I_s}(\alpha)=1.$$

Получили, что $\tau(\alpha)$, $\alpha\in V_n$ — независимые неодинаково распределённые в $\mathbb{R}^r$ случайные векторы с единичной средней ковариационной матрицей и нулевым средним.

Рассмотрим ляпуновскую дробь $l_{s,2^n}$, определённую по формуле

$$l_{s,2^n}=\sup_{\|t\|=1,t\in\mathbb{R}^r}\frac{\sum\limits_{\alpha\in V_n}\mathsf{E}\left(|(t,\tau(\alpha))|^s\right)}{\left(\sum\limits_{\alpha\in V_n}\mathsf{E}\left((t,\tau(\alpha))^2\right)\right)^{s/2}}.$$

Во введённых обозначениях выполняется теорема 8.6 из [14], согласно которой, если каждый вектор $\tau(\alpha)$ имеет конечный четвертый абсолютный момент $\rho_4(\tau(\alpha))=$

$= \mathsf{E}\|\tau(\alpha)\|^4$ и ляпуновская дробь $l_{4,2^n}$ не превосходит единицы, то для всех $t \in \mathbb{R}^r$, таких, что $\|t\| \leqslant \frac{1}{2} l_{4,2^n}^{-1/4}$, справедливо неравенство

$$\left|\varphi_{w_r}(t) - e^{-\frac{1}{2}\|t\|^2}\left(1 + i^6 2^{-n/2}\mu_3(t)\right)\right| \leqslant$$
$$\leqslant \frac{7}{40} l_{4,2^n}\|t\|^4 e^{-\frac{1}{2}\|t\|^4} + \left(\frac{9}{500} l_{4,2^n}^2\|t\|^8 + \frac{1}{36} l_{3,2^n}^2\|t\|^6\right) e^{-\frac{383}{1000}\|t\|^2},$$

где $\mu_3(t) = 2^{-n} \sum\limits_{\alpha \in V_n} E\left((t, \tau(\alpha))^3\right)$. Легко видеть, что

$$\rho_4(\tau(\alpha)) = \left(\sum_{s=1}^{r}\left(2^{\frac{|I_s|}{2}}\beta_{I_S}(\alpha)\right)^2\right)^2 = \left(\sum_{s=1}^{r} 2^{|I_s|}\beta_{I_S}(\alpha)\right)^2 \leqslant \delta^2.$$

В обозначениях (8.11) в [14] $\rho_4 = 2^{-n} \sum\limits_{\alpha \in V_n} \rho_4(\tau(\alpha))$.

Очевидно, что $\rho_4 \leqslant \delta^2$, $\mathsf{E}\left((t, \tau(\alpha))^3\right) = 0$ и $\mu_3(t) = 0$.

В силу неравенства (8.12) из [14] $l_{4,2^n} \leqslant 2^{-n}\delta^2$, $l_{3,2^n} \leqslant 2^{-n/2}\delta^{3/2}$. Следовательно, для всех $t \in \mathbb{R}^r$, таких, что $\|t\| \leqslant 2^{n/4-1}\delta^{-1/2} \leqslant 2^{n/4-1}(\rho_4)^{-1/4} \leqslant \frac{1}{2} l_{4,2^n}^{-1/4}$, выполняется утверждение теоремы. ■

Теперь, используя утверждение 8, докажем теорему о скорости сходимости распределения w_r к распределению Φ стандартного r-мерного нормального закона.

Теорема 2. Пусть m, n — произвольные натуральные числа, L — множество борелевских выпуклых подмножеств $\mathbb{R}^r$, выполняется набор условий 1 и дано случайное отображение $f = (f_1, f_2, \ldots, f_m) \in B_n^m$. Пусть для n выполняется

$$n > \max\left\{\delta^2 - 1,\ 12 + 2\log_2\left(9\delta(r+2)^2\right)\right\}.$$

Тогда для случайного вектора w_r из формулировки утверждения 8 с распределением Q_n верно следующее неравенство:

$$\sup_{C \in \mathfrak{C}} |Q_n(C) - \Phi(C)| \leqslant \frac{4}{3}\Big(b_1(r)\,2^{-n/2} + b_2(r)\,2^{-n/2}n^{-1/2} + b_3(r)\,2^{-n}n^{r/2} +$$
$$+ b_4(r)\,2^{-3n/2}n^{-3/2} + b_5(r)\,2^{-2n}n^{r/2} + b_6(r)\,e^{-\frac{2^{n/2}}{280\sqrt{\delta}}}2^{-n/4}n^{r/2} +$$
$$+ b_7(r)\,e^{-\frac{2^{n/2}}{16\sqrt{\delta}}}2^{-n/4}n^{r/2} + b_8(r)\,e^{-\frac{2^{n/2}}{16\sqrt{\delta}}}2^{-3n/4}n^{r/2}\Big),$$

где Φ — распределение случайной величины со стандартным r-мерным нормальным распределением,

$$b_1(r) = \frac{2^5 r^{4/3}\delta^{3/2}\Gamma\left((r+1)/2\right)}{3\pi^{1/3}\Gamma(r/2)} + \frac{11r\delta^{3/2}}{2} +$$
$$+ \frac{\left(4 + e^{3/2}\right)\delta^{3/2}}{6e^{3/2}\sqrt{2\pi}} + \frac{(r-1)\,\delta^{3/2}}{2r^{1/2}\pi e^{1/2}} + \frac{2^{1/2}\delta^{3/2}\left(r^{3/2} - 3r^{1/2} + 2\right)}{\pi^{3/2}},$$

$$b_3(r) = \frac{2^{(r-1)/2} r^{(r-2)/2}(\ln 2)^{r/2}\delta^2}{\left(\Gamma(r/2)\right)^2}\left(\frac{7}{20}2^{\frac{r}{4}}\Gamma\left(\frac{r+4}{4}\right) + \frac{\delta}{18}\left(\frac{1000}{383}\right)^{\frac{r+6}{2}}\Gamma\left(\frac{r+6}{2}\right)\right),$$

$$b_4(r)=\frac{2^3r^{5/2}\delta^3}{\pi(\log 2)^{3/2}},b_5(r)=\frac{9\cdot 2^{(r-3)/2}r^{(r-2)/2}(\ln 2)^{r/2}\delta^4\left(\frac{1000}{383}\right)^{\frac{r+8}{2}}\Gamma\left(\frac{r+8}{2}\right)}{125(\Gamma(r/2))^2},$$

$$b_2(r)=\frac{r}{(\pi\ln 2)^{1/2}},b_6(r)=\frac{2^{r+3}\delta^{1/2}r^{(r-2)/2}(\ln 2)^{r/2}}{(\Gamma(r/2))^2}\left(\frac{3}{3-2\sqrt{2}}\right)^{(1+r)/2},$$

$$b_7(r)=\frac{\delta^{1/2}2^{r+3}r^{(r-2)/2}(\ln 2)^{r/2}}{(\Gamma(r/2))^2},b_8(r)=\frac{\delta^2 2^{r+7/2}r^{(r-2)/2}(\ln 2)^{r/2}}{3(\Gamma(r/2))^2}.$$

Здесь $\Gamma(x)$ — значение гамма-функции Эйлера в точке x.

Доказательство. Верно следующее равенство:

$$|\mathsf{P}(w_r\in C)-\Phi(C)|=\left|\int\limits_{\mathbb{R}^r}I_C d(Q_n-\Phi)\right|,$$

где I_C — индикатор множества C.

Рассмотрим случайный вектор K со значениями в $\mathbb{R}^r$ с плотностью

$$p_K(x_1\dots x_r)=\left(\frac{3a}{2\pi}\right)^r\prod_{s=1}^r\left(\frac{\sin ax_s}{ax_s}\right)^4,$$

где $a=2\pi^{-1/3}r^{5/6}$. Сглаживающая вероятностная мера, порождённая этим вектором, активно используется в [14].

Рассмотрим случайный вектор εK с распределением K_ε. Согласно неравенству (13.12) из [14],

$$\mathsf{P}(\varepsilon K\in\mathbb{R}^r\backslash B(0:\varepsilon))\leqslant\mathsf{P}(K\in\mathbb{R}^r\backslash B(0:1))\leqslant\frac{1}{8},$$

где $B(x:\varepsilon)$ — открытый шар в $\mathbb{R}^r$ радиуса ε с центром в x. Тогда

$$\mathsf{P}(\varepsilon K\in B(0:\varepsilon))\geqslant\frac{7}{8}>\frac{1}{2}.$$

Следовательно, попадаем в условия следствия 11.5 в [14]:

$$\left|\int\limits_{\mathbb{R}^r}I_C d(Q_n-\Phi)\right|\leqslant\frac{4}{3}\left(\frac{1}{2}w_{I_C}(\mathbb{R}^r)\,\|(Q_n-\Phi)*K_\varepsilon\|+w^*_{I_C}(2\varepsilon:\Phi)\right),$$

где $*$ — внутренняя операция свёртки (композиции) двух конечных обобщённых мер; $w_{I_C}(S)=\sup\limits_{x,y\in S}|I_C(x)-I_C(y)|$ — колебание функции I_C на множестве S; вариационная норма [14] на классе всех конечных обобщённых мер, равная полной вариации меры, обозначена как $\|(Q_n-\Phi)*K_\varepsilon\|$,

$$w^*_{I_C}(2\varepsilon:\Phi)=\sup_{y\in\mathbb{R}^r}\int\limits_{\mathbb{R}^r}w_{I_C}(B(x-y:2\varepsilon))\,\Phi(dx).$$

Очевидно, что $w_{I_C}(\mathbb{R}^r)=1$, а, согласно неравенству (13.42) из [14],

$$w^*_{I_C}(2\varepsilon:\Phi)\leqslant\frac{2^{5/2}\Gamma((r+1)/2)}{3\Gamma(r/2)}\varepsilon.$$

Теперь рассмотрим поведение величины $\|(Q_n - \Phi) * K_\varepsilon\|$. Из определения вариационной нормы следует, что

$$\|(Q_n - \Phi) * K_\varepsilon\| = 2 \sup_{B \in B^r} |(Q_n - \Phi) * K_\varepsilon (B)|,$$

где B^r — борелевская сигма-алгебра подмножеств из $\mathbb{R}^r$.

Для каждого борелевского множества B и $k > 0$ определим множества

$$B_1 = B \cap B(0 : k), \quad B_2 = B \backslash B_1.$$

Оценим $|(Q_n - \Phi) * K_\varepsilon (B_i)|$, $i \in \{1, 2\}$.

Рассмотрим конечную обобщённую меру $P_1(\alpha)$ с плотностью

$$\varphi(x_1 \dots x_r) \times \left[\frac{1}{6}\left(\chi_{(3,0,\dots,0)}\left(x_1^3 - 3x_1\right) + \dots + \chi_{(0,0,\dots,3)}\left(x_r^3 - 3x_r\right)\right) + \right.$$
$$+\frac{1}{2}\left(\chi_{(2,1,\dots,0)}\left(x_1^2 x_2 - x_2\right) + \chi_{(0,\dots,1,2)}\left(x_r^2 x_{r-1} - x_{r-1}\right)\right) +$$
$$\left. +\chi_{(1,1,1,0,\dots,0)} x_1 x_2 x_3 + \dots + \chi_{(0,\dots,1,1,1)} x_{r-2} x_{r-1} x_r\right] = p_1^\alpha (x_1 \dots x_r),$$

где $\chi_{(\gamma_1,\dots,\gamma_k)} = \chi_\gamma$ — семиинварианты (кумулянты) вероятностной меры, порождённой случайным вектором $\tau(\alpha)$, порядка γ; $\varphi(x_1 \dots x_r)$ — плотность распределения случайного вектора со стандартным r-мерным нормальным распределением.

Согласно равенству (7.22) из [14], $\int\limits_{\mathbb{R}^r} p_1^\alpha (x_1 \dots x_r)\, dx = 0$. Пусть $P_1 = 2^{-n} \sum\limits_{\alpha \in V_n} p_1^\alpha (x_1 \dots x_r)$.

Данная мера введена в равенстве (2.10) в [15]. Имеем

$$|(Q_n - \Phi) * K_\varepsilon (B_1)| \leqslant |H_n * K_\varepsilon (B_1)| + 2^{-n/2} |P_1 * K_\varepsilon (B_1)|,$$

где $H_n = Q_n - \Phi - 2^{-n/2} P_1$.

Обозначим через $\widehat{H_n} = \int\limits_{\mathbb{R}^r} e^{i(t,x)} H_n(dx)$ преобразование Фурье обобщённой меры H_n. Согласно неравенству (13.22) из [14], получим

$$|H_n * K_\varepsilon (B_1)| \leqslant (2\pi)^{-r} \lambda_r (B_1) \int\limits_{\mathbb{R}^r} \left|\widehat{H_n}(t)\, \widehat{K_\varepsilon}(t)\right| dx,$$

где λ_r — мера Лебега на $\mathbb{R}^r$.

С учётом вычисленного в [14] преобразования Фурье для P_1 получаем, что верно равенство

$$\widehat{H_n} = \int\limits_{\mathbb{R}^r} e^{i(t,x)} H_n(dx) = \int\limits_{\mathbb{R}^r} e^{i(t,x)} \left(Q_n - \Phi - n^{-1/2} P_1\right)(dx) =$$
$$= \widehat{Q_n} - e^{-\frac{1}{2}\|t\|^2} \left(1 + \frac{i^3}{6} n^{-1/2} \mu_3(t)\right), \text{ где } \mu_3(t) = 2^{-n} \sum_{\alpha \in V_n} E\left((t, \tau(\alpha))^3\right).$$

Легко показать, что $E\left((t, \tau(\alpha))^3\right) = 0$.

Возьмем в качестве ε величину $a r^{1/2} \rho_3 2^{-(n-3)/2}$, где $\rho_3 = 2^{-n} \sum\limits_{\alpha \in V_n} \rho_3 (\tau(\alpha))$, $\rho_3 (\tau(\alpha)) = \mathsf{E}\|\tau(\alpha)\|^3$. Очевидно, что $\rho_3 \leqslant \delta^{3/2}$.

Согласно соотношению (13.36) в [14], верно неравенство

$$\int\limits_{\mathbb{R}^r}\left|\widehat{H_n}\,(t)\,\widehat{K_\varepsilon}\,(t)\right|dt\leqslant\int\limits_{\|t\|<2^{(n+1)/2}(\rho_3)^{-1}}\left|\widehat{H_n}\,(t)\right|dt=$$

$$=\int\limits_{\|t\|\leqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac14}}\left|\widehat{H_n}\,(t)\right|dt+\int\limits_{2^{\frac{n}{4}-1}(\rho_4)^{-\frac14}<\|t\|<2^{(n+1)/2}(\rho_3)^{-1}}\left|\widehat{H_n}\,(t)\right|dt,$$

где ρ_4 введено в конце доказательства утверждения 8. Там же показано, что утверждение 8 верно при всех $\|t\|\leqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac14}$. Следовательно,

$$\int\limits_{\|t\|\leqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac14}}\left|\widehat{H_n}\,(t)\right|dt=\int\limits_{\|t\|\leqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac14}}\left|\widehat{Q_n}-e^{-\frac12\|t\|^2}\right|dt\leqslant$$

$$\leqslant\frac{7}{5}2^{-n-3}\delta^2\int\limits_{\|t\|\leqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac14}}\|t\|^4e^{-\frac12\|t\|^4}dt+\frac{9}{125}2^{-2n-2}\delta^4\times$$

$$\times\ldots\int\limits_{\|t\|\leqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac14}}\|t\|^8e^{-\frac{383}{1000}\|t\|^2}dt+\frac{2^{-n-2}}{9}\delta^3\int\limits_{\|t\|\leqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac14}}\|t\|^6e^{-\frac{383}{1000}\|t\|^2}dt.$$

Легко можно показать, что верны следующие неравенства:

$$\int\limits_{\|t\|\leqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac12}}\|t\|^4e^{-\frac12\|t\|^4}dt\leqslant\int\limits_{\mathbb{R}^r}\|t\|^4e^{-\frac12\|t\|^4}dt=\frac{2\pi^{r/2}}{\Gamma\,(r/2)}\int\limits_0^{+\infty}x^{r+3}e^{-\frac12x^4}dx,$$

$$\int\limits_{\|t\|\leqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac12}}\|t\|^8e^{-\frac{383}{1000}\|t\|^2}dt\leqslant\frac{2\pi^{r/2}}{\Gamma\,(r/2)}\int\limits_0^{+\infty}x^{r+7}e^{-\frac{383}{1000}x^2}dx,$$

$$\int\limits_{\|t\|\leqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac12}}\|t\|^6e^{-\frac{383}{1000}\|t\|^2}dt\leqslant\frac{2\pi^{r/2}}{\Gamma\,(r/2)}\int\limits_0^{+\infty}x^{r+5}e^{-\frac{383}{1000}x^2}dx.$$

Из равенства $\int\limits_0^{+\infty}x^me^{-ax^n}dx=a^{-(m+1)/n}\frac1n\Gamma\left((m+1)/n\right)$ следует, что

$$\int\limits_{\|t\|\leqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac14}}\left|\widehat{H_n}\,(t)\right|dt\leqslant\tfrac{\pi^{r/2}}{\Gamma(r/2)}\delta^2 2^{-n-1}\left(\tfrac{7}{20}2^{r/4}\Gamma\left(\tfrac{r+4}{4}\right)+\right.$$

$$\left.+\frac{9\delta^2}{250}2^{-n}\left(\frac{1000}{383}\right)^{(r+8)/2}\Gamma\left(\frac{r+8}{2}\right)+\frac{\delta}{18}\left(\frac{1000}{383}\right)^{(r+6)/2}\Gamma\left(\frac{r+6}{2}\right)\right).$$

Согласно оценке (13.39) в [14], при $n\geqslant\delta^2\geqslant\rho_4$ верно неравенство

$$\int\limits_{2^{\frac{n}{4}-1}(\rho_4)^{-\frac14}<\|t\|<2^{(n+1)/2}(\rho_3)^{-1}}\left|\widehat{H_n}\,(t)\right|dt\leqslant\int\limits_{\|t\|\geqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac14}}e^{\|t\|^2\left(2\sqrt2-3\right)/6}dt+$$

$$+\int\limits_{\|t\|\geqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac14}}e^{-\frac12\|t\|^2}dt+\frac16\rho_32^{-n/2}\int\limits_{\|t\|\geqslant 2^{\frac{n}{4}-1}(\rho_4)^{-\frac14}}\|t\|^3e^{-\frac12\|t\|^2}dt.$$

Следовательно,

$$\int\limits_{2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}<\|t\|<2^{(n+1)/2}(\rho_3)^{-1}} \left|\widehat{H_n}(t)\right| dt \leqslant$$

$$\leqslant \frac{2\pi^{r/2}}{\Gamma(r/2)}\left(\left(\frac{6}{3-2\sqrt{2}}\right)^{r/2}\int\limits_{2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}\sqrt{\frac{3-2\sqrt{2}}{6}}}^{+\infty} x^{r-1}e^{-x^2}dx+\right.$$

$$\left.+2^{r/2}\int\limits_{2^{\frac{n}{4}-\frac{3}{2}}(\rho_4)^{-\frac{1}{4}}}^{+\infty} x^{r-1}e^{-x^2}dx+\frac{1}{3}\rho_3 2^{(r+1-n)/2}\int\limits_{2^{\frac{n}{4}-\frac{3}{2}}(\rho_4)^{-\frac{1}{4}}}^{+\infty} x^{r+2}e^{-x^2}dx\right).$$

Для всех $n > 12 + 2\log_2\left(9\delta(r+2)^2\right)$ подынтегральные функции можно ограничить функцией $e^{-x^2}/2$ и, использовав известное неравенство, получить

$$\int\limits_{2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}<\|t\|<2^{(n+1)/2}(\rho_3)^{-1}} \left|\widehat{H_n}(t)\right| dt \leqslant \frac{4\pi^{r/2}\delta^{1/2}}{\Gamma(r/2)}\times$$

$$\times\left(\left(\frac{6}{3-2\sqrt{2}}\right)^{(1+r)/2}2^{-n/4}e^{-\frac{2^{n/2}}{280\sqrt{\delta}}}+\left(2^{r/2}+\frac{\delta^{3/2}}{3}2^{(r+1-n)/2}\right)e^{-\frac{2^{n/2}}{16\sqrt{\delta}}}2^{(2-n)/4}\right).$$

Применяя лемму 13.1 из [14] и учитывая, что $\rho_3 \leqslant \delta^{3/2}$, получаем

$$2^{-n/2}\left|P_1 * K_\varepsilon(B_1)\right| \leqslant 2^{-(n+2)/2}\|P_1\| \leqslant$$

$$\leqslant\left(\frac{4+e^{3/2}}{6e^{3/2}\sqrt{2\pi}}+\frac{(r-1)}{2r^{1/2}\pi e^{1/2}}+\frac{2^{1/2}\left(r^{3/2}-3r^{1/2}+2\right)}{\pi^{3/2}}\right)\delta^{3/2}2^{-n/2}.$$

Собирая все оценки воедино, с учётом того, что $\lambda_r(B_1) \leqslant \frac{2\pi^{r/2}}{r\Gamma(r/2)}k^r$, получаем, что верно неравенство

$$\left|(Q_n-\Phi) * K_\varepsilon(B_1)\right| \leqslant \frac{2k^r}{r2^r\left(\Gamma(r/2)\right)^2}\left(\left(\delta^2 2^{-n-1}\left(\frac{7}{20}2^{\frac{r}{4}}\Gamma\left(\frac{r+4}{4}\right)+\right.\right.\right.$$

$$\left.+\frac{9\delta^2}{250}2^{-n}\left(\frac{1000}{383}\right)^{\frac{r+8}{2}}\Gamma\left(\frac{r+8}{2}\right)+\frac{\delta}{18}\left(\frac{1000}{383}\right)^{\frac{r+6}{2}}\Gamma\left(\frac{r+6}{2}\right)\right)+$$

$$+4\delta^{1/2}\left(\left(\frac{6}{3-2\sqrt{2}}\right)^{(1+r)/2}2^{-n/4}e^{-\frac{2^{n/2}}{280\sqrt{\delta}}}+\left(2^{r/2}+\frac{\delta^{3/2}}{3}2^{(r+1-n)/2}\right)e^{-\frac{2^{n/2}}{16\sqrt{\delta}}}2^{(2-n)/4}\right)\Bigg)+$$

$$\left.+\left(\frac{4+e^{3/2}}{6e^{3/2}\sqrt{2\pi}}+\frac{(r-1)}{2r^{1/2}\pi e^{1/2}}+\frac{2^{1/2}\left(r^{3/2}-3r^{1/2}+2\right)}{\pi^{3/2}}\right)\delta^{3/2}2^{-n/2}.\right.$$

Теперь рассмотрим $|(Q_n-\Phi) * K_\varepsilon(B_2)|$. Согласно оценкам (13.27) и (13.28) в [14], верны следующие неравенства:

$$\left|(Q_n-\Phi) * K_\varepsilon(B_2)\right| \leqslant \max\left\{\mathrm{P}\left(\left\|2^{-\frac{n}{2}}\sum_{\alpha\in V_n}\tau(\alpha)\right\| \geqslant k/2\right), \frac{2^{3/2}r^{3/2}e^{-k^2/8r}}{k\pi^{1/2}}\right\}+$$

$$+\frac{2^{-(3n-15)/2}r^4(\rho_3)^2}{\pi k^3},$$

$$\mathsf{P}\left(\left\|2^{-\frac{n}{2}}\sum_{\alpha\in V_n}\tau(\alpha)\right\|\geqslant k/2\right)\leqslant\sum_{s=1}^{r}\mathsf{P}\left(\left|2^{-\frac{n}{2}}\sum_{\alpha\in V_n}\tau_s(\alpha)\right|\geqslant\frac{k}{2\sqrt{r}}\right),$$

где $\tau_s(\alpha)$ — s-е координаты случайных векторов $\tau(\alpha)$.

Согласно теореме Берри — Эссена для независимых разнораспределённых случайных величин [14], верно неравенство

$$\sum_{s=1}^{r}P\left(\left|2^{-n/2}\sum_{\alpha\in V_n}\tau_s(\alpha)\right|\geqslant\frac{k}{2\sqrt{r}}\right)\leqslant\frac{11}{2}\rho_3 r2^{-n/2}+r\int\limits_{|t|\geqslant k/2}\varphi(t)\,dt\leqslant$$

$$\leqslant\frac{11}{2}\delta^{3/2}r2^{-n/2}+\frac{2^{3/2}r^{3/2}e^{-\frac{k^2}{8r}}}{k\pi^{1/2}},$$

где $\varphi(t)$ — плотность стандартного нормального распределения

Если принять $k=(8rn\log 2)^{1/2}$, то, собрав все неравенства вместе, получим утверждение теоремы. ■

В теореме 2 получена оценка расстояния между распределением случайного вектора $2^{-n/\beta}W(f)$ и r-мерным стандартным нормальным распределением в обобщённой метрике полной вариации [12] по классу всех выпуклых борелевских множеств, из которой при $n\to\infty$ следует асимптотическая нормальность и локальная предельная теорема.

В отличие от следствия теоремы 13.3 из [14], где показано, что

$$|Q_n(B)-\Phi(C)|\leqslant C(r)\,\rho_4 2^{-n/2},$$

в теореме 2 удалось найти зависимость оценки скорости сходимости к нормальному закону от размерности вектора.

4. Предельные теоремы для вектора, состоящего из части автокорреляционных коэффициентов компонент случайного двоичного отображения

Рассмотрим вектор

$$A(f)=\left(r_{I_s}^{J_s}(f):I_s\subset\{1,\ldots,n\};J_s\subset\{1,\ldots,m\};I_s\neq\varnothing,J_s\neq\varnothing;s\in\{1,\ldots,r\}\right),$$

состоящий из r аддитивных автокорреляционных коэффициентов, где r — некоторое натуральное число и наборы множеств $(J_1,I_1),\ldots,(J_r,I_r)$ удовлетворяют таким условиям:

Условия 2. Пусть выполняется следующее:

1) Зафиксирован набор непустых попарно различных подмножеств $J_1^*,\ldots,J_p^*$ множества $\{1,\ldots,m\}$, $p\in\{1,\ldots,2^m-1\}$.
2) Для каждого $q\in\{1,\ldots,p\}$ зафиксированы натуральное $d_q\in\{1,\ldots,2^n\}$ и набор произвольных попарно неравных непустых подмножеств $I_{q,1},\ldots,I_{q,d_q}$ множества $\{1,\ldots,n\}$.

Обозначим $r=\sum\limits_{q=1}^{p}d_q$, $k=\left|\bigcup\limits_{q=1}^{p}\left(\bigcup\limits_{j=1}^{d_q}I_{q,j}\right)\right|$, а пары множеств $(J_1^*,I_{1,1}),\ldots,(J_1^*,I_{1,d_1})$, $(J_2^*,I_{2,1}),\ldots,\left(J_p^*,I_{p,d_p}\right)$ — через $(J_1,I_1),\ldots,(J_d,I_d)$.

Обозначим распределение случайного вектора $2^{-(n+1)/2}A(f)$ через R_n и найдём расстояние между ним и r-мерным стандартным нормальным распределением в обобщённой метрике полной вариации [12] по классу всех выпуклых борелевских множеств.

Теорема 3. Дано случайное отображение $f = (f_1, f_2, \ldots, f_m) \in B_n^m$ и выполняется набор условий 2. Тогда для любого выпуклого борелевского множества B выполняется неравенство

$$|R_n(B) - \Phi(B)| \leqslant 100 r^{7/4} 2^{2k-n/2}.$$

Доказательство. Пусть, без ограничения общности, $\bigcup\limits_{q=1}^{p}\left(\bigcup\limits_{j=1}^{d_q} I_{q,j}\right) = \{1, \ldots, k\}$.

Обозначим $e_{I_{q,j}} \in V_n$, $j \in \{1, \ldots, d_q\}$, $q \in \{1, \ldots, p\}$, через $\gamma_1, \ldots, \gamma_r$, где $e_I \in V_n$ введено при определении r_I^J.

Пусть $f^{J_i}(\beta) = \rho_i(\beta)$ для любых $i \in \{1, \ldots, r\}$. Запишем

$$\begin{pmatrix} \|\rho_1(\beta) \oplus \rho_1(\beta \oplus \gamma_1)\| \\ \ldots \\ \|\rho_r(\beta) \oplus \rho_r(\beta \oplus \gamma_r)\| \end{pmatrix} = \sum_{\beta \in V_n} \begin{pmatrix} \rho_1(\beta) \oplus \rho_1(\beta \oplus \gamma_1) \\ \ldots \\ \rho_r(\beta) \oplus \rho_r(\beta \oplus \gamma_r) \end{pmatrix}.$$

Разобьём в получившейся сумме область суммирования на 2^{n-k} областей, соответствующих векторам β с одинаковыми последними $n-k$ координатами, набор которых обозначим α. Очевидно, что

$$\rho_{1+\sum\limits_{i=1}^{q-1} d_i}(\beta) = \ldots = \rho_{\sum\limits_{i=1}^{q} d_i}(\beta) = g_q(\beta),$$

где g_q, $q \in \{1, \ldots, p\}$, — попарно независимые случайные величины. Тогда

$$\sum_{\beta \in V_n} \begin{pmatrix} \rho_1(\beta) \oplus \rho_1(\beta \oplus \gamma_1) \\ \ldots \\ \rho_r(\beta) \oplus \rho_r(\beta \oplus \gamma_r) \end{pmatrix} = \sum_{\alpha \in V_{n-k}} 2(\eta_\alpha^{q,i}, q \in \{1, \ldots, p\}, i \in \{1, \ldots, d_q\})^T = \sum_{\alpha \in V_{n-k}} \eta_\alpha,$$

где $\eta_\alpha^{q,i} = \dfrac{1}{2} \sum\limits_{t \in V_k} (g_q(t\alpha) \oplus g_q(t\alpha \oplus \gamma_{q,i}))$.

Каждая компонента $\eta_\alpha^{q,i}$, $i \in \{1, \ldots, d_q\}$, $q \in \{1, \ldots, p\}$, имеет биномиальное распределение с параметрами $\left(2^{k-1}, 1/2\right)$. Следовательно, математическое ожидание каждой компоненты равно $\mathsf{E}\eta_\alpha^{q,i} = 2^{k-2}$, а дисперсия $\mathrm{D}\,\eta_\alpha^{q,i} = 2^{k-3}$.

Аналогично доказательству основной теоремы в [5], можно показать, что ковариационная матрица вектора η_α равна $2^{k-3}E_r$, где E_r — единичная матрица соответствующего размера.

Пусть f — случайная функция из B_n^m. Рассмотрим вектор $a(f) = 2^{-(n+1)/2} A(f)$.

Из определения автокорреляционных коэффициентов следует, что

$$a(f) = 2^{-\frac{n-k}{2}} \sum_{\alpha \in V_{n-k}} \left(2^{\frac{3-k}{2}}\left(2^{k-2} - \eta_\alpha^{q,i}\right), q \in \{1, \ldots, p\}, i \in \{1, \ldots, d_q\}\right)^T = 2^{-\frac{n-k}{2}} \sum_{\alpha \in V_n} \xi(\alpha).$$

Рассмотрим набор из 2^{n-k} величин $\xi(\alpha)$, $\alpha \in V_{n-k}$, — независимых одинаково распределённых в $\mathbb{R}^r$ случайных векторов с единичной ковариационной матрицей и нулевым средним. В этих условиях, как и в теореме 1, выполняется результат из [11]. Несложно показать, что

$$\mathsf{E}(\xi(\alpha))^3 \leqslant r^{\frac{3}{2}} 2^{\frac{3k-3}{2}}.$$

Следовательно, выполняется неравенство $|R_n(B) - \Phi(B)| \leqslant 400 r^{1/4} r^{3/2} 2^{(3k-3)/2} 2^{-(n-k)/2}$. Теорема доказана. ■

Из этой теоремы следует равномерная по r оценка расстояния между распределением вектора $2^{-(n+1)/2}A(f)$ и многомерным стандартным нормальным распределением в равномерной метрике, стремящаяся к нулю, т. е. опять получаются асимптотическая нормальность и интегральная предельная теорема.

Из доказательства теоремы 3 следует равенство

$$\left(r_{I_s}^{J_s}(f) : s \in \{1,\dots,r\}\right) = \sum_{\alpha\in V_n} \xi(\alpha) = \sum_{\alpha\in V_{n-k}} \left(4\left(2^{k-2} - \eta_\alpha^{q,i}\right), q \in \{1,\dots,p\}, i \in \{1,\dots,d_q\}\right)^T,$$

где случайные величины $\eta_\alpha^{q,i}$ введены при доказательстве теоремы 3.

Рассмотрим набор из 2^{n-k} величин $\xi(\alpha)$, $\alpha \in V_{n-k}$, — независимых одинаково распределённых в $\mathbb{R}^r$ случайных векторов с ковариационной матрицей $2^{k+1}E_r$ и нулевым средним.

Легко показать, что $\|\xi(\alpha)\| \leqslant \sqrt{r}2^k$ и $E\left(\|\xi(\alpha)\|^\beta\right) \leqslant r^{\beta/2}2^{k\beta} < \infty$ при всех вещественных $\beta \in (0,2)$. Таким образом, попадаем в условия основной теоремы из [9], согласно которой верно

Утверждение 9. Пусть $n \to \infty$, m — произвольное натуральное число, $\beta \in \in (0,2)$ — вещественное число. Тогда для любых попарно различных наборов множеств $(J_1, I_1), \dots, (J_r, I_r)$, удовлетворяющих условиям 2, норма вектора $2^{-n/\beta}A(f)$ сходится к нулю с вероятностью 1.

Данное утверждение при $\beta = 1$ является формулировкой усиленного закона больших чисел для случайных векторов $\xi(\alpha)$, $\alpha \in V_n$.

Теперь рассмотрим вопрос о скорости сходимости к нулю нормы вектора $2^{-n/\beta}A(f)$. Так как $\|\xi(\alpha)\| \leqslant \sqrt{r}2^k$ и $\mathsf{E}\left(\|\xi(\alpha)\|^2\right) \leqslant r2^{2k}$, то при всех $n - k \geqslant \log_2 r$ попадаем в условия основной теоремы из [16], из которой следует

Утверждение 10. Пусть n, m — произвольные натуральные числа, $\beta \in (0,2)$ — вещественное число. Тогда для любых попарно различных $(J_1, I_1), \dots, (J_r, I_r)$, удовлетворяющих условиям 2, таких, что $n - k \geqslant \log_2 r$, и для любого $\varepsilon > 0$ верно

$$\mathsf{P}\left\{\left\|2^{-n/\beta}A(f)\right\| \geqslant \varepsilon\right\} \leqslant \left(1 + \frac{e^{5/12}}{\sqrt{2\pi}}\right)\exp\left\{-\frac{\varepsilon^2}{re^2}2^{\frac{(2-\beta)n}{\beta}-k-3}\right\}.$$

Заключение

В данной работе удалось доказать асимптотическую нормальность совместного распределения части автокорреляционных и спектральных коэффициентов и весов подфункций компонент двоичных вектор-функций. Следующий этап в изучении векторов из части этих характеристик, в том числе и растущей размерности, — это построение локальных предельных теорем, полезных для изучения криптографических свойств функций. В частности, стоят задачи обобщения на m-мерный случай результатов [4, 6] и усиления фактически доказанной в [5] локальной предельной теоремы для вектора, состоящего из части автокорреляционных коэффициентов одной компоненты с I, мощность которых равна 1.

ЛИТЕРАТУРА

1. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 472 с.
2. *Ященко В. В.* Свойства булевых отображений, сводимые к свойствам их координатных функций // Вестник МГУ. Сер. Математика. 1997. Т. 33. № 1. С. 11–13.

3. *Carlet C.* Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Encyclopedia of Mathematics and its Applications. V. 134. New York: Cambridge University Press, 2010. P. 398–472.
4. *Денисов О. В.* Локальная предельная теорема для распределения части спектра случайной двоичной функции // Дискретная математика. 2000. Т. 12. № 1. С. 82–95.
5. *Панков К. Н.* Верхняя граница для числа функций, удовлетворяющих строгому лавинному критерию // Дискретная математика. 2005. Т. 17. № 2. С. 95–101.
6. *Рязанов Б. В.* О распределении спектральной сложности булевых функций // Дискретная математика. 1994. Т. 6. № 2. С. 111–129.
7. *Таранников Ю. В.* Комбинаторные свойства дискретных структур и приложения к криптологии. М.: МЦНМО, 2011. 152 с.
8. *Халявин А. В.* Оценка нелинейности корреляционно-иммунных булевых функций // Прикладная дискретная математика. 2011. № 1. С. 34–69.
9. *Азларов Т. А., Володин Н. А.* Законы больших чисел для одинаково распределенных банаховозначных случайных величин // Теория вероятностей и её применения. 1981. Т. 26. № 3. С. 584–590.
10. *Кахан Ж.-П.* Случайные функциональные ряды. М.: Мир, 1973. 304 с.
11. *Bentkus V.* On the dependence of the Berry-Esseen bound on dimension // J. Stat. Plan. Infer. 2003. V. 113. No. 2. P. 385–402.
12. *Золотарев В. М.* О свойствах и связях некоторых типов метрик // Записки научных семинаров ЛОМИ. 1979. Т. 87. С. 18–35.
13. *Padgett W. J. and Taylor R. L.* Laws of Large Numbers for Normed Linear Spaces and Certain Frechet Spaces. New York: Springer, 1973. 117 p.
14. *Бхаттачария Р. Н., Ранга Р.* Аппроксимация нормальным распределением и асимптотические разложения. М.: Наука, 1982. 288 с.
15. *Bhattacharya R. N.* Rates of weak convergence for the multidimensional central limit theorem // Теория вероятностей и ее применения. 1970. Т. 15. № 1. С. 69–85.
16. *Прохоров Ю. В.* Распространение неравенств С. Н. Бернштейна на многомерный случай // Теория вероятностей и её применения. 1968. Т. 13. № 2. С. 266–274.

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

DOI 10.17223/20710410/18/3

УДК 512.548.7, 512.554

КВАЗИГРУППЫ И КОЛЬЦА В КОДИРОВАНИИ И ПОСТРОЕНИИ КРИПТОСХЕМ

В. Т. Марков, А. В. Михалёв, А. В. Грибов, П. А. Золотых, С. С. Скаженик

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

E-mail: markov@mech.math.msu.su, alexey.gribov@yandex.ru, pzolotykh@gmail.com

Исследуются различные криптосхемы и коды над ассоциативными и неассоциативными структурами. Построены схема шифрования над градуированным кольцом, криптосхема над лупой Муфанг, протокол выработки общего ключа и линейно оптимальные коды.

Ключевые слова: *неассоциативные алгебраические структуры, градуированное кольцо, квазигрупповое кольцо, лупа Муфанг, коммутаторные квазигруппы, схема шифрования, линейно оптимальный код.*

Введение

В работе в п. 1 представлены необходимые теоретические сведения. В п. 2 построена криптосхема над градуированным кольцом с мультипликативным базисом. Это обобщает построение криптосхемы над групповым кольцом. При этом неоднозначность выбора градуировки и мультипликативного базиса расширяет множество подходящих алгебраических структур для шифрования. Похожая схема была построена в [1]. В п. 3 построен протокол выработки общего секретного ключа и сконструирована криптосхема, где все вычисления проводятся в лупе Муфанг.

В п. 4 с помощью квазигрупповых колец построены две цепочки линейно оптимальных $[n, n-3, 3]_q$-кодов для $n = 2q$ и $n = 2q-2$. Для построения $[2q, 2q-2, 3]_q$-кодов используется представление кодов Рида — Соломона как идеалов группового кольца $\mathbb{F}_{p^n}G$, где G — это p-элементарная абелева группа порядка p^n. В качестве иллюстрации приводятся линейно оптимальные коды, построенные с помощью коммутаторных квазигрупп для группы диэдра D_n.

1. Основные понятия

Приведём основные понятия и утверждения, необходимые для дальнейшего изложения (см., например, [2]).

Определение 1. *Группоид* — непустое множество с заданной бинарной операцией.

Пусть $(G, \cdot)$ — группоид и a — некоторый элемент из G. Рассмотрим отображения $L(a) : G \to G$, $R(a) : G \to G$ для любого $a \in G$. Определим их следующим образом: $xL(a) = x \cdot a$, $xR(a) = a \cdot x$ для любых $x \in G$.

Определение 2. *Квазигруппа* — такой группоид $(G, \cdot)$, что отображения $L(a)$, $R(a)$ являются биекциями для любого $a \in G$.

Это определение эквивалентно следующему: группоид $(G, \cdot)$ называется квазигруппой, если для любых $a, b \in G$ уравнения $x \cdot a = b$, $a \cdot y = b$ всегда разрешимы, причём однозначно.

Определение 3. Группоид $(G, \cdot)$ называется *лупой*, если $(G, \cdot)$ является квазигруппой с единицей. Для любого элемента a лупы $(G, \cdot)$ определим элементы a^λ и a^ρ условиями $a^\lambda \cdot a = 1$ и $a \cdot a^\rho = 1$

Определение 4. Лупа $(L, \cdot)$ с единичным элементом 1 называется *лупой Муфанг*, если выполняется тождество $(xy)(zx) = [x(yz)]x$ для любых $x, y, z \in L$.

Свойства элементов лупы Муфанг описывает

Теорема 1 [3]. Для элементов лупы Муфанг верны следующие тождества:

1) $y^\lambda = y^\rho$, что позволяет обозначить $y^\lambda = y^\rho = y^{-1}$;
2) $(xy)x = x(yx)$;
3) $(xy)(zx) = x[(yz)x]$;
4) $(xy)y^{-1} = x$;
5) $[(yx)z]x = y[x(zx)]$;
6) $[(xz)x]y = x[z(xy)]$;
7) $(xx)y = x(xy)$;
8) $(xy)y = x(yy)$.

Лемма 1 [4]. Пусть $(L, \cdot)$ — лупа Муфанг, тогда для любых $x, y \in L$

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Доказательство. Ясно, что $(xy)^{-1}(xy) = 1$. Тогда $[(xy)^{-1}(xy)]y^{-1} = y^{-1} = ((xy)^{-1})[(xy)y^{-1}] = (xy)^{-1}[x(yy^{-1})] = (xy)^{-1}x$, а следовательно, $(xy)^{-1} = y^{-1}x^{-1}$. ■

Одной из наиболее важных является следующая теорема.

Теорема 2 [3]. Пусть $(L, \cdot)$ — лупа Муфанг. Если для $x, y, z \in L$ выполняется $x(yz) = (xy)z$, то x, y, z порождают подгруппу в L.

Следствие 1. Любая лупа Муфанг $(M, \cdot)$ является ди-ассоциативной, т. е. любые два элемента порождают подгруппу в M.

Следствие 2. Любая лупа Муфанг $(M, \cdot)$ является лупой с ассоциативными степенями.

Рассмотрим класс луп, который называется лупами Пейджа.

Определение 5. Неассоциативная, конечная и простая лупа Муфанг M называется *лупой Пейджа*.

Следующее описание луп Пейджа представлено в работе [5]. Пусть $\mathbb{F}_q$ — конечное поле. Для $\alpha, \beta \in F_q^3$ определим операции $\cdot, \times$ следующим образом:

$$\alpha \cdot \beta = \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3,$$
$$\alpha \times \beta = (\alpha_2\beta_3 - \alpha_3\beta_2, \alpha_3\beta_1 - \alpha_1\beta_3, \alpha_1\beta_2 - \alpha_2\beta_1).$$

Алгеброй Цорна $Z(q)$ называется множество (2×2)-матриц $\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}$, где $a, b \in \mathbb{F}_q$ и $\alpha, \beta \in \mathbb{F}_q^3$, со следующей операцией:

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \cdot \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha\delta & a\gamma + d\alpha - \beta \times \delta \\ c\beta + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}.$$

Все элементы $Z(q)$ с определителем $M = ab - \alpha\beta = 1$ образуют лупу Пейджа $M^*(q)$ с нейтральным элементом $e = \begin{pmatrix} 1 & (0,0,0) \\ (0,0,0) & 1 \end{pmatrix}$.

Л. Пейдж в [6] показал, что $|M^*(q)| = q^3(q^4-1)$, когда q чётное, и $|M^*(q)| = q^3(q^4-1)/2$, если q нечётное.

Пусть $SL_2(q)$ — специальная линейная группа (2×2)-матриц с определителем, равным 1, над полем $\mathbb{F}_q$. Обозначим через $L_2(q)$ проективную группу $SL_2(q)/Z(SL_2(q))$.

П. Войтеховски [7] доказал следующую теорему.

Теорема 3. Пусть $S \subseteq Z$ — множество порядков всех элементов лупы $M^*(q)$ и T — множество порядков элементов $L_2(q)$. Тогда $S = T$ и порядок элемента $\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \in M^*(q)$ совпадает с порядком элемента $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in L_2(q)$ при $(\alpha,\beta) = (0,0)$ и с порядком элемента $\begin{pmatrix} a & 1 \\ \alpha\cdot\beta & b \end{pmatrix}$ из $L_2(q)$ при $\alpha \neq 0$.

Введём понятие *квазигруппового* (*лупового*) *кольца*. Пусть K — ассоциативное кольцо с единицей, L — лупа или квазигруппа. Рассмотрим множество KL, состоящее из всех формальных сумм вида $\sum\limits_{l\in L} \alpha_l \cdot l \ \ (\alpha_l \in K)$, в которых конечное число элементов α_l отлично от нуля. Два элемента $a, b \in KL$ считаются равными тогда и только тогда, когда $\alpha_l = \beta_l$ для всех $l \in L$.

На множестве KL определены операции сложения и умножения следующим образом: если $a = \sum\limits_{l\in L} \alpha_l \cdot l$ и $b = \sum\limits_{l\in L} \beta_l \cdot l$ — элементы KL, то $a + b = \sum\limits_{l\in L} (\alpha_l + \beta_l)\cdot l$, $ab = \sum\limits_{l\in L} \Big(\sum\limits_{\substack{m,h\in L: \\ mh=l}} \alpha_m\beta_h \Big) l$. Относительно этих операций множество KL является неассоциативным кольцом с единицей. Удобно отождествить $l \in L$ с элементом $1\cdot l \in KL$, а $\alpha \in K$ — с элементом $\alpha \cdot e$, где e — единица лупы, тогда K и L являются подмножествами в KL.

Пусть теперь R — ассоциативное кольцо с единицей $1 \in R$. Рассмотрим группу G в мультипликативной записи с нейтральным элементом $e \in G$.

Определение 6. Кольцо R называется *G-градуированным*, если существует такое семейство $\{R_\sigma : \sigma \in G\}$ аддитивных подгрупп R_σ аддитивной группы R, что $R = \bigoplus\limits_{\sigma\in G} R_\sigma$, $R_\sigma R_\tau \subseteq R_{\sigma\tau}$ для всех $\sigma, \tau \in G$. *Строго градуированным* называется G-градуированное кольцо R, для которого выполнено равенство $R_\sigma R_\tau = R_{\sigma\tau}$ для всех $\sigma, \tau \in G$. *Однородным степени* σ называется элемент $x \in R_\sigma$.

Будем обозначать множество обратимых по умножению элементов в кольце R символом $U(R)$.

Лемма 2. Пусть $R = \bigoplus\limits_{\sigma\in G} R_\sigma$ — G-градуированное кольцо. Тогда

1) $1 \in R_e$ и R_e является подкольцом кольца R;
2) обратный элемент r^{-1} к обратимому однородному элементу r также однородный;
3) G-градуированное кольцо R строго градуированно тогда и только тогда, когда $1 \in R_\sigma R_{\sigma^{-1}}$ для любого $\sigma \in G$.

Доказательство.

1. По определению $R_eR_e \subseteq R_e$; поэтому достаточно показать, что $1 \in R_e$. Пусть $1 = \sum\limits_{\sigma\in G} r_\sigma$, где $r_\sigma \in R_\sigma$. Для любого $h_\lambda \in R_\lambda$ получаем $h_\lambda = h_\lambda \cdot 1 = \sum\limits_{\sigma\in G} h_\lambda r_\sigma$ и

$h_\lambda r_\sigma \in R_{\lambda\sigma}$. Поэтому для любого $\sigma \neq e$ выполнено $h_\lambda r_\sigma = 0$. Итак, $1 \cdot r_\sigma = 0$, следовательно, $r_\sigma = 0$ для любого $\sigma \neq e$. Отсюда $1 = r_e \in R_e$.

2. Пусть $r \in U(R) \cap R_\lambda$. Если $r^{-1} = \sum\limits_{\sigma\in G} (r^{-1})_\sigma$, то $1 = rr^{-1} = \sum\limits_{\sigma\in G} r(r^{-1})_\sigma$. Так как $1 \in R_e$ и $r(r^{-1})_\sigma \in R_{\lambda\sigma}$, то $r(r^{-1})_\sigma = 0$ для любых $\sigma \neq \lambda^{-1}$. Но из того, что $r \in U(R)$ — обратимый элемент, следует соотношение $(r^{-1})_\sigma \neq 0$ для $\sigma \neq \lambda^{-1}$, и в итоге $r^{-1} = (r^{-1})_{\lambda^{-1}} \in R_{\lambda^{-1}}$ — тоже однородный элемент степени λ^{-1}.

3. Предположим, что $1 \in R_\sigma R_{\sigma^{-1}}$ для любого $\sigma \in G$, и докажем, что градуировка строгая. В самом деле, для любых $\sigma, \tau \in G$ имеем цепочку равенств

$$R_{\sigma\tau} = R_e R_{\sigma\tau} = (R_\sigma R_{\sigma^{-1}}) R_{\sigma\tau} = R_\sigma (R_{\sigma^{-1}} R_{\sigma\tau}) \subseteq R_\sigma R_\tau.$$

Это показывает, что $R_{\sigma\tau} = R_\sigma R_\tau$, что означает строгость градуировки.

Обратное утверждение очевидно: $1 \in R_e = R_\sigma R_{\sigma^{-1}}$. ■

Следствие 3. Справедливы равенства $R_e R_\sigma = R_\sigma R_e = R_\sigma$, т. е. R_σ есть R_e-бимодуль.

Пусть R — конечномерная некоммутативная алгебра над полем $\mathbb{F}$.

Определение 7. *Мультипликативным базисом* конечномерной алгебры R называется такой её базис B, что $B \cup \{0\}$ замкнуто относительно умножения.

Пример 1. Для алгебры $(n \times n)$-матриц $M_n(\mathbb{F})$ над полем $\mathbb{F}$ естественным мультипликативным базисом является стандартный базис, состоящий из матричных единиц E_{ij}, у которых на ij-й позиции стоит 1, а остальные элементы — нули.

Пример 2. Для любой конечномерной (полу)групповой алгебры $\mathbb{F}G$ моноида G в качестве мультипликативного базиса можно выбрать моноид G.

Для обобщения предыдущего примера рассмотрим обобщенные полугрупповые алгебры, обозначаемые $\Sigma(\Delta, R)$ и введённые в [8]. Здесь Δ — некоторое конечное множество, снабжённое частичным ассоциативным умножением. В свою очередь, $\Sigma(\Delta, R)$ — действительное векторное пространство функций из Δ в R. Мультипликативная структура на $\Sigma(\Delta, R)$ индуцируется умножением на Δ.

Пример 3. Любая конечномерная обобщённая полугрупповая алгебра $\Sigma(\Delta, R)$ имеет мультипликативный базис — так называемые характеристические функции χ_δ, $\delta \in \Delta$.

2. Криптосхемы над градуированными кольцами с мультипликативным базисом

2.1. Конструирование автоморфизмов градуированного кольца

В [9] рассматриваются автоморфизмы лупового кольца KL. Из автоморфизмов $\varphi \in \mathrm{Aut}(K)$ и $\psi \in \mathrm{Aut}(L)$ конструируется $\chi \in \mathrm{Aut}(KL)$ по следующему правилу: для любого $h = a_{l_1} l_1 + \ldots + a_{l_n} l_n$, $h \in KL$, по определению полагается $\chi(h) = \varphi(a_{l_1})\psi(l_1) + \ldots + \varphi(a_{l_n})\psi(l_n)$. Таким образом, если известна структура групп автоморфизмов $\mathrm{Aut}(K)$ и $\mathrm{Aut}(L)$ по отдельности, то есть возможность строить достаточно много автоморфизмов из $\mathrm{Aut}(KL)$. Заметим, что даже для произвольного группового кольца полного описания его группы автоморфизмов ещё не получено.

Пусть теперь R — кольцо, градуированное конечной группой G. По лемме 2 R_e — подкольцо в R, а по следствию 3 подгруппа R_σ есть R_e-бимодуль для любого $\sigma \in G$. Если описана группа автоморфизмов для подкольца R_e, то в общем случае, фиксируя

$\varphi \in \mathrm{Aut}(R_e)$, мы ещё не определяем однозначно автоморфизм для всего R. В самом деле, для этого необходимо распространить действие φ и на модули R_σ и таким образом получить $\chi \in \mathrm{Aut}(R)$. Для этого необходимо, чтобы $\chi(r_{\sigma_1} r_{\sigma_2}) = \chi(r_{\sigma_1})\chi(r_{\sigma_2})$ для $r_{\sigma_1} \in R_{\sigma_1}$, $r_{\sigma_2} \in R_{\sigma_2}$, $r_{\sigma_1} r_{\sigma_2} \in R_{\sigma_1\sigma_2}$.

Но если у кольца R существует мультипликативный базис B над R_e, то $R = R_e B$. Поэтому автоморфизм φ естественным образом продолжается до автоморфизма χ всего кольца R. В силу того, что B образует полугруппу по умножению, зададим $\psi \in \mathrm{Aut}(B)$ по аналогии с [9]. Этот автоморфизм будет перемешивать сам мультипликативный базис.

Заметим, что в случае (полу)группового кольца, рассматриваемого в естественной градуировке, такая конструкция в точности совпадает с построением его автоморфизма по отдельным автоморфизмам кольца и (полу)группы. Но даже для (полу)группового кольца, меняя градуировку или выбирая другой мультипликативный базис, получаем, вообще говоря, уже новые структуры для шифрования со своими автоморфизмами. Это расширяет множество подходящих для криптосхемы структур.

Пример 4. Рассмотрим $M_n(\mathbb{F})$, где $\mathbb{F} = R_n(K, J)$ — радикальное кольцо матриц. Пусть K — ассоциативное кольцо с единицей, J — идеал в K, $M_n(J)$ — кольцо $(n \times n)$-матриц над идеалом J. По определению из [10]

$$R_n(K, J) = NT_n(K) + M_n(J),$$

где $NT_n(K)$ — нижнетреугольные матрицы над кольцом K. Тогда $|\mathrm{Aut}(R_n(Z_{p^m}, (p^d)))| = (p^m - p^{m-1})^{n-1} \cdot p^{(2m-d)C_n^2 + d(n-2)}$, где $d|m$, $d < m$.

Автоморфизм $\psi \in \mathrm{Aut}(B)$ зададим по правилу $\psi(E_{ij}) = E_{\sigma(i)\sigma(j)}$, причём $\sigma \in S_n$. Так как $R_e = \mathbb{F}$, то $\mathrm{Aut}(R_e) = \mathrm{Aut}(\mathbb{F})$, а следовательно, количество индуцированных автоморфизмов равно

$$|\mathrm{Aut}(R_e)| \cdot |\mathrm{Aut}(B)| \geqslant |S_n| \cdot |\mathrm{Aut}(R_n(Z_{p^m}, (p^d)))| = n! \cdot (p^m - p^{m-1})^{n-1} \cdot p^{(2m-d)\cdot C_n^2 + d(n-2)}.$$

Таким образом, данная структура имеет достаточно богатую индуцированную группу автоморфизмов.

2.2. Построение криптосхемы

Участник A :

1) Выбирает градуированное кольцо R с мультипликативным базисом, такое, что группы автоморфизмов $\mathrm{Aut}(B)$ и $\mathrm{Aut}(R_e)$ некоммутативны. Предполагается, что группы $\mathrm{Aut}(B)$ и $\mathrm{Aut}(R_e)$ достаточно богаты некоммутирующими элементами большого порядка с нетривиальными централизаторами большого порядка. Положим $|\mathrm{Aut}(B)| \geqslant \geqslant t_1$, $|\mathrm{Aut}(R_e)| \geqslant t_2$. Здесь и далее t_i — параметры безопасности, которые по предположению экспоненциально зависят от порядка градуированного кольца R.

Фиксирует градуировку и этот базис (в случае, если кольцо допускает несколько различных базисов) с учётом вышеперечисленных условий. Эта информация объявляется по открытому каналу. Обозначим базис через B, а группу, по которой градуировано кольцо, — через G, тогда общеизвестны $\big(R, B, G\big)$.

2) Задает автоморфизм $\sigma \in \mathrm{Aut}(R_e)$ так, чтобы порядок $|\sigma| \geqslant t_3$, причём σ должен иметь нетривиальный централизатор и $|C(\sigma) \setminus \langle\sigma\rangle| \geqslant t_4$.

Конструирует автоморфизм $\eta \in \mathrm{Aut}(B)$ так, чтобы $|\eta| \geqslant t_5$, причём η должен иметь нетривиальный централизатор и $|C(\eta) \setminus \langle\eta\rangle| \geqslant t_6$.

3) Случайно выбирает автоморфизм $\tau \in C(\sigma) \setminus \langle\sigma\rangle$.

4) Случайно выбирает $\omega \in C(\eta) \setminus \langle\eta\rangle$.

5) По τ и ω строит секретный автоморфизм $\varphi \in \mathrm{Aut}(R)$ так: для любого $h \in R$ вида $h = a_{b_1}b_1 + \ldots + a_{b_n}b_n$, где $a_{b_1}, \ldots, a_{b_n} \in R_e$, полагает

$$\varphi(h) = \tau(a_{b_1})\omega(b_1) + \cdots + \tau(a_{b_n})\omega(b_n).$$

6) Выбирает элементы $a \in R$, $x \in R$ с нулевыми левыми аннуляторами. Это условие необходимо для последующей расшифровки.

7) Вычисляет $\varphi(x)$ и $\varphi(a)$.

Таким образом, открытым ключом участника A является

$$\Big(\sigma, \eta, x, \varphi(x), a, \varphi(a)\Big).$$

Отметим, что при должных параметрах безопасности t_3, t_4, t_5, t_6 автоморфизмов, подходящих для открытого ключа, достаточно много. Сформированный открытый ключ участник A передает участнику B по открытому каналу.

Участник B:

1) Выбирает натуральные числа i, j, k, l.

2) Используя открытый ключ участника A, получает пары автоморфизмов (σ^i, η^j), (σ^k, η^l) и по ним строит автоморфизмы $\psi, \chi \in \mathrm{Aut}(KL)$ таким же способом, как и участник A, т. е. для любого $h \in KL$ вида $h = a_{l_1}l_1 + \cdots + a_{l_n}l_n$ полагает $\psi(h) = \sigma^i(a_{l_1})\eta^j(l_1) + \cdots + \sigma^i(a_{l_n})\eta^j(l_n)$, $\chi(h) = \sigma^k(a_{l_1})\eta^l(l_1) + \cdots + \sigma^k(a_{l_n})\eta^l(l_n)$. Автоморфизмы ψ, χ будем называть сеансовыми.

3) Вычисляет $\chi(a) \cdot \psi(x)$.

4) Вычисляет $\chi(\varphi(a)) \cdot \psi(\varphi(x))$. Так как элементы a и x были выбраны с нулевым левым аннулятором, то и у этого произведения будет нулевой левый аннулятор.

5) Записывает исходный текст, который надо передать, в виде $m \in R$ и вычисляет $m \cdot [\chi(\varphi(a)) \cdot \psi(\varphi(x))]$. При необходимости исходный текст разбивается на блоки и каждый блок шифруется отдельно с разными секретными ключами.

6) Отправляет для A криптограмму

$$\Big(\chi(a) \cdot \psi(x),\ m \cdot \big[\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)\big]\Big).$$

Получив криптограмму, участник A расшифровывает её:

1) Используя секретный автоморфизм φ, вычисляет $q = \varphi\big(\chi(a) \cdot \psi(x)\big)$.

2) Расшифровывает посланный текст, пользуясь тем, что χ, ψ и φ коммутируют. Таким образом, участник A знает $h = m \cdot [\chi(\varphi(a)) \cdot \psi(\varphi(x))]$ и $\varphi\big(\chi(a) \cdot \psi(x)\big)$. Для расшифровки сообщения m достаточно решить линейную систему $m \cdot q = h$ с коэффициентами из кольца R_e.

В самом деле, так как $\tau \in C(\sigma) \setminus \langle\sigma\rangle$ и $\omega \in C(\eta) \setminus \langle\eta\rangle$, то коммутируют между собой попарно автоморфизмы τ и σ, а также ω и η. Поэтому коммутируют и сконструированные на их основе автоморфизмы φ и ψ, φ и χ. Вследствие этого $\chi(\varphi(a)) \cdot \psi(\varphi(x)) = \varphi\big(\chi(a) \cdot \psi(x)\big) = q$. Кроме того, элемент $\chi(\varphi(a)) \cdot \psi(\varphi(x))$ выбран с нулевым левым аннулятором. Поэтому система уравнений $m \cdot q = h$ с коэффициентами из кольца R_e имеет единственное решение.

2.3. Анализ атак на криптосистему

Рассмотрим следующую задачу. Пусть R — некоторая алгебраическая структура, A — некоторое подмножество автоморфизмов в $\mathrm{Aut}\, R$, α — случайно выбранный

элемент из A. Предположим, что известно некоторое множество пар $(x_i, \alpha(x_i))$, $i = 1, \ldots, n$, где $x_i \in R$. Требуется найти автоморфизм $\alpha' \in A$, такой, что $\alpha'(x_i) = \alpha(x_i)$ для всех $i = 1, \ldots, n$. Обозначим эту задачу как $\Omega_n(A, R)$.

Заметим, что при отсутствии существенной информации о множествах A и R задача $\Omega_n(A, R)$ является вычислительно трудной, поскольку она разрешима только полным перебором всех элементов множества A и проверкой условия $\alpha'(x_i) = \alpha(x_i)$, $i = 1, \ldots, n$, для каждого выбранного $\alpha' \in A$.

Рассмотрим некоторые атаки на криптосистему.

Атака только с криптограммой

Пусть криптоаналитик располагает открытым ключом участника A и криптограммой. Перед ним стоит следующая задача: по известным парам $\big(a, \varphi(a)\big)$, $\big(x, \varphi(x)\big)$ найти такой $\alpha \in \mathrm{Aut}(R)$, индуцированный автоморфизмами (σ', η'), что $\varphi(a) = \alpha(a)$, $\varphi(x) = \alpha(x)$. К тому же необходимо, чтобы $\sigma' \in C(\sigma) \setminus \langle\sigma\rangle$, а $\eta' \in C(\eta) \setminus \langle\eta\rangle$.

Построим α. Положим $\alpha(a) := \varphi(a)$, $\alpha(x) := \varphi(x)$. Таким образом, определены $\alpha(ax) = \alpha(a) \cdot \alpha(x) := \varphi(a) \cdot \varphi(x)$ и $\alpha(xa) = \alpha(x) \cdot \alpha(a) := \varphi(x) \cdot \varphi(a)$. Но доопределить α на элемент $\chi(a) \cdot \psi(x)$ можно лишь перебором его образа с последующей проверкой того, что $\sigma' \in C(\sigma) \setminus \langle\sigma\rangle$, а $\eta' \in C(\eta) \setminus \langle\eta\rangle$. Это вычислительно не легче перебора всех автоморфизмов, индуцированных парами $(\sigma', \eta') \in \big(C(\sigma) \setminus \langle\sigma\rangle\big) \times \big(C(\eta) \setminus \langle\eta\rangle\big)$, удовлетворяющих начальным условиям $\alpha(a) = \varphi(a)$ и $\alpha(x) = \varphi(x)$. В итоге получаем задачу $\Omega_2(Y, R)$, где Y — это множество автоморфизмов R, полученных с помощью пар $(\sigma', \eta') \in \big[\big(C(\sigma) \setminus \langle\sigma\rangle\big) \times \big(C(\eta) \setminus \langle\eta\rangle\big)\big]$, что эквивалентно полному перебору секретных ключей.

Для оценки сложности вскрытия криптосистемы злоумышленником рассмотрим мощность множества, элементы которого необходимо перебрать. Тогда сложность данной атаки равна $t_4 \cdot t_6$. Поэтому при надлежащем выборе параметров безопасности задача является вычислительно трудной.

В случае, если криптоаналитик располагает несколькими криптограммами, даже при условии фиксированных автоморфизмов σ и η задача взлома всё равно сводится к полному перебору секретных ключей, так как предполагается, что они каждый раз выбираются разными.

Атака на сеансовые автоморфизмы ψ и χ

Другой способ атаки — найти автоморфизмы ψ и χ, а затем решить относительно m уравнение $m \cdot \big[\chi\big(\varphi(a)\big) \cdot \psi\big(\varphi(x)\big)\big] = h$, где h известен из криптограммы. Пусть ψ построен с помощью автоморфизмов (σ_1, η_1), а автоморфизм χ — с помощью (σ_2, η_2). Для того чтобы найти ψ и χ, криптоаналитику необходимо осуществить перебор образов $\psi(x)$, $\chi(a)$, таких, что $\chi(a)\psi(x) = h_1$, где h_1 известен из криптограммы, и проверить соотношения $(\sigma_1, \eta_1) \in (\langle\sigma\rangle, \langle\eta\rangle)$ и $(\sigma_2, \eta_2) \in (\langle\sigma\rangle, \langle\eta\rangle)$. Это вычислительно не легче, чем перебрать пары $(\sigma_1, \eta_1) \in (\langle\sigma\rangle, \langle\eta\rangle)$ и $(\sigma_2, \eta_2) \in (\langle\sigma\rangle, \langle\eta\rangle)$ (а это полный перебор соответствующих автоморфизмов) с последующей проверкой условия $\chi(a)\psi(x) = h_1$. Следовательно, определённая выше сложность атаки равна $t_3^2 \cdot t_5^2$. При правильном выборе соответствующих параметров безопасности эта задача является вычислительно трудной.

Атака с выбранным исходным текстом

Эта атака основана на попытке криптоаналитика получить $\chi(\varphi(a))\psi(\varphi(x)) \in R$ с последующим решением уравнения $m \cdot \chi(\varphi(a))\psi(\varphi(x)) = h$ относительно m посредством нового сеанса связи с участником B в качестве участника A. Даже если

участник B повторяет тот же исходный текст m, он должен сконструировать новые сеансовые автоморфизмы $\psi' \neq \psi$ и $\chi' \neq \chi$. Поэтому криптоаналитик получит не $m \cdot \chi(\varphi(a))\psi(\varphi(x))$, а $m \cdot \chi'(\varphi(a))\psi'(\varphi(x))$. И даже если он решит новое уравнение относительно $\chi'(\varphi(a))\psi'(\varphi(x))$, никакой новой информации относительно $\chi(\varphi(a))\psi(\varphi(x))$ он не получит.

3. Криптосхемы на основе луп

3.1. Протокол выработки общего секретного ключа

Рассмотрим протокол выработки общего ключа, построенный при помощи лупы Муфанг.

Пусть L — общеизвестная лупа Муфанг; $a, b, c \in L$ — общеизвестные элементы. Пусть M, K и N — порядки элементов a, b и c соответственно. Протокол выработки секретного ключа выглядит следующим образом:

1. Абонент A выбирает случайные натуральные числа $m < M$, $k < K$, $n < N$ и посылает абоненту B пару $(u_1, u_2) = (a^m b^k, b^k c^n)$.

2. Абонент B выбирает случайные натуральные числа $r < M$, $l < K$, $s < N$ и посылает сообщение $(v_1, v_2) = (a^r b^l, b^l c^s)$.

3. Абонент A вычисляет $(a^m v_1)b^k$ и $(b^k v_2)c^n$.

4. Абонент B вычисляет $(a^r u_1)b^l$ и $(b^l u_2)c^s$.

Общим ключом абонентов A и B является

$$K_{AB} = (a^{m+r}b^{k+l})(b^{k+l}c^{n+s}).$$

Непосредственно из теоремы 1 получаем

Утверждение 1. Если L — лупа Муфанг, $a, b \in L$, то

$$(a^n(a^r b^s))b^m = a^n((a^r b^s)b^m) = (a^s(a^n b^m))b^s = a^r((a^n b^m)b^s) = a^{r+n}b^{s+m}.$$

Таким образом, ключ абонента A: $K_A = ((a^m v_1)b^k)(b^k v_2)c^n) = (a^{m+r}b^{k+l})(b^{k+l}c^{n+s}) = = K_{AB}$; ключ абонента B: $K_B = ((a^r u_1)b^l)((b_l u_2)c^s) = K_{AB}$; $K_A = K_B$.

Отметим, что элементы a, b, c лупы L являются общеизвестными, а натуральные числа r, k, s, m, l, n — секретными.

Замечание 1. Покажем, что знание одного из секретных чисел достаточно для получения секретного ключа. Действительно, пусть злоумышленник каким-либо образом получил число m, тогда, сделав следующие вычисления: $(a^{-m}u_1) = b^k$, $b^{-k}u_2 = c^n$, $\left((a^m v_1)b^k\right)\left(b^k(v_2 c^n)\right) = K$, злоумышленник получает секретный ключ K.

Таким образом, стойкость протокола не превышает сложности нахождения одного секретного ключа.

Замечание 2. Злоумышленник для нахождения ключа может решить задачу дискретного логарифмирования в подгруппе $\langle a, b\rangle \subseteq L$ или $\langle b, c\rangle \subseteq L$, либо перебором найти элемент лупы, который является общим ключом.

Для примера рассмотрим класс луп Пейджа.

В качестве a, b, c можно выбрать элементы вида $\begin{pmatrix} \eta & e_1 \\ (0,0,0) & \eta^{-1} \end{pmatrix}$, $\begin{pmatrix} \theta & e_2 \\ (0,0,0) & \theta^{-1} \end{pmatrix}$, $\begin{pmatrix} \zeta & e_3 \\ (0,0,0) & \zeta^{-1} \end{pmatrix}$, где η, θ, ζ — примитивные элементы поля $\mathbb{F}_q$. Порядки данных элементов равны $(q-1)/2$.

3.2. Схема шифрования

Пусть L — конечная лупа и задана последовательность $\alpha = [A_1, \ldots, A_s]$, где $A_i \in L^r$ для некоторого натурального числа r, т. е. $A_i = (a_{i,1}, \ldots, a_{i,r})$, $a_{i,j} \in L$. Для каждого $i = 1, \ldots, s$ обозначим через A'_i элемент лупового кольца $\sum\limits_j a_{i,j} \in ZA$. Тогда $A'_1 \cdot \ldots \cdot A'_s = \sum a_l l$.

Определение 8. Последовательность $\alpha = [A_1, \ldots, A_s]$ называется $[s, r]$-покрытием для L, если для элемента лупового кольца $\sum a_l l = A'_1 \cdot \ldots \cdot A'_s$ выполняются условия: $a_l > 0$ для всех $l \in L$ и $|A_i| = r$, $i = 1, \ldots, s$.

Рассмотрим криптосхему, которая основана на $[s, r]$-покрытиях лупы Муфанг. Пусть L — конечная лупа Муфанг и $\alpha = (a_{i,j})$ — $[s, r]$-покрытие лупы L. В работе [11] показано, что сложность задачи разложения на множители $g = a_{1,j_1} \cdot a_{2,j_2} \cdot a_{3,j_3} \cdot \ldots \cdot a_{s,j_s}$ в конечной группе G эквивалентна сложности задачи дискретного логарифмирования в группе G. Тогда, в общем случае, задача разложения элемента лупы $l \in L$ на множители $l = (a_{1,j_1} \cdot (a_{2,j_2} \cdot (a_{3,j_3} \cdot \ldots \cdot a_{s,j_s})$ с неизвестной расстановкой скобок имеет не меньшую сложность, чем аналогичная задача в конечной группе.

Участник A:

1) Выбирает две лупы Муфанг L, M с достаточно большим количеством порождающих. Генерирует случайное $[s, r]$-покрытие $\alpha = (a_{i,j})$ для L.

2) Выбирает эпиморфизм $f : L \to M$, который он хранит в секрете, и вычисляет $\beta = (b_{i,j}) = f(\alpha) = f(a_{i,j})$. Заметим, что β является $[s, r]$-покрытием для лупы M.

Открытым ключом является

$$(\{\alpha\}, \{\beta\}).$$

Участник B:

1) Формирует сообщение $x \in M$.

2) Выбирает произвольное y_1 из покрытия α, причём расстановка скобок осуществляется произвольным способом. Таким образом, $y_1 = a_{1,j_1} \cdot (a_{2,j_2} \cdot (a_{3,j_3} \cdot \ldots \cdot a_{s,j_s})$.

3) Образует $y_2 \in \beta$ с аналогичной п. 2 расстановкой скобок.

4) Формирует $y_3 = xy_2$.

5) Посылает участнику A криптограмму (y_1, y_3).

Участник A, получив пару (y_1, y_3), вычисляет $f(y_1) = y_2$ и $y_3 y_2^{-1}$. Так как M — лупа Муфанг, то $y_3 y_2^{-1} = (xy_2)y_2^{-1} = x$.

Замечание 1. С практической точки зрения участнику А лучше заранее составить таблицу значений для эпиморфизма f.

Замечание 2. Конструкция легко может быть обобщена на произвольную квазигруппу, если умножение на y_2^{-1} справа в алгоритме расшифрования заменить на правое деление.

Замечание 3. Любое $[s, r]$-покрытие можно представить в виде матрицы $\alpha = (a_{i,j})$, где $a_{i,j} \in L$, $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant r$. Тогда с практической точки зрения $[s, r]$-покрытие удобно задавать случайной $(s \times r)$-матрицей с проверкой необходимых условий.

4. Линейно оптимальные коды в квазигрупповых кольцах

4.1. Предварительные сведения

Кодом длины n над алфавитом Ω называется подмножество $\mathcal{C} \subseteq \Omega^n$. Пусть $|\mathcal{C}| = q^k$, тогда $k = \log_q |\mathcal{C}|$ называется (*комбинаторной*) *размерностью* кода $\mathcal{C}$. На множестве $\mathcal{C}$

определим метрику (расстояние Хэмминга)

$$\mathrm{d}(a,b) = |\{i \in \{1,2,\ldots,n\} : a_i \neq b_i\}|,$$

где $a = (a_1,\ldots,a_n)$, $b = (b_1,\ldots,b_n)$.

Теперь определим расстояние кода:

$$d = \mathrm{d}(\mathcal{C}) = \min\{\mathrm{d}(a,b) : a,b \in \mathcal{C}, a \neq b\}.$$

Код с определёнными выше параметрами q,n,k,d называется $[n,k,d]_q$-*кодом* (подробнее см. [12, 13]).

Одной из задач алгебраической теории кодов является конструирование кодов, оптимизирующих один из параметров n,k,d при фиксированных значениях остальных двух и q.

Теорема 4 (граница Синглтона [12, 13]). Для любого $[n,k,d]_q$-кода выполнено неравенство $k \leqslant n-d+1$.

Определение 9. $[n,k,d]_q$-Код $\mathcal{C}$ называется *МДР-кодом*, если $k = n-d+1$.

Важный класс МДР-кодов исследуется в [14].

Если множество Ω снабжено алгебраической структурой (например, конечного поля, кольца или модуля) и код $\mathcal{C}$ согласован с этой структурой (например, если $\Omega = \mathbb{F}_q$ — конечное поле, то $\mathcal{C}$ должен быть подпространством в $\Omega = \mathbb{F}_q^n$), то код $\mathcal{C}$ называют *линейным кодом над* Ω.

Определение 10. Линейный $[n,k,d]_q$-код называется *линейно оптимальным*, если k — максимально возможная размерность линейного над полем $\Omega = \mathbb{F}_q$ кода длины n с расстоянием d.

Очевидно, что любой МДР-код оптимален. Сверх того, можно указать следующий признак линейной оптимальности.

Обозначим через $n(k,q)$ (соответственно, $m(k,q)$) максимальную длину МДР-кода комбинаторной размерности k над алфавитом из q элементов (соответственно, линейного МДР-кода над полем $\mathbb{F}_q$ для примарного числа q). Ясно, что $m(k,q) \leqslant n(k,q)$.

Утверждение 2. Пусть n,k — натуральные числа, q — такое примарное число, что $n > m(k+1,q)$. Тогда любой линейный $[n,n-k,k]_q$-код линейно оптимален.

Доказательство. Действительно, в противном случае существует линейный $[n,k+1,n-k]_q$-код. Но такой код является МДР-кодом, следовательно, $n \leqslant m(k+1,q)$. Получаем противоречие. ■

Одним из способом получения линейных над полем $\mathbb{F}_q$ кодов с экстремальными свойствами является следующая конструкция. Для конечной лупы $L = \{l_1,\ldots,l_n\}$ сформируем луповую алгебру $A = \mathbb{F}_q L$ и для каждого левого идеала $I \leqslant {}_A A$ определим код $\mathcal{C} = \mathcal{C}(I)$ как набор всех слов $(\alpha_1,\ldots,\alpha_n) \in \mathbb{F}_q^n$, таких, что $\sum \alpha_i l_i \in I$. Такие коды называются луповыми [15]. Каждая луповая алгебра (и даже квазигрупповая алгебра) содержит 2 *тривиальных МДР-кода*: $[n,1,n]$-код $\mathcal{C}(I_0)$, соответствующий левому идеалу $\mathbb{F}_q(\sum_{l\in L} l)$, и $[n,n-1,2]$-код $\mathcal{C}(\Delta)$, соответствующий фундаментальному идеалу

$$\Delta(A) = \left\{ \sum_{l\in L} \alpha(l) l : \sum_{l\in L} \alpha(l) = 0 \right\},$$

который является левым и правым аннулятором идеала I_0.

Компьютерные вычисления в [15] в случае луповых алгебр маленьких порядков ($q \leqslant 5$, $|L| \leqslant 7$) показали, что в большинстве случаев, когда лупа L неассоциативна, её решётка левых идеалов тривиальна, и поэтому она не содержит интересных луповых кодов. Исключение составляют линейно оптимальные $[6,2,4]_q$-коды для $q \in \{2,3\}$, а также $[6,3,3]_q$-коды для $q \in \{3,4\}$.

В данной работе строятся цепочки линейных $[n, n-3, 3]_q$-кодов над $\mathbb{F}_q$ для $n = 2q$ и $n = 2q-2$. Эти коды являются линейно оптимальными, что следует из утверждения 2, а также из того, что $n(k,q) = k+1$ при $q \leqslant k$ (см. [12, 13]).

Заметим, что линейный $[n, n-3, 3]_q$-код над $\mathbb{F}_q$ может быть легко построен с помощью укорочения $[N, N-3, 3]_q$-кода Хэмминга ([16, 17]), где $N = q^2+q+1$. Основной результат заключается в построении таких кодов как луповых кодов.

4.2. Коды Рида – Соломона как групповые коды

Пусть $q = p^l > 2$, $P = \mathbb{F}_q$, G — конечная группа. Единичный элемент поля P обозначим 1, единичный элемент группы G (он же единичный элемент группового кольца PG) обозначим e.

Следующее представление кодов Рида — Соломона как групповых кодов, впервые описанное в [18], играет ключевую роль в построении линейных луповых $[2q, 2q-3, 3]_q$-кодов.

Теорема 5. Пусть $(H, \cdot)$ — p-элементарная абелева группа порядка $q = p^l$. Фиксируем изоморфизм абелевых групп $\varphi : (H, \cdot) \to (P, +)$ и рассмотрим следующие элементы:

$$u_s = \sum_{h \in H} \varphi(h)^s h \in PH, \quad s = 0, \ldots, q-2. \tag{1}$$

Тогда для каждого i, $1 \leqslant i \leqslant q-1$, подпространство $\mathcal{R}_i = Pu_0 + \ldots + Pu_{i-1} \leqslant {}_P PH$ является $[q, i, q+1-i]_q$-МДР кодом Рида — Соломона и идеалом в PH. В частности,

$$\mathcal{R}_{q-1} = \Delta(PH). \tag{2}$$

Если $s = p^c$ для некоторого $1 \leqslant c \leqslant n-1$, то

$$\mathcal{R}_s = PHu_{s-1} \tag{3}$$

является главным идеалом.

Доказательство. Занумеруем элементы группы H: $H = \{h_1, \ldots, h_q\}$, и положим $w_r = \varphi(h_r)$, $1 \leqslant r \leqslant q$. Тогда $P = \{w_1, \ldots, w_q\}$ и элементы (1) имеют вид $u_s = \sum\limits_{r=1}^{q} w_r^s h_r$. Теперь легко видеть, что код $\mathcal{K}(\mathcal{R}_i) \leqslant {}_P PH$, соответствующий пространству $\mathcal{R}_i$, имеет порождающую матрицу

$$G_i = \begin{pmatrix} w_1^0 & w_2^0 & \ldots & w_q^0 \\ \ldots & \ldots & \ldots & \ldots \\ w_1^{i-1} & w_2^{i-1} & \ldots & w_q^{i-1} \end{pmatrix},$$

т. е. является $[q, i, q-i+1]_q$-кодом Рида — Соломона [12, 13]. Заметим, что пока использована только биективность φ.

С учётом того, что φ является изоморфизмом групп, докажем, что $\mathcal{R}_s$, $1 \leqslant s \leqslant q-1$, является идеалом в кольце $R = PH$. Достаточно показать, что $a\mathcal{R}_s \subseteq \mathcal{R}_s$ для любого $a \in H$. Докажем это индукцией по s. При $s = 1$ имеем

$$a\mathcal{R}_1 = Pau_0 = Pa \sum_{h \in H} \varphi(h)^0 h = P \sum_{h \in H} ah = P \sum_{h \in H} h = Pu_0 = \mathcal{R}_1.$$

При $s > 0$

$$au_s = \sum_{h\in H} \varphi(h)^s ah = \sum_{h\in H} \varphi(ha^{-1})^s h,$$

и, поскольку φ — гомоморфизм,

$$au_s = \sum_{h\in H} [\varphi(h) - \varphi(a)]^s h = \sum_{h\in H} \left[\varphi(h)^s + \sum_{t=1}^{s} (-1)^t \binom{s}{t} \varphi(h)^{s-t}\varphi(a)^t\right] h =$$

$$= \sum_{h\in H} \varphi(h)^s h + \sum_{t=1}^{s} (-1)^t \binom{s}{t} \varphi(a)^t \sum_{h\in H} \varphi(h)^{s-t} h.$$

Окончательно получаем

$$au_s = u_s + \sum_{t=1}^{s} (-1)^t \binom{s}{t} \varphi(a)^t u_{s-t} \in u_s + \mathcal{R}_s \subset \mathcal{R}_{s+1}. \tag{4}$$

Итак, $a\mathcal{R}_1 \subseteq \mathcal{R}_1$, и, учитывая, что по предположению индукции $a\mathcal{R}_s \subseteq \mathcal{R}_s$, получаем

$$a\mathcal{R}_{s+1} = Pau_s + a\mathcal{R}_s \subseteq Pu_s + \mathcal{R}_s + a\mathcal{R}_s = \mathcal{R}_{s+1},$$

что и требовалось.

Чтобы доказать равенство (2), покажем, что $\sum\limits_{\omega\in P} \omega^s = 0$ для $s = 0, \ldots, q-2$. Пусть $\alpha \in P : \langle\alpha\rangle = P^*$, тогда $\alpha^s \left(\sum\limits_{\omega\in P} \omega^s\right) = \sum\limits_{\omega\in P} \omega^s$, $s = 0, \ldots, q-2$, откуда получаем требуемое, так как $\alpha^s \neq 1$ при $s < q-1$. Таким образом, $\mathcal{R}_{q-1} \subseteq \Delta(PH)$. С другой стороны, $\dim_P \mathcal{R}_{q-1} = q-1 = \dim_P \Delta(PH)$, следовательно, $\mathcal{R}_{q-1} = \Delta(PH)$.

Доказательство равенства (3) основывается на хорошо известном результате Лукаса (см., например, [12]). Пусть r_{ts} — остаток по модулю p числа $(-1)^t \binom{s}{t}$ и $s = s_0 + ps_1 + \ldots + p^{l-1}s_{n-1}$, $t = t_0 + pt_1 + \ldots + p^{l-1}t_{n-1}$, где $p_i, t_j \in \{0, \ldots, p-1\}$, причём $s_i \leqslant t_i$. Тогда

$$r_{ts} \equiv (-1)^t \binom{s_0}{t_0}\binom{s_1}{t_1}\ldots\binom{s_{n-1}}{t_{n-1}} \pmod p.$$

Тем самым доказано следующее утверждение.

Лемма 3. Если $s = p^c$, то $r_{t,s-1} \in P^*$ для любого $1 \leqslant t \leqslant s-1$.

Теперь перепишем (4) в виде

$$\sum_{t=1}^{s-1} r_{t,s-1}\varphi(a)^t u_{s-1-t} = (a-e)u_{s-1}.$$

Выберем $s-1$ различных элементов $a_1, \ldots, a_{s-1} \in H \setminus \{e\}$ и положим $w_i = \varphi(a_i)$, $i = 1, \ldots, s-1$. Тогда, имея u_{s-1}, можем построить систему уравнений относительно неизвестных параметров $u_0, \ldots, u_{s-2}$:

$$\begin{pmatrix} r_{1,s-1}w_1 & r_{2,s-1}w_1^2 & \ldots & r_{s-1,s-1}w_1^{s-1} \\ r_{1,s-1}w_2 & r_{2,s-1}w_2^2 & \ldots & r_{s-1,s-1}w_2^{s-1} \\ \ldots & \ldots & \ldots & \ldots \\ r_{1,s-1}w_{s-1} & r_{2,s-1}w_{s-1}^2 & \ldots & r_{s-1,s-1}w_{s-1}^{s-1} \end{pmatrix} \begin{pmatrix} u_{s-2} \\ u_{s-3} \\ \ldots \\ u_o \end{pmatrix} = \begin{pmatrix} (a_1-e)u_{s-1} \\ (a_2-e)u_{s-1} \\ \ldots \\ (a_{s-1}-e)u_{s-1} \end{pmatrix}. \tag{5}$$

Если $s = p^c$, то по лемме 3 матрица в левой части системы (5) обратима (и, следовательно, система имеет единственное решение). Это означает, что $u_0, ..., u_{s-2} \in PHu_{s-1}$. Таким образом, (3) верно. ■

Близкие описания кодов Рида — Соломона получены в [19, 20].

4.3. Линейно оптимальные $[2q, 2q-3, 3]_q$-коды

Как и выше, p — простое, $q = p^n > 2$ и $P = \mathbb{F}_q$.

Сформулируем основной результат этого пункта.

Теорема 6. Пусть L — лупа порядка $2q$, содержащая p-элементарную абелеву группу H порядка q. Пусть также существует элемент $b \in L \setminus H$, обладающий следующими свойствами:

1) $\exists \dot{k} \in \{1, \ldots, p-1\} \quad \forall l \in L \setminus H \ \ \exists \dot{h}_l \in H \quad \forall h \in H \ \ lh = b(\dot{h}_l h^{\dot{k}})$;
2) $\exists \ddot{k} \in \{1, \ldots, p-1\} \quad \forall l \in L \setminus H \ \ \exists \ddot{h}_l \in H \quad \forall h \in H \ \ l(bh) = \ddot{h}_l h^{\ddot{k}}$;
3) $\forall \alpha \in H \ \ \exists h_\alpha \in H \quad \forall h \in H \ \ \alpha(bh) = b(h_\alpha h)$.

Тогда, если степень расширения n чётная или если $P = \mathbb{F}_p$ и

$$\exists k \in P \ k^2 = \dot{k}^{-1}\ddot{k}, \tag{6}$$

то в решётке левых идеалов PL содержится структура, изображенная на рис. 1.

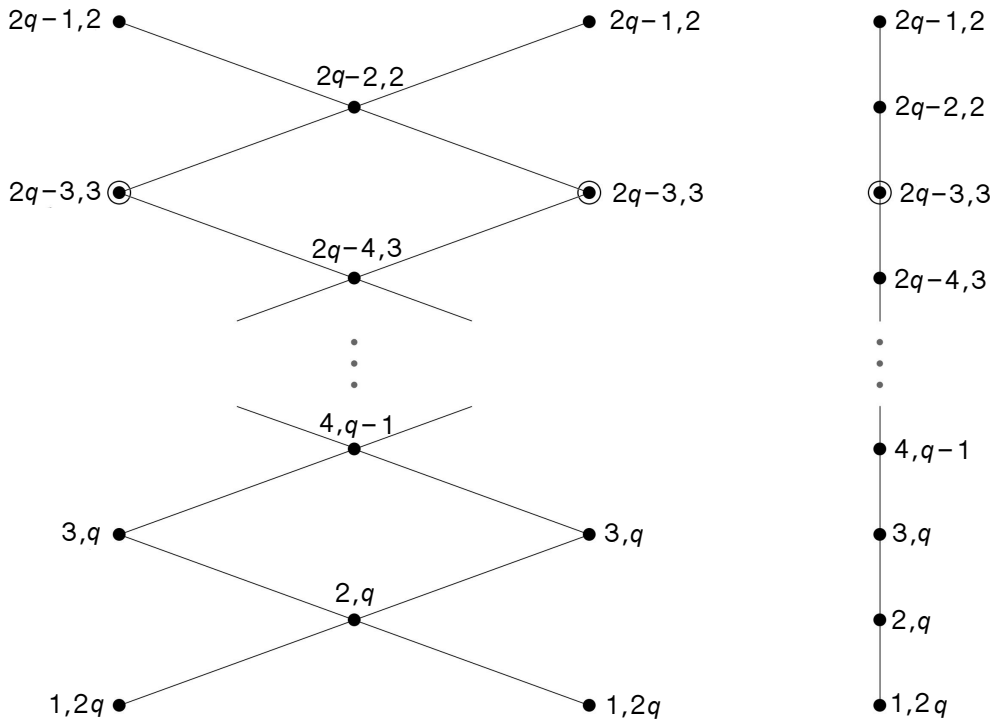

Рис. 1. Решётка идеалов PL при $\operatorname{char} P \neq 2$ (слева) и при $\operatorname{char} P = 2$ (справа). Каждый круг обозначает левый идеал PL, а k, d — сопровождающие числа, где k обозначает размерность, d — расстояние соответствующего кода. Любые два идеала соединены линией тогда и только тогда, когда нижний содержится в верхнем

Выделенные на рис. 1 идеалы соответствуют линейно оптимальным $[2q, 2q-3, 3]_q$-кодам.

Доказательство. Сохраним старые обозначения: пусть $\varphi : (H, \cdot) \to (P, +)$ — изоморфизм абелевых групп; $\mathcal{R}_i = Pu_0 + \ldots + Pu_{i-1} \leqslant {}_P PH$, $1 \leqslant i \leqslant q-1$.

Заметим, что если n чётное, то условие (6) выполнено, так как многочлен $x^2 - \dot{k}^{-1}\ddot{k} \in \mathbb{F}_p[x]$ раскладывается в $\mathbb{F}_{p^2}$ на линейные множители. Обозначим $\pm k_i$ квадратные корни из $(\dot{k}^{-1}\ddot{k})^i$.

С помощью $v_i \in \mathcal{R}_{i+1} \setminus \mathcal{R}_i$ построим

$$\sigma_i^+ = ev_i + b(k_i v_i), \quad \sigma_i^- = ev_i - b(k_i v_i),$$

если $\operatorname{char} P = 2$, то $\sigma_i^+ = \sigma_i^i$.

Тогда искомые идеалы имеют вид

$$\mathcal{L}_i = e\mathcal{R}_i + b\mathcal{R}_i \lhd PL,$$
$$\mathcal{M}_i^+ = e\mathcal{R}_i + b\mathcal{R}_i + P\sigma_i^+ \lhd PL, \qquad \mathcal{M}_i^- = e\mathcal{R}_i + b\mathcal{R}_i + P\sigma_i^- \lhd PL,$$

если $\operatorname{char} P = 2$, то $\mathcal{M}_i^+ = \mathcal{M}_i^i$.

Этим идеалам соответствуют луповые коды: $\mathcal{C}(\mathcal{L}_i)$ есть $[2q, 2i, q+1-i]_q$-код; $\mathcal{C}(\mathcal{M}_i^+)$ — $[2q, 2i+1, q+1-i]_q$-код; $\mathcal{C}(\mathcal{M}_i^-)$ — $[2q, 2i+1, q+1-i]_q$-код.

Так как $b \in L \setminus H$, то $L = H \cup bH$ и, следовательно, $PL = PH \dot{+} bPH$. Значит, $\mathcal{L}_i = e\mathcal{R}_i + b\mathcal{R}_i$ имеет размерность $2i$ и расстояние $q+1-i$.

Далее, так как $\mathcal{M}_i^+ = \mathcal{L}_i + P\sigma_i^+$, где $\sigma_i^+ = ev_i + b(k_i v_i)$ и $v_i \in \mathcal{R}_{i+1} \setminus \mathcal{R}_i$, то $\sigma_i^+ \notin \mathcal{L}_i$ и, следовательно, $\dim(\mathcal{L}_i) = 2i+1$. Аналогично для $\mathcal{M}_i^-$.

Теперь определим расстояние $\mathcal{M}_i^+$. Так как $\mathcal{M}_i^+ \supseteq e\mathcal{R}_i$, то $\mathrm{d}(\mathcal{M}_i^+) \leqslant \mathrm{d}(R_i) = q+1-i$. С другой стороны, включение $v_i \in \mathcal{R}_{i+1} \setminus \mathcal{R}_i$ влечёт неравенство

$$\mathrm{d}(v_i, \mathcal{R}_i) = \min\{\mathrm{d}(v_i, u) : u \in \mathcal{R}_i\} \geqslant q+1-(i+1) = q-i. \tag{7}$$

Рассмотрим произвольный элемент $x \in \mathcal{M}_i^+ \setminus \{0\}$, $x = ex_1 + bx_2 + \alpha\sigma_i^+$, где $x_1, x_2 \in \mathcal{R}_i$, $\alpha \in P$. Очевидно, что $||x|| = ||x_1 + \alpha v_i|| + ||b(x_2 + \alpha v_i)|| = ||x_1 + (\alpha k_i)v_i|| + ||x_2 + (\alpha k_i)v_i||$. Если $\alpha = 0$, то $x \in \mathcal{L}_i$ и $||x|| \geqslant q+1-i$. Иначе $||x_1 + \alpha v_1|| \geqslant q-i$ и $||x_2 + (\alpha k_i)v_2|| \geqslant q-i$ согласно (7). Таким образом, $||x|| \geqslant 2(q-i) \geqslant q+1-i$, если $i \leqslant q-1$. Окончательно, $\mathrm{d}(\mathcal{M}_i^+) = q+1-i$.

Аналогично доказывается, что $\mathrm{d}(\mathcal{M}_i^-) = q+1-i$.

Осталось показать, что $\mathcal{L}_i$, $\mathcal{M}_i^+$, $\mathcal{M}_i^+$ являются L-кодами, т. е. левыми иделами PL.

Сначала покажем, что $\mathcal{L}_i \lhd PL$. Достаточно проверить, что $\alpha\mathcal{L}_i \subseteq \mathcal{L}_i$, $\alpha \in H$, и $l\mathcal{L}_i \subseteq \mathcal{L}_i$, $l \in L \setminus H$. Учитывая свойство 3 из условия теоремы и то, что $\mathcal{R}_i \lhd PH$, получаем

$$\alpha\mathcal{L}_i = \alpha(e\mathcal{R}_i + b\mathcal{R}_i) = \alpha\mathcal{R}_i + \alpha(b\mathcal{R}_i) = \alpha\mathcal{R}_i + b(h_\alpha\mathcal{R}_i) \subseteq \mathcal{R}_i + b(\mathcal{R}_i) = \mathcal{L}_i.$$

Лемма 4. Пусть $v = \sum\limits_{h\in H} \alpha(h)h \in \mathcal{R}_i$. Определим $\psi_k(v) = \sum\limits_{h\in H} \alpha(h)h^k \in \mathcal{R}_i$, где $k \in \mathbb{Z}$, $p \nmid k$. Пусть μ таково, что $\mu p \equiv 1 \pmod p$. Тогда

$$\psi_k(v) \equiv \mu^{i-1} v \pmod{\mathcal{R}_{i-1}}. \tag{8}$$

В частности,

$$\psi_k(\mathcal{R}_i) \subseteq \mathcal{R}_i. \tag{9}$$

Доказательство. Напомним, что $\mathcal{R}_i = Pu_0 + \ldots + Pu_{i-1}$. Заметим, что отображение ψ_k линейное. Рассмотрим $\psi_k(u_s) = \psi_k\left(\sum\limits_{h\in H} \varphi(h)^s h\right) = \sum\limits_{h\in H} \varphi(h)^s h^k = \sum\limits_{h\in H} \varphi(h^\mu)^s h$ (это следует из того, что все элементы из $H \setminus \{e\}$ имеют порядок p). Так как φ — гомоморфизм, то $\psi_k(u_s) = \sum\limits_{h\in H} (\mu\varphi(h))^s h = \mu^s u_s$, откуда получаем (8) и (9). ■

Теперь можно показать, что $l\mathcal{L}_i \subseteq \mathcal{L}_i$:

$$l\mathcal{L}_i = l(e\mathcal{R}_i + b\mathcal{R}_i) = \ddot{h}_l\psi_{\ddot{k}}(\mathcal{R}_i) + b(\dot{h}_l\psi_{\dot{k}}(\mathcal{R}_i)) \subseteq \ddot{h}_l\mathcal{R}_i + b(\dot{h}_l\mathcal{R}_i) \subseteq \mathcal{R}_i + bR_i = \mathcal{L}_i.$$

Мы воспользовались свойством (9), свойствами 1, 2 из условия и тем, что $\mathcal{R}_i \lhd PH$.

Рассмотрим $\mathcal{M}_i^+ \leqslant {}_PPL$. Так как уже доказано, что $\mathcal{L}_i \lhd PL$, то достаточно проверить, что $\alpha\sigma_i^+ \subseteq \mathcal{M}_i^+$, $\alpha \in H$, и $l\sigma_i^+ \subseteq \mathcal{M}_i^+$, $l \in L \setminus H$. Справедливы равенства

$$\alpha\sigma_i^+ = \alpha(ev_i + b(k_iv_i)) = \alpha v_i + b(h_\alpha k_i v_i) =$$
$$= (\alpha - e)v_i + ev_i + b((h_\alpha - e)k_iv_i + e(k_iv_i)) = \sigma_i^+ + (\alpha - e)v_i + b((h_\alpha - e)k_iv_i).$$

Заметим, что из (4) следует соотношение $hv_i \equiv v_i \pmod{\mathcal{R}_{i-1}}$ для всех $v_i \in \mathcal{R}_i$, $h \in H$, значит, $(\alpha - e)v_i + b((h_\alpha - e)k_iv_i) \in \mathcal{L}_i$.

Далее, по свойствам 1, 2 и лемме 4 получим

$$l\sigma_i^+ = l(ev_i + b(k_iv_i)) = b(\dot{h}_l\psi_{\dot{k}}(v_i)) + \ddot{h}_l\psi_{\ddot{k}}(k_iv_i) =$$
$$= k_i\ddot{h}_l\psi_{\ddot{k}}(v_i) + b(\dot{h}_l\psi_{\dot{k}}(v_i)) \equiv k_i\ddot{\mu}^iv_i + b(\dot{\mu}^iv_i) \pmod{\mathcal{L}_i},$$

где $\dot{\mu}\dot{k} \equiv \ddot{\mu}\ddot{k} \equiv 1 \pmod p$. Остаётся заметить, что $k_i\ddot{\mu}^iv_i + b(\dot{\mu}^iv_i) = k_i\ddot{\mu}^i\sigma_i^+$, так как $k_i^2 \equiv (\dot{\mu}\ddot{\mu}^{-1})^i \pmod p$.

Доказательство для $\mathcal{M}_i^-$ аналогично.

Неравенство $\mathcal{M}_i^+ \neq \mathcal{M}_i^-$ следует из того, что $\mathcal{M}_i^+ + \mathcal{M}_i^- = \mathcal{L}_{i+1}$, а $\dim(\mathcal{L}_{i+1}) > \dim(\mathcal{M}_i^+) = \dim(\mathcal{M}_i^-)$.

Таким образом, мы построили всю решётку идеалов, за исключением идеалов размерности 1. Построим их:

$$\mathcal{M}_0^+ = P\left(\sum_{l\in L} l\right), \qquad \mathcal{M}_0^- = P\left(\sum_{h\in H} h - \sum_{l\in L\setminus H} l\right).$$

Теорема доказана. ■

Замечание. Если существует элемент $b \in L \setminus H$, удовлетворяющий условию теоремы 6, то и любой другой элемент из $L \setminus H$ тоже удовлетворяет этому условию.

4.4. Линейно оптимальные $[2q-2, 2q-5, 3]_q$-коды

Сохраним обозначения $P = \mathbb{F}_q$, $q = p^n$.

Теорема 7. Пусть L — лупа порядка $2q-2$, содержащая циклическую абелеву группу H порядка $q-1$. Пусть также существует элемент $b \in L \setminus H$, обладающий следующими тремя свойствами:

1) $\forall l \in L \setminus H \ \ \exists \dot{h}_l \in H \quad \forall h \in H \ \ lh = b(\dot{h}_l h)$;
2) $\forall l \in L \setminus H \ \ \exists \ddot{h}_l \in H \quad \forall h \in H \ \ l(bh) = \ddot{h}_l h$;
3) $\forall \alpha \in H \ \ \exists h_\alpha \in H \quad \forall h \in H \ \alpha(bh) = h_\alpha h$.

Тогда если $\operatorname{char} P \neq 2$, то в решётке левых идеалов PL содержится $\varphi(q-1)$ (φ — функция Эйлера) структур следующего вида (все идеалы, участвующие в структурах, попарно различны):

$$\mathcal{L}_i \subseteq \mathcal{M}_i^-, \quad \mathcal{M}_i^+ \subseteq \mathcal{N}_i, \quad i = 1, 2, \ldots, q-1,$$

причём $\mathcal{C}(\mathcal{M}_i^\pm)$ являются линейно оптимальными $[2q-5, 2q-3, 3]_q$-кодами.

Если $\operatorname{char} P = 2$, то в решётке левых идеалов PL содержится $\varphi(q-1)$ цепочек следующего вида (все идеалы, участвующие в цепочках, попарно различны):

$$\mathcal{L}_i \subseteq \mathcal{M}_i \subseteq \mathcal{N}_i, \quad i = 1, 2, \ldots, q-1,$$

причём $\mathcal{C}(\mathcal{M}_i)$ являются линейно оптимальными $[2q-5, 2q-3, 3]_q$-кодами.

Доказательство. По условию $H = \langle a \rangle_{q-1}$, поэтому $PH \cong \mathbb{F}_p[x]/(x^{q-1}-1)$ и все идеалы PH имеют вид $([g(x)])$, где $g(x) \mid x^{q-1}-1$. Заметим, что так как $|P^*| = q-1$, то многочлен $x^{q-1}-1$ раскладывается в P на (различные) линейные множители.

Для каждого примитивного $\alpha_i \in P$, $i = 1, \ldots, \varphi(q-1)$, определим

$$\mathcal{V}_i = ([(x-1)(x-\alpha_i)]) \lhd PH, \quad \mathcal{W}_i = ([(x-\alpha_i)]) \lhd PH.$$

Ясно, что $\dim(\mathcal{V}_i) = q-1-2 = q-3$, $\dim(\mathcal{W}_i) = q-1-1 = q-2$. Найдём теперь расстояния. Очевидно, что $\mathrm{d}(\mathcal{C}(\mathcal{W}_i)) = 2$. Чтобы определить расстояние $\mathcal{C}(\mathcal{V}_i)$, заметим, что вектор v принадлежит $\mathcal{C}(\mathcal{V}_i)$ тогда и только тогда, когда

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \alpha_i & \alpha_i^2 & \ldots & \alpha_i^{q-2} \end{pmatrix} v = 0. \tag{10}$$

Так как $\mathrm{ord}\,(\alpha_i) = q-1$, то гарантированный ранг проверочной матрицы из (10) равен 2, следовательно, $\mathrm{d}(\mathcal{C}(\mathcal{V}_i)) = 3$.

С помощью $\mathcal{V}_i$ и $\mathcal{W}_i$ построим

$$\mathcal{L}_i = e\mathcal{V}_i + b\mathcal{V}_i, \quad \mathcal{N}_i = e\mathcal{W}_i + b\mathcal{W}_i.$$

По свойствам 1, 2, 3 легко проверяется, что $\mathcal{L}_i$ и $\mathcal{N}_i$ являются идеалами в PL. Далее, так как $b \in L \setminus H$, то $L = H \cup bH$, а значит, $PL = PH \dot{+} bPH$. Поэтому $\dim(\mathcal{L}_i) = 2(q-3) = 2q-6$, $\dim(\mathcal{N}_i) = 2(q-2) = 2q-4$, $\mathrm{d}(\mathcal{C}(\mathcal{L}_i)) = \mathrm{d}(\mathcal{C}(\mathcal{V}_i)) = 3$, $\mathrm{d}(\mathcal{C}(\mathcal{N}_i)) = \mathrm{d}(\mathcal{C}(\mathcal{W}_i)) = 2$.

Обозначим $\sigma_i^+ = ev_i + bv_i$, $\sigma_i^- = ev_i - bv_i$, где $v_i \in \mathcal{W}_i \setminus \mathcal{V}_i$ (если $\mathrm{char}\, P = 2$, то $\sigma_i^+ = \sigma_i^-$), и построим $\mathcal{M}_i^+, \mathcal{M}_i^- \leqslant {}_P PL$ (если $\mathrm{char}\, P = 2$, то $\mathcal{M}_i^+ = \mathcal{M}_i^- = \mathcal{M}$):

$$\mathcal{M}_i^+ = \mathcal{L}_i + P\sigma_i^+, \quad \mathcal{M}_i^- = \mathcal{L}_i + P\sigma_i^-.$$

Размерность $\mathcal{M}_i^\pm$ равна $2q-5$, так как $\sigma_i^\pm \neq \mathcal{L}_i$. Поскольку $\mathrm{d}(v_i, \mathcal{V}_i) \geqslant 2$, то $\mathrm{d}(\sigma_i^\pm, \mathcal{L}_i) \geqslant$ $\geqslant 4 > \mathrm{d}(\mathcal{C}(\mathcal{L}_i)) = 3$. Следовательно, $\mathrm{d}(\mathcal{C}(\mathcal{M}_i)) = \mathrm{d}(\mathcal{C}(\mathcal{L}_i)) = 3$. Далее нам понадобится следующее утверждение.

Лемма 5. Если $v_i \in \mathcal{W}_i$, то $(\alpha - e)v_i \in \mathcal{V}_i$ для всех $\alpha \in H$.

Доказательство. Вектору v_i соответствует $[v_i(x)] \in \mathbb{F}_q[x]/(x^{q-1}-1)$. Пусть $\alpha = a^k$, тогда $(\alpha - e)$ соответствует $[x^k - 1]$. Остаётся заметить, что $[v_i(x)(x^k-1)] \in$ $\in ([(x-1)(x-\alpha_i)]) = \mathcal{V}_i$, так как $(x-1) \mid (x^k-1)$. ■

Покажем, что $\mathcal{M}_i^+ \lhd PL$. Так как $\mathcal{L}_i \lhd PL$, то достаточно показать, что $\alpha\sigma_i^+ \in \mathcal{M}_i$, $l\sigma_i \in \mathcal{M}_i$ для всех $\alpha \in H$, $l \in L \setminus H$. Действительно, по лемме 5 и свойству 3 из условия получим

$$\alpha\sigma_i = \alpha(ev_i + bv_i) = \alpha v_i + b(h_\alpha v_i) =$$
$$= (\alpha - e)v_i + ev_i + b((h_\alpha - e)v_i + ev_i) = \sigma_i + (\alpha - e)v_i + b((h_\alpha - e)v_i) \equiv \sigma_i \pmod{\mathcal{L}_i},$$

а по лемме 5 и свойствам 1, 2

$$l\sigma_i = l(ev_i + bv_i) = \ddot{h}_l v_i + b(\dot{h}_l)v_i \equiv ev_i + bv_i \pmod{\mathcal{L}_i}.$$

При рассмотрении σ_i^- получим, что

$$\alpha\sigma_i^- \equiv \sigma_i^- \pmod{\mathcal{L}_i}, \quad l\sigma_i^- \equiv -\sigma_i^- \pmod{\mathcal{L}_i}, \quad \alpha \in H,\ l \in L \setminus H.$$

Покажем, что все идеалы $\mathcal{M}_i^\pm$ различны. Действительно, $\mathcal{M}_i^+ + \mathcal{M}_i^- = \mathcal{N}_i$, а $\mathcal{M}_i^\pm + \mathcal{M}_j^\pm \supseteq \mathcal{L}_i + \mathcal{L}_j = e\mathcal{S} \dot{+} b\mathcal{S}$, где $\mathcal{S} = (a-e) \lhd PH$, $\dim(\mathcal{S}) = q-2$. Таким образом, $\dim(\mathcal{N}_i) = \dim(\mathcal{L}_i + \mathcal{L}_j) = 2q-4 > \dim(\mathcal{M}_i^\pm)$, что доказывает требуемое. ■

4.5. Коммутаторные квазигруппы

Примеры неассоциативных луп, рассматриваемых в теоремах 6 и 7, можно построить с помощью коммутаторных квазигрупп, конструкция которых описывается ниже.

Конструкция и алгебраические свойства коммутаторных квазигрупп

Пусть G — конечная группа. Зафиксируем целые числа c, d и определим новое умножение на элементах G по следующему правилу:

$$x *_{c,d} y = x^{1-d} y^c x^d y^{1-c} = x[x^{-d}, y^c]y, \quad x, y \in G.$$

Получившийся группоид обозначается $(G)_{c,d}$ и называется *коммутаторным группоидом* (или *коммутаторной квазигруппой*, если он удовлетворяет определению квазигруппы) для группы G с параметрами c, d.

Утверждение 3. Обозначим через e единичный элемент G, $Z(G)$ — центр группы и $m = \exp(G/Z(G))$.

1) Если группа G удовлетворяет тождеству $[x^c, y^{d-1}] = e$ (соответственно, $[x^{c-1}, y^d] = e$), то операции в $(G)_{c,d}$ и $(G)_{c,1}$ (соответственно, в $(G)_{c,d}$ и $(G)_{1,d}$) совпадают.
2) $(G)_{0,d} = (G)_{c,0} = G \quad \forall c, d \in \mathbb{Z}$.
3) $(G)_{1,1} = G^{op}$, где G^{op} — инверсная группа.
4) $(G)_{c,d} \cong (G)^{op}_{c,d} \quad \forall c, d \in \mathbb{Z}$.
5) Если $[x, y] = e$ в G, то $x * y = xy$.
6) Если $u \equiv c \pmod m$, $v \equiv d \pmod m$, то $(G)_{u,v} = (G)_{c,d}$.
7) Пусть $m_1, \ldots, m_k$ — список всех различных порядков элементов группы G. Если $c \equiv i_k \pmod{m_k}$, $d \equiv j_k \pmod{m_k}$, где $i_k, j_k \in \{0, 1\}$, то группоид $G_{c,d}$ является лупой.

Доказательство. Пункты 1–5 доказываются простой проверкой. Докажем п. 6 и 7.

6. Пусть $u = c + kn$, $v = d + nm$. Тогда

$$[x^{-v}, y^u] = x^{-d} x^{-nm} y^c y^{km} x^d x^{nm} y^{-c} y^{-km} = x^{-d} y^c x^d x^{-nm} y^{km} x^{nm} y^{-km} = [x^{-d}, y^c],$$

так как $x^{nm}, y^{km} \in Z(G)$.

7. Покажем, что уравнения $x * a = b$, $a * y = b$ разрешимы при любых $a, b \in G$. Рассмотрим первое уравнение (второе рассматривается аналогично). Из условия следует, что $x * y \in \{xy, yx\}$, причём если $\operatorname{ord}(\tilde{x}) = \operatorname{ord}(x)$, $\operatorname{ord}(\tilde{y}) = \operatorname{ord}(y)$ и $x * y = xy$ (соответственно, $x * y = yx$), то и $\tilde{x} * \tilde{y} = \tilde{x}\tilde{y}$ (соответственно, $\tilde{x} * \tilde{y} = \tilde{y}\tilde{x}$). Если $ba^{-1} * a = b$, то положим $x = ba^{-1}$, иначе положим $x = a^{-1}b$. Получили, что $(G)_{c,d}$ является квазигруппой. Остаётся заметить, что e — её единица. ■

Пункт 6 показывает, что количество неизоморфных группоидов в множестве $(G)_{c,d}$, $c, d \in \mathbb{Z}$, есть мера некоммутативности группы G.

Группоид $(G)_{c,d}$ всегда содержит единичный элемент, но не всегда является лупой. В общем случае условия на G, c, d, которые гарантируют, что $(G)_{c,d}$ является лупой, неизвестны, но в некоторых случаях у нас есть ответ.

Коммутаторные квазигруппы для группы диэдра D_n

В табл. 1 приведены явные формулы умножения в $(D_n)_{c,d}$, которые зависят только от чётности c, d.

Таблица 1

Формулы умножения в $(D_n)_{c,d}$

Варианты	c – н, d – н	c – ч, d – н	c – н, d – ч
$a^k * a^l$	a^{k+l}	a^{k+l}	a^{k+l}
$a^k * ba^l$	$ba^{k(2d-1)+l}$	ba^{l-k}	$ba^{k(2d-1)+l}$
$ba^k * a^l$	$ba^{k+l(1-2c)}$	$ba^{k+l(1-2c)}$	ba^{k+l}
$ba^k * ba^l$	a^{k-l}	a^{l-k}	a^{l-k}

Утверждение 4. Табл. 2 показывает, при каких c и d группоид $(D_n)_{c,d}$ является лупой.

Таблица 2

$c \diagdown d$	ч, $2d-1 \in \mathbb{Z}_n^*$	ч, $2d-1 \notin \mathbb{Z}_n^*$	н, $2d-1 \in \mathbb{Z}_n^*$	н, $2d-1 \notin \mathbb{Z}_n^*$
ч, $2c-1 \in \mathbb{Z}_n^*$	+	+	+	+
ч, $2c-1 \notin \mathbb{Z}_n^*$	+	+	−	−
н, $2c-1 \in \mathbb{Z}_n^*$	+	−	+	−
н, $2c-1 \notin \mathbb{Z}_n^*$	+	−	−	−

Примечание. «+» – лупа, «−» – не лупа.

Утверждение 5. Если $c, d \in \{1, \ldots, \exp(D_n/Z(D_n)) - 1\}$, то $(D_n)_{c,d}$ — полугруппа тогда и только тогда, когда $c = d = 1$ (в этом случае $(D_n)_{c,d} = (D_n)^{op} \cong D_n$) или когда c и d оба чётные (в этом случае $(D_n)_{c,d} = D_n$).

Утверждение 6. При различных парах $c, d \in \{1, \ldots, \exp(D_n/Z(D_n)) - 1\}$, таких, что c, d оба нечётные и $2c-1, 2d-1 \in \mathbb{Z}_n^*$, соответствующие им лупы $(D_n)_{c,d}$ неизоморфны.

Доказательство. Пусть это не так и $(D_n)_{c_1,d_1} \cong (D_n)_{c_2,d_2}$, $(c_1, d_1) \neq (c_2, d_2)$, а φ — соответствующий изоморфизм. Пусть для определённости $c_1 \neq c_2$ (случай $d_1 \neq d_2$ рассматривается аналогично). Так как $(D_n)_{c_1,d_1}$, $(D_n)_{c_2,d_2}$ — лупы с ассоциативными степенями, то порядки элементов при изоморфизме сохраняются. Можно считать, что $n > 2$ (иначе группа D_n коммутативная и доказывать нечего). При $n > 2$ имеем

$$\varphi(a) = a^m,\ \varphi(a^k) = a^{mk},\ \varphi(b) = ba^l \quad (m, n) = 1.$$

Далее,

$$\varphi(ba^k) = \varphi(b *_{c_1,d_1} a^{k(1-2c_1)^{-1}}) = \varphi(b) *_{c_2,d_2} \varphi(a^{k(1-2c_1)^{-1}}) = ba^{l+m(1-2c_1)^{-1}(1-2c_2)k},$$

где $*_{c_1,d_1}$ ($*_{c_2,d_2}$) — умножение в группоиде $(D_n)_{c_1,d_1}$ ($(D_n)_{c_2,d_2}$), откуда

$$\varphi(ba^{k_1} *_{c_1,d_1} ba_2^k) = a^{m(1-2c_1)^{-1}(1-2c_2)(k_1-k_2)}.$$

С другой стороны,

$$ba^{k_1} *_{c_1,d_1} ba^{k_2} = a^{k_1-k_2},$$

поэтому

$$\forall k_1, k_2 \in \mathbb{Z}_n, m \in \mathbb{Z}_n^*\ \ a^{m(1-2c1)^{-1}(1-2c_2)(k_1-k_2)} = a^{m(k_1-k_2)},$$

значит, $1 - 2c_1 \equiv 1 - 2c_2 \pmod n$. Если n нечётное, то $c_1 \equiv c_2 \pmod n$, откуда $c_1 = c_2$, так как оба нечётные и не превосходят $2n - 1$. Если n чётное, но $4 \nmid n$, то

$c_1 = c_2 \pmod{n/2}$. Так как $n/2$ нечётное, а $\exp(D_n/Z(D_n)) - 1 = n - 1$, то $c_1 = c_2$. Наконец, если $4 \mid n$, то $c_1 \equiv c_2 \pmod{n/2}$, и так как $c_1, c_2 \leqslant n/2 - 1$, то $c_1 = c_2$. ■

Линейно оптимальные $(D_n)_{c,d}$-коды

Следующая лемма показывает, при каких значениях c и d группоид $(D_n)_{c,d}$ удовлетворяет условиям теорем 6 и 7.

Лемма 6. Пусть группоид $(D_n)_{c,d}$ является неассоциативной лупой и n — простое число. Тогда эта лупа удовлетворяет условиям 1, 2, 3 из теоремы 6.

Пусть группоид $(D_n)_{c,d} = (D_{p^l-1})_{c,d}$ является неассоциативной лупой и $n = p^l - 1$. Эта лупа удовлетворяет условиям 1, 2, 3 из теоремы 7, если и только если выполнено одно из следующих условий:

— c нечётное, d нечётное, $2c \equiv 2 \pmod{n}$;
— c чётное, d нечётное $2c \equiv 0 \pmod{n}$;
— c нечётное, d чётное.

Доказательство. Из утверждения 5 известно, что если c и d оба чётные, то группоид $(D_n)_{c,d}$ является полугруппой, поэтому такие c и d не подходят по условию.

Пользуясь формулами из табл. 1, рассмотрим оставшиеся три случая, в каждом из которых проверим выполнение условий 1, 2, 3.

1) c — нечётное, d — нечётное. По утверждению 4 имеем $2c - 1, 2d - 1 \in \mathbb{Z}_n^*$. Тогда
   а) $ba^k * a^l = ba^{k+l(1-2c)} = b * (a^{k(1-2c)^{-1}} * a^l)$;
   б) $ba^k * (b * a^l) = ba^k * ba^{l(1-2c)} = a^{k-l(1-2c)} = a^k * a^{l(2c-1)}$;
   в) $a^k * (b * a^l) = a^k * (ba^{l(1-2c)}) = ba^{k(2d-1)+l(1-2c)} = b * a^{k(2d-1)(1-2c)+l} = b * (a^{k(2d-1)(1-2c)} * a^l)$.
   Видно, что условия теоремы 7 выполнены тогда и только тогда, когда $2c - 1 \equiv 1 \pmod{n}$, а условия теоремы 6 выполнены всегда ($\dot{k} = 1$, $\ddot{k} = 2c - 1$).
2) c — чётное, d — нечётное. Согласно утверждению 4, $2c - 1 \in \mathbb{Z}_n^*$. Тогда
   а) $ba^k * a^l = ba^{k+l(1-2c)} = b * (a^{k(1-2c)^{-1}} * a^l)$;
   б) $ba^k * (b * a^l) = ba^k * ba^{l(1-2c)} = a^{l(1-2c)-k} = a^{-k} * a^{l(1-2c)}$;
   в) $a^k * (b * a^l) = a^k * (ba^{l(1-2c)}) = ba^{l(1-2c)-k} = b * a^{l-k(1-2c)^{-1}} = b * (a^{k(2c-1)} * a^l)$.
   Условия теоремы 7 выполнены тогда и только тогда, когда $1 - 2c \equiv 1 \pmod{n}$, а условия теоремы 6 выполнены всегда ($\dot{k} = 1$, $\ddot{k} = 1 - 2c$).
3) c — нечётное, d — чётное:
   а) $ba^k * a^l = ba^{k+l} = b * (a^k * a^l)$;
   б) $ba^k * (b * a^l) = ba^k * ba^l = a^{l-k} = a^{-k} * a^l$;
   в) $a^k * (b * a^l) = a^k * (ba^l) = ba^{k(2d-1)+l} = b * a^{k(2d-1)+l} = b * (a^{k(2d-1)} * a^l)$.

Лемма доказана. ■

Пусть p простое, $p > 2$, $P = \mathbb{F}_p$.

Теорема 8. Пусть $(D_p)_{c,d}$ является неассоциативной лупой и выполнено одно из следующих условий:

— c нечётное, d нечётное, существует $x \in \mathbb{Z}$, такой, что $x^2 \equiv 2c - 1 \pmod{p}$;
— c чётное, d нечётное, существует $x \in \mathbb{Z}$, такой, что $x^2 \equiv 1 - 2c \pmod{p}$;
— c нечётное, d чётное.

Тогда луповая алгебра $P(D_p)_{c,d}$ содержит по крайней мере два идеала, отвечающих линейно оптимальным $[2p, 2p - 3, 3]_p$-кодам.

Доказательство. Следует из леммы 6 и теоремы 6. ■

Пусть $q = p^l > 2$, $P = \mathbb{F}_q$.

Теорема 9. Пусть $(D_{q-1})_{c,d}$ является неассоциативной лупой и выполнено одно из следующих условий:

— c нечётное, d нечётное, $2c \equiv 2 \pmod{n}$;
— c чётное, d нечётное, $2c \equiv 0 \pmod{n}$;
— c нечётное, d чётное.

Тогда если $p > 2$ (соответственно, $p = 2$), то луповая алгебра $P(D_{q-1})_{c,d}$ содержит по крайней мере $2\varphi(q-1)$ (соответственно, $\varphi(q-1)$) идеалов, отвечающих линейно оптимальным $[2q-2, 2q-5, 3]_q$-кодам.

Доказательство. Следует из леммы 6 и теоремы 7. ■

В качестве иллюстрации к теореме 8 рассмотрим $\mathbb{F}_5(D_5)_{c,d},\ c,d \in \{1,\dots,9\}$. Табл. 3 показывает, при каких парах c и d группоиды $(D_n)_{c,d}$ являются лупами и когда эти лупы изоморфны.

Таблица 3

$c \diagdown d$	1	2	3	4	5	6	7	8	9
1	0	1	–	2	3	3	2	–	1
2	4	0	4	0	4	0	4	0	4
3	–	1	–	2	–	3	–	–	–
4	5	0	5	0	5	0	5	0	5
5	6	1	–	2	7	3	8	–	9
6	6	0	6	0	6	0	6	0	6
7	5	1	–	2	10	3	11	–	12
8	–	0	–	0	–	0	–	0	–
9	4	1	–	2	13	3	14	–	15

Примечание. «–» — не лупа; 0 — D_5;
1–15 — неассоциативные лупы.

Учитывая, что $x^2 = \pm 1$ при $x \in \mathbb{F}_5^*$, получаем, что условию теоремы 8 удовлетворяют только $\mathbb{F}_5(D_5)_{1,2},\ \mathbb{F}_5(D_5)_{1,4},\ \mathbb{F}_5(D_5)_{1,5},\ \mathbb{F}_5(D_5)_{5,1},\ \mathbb{F}_5(D_5)_{5,5},\ \mathbb{F}_5(D_5)_{5,7},\ \mathbb{F}_5(D_5)_{5,9}$.

Компьютерные вычисления показали, что среди $\mathbb{F}_5(D_5)_{c,d}$ *только* эти алгебры содержат линейно оптимальные коды. Более того, их решётка идеалов в точности совпадает с решёткой, представленной на рис. 1 (слева).

Отметим, что здесь не приведены примеры луп, порождающих $[2q, q-3, 3]_q$-коды, когда поле $\mathbb{F}_q$ не простое. Если $p = \operatorname{char}\mathbb{F}_q > 2$, то такие примеры легко построить с помощью $G_{c,d}$, где $G = \langle b\rangle_2 \leftthreetimes H$, а $H = \mathbb{Z}_p^l$ — p-элементарная группа, $bhb = h^{-1}$ для всех $h \in H$. Из того, что для всех $g_1, g_2 \in G$ либо $[g_1, g_2] = e$, либо $\langle g_1, g_2\rangle \cong D_p$, следует, что свойства таких группоидов полностью аналогичны $(D_p)_{c,d}$. В частности, для $\mathbb{F}_q G_{c,d}$ верен аналог теоремы 8.

В заключение заметим, что существуют лупы с неассоциативными степенями (а значит, не являющиеся коммутаторными квазигруппами), удовлетворяющие условиям теорем 6 или 7. Такие лупы можно построить с помощью следующей конструкции (рассматриваем теорему 6, для теоремы 7 всё аналогично). Пусть

$$H = \{e, h_1, \dots, h_{q-1}\} = Z_p^l, \quad q = p^l,$$

а $L = \{e, h_1, \dots, h_{q-1}, b, \dots, bh_{q-1}\}$ — расширение H, умножение $*$ в котором определено следующим образом:

$$h_i * h_j = h_i h_j, \quad b * h_i = bh_j, \quad be = e, \quad bh_i * hj = b * (h_i h_j),$$
$$bh_i * bh_j = \sigma(h_i)h_j, \quad h_i * bh_j = b * (\tau(h_i)h_j),$$

где σ, τ — произвольные перестановки на множестве H. При таком определении группоид $(L, *)$ является квазигруппой, а если ещё добавить условие $\tau(e) = e$, то он будет лупой, которая очевидно удовлетворяет теореме 6. Рассмотрим $(b * b) * b$ и $b * (b * b)$:

$$(b * b) * b = \sigma(e) * b = b * (\tau(\sigma(e))), \quad b * (b * b) = b * \sigma(e).$$

Если $\sigma(e) \neq e$ и $\tau(\sigma(e)) \neq \sigma(e)$, то $(b * b) * b \neq b * (b * b)$ и лупа L является лупой с неассоциативными степенями. Кроме того, поскольку $\dot{k} = \ddot{k} = 1$, в $\mathbb{F}_q L$ содержится идеал, отвечающий линейно оптимальному $[2q, 2q-3, 3]_q$-коду.

Интересно, что при $q = 3$ существуют четыре неассоциативные неизоморфные лупы, удовлетворяющие теореме 6, они же удовлетворяют и теореме 7, а следовательно, доставляют линейно оптимальные $[6, 3, 3]_3$- и $[6, 3, 3]_4$-коды. Согласно [15], этими четырьмя лупами исчерпываются все неассоциативные лупы порядка 6, доставляющие линейно оптимальные коды. Лишь одна из этих луп является коммутаторной квазигруппой, а именно $(D_3)_{1,3}$.

Авторы выражают благодарность М. М. Глухову за конструктивные предложения, а также А. М. Зубкову и А. А. Нечаеву за критические замечания, способствующие улучшению изложения.

ЛИТЕРАТУРА

1. *Росошек С. К.* Криптосистемы групповых колец // Вестник Томского госуниверситета. Приложение. 2003. № 6. С. 57–62.
2. *Белоусов В. Д.* Основы теории квазигрупп и луп. М.: Наука, 1967. 223 с.
3. *Pflugfelder H. O.* Quasigroups and Loops: Introduction. Berlin: Heldermann, 1990.
4. *Smith J. D. H.* An Introduction to Quasigroups and their Representations. Boca Raton: Chapman&Hall/CRC, 2007.
5. *Vojtechovsky P.* Generators for finite simple Moufang loops // J. Group Theory. 2003. No. 6. P. 169–174.
6. *Paige L. J.* A class of simple Moufang loops // Proc. Amer. Math. Soc. 1956. V. 7. No. 3. P. 471–482.
7. *Vojtechovsky P.* Finite simple Moufang loops // PhD thesis. Department of Mathematics, Iowa State University, Ames, 2001.
8. *Conrad P.* Generalized semigroup rings // J. Indian Math. Soc. 1957. V. 21. P. 73–95.
9. *Грибов А. В., Золотых П. А., Михалёв А. В.* Построение алгебраической криптосистемы над квазигрупповым кольцом // Математические вопросы криптографии. 2010. Т. 1. № 4. С. 23–33.
10. *Kuzucuoglu F. and Levchuk V. M.* The automorphism group of certain radical matrix rings // J. Algebra. 2001. V. 243. No. 2. P. 473–485.
11. *Magliveras S. S., Stinson D. R., and Tran van Trung.* New approaches to designing public key cryptosystem using one-way functions and trap-doors in finite groups // J. Cryptology. 2008. V. 15. No. 4. P. 285–297.
12. *МакВиллъямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
13. *Heise W. and Quattrocci P.* Informations und Codierungstheorie. Berlin; Heidelberg: Springer, 1995.
14. *Гонсалес С., Коусело Е., Марков В. Т., Нечаев А. А.* Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы // Дискретная математика. 1998. Т. 10. № 2. С. 3–29.
15. *Гонсалес С., Коусело Е., Марков В. Т., Нечаев А. А.* Групповые коды и их неассоциативные обобщения // Дискретная математика. 2004. Т. 14. № 1. С. 146–156.

16. *Brouwer A. E.* Bounds on linear codes // Handbook of Coding Theory. Amsterdam: Elsevier, 1998. P. 295–461.
17. *Grassl M.* Searching for linear codes with large minimum distance // Discovering Mathematics with Magma. Berlin; Heidelberg: Springer, 2006. V. 19. P. 287–313.
18. *Couselo E., Gonzalez S., Markov V., et al.* Some constructions of linearly optimal group codes // Linear Algebra and its Applications. 2010. No. 433. P. 356–364.
19. *Charpin P.* Les codes e Reed-Solomon en tant qu'idr̀eaux d'une alg‘ebre modulaire (French. English summary) // C. R. Acad. Sci. Paris. 1982. V. 294. No. 17. P. 597–600.
20. *Landrock P. and Manz O.* Classical codes as ideals in group algebras // Designs, Codes and Cryptography. 1992. No. 2. P. 273–285.

2012 Математические методы криптографии №4(18)
DOI 10.17223/20710410/18/4
УДК 519.7

О ВЕРОЯТНОСТИ ПРОТЯЖКИ ОДНОБИТОВОЙ РАЗНОСТИ ЧЕРЕЗ СЛОЖЕНИЕ И ВЫЧИТАНИЕ ПО МОДУЛЮ

А. И. Пестунов

Институт вычислительных технологий СО РАН, г. Новосибирск, Россия

E-mail: pestunov@gmail.com

Доказано, что вероятность протяжки однобитовой разности через сложение и вычитание по модулю равна 1, если этот бит является старшим, и 1/2, если этот бит отличен от старшего. Проведённые эксперименты подтверждают эти результаты.

Ключевые слова: *блочный шифр, дифференциальный криптоанализ, разностный анализ.*

Введение

Разностный (дифференциальный) анализ [1] вместе со всевозможными своими разновидностями (см., например, [2 – 5]) является одним из наиболее распространённых методов исследования стойкости блочных шифров. К настоящему моменту в рамках этого подхода разработано довольно много атак, однако крайне редко построение характеристик и дифференциалов, лежащих в основе данных атак, а также вычисление их вероятностей обосновывается строго математически.

Отметим некоторые работы, посвящённые теоретической обоснованности разностного анализа. В [6] предложена модель так называемого марковского шифра, в рамках которой вычисляются вероятности характеристик и дифференциалов. В [7] сформулирована гипотеза стохастической эквивалентности, используемой, например, при оценке вероятности успеха разностных атак. В [8] разработана модель, в рамках которой можно создать шифр, доказуемо стойкий к разностному и линейному анализу. Работа [9] посвящена изложению разностного анализа в общем виде применительно к произвольным итеративным блочным шифрам с аддитивным раундовым ключом.

Другой важной проблемой является изучение возможности так называемой *протяжки* (propagation) разности через различные операции, используемые в блочном шифре, т. е. в оценивании вероятности того, что пара блоков (подблоков) с определённой разностью преобразуется в пару блоков с такой же или другой, но также определённой разностью. В частности, в работе по разностному анализу шифра RC5 [10] утверждается, что однобитовая разность остаётся неизменной после операции сложения с вероятностью 1/2 или с вероятностью 1, если этот единственный бит — старший. Данное утверждение никак не обосновывается, за исключением того, что проводятся некоторые эксперименты, подтверждающие достоверность разработанной атаки. В работах по разностному анализу шифров MARS [11] и CAST-256 [12] также используется этот факт со ссылкой на [10].

В настоящей работе данные факты доказываются математически строго и осуществляется экспериментальная проверка полученных теоретических результатов. Под протяжкой разности двоичных векторов $X \oplus Y$ через операцию $\circ$ понимается разность $D = (X \circ Z) \oplus (Y \circ Z)$ со случайным двоичным вектором Z. Вероятность того, что $D = X \oplus Y$, называется вероятностью этой протяжки.

1. Предварительные замечания

Проиллюстрируем обозначенную проблему на примере операций XOR и циклического сдвига, которые обозначим соответственно через $\oplus$ и $<<<$. Пусть даны два блока (подблока) X и Y с определённой разностью Δ, другими словами, $X \oplus Y = \Delta$.

Поскольку $\oplus$ — коммутативная операция, то

$$(X \oplus Z) \oplus (Y \oplus Z) = X \oplus Y.$$

Это означает, что операция XOR не изменяет разность, и вероятность протяжки разности через неё равна 1. Для наглядности изобразим этот факт следующим образом:

$$\Delta \xrightarrow[p=1]{\oplus Z} \Delta.$$

Подобным свойством обладает и операция циклического сдвига: она подчиняется закону дистрибутивности, поэтому

$$(X^{<<<Z}) \oplus (Y^{<<<Z}) = (X \oplus Y)^{<<<Z}.$$

Следовательно,

$$\Delta \xrightarrow[p=1]{<<<Z} \Delta^{<<<Z}.$$

Что касается арифметических операций, то в общем случае при произвольно взятой разности Δ не существует такой разности Δ^*, чтобы выполнялось

$$\Delta \xrightarrow[p=1]{\boxplus Z} \Delta^*,\ \Delta \xrightarrow[p=1]{\boxminus Z} \Delta^* \text{ или } \Delta \xrightarrow[p=1]{\circledast Z} \Delta^*.$$

Тем не менее в ряде случаев можно осуществить протяжку разности с достаточно большой вероятностью, в частности, в данной работе рассматривается случай однобитовой разности.

Обозначения, используемые в работе: s — длина двоичного вектора (в битах); $\{0,1\}^s$ — множество всех двоичных векторов длины s; $X \sim \mathcal{U}\{0,1\}^s$ — случайная величина X имеет равномерное распределение на $\{0,1\}^s$; $\boxplus$, $\boxminus$, $\circledast$ — соответственно сложение, вычитание и умножение по модулю 2^s; $X^{[i]}$ — i-й бит двоичного вектора X (0 — младший, $(s-1)$ — старший); $X^{[s_1,\ldots,s_2]}$ — двоичный вектор длины $(s_1 - s_2 + 1)$, $s_1 \geqslant s_2$, составленный из битов вектора X с номерами $s_1, \ldots, s_2$.

2. Теоретические результаты

Теорема 1. Пусть X, Y, $Z \in \{0,1\}^s$ и $X \oplus Y = 2^m$, где $0 \leqslant m \leqslant s-1$. Тогда

а) $(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m$, если $m = s-1$;

б) $\mathrm{P}\big((X \boxplus Z) \oplus (Y \boxplus Z) = 2^m\big) = 1/2$, если $m < s-1$ и $X, Y, Z \sim \mathcal{U}\{0,1\}^s$.

Доказательство. В пп. 1–2 производится представление используемых величин в удобном виде; п. 3 посвящён доказательству утверждения *а*; в пп. 4–7 доказывается утверждение *б*.

1. Условие $X \oplus Y = 2^m$ означает, что либо $Y^{[m]} = 0$ и $X = Y + 2^m$, либо $X^{[m]} = 0$ и $Y = X + 2^m$. Не ограничивая общности, положим, что $X^{[m]} = 0$ и $Y = X + 2^m$.

Представим X, Y и Z следующим образом:

$$X = x_1 \cdot 2^{m+1} + x_2,\ Y = x_1 \cdot 2^{m+1} + 2^m + x_2 \text{ и } Z = z_1 \cdot 2^{m+1} + \delta \cdot 2^m + z_2,$$

где $x_1 = X^{[s-1,\ldots,m+1]}$, $x_2 = X^{[m-1,\ldots,0]}$, $z_1 = Z^{[s-1,\ldots,m+1]}$, $z_2 = Z^{[m-1,\ldots,0]}$, $\delta = Z^{[m]}$.

Рассмотрим величины X и Y как s-битовые векторы и изобразим их схематично:

$$X = (\overbrace{?,\ldots,?}^{x_1}, 0, \overbrace{?,\ldots,?}^{x_2}); \quad Y = (\overbrace{?,\ldots,?}^{x_1}, 1, \overbrace{?,\ldots,?}^{x_2});$$

$$x_1 \cdot 2^{m+1} = (\overbrace{?,\ldots,?}^{x_1}, 0, \overbrace{0,\ldots,0}^{m\,\text{бит}}); \; 2^m = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, 1, \overbrace{0,\ldots,0}^{m\,\text{бит}}); \; x_2 = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, 0, \overbrace{?,\ldots,?}^{x_2}).$$

Аналогичная схематичная запись для Z примет следующий вид:

$$Z = (\overbrace{?,\ldots,?}^{z_1}, \delta, \overbrace{?,\ldots,?}^{z_2}); \quad z_1 \cdot 2^{m+1} = (\overbrace{?,\ldots,?}^{z_1}, 0, \overbrace{0,\ldots,0}^{m\,\text{бит}});$$

$$\delta \cdot 2^m = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, \delta, \overbrace{0,\ldots,0}^{m\,\text{бит}}); \quad z_2 = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, 0, \overbrace{?,\ldots,?}^{z_2}).$$

2. Представим выражения $X \boxplus Z$ и $Y \boxplus Z$, используя введённые в п. 1 обозначения:

$$X \boxplus Z = (x_1 + z_1) \cdot 2^{m+1} + \delta \cdot 2^m + (z_2 + x_2) \pmod{2^s}; \tag{1}$$

$$Y \boxplus Z = (x_1 + z_1) \cdot 2^{m+1} + (\delta + 1) \cdot 2^m + (z_2 + x_2) \pmod{2^s}. \tag{2}$$

Из определений для x_2 и z_2 следует, что $x_2 \leqslant 2^m - 1$ и $z_2 \leqslant 2^m - 1$, поэтому $x_2 + z_2 < 2^{m+1}$, значит, эту сумму можно записать следующим образом:

$$x_2 + z_2 = \gamma \cdot 2^m + v, \text{ где } \gamma = (x_2 + z_2)^{[m]} \text{ и } v = (x_2 + z_2) - \gamma \cdot 2^m. \tag{3}$$

Смысл этого представления заключается в том, что величина $(x_2 + z_2)$ задаётся в виде суммы старшего m-го бита и всех остальных.

Аналогичным образом можно выразить сумму $(x_1 + z_1)$:

$$x_1 + z_1 = \hat{\gamma} \cdot 2^{s-1-m} + u, \text{ где } \hat{\gamma} = (x_1 + z_1)^{[s-1-m]} \text{ и } u = (x_1 + z_1) - \hat{\gamma} \cdot 2^{s-1-m}.$$

Отсюда вытекает, что первое слагаемое в формулах (1) и (2) можно записать так:

$$(x_1 + z_1) \cdot 2^{m+1} = \hat{\gamma} \cdot 2^{s-1-m} \cdot 2^{m+1} + u \cdot 2^{m+1} = \hat{\gamma} \cdot 2^s + u \cdot 2^{m+1}. \tag{4}$$

Подставим выражения (3) и (4) в формулы (1) и (2); с учётом того, что $\hat{\gamma} \cdot 2^s = 0 \pmod{2^s}$, получим

$$X \boxplus Z = u \cdot 2^{m+1} + (\gamma + \delta) \cdot 2^m + v \pmod{2^s}; \tag{5}$$

$$Y \boxplus Z = u \cdot 2^{m+1} + (\gamma + \delta + 1) \cdot 2^m + v \pmod{2^s}. \tag{6}$$

Слагаемые, присутствующие в этих суммах, изобразим схематично:

$$u \cdot 2^{m+1} = (\overbrace{?,\ldots,?}^{u}, 0, \overbrace{0,\ldots,0}^{m\,\text{бит}}); \quad \gamma \cdot 2^m = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, \gamma, \overbrace{0,\ldots,0}^{m\,\text{бит}});$$

$$\delta \cdot 2^m = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, \delta, \overbrace{0,\ldots,0}^{m\,\text{бит}}); \quad v = (\overbrace{0,\ldots,0}^{s-1-m\,\text{бит}}, 0, \overbrace{?,\ldots,?}^{v}).$$

3. Докажем утверждение *а* теоремы. Заметим, что $x_1 = z_1 = 0$ при $m = s$, поэтому $u = 0$ и выражения (5) и (6) примут вид

$$X \boxplus Z = (\gamma + \delta) \cdot 2^{s-1} + v \pmod{2^s}; \tag{7}$$

$$Y \boxplus Z = (\gamma + \delta + 1) \cdot 2^{s-1} + v \pmod{2^s}. \tag{8}$$

Согласно введённым обозначениям, $v < 2^{s-1}$, поэтому $v^{[s-1]} = 0$. В то же время $(s-2)$ младших бит у выражений $(\gamma+\delta)\cdot 2^{s-1}$ и $(\gamma+\delta+1)\cdot 2^{s-1}$ равны нулю. Из формул (7) и (8) следует, что

$$\big((X \boxplus Z) \oplus (Y \boxplus Z)\big)^{[i]} = 0,\ i = 0, 1, \ldots, s-2.$$

Таким образом, осталось доказать, что $\big((X \boxplus Z) \oplus (Y \boxplus Z)\big)^{[s-1]} = 1$.

Рассмотрим два случая: $(\gamma + \delta) \bmod 2 = 0$ и $(\gamma + \delta) \bmod 2 = 1$.

В первом случае $(\gamma + \delta) \cdot 2^{s-1} = 0 \pmod{2^s}$, а $(\gamma + \delta + 1) \cdot 2^{s-1} = 1 \pmod{2^s}$. Значит,

$$(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m.$$

Во втором случае $(\gamma + \delta) \cdot 2^{s-1} = 1 \pmod{2^s}$, а $(\gamma + \delta + 1) \cdot 2^{s-1} = 0 \pmod{2^s}$. Следовательно, в этом случае также

$$(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m,$$

и утверждение *а* доказано.

4. Перейдём к доказательству утверждения *б*. Обозначим через $\mathcal{A}$ рассматриваемое событие $(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m$ и, используя формулу полной вероятности [13, с. 39], запишем

$$\mathrm{P}(\mathcal{A}) = \mathrm{P}(\mathcal{A}|\delta = 0)\mathrm{P}(\delta = 0) + \mathrm{P}(\mathcal{A}|\delta = 1)\mathrm{P}(\delta = 1).$$

По условию теоремы $Z \sim \mathcal{U}\{0,1\}^s$, поэтому $\mathrm{P}(\delta = 0) = \mathrm{P}(\delta = 1) = 1/2$. Следовательно,

$$\mathrm{P}(\mathcal{A}) = \big(\mathrm{P}(\mathcal{A}|\delta = 0) + \mathrm{P}(\mathcal{A}|\delta = 1)\big)/2. \tag{9}$$

5. Вычислим $\mathrm{P}(\mathcal{A}|\delta = 0)$. Рассмотрим случаи $\gamma = 0$ и $\gamma = 1$.

При $\delta = 0$ и $\gamma = 0$ выражения (5) и (6) примут вид

$$X \boxplus Z = (u \cdot 2^{m+1} + v) \bmod 2^s = u \cdot 2^{m+1} + v;$$
$$Y \boxplus Z = (u \cdot 2^{m+1} + 2^m + v) \bmod 2^s = u \cdot 2^{m+1} + 2^m + v.$$

Покажем схематично:

$$X \boxplus Z = (\overbrace{?, \ldots, ?}^{u}, 0, \overbrace{?, \ldots, ?}^{v}); \quad Y \boxplus Z = (\overbrace{?, \ldots, ?}^{u}, 1, \overbrace{?, \ldots, ?}^{v}).$$

Отсюда следует, что $(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m$.

Таким образом, если $\gamma = 0$, то $(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m$ с вероятностью 1.

Рассмотрим случай $\gamma = 1$. Выражения (5) и (6) примут вид

$$X \boxplus Z = u \cdot 2^{m+1} + 2^m + v \pmod{2^s};$$
$$Y \boxplus Z = u \cdot 2^{m+1} + 2^m + 2^m + v = (u+1) \cdot 2^{m+1} + v \pmod{2^s}.$$

Или схематично:

$$X \boxplus Z = (\overbrace{?, \ldots, ?}^{u}, 1, \overbrace{?, \ldots, ?}^{v}); \quad Y \boxplus Z = (\overbrace{?, \ldots, ?}^{(u+1) \bmod 2^{s-1-m}}, 0, \overbrace{?, \ldots, ?}^{v}).$$

Для наступления события $\mathcal{A}$ необходимо выполнение условия $u + 1 = u \pmod{2^{s-1-m}}$, однако такого u не существует, следовательно, при $\gamma = 1$ выполнено $\mathrm{P}(\mathcal{A}|\delta = 0) = 0$. Таким образом, $\mathrm{P}(\mathcal{A}|\delta = 0) = \mathrm{P}(\gamma = 0)$.

6. Аналогично рассуждениям из п. 5 вычислим $\mathrm{P}(\mathcal{A}|\delta = 1)$. Рассмотрим случай $\gamma = 1$, тогда выражения (5) и (6) примут вид

$$X \boxplus Z = (u+1)\cdot 2^{m+1} + v \pmod{2^s}; \quad Y \boxplus Z = (u+1)\cdot 2^{m+1} + 2^m + v \pmod{2^s},$$

или схематично:

$$X \boxplus Z = (\overbrace{?,\ldots,?}^{(u+1) \bmod 2^{s-1-m}}, 0, \overbrace{?,\ldots,?}^{v}); \quad Y \boxplus Z = (\overbrace{?,\ldots,?}^{(u+1) \bmod 2^{s-1-m}}, 1, \overbrace{?,\ldots,?}^{v}).$$

Таким образом, если $\gamma = 1$, то $(X \boxplus Z) \oplus (Y \boxplus Z) = 2^m$ с вероятностью 1.

Если $\gamma = 0$, то выражения (5) и (6) примут вид

$$X \boxplus Z = u\cdot 2^{m+1} + 2^m + v \pmod{2^s}; \quad Y \boxplus Z = (u+1)\cdot 2^{m+1} + v \pmod{2^s},$$

или схематично:

$$X \boxplus Z = (\overbrace{?,\ldots,?}^{u}, 1, \overbrace{?,\ldots,?}^{v}); \quad Y \boxplus Z = (\overbrace{?,\ldots,?}^{(u+1) \bmod 2^{s-1-m}}, 0, \overbrace{?,\ldots,?}^{v}).$$

Для наступления события $\mathcal{A}$ необходимо выполнение условия $u + 1 = u \pmod{2^{s-1-m}}$, однако такого u не существует, следовательно, при $\gamma = 0$ получим $\mathrm{P}(\mathcal{A}|\delta = 1) = 0$.

Таким образом, $\mathrm{P}(\mathcal{A}|\delta = 1) = \mathrm{P}(\gamma = 1)$.

7. Подставляя вероятности, вычисленные в пп. 4–5, в формулу (9), получим

$$\mathrm{P}(\mathcal{A}) = \big(\mathrm{P}(\gamma = 0) + \mathrm{P}(\gamma = 1)\big)/2 = 1/2.$$

Следовательно, утверждение *б* теоремы доказано. ■

Следствие 1. Пусть $X, Y, Z \in \{0,1\}^s$ и $X \oplus Y = 2^m$, где $0 \leqslant m \leqslant s-1$. Тогда

а) $(X \boxminus Z) \oplus (Y \boxminus Z) = 2^m$, если $m = s-1$;

б) $\mathrm{P}\big((X \boxminus Z) \oplus (Y \boxminus Z) = 2^m\big) = 1/2$, если $m < s-1$ и $X, Y, Z \sim \mathcal{U}\{0,1\}^s$.

Доказательство. Если Z, Z' — случайные величины и $Z \sim \mathcal{U}\{0,1\}^s$, $Z' = -Z \pmod{2^s}$, то $Z' \sim \mathcal{U}\{0,1\}^s$, поскольку для каждого $x \in \{0,1\}^s$ существует единственный $y \in \{0,1\}^s$, такой, что $-x = y \pmod{2^s}$. Следовательно, для Z' выполнены условия теоремы 1, и следствие доказано. ■

3. Экспериментальное подтверждение теоретических результатов

Проверку утверждений *б* теоремы и следствия проведём двумя способами. Во-первых, предположим, что вероятность протяжки разности неизвестна, и вычислим для неё несмещённую состоятельную оценку. Во-вторых, при помощи критерия хи-квадрат [14] проверим гипотезу о том, что вероятность протяжки разности равна $1/2$. Эксперименты проведены при $s = 32$ и $m = 0, \ldots, 31$.

Для каждого m сгенерируем две выборки $\mathcal{X} = (X_1, \ldots, X_n)$ и $\mathcal{Z} = (Z_1, \ldots, Z_n)$, где $X_i, Z_i \sim \mathcal{U}\{0,1\}^{32}$ и $n = 10000$. Затем сформируем выборку $\mathcal{Y}^m = (Y_1^m, \ldots, Y_n^m)$, где $Y_i^m = X_i \oplus 2^m$.

Введём следующие величины ($i = 1, \ldots, n$):

$$\xi_i^m = \begin{cases} 1, & \text{если } (X_i \boxplus Z_i) \oplus (Y_i^m \boxplus Z_i) = 2^m, \\ 0, & \text{если } (X_i \boxplus Z_i) \oplus (Y_i^m \boxplus Z_i) \neq 2^m; \end{cases}$$

$$\eta_i^m = \begin{cases} 1, & \text{если } (X_i \boxminus Z_i) \oplus (Y_i^m \boxminus Z_i) = 2^m, \\ 0, & \text{если } (X_i \boxminus Z_i) \oplus (Y_i^m \boxminus Z_i) \neq 2^m. \end{cases}$$

Проверку утверждений теоремы и следствия проведём при помощи выборок $\Xi^m = (\xi_1^m, \ldots, \xi_n^m)$ и $\Theta^m = (\eta_1^m, \ldots, \eta_n^m)$ соответственно. При $m = 31$ проверим, что $\xi_i^m = \eta_i^m = 1$, $i = 1, \ldots, n$. При $m < 31$ проверим, что эти случайные величины имеют распределение Бернулли с параметром $1/2$, т. е.

$$\mathrm{P}(\xi_i^m = 0) = \mathrm{P}(\xi_i^m = 1) = \mathrm{P}(\eta_i^m = 0) = \mathrm{P}(\eta_i^m = 1) = 1/2.$$

Для этого вычислим величины $\nu_{\boxplus}^m = \sum\limits_{i=1}^{n} \xi_i^m$, $\nu_{\boxminus}^m = \sum\limits_{i=1}^{n} \eta_i^m$.

Кроме того, поскольку параметр распределения Бернулли является математическим ожиданием, а несмещённой состоятельной оценкой для него является выборочное среднее, то вычислим и его. Выборочные средние для выборок Ξ^m и Θ^m вычисляются по формулам $\nu_{\boxplus}^m/n$ и $\nu_{\boxminus}^m/n$ соответственно.

Очевидно, что если проверяемая гипотеза верна, то

$$\nu_{\boxplus}^m \approx \nu_{\boxminus}^m \approx n/2 = 5000.$$

Далее по каждому $\nu_{\boxplus}^m$ и $\nu_{\boxminus}^m$ вычисляем статистику хи-квадрат при $p = 1/2$ по следующей формуле [14]:

$$x_p^2(\nu) = \frac{(\nu - np)^2}{np} + \frac{((n - \nu) - n(1 - p))^2}{n(1 - p)}. \tag{10}$$

Результаты приведены в таблице, из которой видно, что выборочные средние $\nu_{\boxplus}^m/n$ и $\nu_{\boxminus}^m/n$ близки к $1/2$.

Для использования критерия хи-квадрат рассмотрим квантиль этого распределения уровня 0,05 с одной степенью свободы: $\chi_{1;0,05} = 3{,}84$. Как видно из таблицы, статистика $x_{0,5}^2$ превышает эту квантиль только в трёх случаях из 62 (эти значения выделены жирным шрифтом). Данные превышения могут быть отнесены к статистической погрешности, поскольку при используемой квантили ошибка первого рода составляет 5 %. Если взять $\chi_{1;0,01} = 6{,}64$, то превышений не будет.

Для генерации псевдослучайных чисел из выборок $\mathcal{X}$ и $\mathcal{Z}$ использован шифр MARS [15], состоящий из 10 раундов, поскольку в работе [16] показано, что уже такое сокращённое количество раундов обеспечивает удовлетворительные статистические свойства данного шифра. Программная реализация шифра MARS взята из библиотеки Б. Глэдмена [17], где на языке C++ реализованы шифры-кандидаты конкурса AES.

Для проверки утверждений a теоремы и следствия выбрано $n = 2^{32}$ и в качестве выборки $\mathcal{X}$ взяты не случайные числа, а все возможные значения. Выборка $\mathcal{Z}$ попрежнему формировалась из псевдослучайных чисел при помощи 10 раундов шифра MARS. Результаты экспериментов показали, что в 100 % случаев $\xi_i^m = \eta_i^m = 1$.

Экспериментальная проверка утверждений *б* теоремы и следствия

m (№ бита)	$\nu^m_{\boxplus}$	$\nu^m_{\boxplus}/n$	$x^2_{0,5}(\nu^m_{\boxplus})$	$\nu^m_{\boxminus}$	$\nu^m_{\boxminus}/n$	$x^2_{0,5}(\nu^m_{\boxminus})$
0	4990	0,499	0,04	4972	0,497	0,31
1	4957	0,496	0,74	4884	0,488	**5,38**
2	4958	0,496	0,71	4935	0,493	1,69
3	5077	0,508	2,37	4992	0,499	0,03
4	5100	0,510	**4,00**	4963	0,496	0,55
5	4951	0,495	0,96	4975	0,498	0,25
6	4991	0,499	0,03	5059	0,506	1,39
7	5023	0,502	0,21	4976	0,498	0,23
8	5024	0,502	0,23	4987	0,499	0,07
9	5010	0,501	0,04	4965	0,496	0,49
10	4923	0,492	2,37	4982	0,498	0,13
11	5062	0,506	1,54	5045	0,504	0,81
12	5095	0,510	3,61	5049	0,505	0,96
13	4920	0,492	2,56	4968	0,497	0,41
14	5076	0,508	2,31	5038	0,504	0,58
15	5046	0,505	0,85	5041	0,504	0,67
16	5058	0,506	1,35	4970	0,497	0,36
17	5049	0,505	0,96	5101	0,510	**4,08**
18	4960	0,496	0,64	5056	0,506	1,25
19	4945	0,495	1,21	5007	0,501	0,02
20	4975	0,498	0,25	5037	0,504	0,55
21	4989	0,499	0,05	4982	0,498	0,13
22	5017	0,502	0,12	5041	0,504	0,67
23	5033	0,503	0,44	4955	0,495	0,81
24	5073	0,507	2,13	4945	0,495	1,21
25	4914	0,491	2,96	5020	0,502	0,16
26	4961	0,496	0,61	4927	0,493	2,13
27	5083	0,508	2,76	5004	0,500	0,01
28	5009	0,501	0,03	4936	0,494	1,64
29	5041	0,504	0,67	5095	0,510	3,61
30	4970	0,497	0,36	5081	0,508	2,62

Заключение

В настоящей работе рассмотрена проблема теоретического вычисления вероятности протяжки разности через арифметические операции. Точнее, доказано, что вероятность протяжки однобитовой разности через сложение и вычитание по модулю равна $1/2$, если разность расположена не в старшем бите, и 1 — если в старшем.

Следующими шагами, продолжающими данную работу, могут стать исследования вероятности протяжки разности через умножение по модулю и вероятности протяжки разности в зависимости от её веса Хемминга.

ЛИТЕРАТУРА

1. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
2. *Wagner D.* The boomerang attack // LNCS. 1999. V. 1636. P. 156–170.
3. *Kelsey J., Kohno T, and Schneier B.* Amplified boomerang attacks against reduced-round MARS and Serpent // LNCS. 2001. V. 1978. P. 75–93.
4. *Biham E., Biryukov A, and Shamir A.* Cryptanalysis of Skipjack reduced to 31 round using impossible differentials // LNCS. 1999. V. 1592. P. 12–23.
5. *Пестунов А. И.* Блочные шифры и их криптоанализ // Вычислительные технологии. 2007. Т. 12, спец. вып. № 4. С. 42–49.

6. *Lai X. and Massey J.* Markov ciphers and differential cryptanalysis // LNCS. 1991. V. 547. P. 17–38.
7. *Nyberg K. and Knudsen L.* Provable security against a differential attack // J. Cryptology. 1995. No. 8. P. 27–37.
8. *Vaudenay S.* Decorrelation: a theory for block cipher security // J. Cryptology. 2003. No. 16. P. 249–286.
9. *Агибалов Г. П.* Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 1(1). С. 34–42.
10. *Biryukov A. and Kushilevitz E.* Improved cryptanalysis of RC5 // LNCS. 1998. V. 1403. P. 85–99.
11. *Пестунов А. И.* Дифференциальный криптоанализ блочного шифра MARS // Прикладная дискретная математика. 2009. № 4(6). С. 56–63.
12. *Пестунов А. И.* Дифференциальный криптоанализ блочного шифра CAST-256 // Безопасность информационных технологий. 2009. № 4. С. 57–62.
13. *Боровков А. А.* Теория вероятностей. М.: Наука, 1976. 352 с.
14. *Боровков А. А.* Математическая статистика. М.: Наука, 1984. 472 с.
15. *Burwick C. et al.* MARS — a candidate cipher for AES // NIST AES Proposal, 1999.
16. *Пестунов А. И.* Статистический анализ современных блочных шифров // Вычислительные технологии. 2007. Т. 12. № 2. С. 122–129.
17. `www.gladman.me.uk` — Brian Gladman's Home Page. 2012.

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

DOI 10.17223/20710410/18/5

УДК 519.8

ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ РЕШЕНИЙ ВЕКТОРНОЙ ИНВЕСТИЦИОННОЙ БУЛЕВОЙ ЗАДАЧИ В СЛУЧАЕ МЕТРИКИ ГЕЛЬДЕРА В КРИТЕРИАЛЬНОМ ПРОСТРАНСТВЕ[1]

В. А. Емеличев, В. В. Коротков

Белорусский государственный университет, г. Минск, Беларусь

E-mail: emelichev@bsu.by, wladko@tut.by

Проведён анализ устойчивости парето-оптимального портфеля многокритериального дискретного (булева) варианта инвестиционной задачи Марковица с максиминными критериями эффективности Вальда. Получены нижняя и верхняя достижимые оценки радиуса устойчивости такого портфеля в случае, когда в критериальном пространстве параметров задачи задана метрика Гельдера l_p, $1 \leqslant p \leqslant \infty$.

Ключевые слова: *векторная инвестиционная задача, парето-оптимальный инвестиционный портфель, критерий эффективности Вальда, радиус устойчивости портфеля, метрика Гельдера.*

Введение

Большинство управленческих решений принимается в условиях неопределённости и риска, что обусловлено рядом факторов: отсутствием полной информации, наличием противоборствующих тенденций, элементами случайности и т. п. Для управления финансовыми инвестициями Г. Марковицем [1, 2] (см. также [3]) разработана оптимизационная модель, демонстрирующая, как инвестор, выбирая портфель активов, может максимально повысить ожидаемый уровень доходности (экономическую эффективность). Хорошо известно, что сложность вычисления подобных величин сопровождается большим количеством ошибок, приводящих к высокой степени неопределённости начальной информации. Тем самым появляется необходимость учёта неточности и некорректности входных параметров, которые свойственны реальным ситуациям решения практических задач оптимизации. Возникающий при этом вопрос о предельном уровне изменений (возмущений) числовых параметров исходной задачи, сохраняющих оптимальность выбранного решения (портфеля), приводит к ключевому понятию радиуса устойчивости. Конкретное содержание данного понятия зависит от выбора принципа оптимальности (если задача многокритериальная), множества параметров задачи, подверженным возмущениям, а также от структуры, определяющей отношения «близости» в пространстве параметров, т. е. от метрики, заданной в этом пространстве. Нахождению формул или оценок радиуса устойчивости парето-оптимальных решений векторных (многокритериальных) задач дискретной оптимизации посвящен ряд работ (см., например, [4 – 7]).

[1]Работа поддержана грантом Белорусского республиканского фонда фундаментальных исследований № Ф11К-095.

Настоящая работа продолжает начатые в [8 – 12] исследования, посвященные анализу устойчивости решений векторных задач выбора инвестиционных проектов с нелинейными целевыми функциями. В этих работах для инвестиционной задачи с минимаксными критериями рисков Сэвиджа получены нижняя и верхняя достижимые оценки радиуса устойчивости парето-оптимального или лексикографически оптимального инвестиционного портфеля в случаях, когда в трёхмерном пространстве параметров задачи заданы метрики l_1 и l_∞ в разнообразных комбинациях. Данная работа посвящена оценкам радиуса устойчивости парето-оптимального портфеля векторного булева варианта инвестиционной задачи Марковица с максиминными критериями экономической эффективности Вальда в случае, когда в критериальном пространстве параметров задачи задана метрика Гельдера l_p, $1 \leqslant p \leqslant \infty$.

1. Основные определения

Рассмотрим векторный дискретный (булевый) вариант задачи управления инвестициями Марковица. Для этого введём ряд обозначений:

$N_n = \{1, 2, \ldots, n\}$ — альтернативные инвестиционные проекты (активы);

N_m — возможные состояния рынка (рыночные ситуации, сценарии развития);

N_s — виды (показатели) экономической эффективности инвестиционного проекта;

$x = (x_1, x_2, \ldots, x_n)^T$ — инвестиционный портфель, где

$$x_j = \begin{cases} 1, & \text{если проект } j \text{ реализуется,} \\ 0 & \text{в противном случае;} \end{cases}$$

$X \subseteq \mathbf{E}^n \setminus \{0_{(n)}\}$ — множество инвестиционных портфелей, где $\mathbf{E} = \{0, 1\}$; $|X| \geqslant 2$; $0_{(n)}$ — нулевой вектор пространства $\mathbb{R}^n$;

e_{ijk} — ожидаемая оценка экономической эффективности вида $k \in N_s$ инвестиционного проекта $j \in N_n$ в случае, когда рынок находится в состоянии $i \in N_m$;

$E = [e_{ijk}]$ — трёхмерная матрица размера $m \times n \times s$ с элементами из $\mathbb{R}$.

Отметим, что существует несколько подходов к оценке экономической эффективности инвестиционных проектов (NPV, NFV, PI и др.), по-разному учитывающих влияние неопределенности и риска (см., например, [13 – 16]). Поэтому полезной в практических применениях может быть рассмотренная в настоящей работе постановка инвестиционной задачи, которую охарактеризуем как задачу принятия решений при наличии многих критериев (видов эффективности проектов).

На множестве инвестиционных портфелей (булевых векторов) X зададим векторную целевую функцию

$$f(x, E) = (f_1(x, E_1), f_2(x, E_2), \ldots, f_s(x, E_s)),$$

компонентами которой являются максиминные критерии Вальда [17]

$$f_k(x, E_k) = \min_{i \in N_m} E_{ik}x = \min_{i \in N_m} \sum_{j \in N_n} e_{ijk}x_j \to \max_{x \in X}, \qquad k \in N_s,$$

где $E_k \in \mathbb{R}^{m \times n}$ — k-е сечение матрицы $E = [e_{ijk}] \in \mathbb{R}^{m \times n \times s}$; $E_{ik} = (e_{i1k}, e_{i2k}, \ldots, e_{ink})$ — i-я строка этого сечения. Таким образом, следуя критерию Вальда, инвестор, предвидя непредсказуемость состояния рынка, проявляет крайнюю осторожность, оптимизируя эффективность портфеля $E_{ik}x$ (по критерию k) в предположении, что рынок находится в самом невыгодном для него состоянии, а именно тогда, когда эффективность минимальна. Очевидно, что подобный пессимистический подход в оценке рыночной

ситуации целесообразно использовать только тогда, когда речь идёт о необходимости достижения гарантированного результата.

Под векторной (s-критериальной) инвестиционной булевой задачей $Z^s(E)$, $s \in \mathbb{N}$, с критериями Вальда будем понимать задачу поиска множества парето-оптимальных инвестиционных портфелей (множества Парето)

$$P^s(E) = \{x \in X : \nexists x' \in X \ \ (g(x', x, E) \geqslant 0_{(s)} \ \ \& \ \ g(x', x, E) \neq 0_{(s)})\},$$

где

$$g(x', x, E) = (g_1(x', x, E_1), g_2(x', x, E_2), \ \ldots, g_s(x', x, E_s)),$$
$$g_k(x', x, E_k) = f_k(x', E_k) - f_k(x, E_k) = \max_{i \in N_m} \min_{i' \in N_m} (E_{i'k}x' - E_{ik}x), \ k \in N_s.$$

Легко видеть, что в частном случае при $m = 1$ векторная инвестиционная задача $Z^s(E)$ превращается в s-критериальную задачу линейного булева программирования

$$Z^s_B(E): \quad Ex \to \max_{x \in X},$$

где $X \subseteq \mathbf{E}^n$; $E = [e_{1jk}] \in \mathbb{R}^{1 \times n \times s}$ — матрица со строками $E_k = (e_{11k}, e_{12k}, \ldots, e_{1nk}) \in \mathbb{R}^n$, $k \in N_s$. Такой случай можно интерпретировать как ситуацию, при которой состояние рынка не вызывает сомнений ($m = 1$).

В пространствах портфелей $\mathbb{R}^n$ и состояний рынка $\mathbb{R}^m$ зададим линейную метрику l_1, а в критериальном пространстве эффективности $\mathbb{R}^s$ — метрику Гельдера l_p, $1 \leqslant p \leqslant \infty$, т. е. полагаем

$$\|E_{ik}\|_1 = \sum_{j \in N_n} |e_{ijk}|, \quad i \in N_m, \quad k \in N_s,$$
$$\|E_k\|_{11} = \|(\|E_{1k}\|_1, \|E_{2k}\|_1, \ldots, \|E_{mk}\|_1)\|_1 = \sum_{i \in N_m} \sum_{j \in N_n} |e_{ijk}|, \quad k \in N_s,$$

$$\|E\|_{11p} = \|(\|E_1\|_{11}, \|E_2\|_{11}, \ldots, \|E_s\|_{11})\|_p, \tag{1}$$

где, как обычно, норму Гельдера l_p вектора $a = (a_1, a_2, \ldots, a_s) \in \mathbb{R}^s$ определим формулой

$$\|a\|_p = \begin{cases} \Big(\sum\limits_{j \in N_s} |a_j|^p\Big)^{1/p}, & \text{если} \ \ 1 \leqslant p < \infty, \\ \max\{|a_j| : \ j \in N_s\}, & \text{если} \ \ p = \infty. \end{cases}$$

Очевидны неравенства

$$\|E_{ik}\|_1 \leqslant \|E_k\|_{11} \leqslant \|E\|_{11p}, \quad i \in N_m, \ k \in N_s.$$

Известно, что метрика l_p, заданная в пространстве $\mathbb{R}^d$, порождает метрику l_q в сопряжённом пространстве $(\mathbb{R}^d)^*$, причём числа p и q связаны условиями

$$\frac{1}{p} + \frac{1}{q} = 1, \qquad 1 < p < \infty.$$

Как обычно, полагаем $q = 1$, если $p = \infty$, и $q = \infty$, если $p = 1$. Поэтому в дальнейшем считаем, что областью изменений чисел p и q является интервал $[1, \infty]$, а сами числа связаны указанными выше условиями. Кроме того, полагаем, что $1/p = 0$ при $p = \infty$.

Используя очевидное соотношение $E_{ik}x \geqslant -\|E_{ik}\|_1$, $x \in \mathbf{E}^n$, легко убедиться, что при любых портфелях x и x' верны неравенства

$$E_{ik}x - E_{i'k}x' \geqslant -\|E_k\|_{11}, \qquad i,\ i' \in N_m, \quad k \in N_s. \tag{2}$$

Следуя [4, 6, 9, 10], радиусом устойчивости парето-оптимального инвестиционного портфеля $x^0 \in P^s(E)$ задачи $Z^s(E)$ назовем число

$$\rho = \rho^s(x^0, p, m) = \begin{cases} \sup\ \Xi_p, & \text{если } \Xi_p \neq \varnothing, \\ 0, & \text{если } \Xi_p = \varnothing, \end{cases}$$

где

$$\Xi_p = \{\varepsilon > 0 :\ \forall E' \in \Omega_p(\varepsilon) \quad (x^0 \in P^s(E + E'))\};$$

$\Omega_p(\varepsilon) = \{E' \in \mathbb{R}^{m\times n\times s} :\ \|E'\|_{11p} < \varepsilon\}$ — множество возмущающих матриц, $P^s(E+E')$ — множество Парето возмущённой задачи $Z^s(E + E')$. Тем самым радиус устойчивости задаёт предельный уровень возмущений исходных данных задачи (элементов матрицы E), сохраняющих парето-оптимальность портфеля.

2. Леммы

Для вектора $a = (a_1, a_2, \ldots, a_s) \in \mathbb{R}^s$ введём оператор положительной срезки

$$a^+ = [a]^+ = (a_1^+, a_2^+, \ldots, a_s^+),$$

где $a_k^+ = [a_k]^+ = \max\{0, a_k\}$, $k \in N_s$.

Лемма 1. Пусть $1 \leqslant p \leqslant \infty$, $\varphi > 0$, $x^0 \neq x$,

$$\|g^+(x^0, x, E)\|_p \geqslant \varphi. \tag{3}$$

Тогда справедлива формула

$$\forall E' \in \Omega_p(\varphi) \quad \exists l \in N_s \qquad (g_l(x^0, x, E_l + E'_l) > 0). \tag{4}$$

Доказательство. Допустим, напротив, существует такая возмущающая матрица $E^0 \in \Omega_p(\varphi)$, что выполняются неравенства

$$g_k(x^0, x, E_k + E_k^0) \leqslant 0, \quad k \in N_s.$$

Тогда, привлекая (2), легко выводим

$$0 \geqslant g_k(x^0, x, E_k + E_k^0) = \max_{i\in N_m} \min_{i'\in N_m} (E_{i'k}x^0 - E_{ik}x + E_{i'k}^0 x^0 - E_{ik}^0 x) \geqslant g_k(x^0, x, E_k) - \|E_k^0\|_{11},$$

т. е. $$g_k^+(x^0, x, E_k) \leqslant \|E_k^0\|_{11}, \quad k \in N_s.$$

Поэтому благодаря (1) и $E^0 \in \Omega_p(\varphi)$ при $p \in [1, \infty]$ имеем

$$\|g^+(x^0, x, E)\|_p \leqslant \|E^0\|_{11p} < \varphi.$$

Полученное неравенство противоречит условию (3). ■

Методом от противного легко доказать следующую лемму.

Лемма 2. Пусть $x^0 \in P^s(E)$, $\gamma > 0$ и $1 \leqslant p \leqslant \infty$. Если при любом портфеле $x \in X \setminus \{x^0\}$ и каждой возмущающей матрице $E' \in \Omega_p(\gamma)$ найдется такой индекс $l \in N_s$, что справедливо неравенство $g_l(x^0, x, E_l + E'_l) > 0$, то x^0 является парето-оптимальным портфелем возмущённой задачи $Z^s(E + E')$, т. е. $x^0 \in P^s(E + E')$ при $E' \in \Omega_p(\gamma)$.

Лемма 3. Пусть $1 \leqslant p \leqslant \infty$, $x^0 \neq x^*$, $\delta = (\delta_1, \delta_2, \ldots, \delta_s)$, $\delta_k > 0$, $k \in N_s$,

$$\delta_k > g_k^+(x^0, x^*, E_k), \qquad k \in N_s. \tag{5}$$

Тогда при любом числе $\varepsilon > 2\|\delta\|_p$ существует такая возмущающая матрица $E^0 \in \Omega_p(\varepsilon)$, что $x^0 \notin P^s(E + E^0)$.

Доказательство. Для доказательства достаточно построить такую возмущающую матрицу $E^0 \in \Omega_p(\varepsilon)$, где $\varepsilon > 2\|\delta\|_p$, с сечениями E_k^0, $k \in N_s$, чтобы для каждого индекса $k \in N_s$ выполнялось неравенство

$$g_k(x^0, x^*, E_k + E_k^0) < 0. \tag{6}$$

Для этого введём обозначение

$$i(k) = \arg\min\{E_{ik}x^0 : \ i \in N_m\}, \quad k \in N_s,$$

и рассмотрим два возможных случая (при фиксированном индексе $k \in N_s$).

С л у ч а й 1. $x^0 \leqslant x^*$. Тогда ввиду неравенств $x^* \neq x^0 \neq 0_{(n)}$ существует такая пара различных индексов $(u, v) \in N_n \times N_n$, что $x_u^0 = 0$, $x_u^* = 1$, $x_v^0 = x_v^* = 1$. Вновь используя компоненты вектора δ (см. (5)), элементы любого k-го сечения $E_k^0 = [e_{ijk}^0] \in \mathbb{R}^{m\times n}$ возмущающей матрицы $E^0 = [e_{ijk}^0] \in \mathbb{R}^{m\times n\times s}$ зададим по правилу

$$e_{ijk}^0 = \begin{cases} \delta_k, & \text{если } i = i(k),\ j = u, \\ -\delta_k, & \text{если } i = i(k),\ j = v, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Тогда имеем

$$\begin{gathered} E_{i(k)k}^0 x^0 = -\delta_k; \qquad E_{i(k)k}^0 x^* = 0; \\ E_{ik}^0 x^0 = E_{ik}^0 x^* = 0, \qquad i \in N_m \setminus \{i(k)\}; \\ \|E_k^0\|_{11} = 2\delta_k, \quad k \in N_s. \end{gathered}$$

Отсюда легко убеждаемся, что $\|E^0\|_{11p} = 2\|\delta\|_p < \varepsilon$ и для любого индекса $k \in N_s$ справедливы следующие равенства:

$$f_k(x^0, E_k + E_k^0) = \min\Big\{(E_{i(k)k} + E_{i(k)k}^0)x^0, \min_{i\neq i(k)}(E_{ik} + E_{ik}^0)x^0\Big\} = f_k(x^0, E_k) - \delta_k;$$

$$f_k(x^*, E_k + E_k^0) = \min\Big\{(E_{i(k)k} + E_{i(k)k}^0)x^*, \min_{i\neq i(k)}(E_{ik} + E_{ik}^0)x^*\Big\} = f_k(x^*, E_k).$$

Поэтому ввиду (5) получаем требуемое неравенство (6):

$$g_k(x^0, x^*, E_k + E_k^0) = g_k(x^0, x^*, E_k) - \delta_k \leqslant g_k^+(x^0, x^*, E_k) - \delta_k < 0, \quad k \in N_s.$$

С л у ч а й 2. Пусть неравенство $x^0 \leqslant x^*$ не выполняется, т. е. существует такой индекс $u \in N_n$, что $x_u^0 = 1$ и $x_u^* = 0$. Используя компоненты вектора δ (см. (5)), зададим элементы любого k-го сечения $E_k^0 = [e_{ijk}^0] \in \mathbb{R}^{m\times n}$ возмущающей матрицы $E^0 = [e_{ijk}^0] \in \mathbb{R}^{m\times n\times s}$ по правилу

$$e_{ijk}^0 = \begin{cases} -2\delta_k, & \text{если } \ i = i(k),\ j = u, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Тогда имеем

$$E^0_{i(k)k}x^0 = -2\delta_k; \qquad E^0_{i(k)k}x^* = 0;$$
$$E^0_{ik}x^0 = E^0_{ik}x^* = 0, \qquad i \in N_m \setminus \{i(k)\};$$
$$\|E^0_k\|_{11} = 2\delta_k, \quad k \in N_s.$$

Отсюда получаем, что $\|E^0\|_{11p} = 2\|\delta\|_p < \varepsilon$. Кроме того, для любого $k \in N_s$ справедливы равенства

$$f_k(x^0, E_k + E^0_k) = \min\Big\{(E_{i(k)k} + E^0_{i(k)k})x^0, \min_{i\neq i(k)}(E_{ik} + E^0_{ik})x^0\Big\} = f_k(x^0, E_k) - 2\delta_k;$$
$$f_k(x^*, E_k + E^0_k) = \min\Big\{(E_{i(k)k} + E^0_{i(k)k})x^*, \min_{i\neq i(k)}(E_{ik} + E^0_{ik})x^*\Big\} = f_k(x^*, E_k).$$

Поэтому, используя соотношения (5), выводим неравенство (6):

$$g_k(x^0, x^*, E_k + E^0_k) = g_k(x^0, x^*, E_k) - 2\delta_k \leqslant g^+_k(x^0, x^*, E_k) - 2\delta_k < 0, \quad k \in N_s.$$

Лемма доказана. ■

Замечание 1. Легко видеть, что утверждение леммы 3 в случае 1 верно и для $\varepsilon > \|\delta\|_p$. Этим обстоятельством мы воспользуемся, когда будем доказывать достижимость нижней оценки (см. теорему 2).

При $\gamma > 0$ матрицу $W = [u, v] \in \mathbb{R}^{m\times 2}$, $m \geqslant 2$, со столбцами $u = (u_1, u_2, \ldots, u_m)^T$ и $v = (v_1, v_2, \ldots, v_m)^T$ назовем γ-*особой*, если выполняется неравенство

$$\min_{i\in N_m}(u_i + v_i) - \min_{i\in N_m} u_i < \gamma.$$

Лемма 4. Всякая матрица $W = [u, v] \in \mathbb{R}^{m\times 2}$, $m \geqslant 2$, с нормой $\|W\|_{11} = \|(\|u\|_1, \|v\|_1)\|_1 < 2\gamma$, где $\gamma > 0$, является γ-особой.

Доказательство. Проведем индукцию по числу $m \geqslant 2$. Сначала докажем утверждение леммы при $m = 2$. Пусть

$$W = \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}.$$

Убедимся, что неравенство

$$\min\{u_1 + v_1, u_2 + v_2\} - \min\{u_1, u_2\} < \gamma \tag{7}$$

следует из неравенства $\|W\|_{11} < 2\gamma$, т. е. из неравенства

$$|u_1| + |u_2| + |v_1| + |v_2| < 2\gamma. \tag{8}$$

Не исключая общности, будем полагать, что

$$u_1 + v_1 \leqslant u_2 + v_2. \tag{9}$$

Рассмотрим два случая.

С л у ч а й 1. $u_1 \leqslant u_2$. Тогда неравенство (7) ввиду (9) принимает вид $v_1 < \gamma$. Доказательство этого неравенства проведем от противного. Пусть

$$v_1 \geqslant \gamma. \tag{10}$$

Из (9) и (10) имеем $-u_1 + u_2 + v_2 \geqslant \gamma$, а из (8) и (10) выводим $|u_1| + |u_2| + |v_2| < \gamma$. Полученные неравенства приводят к противоречию

$$0 \leqslant |u_2| - u_2 + |v_2| - v_2 < -(u_1 + |u_1|) \leqslant 0.$$

С л у ч а й 2. $u_1 > u_2$. Тогда неравенство (7), согласно (9), превращается в неравенство $u_1 + v_1 - u_2 < \gamma$. Пусть, напротив,

$$u_1 + v_1 - u_2 \geqslant \gamma. \tag{11}$$

Отсюда, учитывая (9), имеем $v_2 \geqslant \gamma$, и в силу (8) получим $|u_1| + |u_2| + |v_1| < \gamma$. Это неравенство вместе с (11) дают противоречие

$$0 \leqslant |u_1| - u_1 + |v_1| - v_1 < -(u_2 + |u_2|) \leqslant 0.$$

Далее будем предполагать, что утверждение леммы верно при $m \geqslant 2$. Покажем, что матрица $W = [u, v] \in \mathbb{R}^{(m+1)\times 2}$ со столбцами $u = (u_1, u_2, \ldots, u_{m+1})^T$, $v = (v_1, v_2, \ldots, v_{m+1})^T$ и нормой $\|W\|_{11} < 2\gamma$ является γ-особой. Положим

$$i_1 = \arg\min\{u_i + v_i : \ i \in N_{m+1}\}, \quad i_2 = \arg\min\{u_i : \ i \in N_{m+1}\},$$

и пусть индекс $h \in N_{m+1}$ таков, что

$$h \neq i_1, \quad h \neq i_2. \tag{12}$$

Через $W' \in \mathbb{R}^{m\times 2}$ обозначим матрицу, полученную из матрицы W путем удаления строки с номером h. Тогда $\|W'\|_{11} \leqslant \|W\|_{11} < 2\gamma$ и по предположению индукции матрица W' является γ-особой, т. е. выполняется неравенство

$$\min_{i\in N_{m+1}\setminus\{h\}} (u_i + v_i) - \min_{i\in N_{m+1}\setminus\{h\}} u_i < \gamma.$$

Кроме того, учитывая (12), нетрудно убедиться, что справедливы равенства

$$\min_{i\in N_{m+1}} (u_i + v_i) = u_{i_1} + v_{i_1} = \min_{i\in N_{m+1}\setminus\{h\}} (u_i + v_i), \quad \min_{i\in N_{m+1}} u_i = u_{i_2} = \min_{i\in N_{m+1}\setminus\{h\}} u_i.$$

Следовательно, матрица W является γ-особой. ■

3. Оценки радиуса устойчивости

Для парето-оптимального портфеля x^0 задачи $Z^s(E)$ введем обозначение

$$\varphi = \varphi^s(x^0, p, m) = \min_{x\in X\setminus\{x^0\}} \|g^+(x^0, x, E)\|_p.$$

Очевидно, что $\varphi \geqslant 0$.

Теорема 1. При любых m, $s \in \mathbb{N}$ и $1 \leqslant p \leqslant \infty$ для радиуса устойчивости $\rho^s(x^0, p, m)$ инвестиционного портфеля $x^0 \in P^s(E)$ задачи $Z^s(E)$ справедливы следующие оценки:

$$\varphi^s(x^0, p, m) \leqslant \rho^s(x^0, p, m) \leqslant 2\varphi^s(x^0, p, m). \tag{13}$$

Доказательство. Пусть $x^0 \in P^s(E)$. Сначала докажем справедливость нижних оценок (13). Не уменьшая общности, будем считать, что $\varphi > 0$ (в противном случае неравенство $\rho \geqslant \varphi$ очевидно). В соответствии с определением числа φ для любого портфеля $x \neq x^0$ справедливо неравенство $\|g^+(x^0, x, E)\|_p \geqslant \varphi$, а поэтому в силу леммы 1 верна формула (4). Тогда (согласно лемме 2) $x^0 \in P^s(E+E')$ при любой возмущающей матрице $E' \in \Omega_p(\varphi)$. Следовательно, $\rho^s(x^0, p, m) \geqslant \varphi^s(x^0, p, m)$.

Далее докажем справедливость верхней оценки (13) при любом числе $p \in [1, \infty]$. Пусть $\varepsilon > 2\varphi > 0$, а портфель $x^* \neq x^0$ таков, что

$$\|g^+(x^0, x^*, E)\|_p = \varphi. \tag{14}$$

Тогда, учитывая непрерывную зависимость нормы l_p вектора от его координат, подберем такой вектор $\delta \in \mathbb{R}^s$ с положительными компонентами, удовлетворяющими неравенствам (5), что $\varepsilon/2 > \|\delta\|_p > \varphi$. Отсюда, согласно лемме 3, при $\varepsilon > 2\varphi$ существует такая возмущающая матрица $E^0 \in \Omega_p(\varepsilon)$, что портфель $x^0 \in P^s(E)$ не является парето-оптимальным портфелем возмущенной задачи $Z^s(E+E^0)$. Тем самым доказано, что для любого числа $\varepsilon > 2\varphi$ справедливо неравенство $\rho^s(x^0, p, m) < \varepsilon$. Следовательно, $\rho^s(x^0, p, m) \leqslant 2\varphi^s(x^0, p, m)$ при любом числе $p \in [1, \infty]$. ■

Замечание 2. Нетрудно видеть, что при обосновании нижней оценки φ допустима принадлежность нулевого вектора $0_{(n)}$ множеству портфелей X. Отсутствие нулевого вектора необходимо лишь при установлении верхней оценки, поскольку доказательство неравенства $\rho^s(x^0, E) \leqslant 2\varphi$ основано на использовании леммы 3.

Следствие 1. Радиус устойчивости $\rho^s(x^0, p, m)$ больше 0 (парето-оптимальный портфель x^0 устойчив) тогда и только тогда, когда $\varphi > 0$.

Докажем достижимость нижней оценки радиуса устойчивости при $m = 1$.

Следствие 2. При любых $s \in \mathbb{N}$ и $1 \leqslant p \leqslant \infty$ для радиуса устойчивости $\rho^s(x^0, p, 1)$ инвестиционного портфеля $x^0 \in P^s(E)$ s-критериальной задачи булева программирования $Z^s_B(E)$ справедлива формула

$$\rho^s(x^0, p, 1) = \varphi^s(x^0, p, 1).$$

Доказательство. Пусть портфель $x^* \neq x^0$ таков, что выполняется равенство

$$\|[E(x^0 - x^*)]^+\|_p = \varphi.$$

Тогда при $\varepsilon > \varphi$ очевидно, что существует вектор $\delta = (\delta_1, \delta_2, \ldots, \delta_s) \in \mathbb{R}^s$, компоненты которого удовлетворяют неравенствам

$$\delta_k > [E_k(x^0 - x^*)]^+, \qquad k \in N_s, \tag{15}$$

$$\varphi < \|\delta\|_p < \varepsilon.$$

Пусть индекс $l \in N_n$ такой, что $x^*_l \neq x^0_l$. Рассмотрим возмущающую матрицу $E^0 = [e^0_{1jk}] \in \mathbb{R}^{1\times n\times s}$, элементы которой зададим по правилу

$$e^0_{1jk} = \begin{cases} \delta_k(x^*_l - x^0_l), & \text{если } \ j = l,\ k \in N_s, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Тогда

$$E_k(x^0 - x^*) = -\delta_k, \quad k \in N_s;$$
$$\|E^0_k\|_1 = \delta_k, \quad k \in N_s;$$
$$\varphi < \|E^0\|_{1p} = \|\delta\|_p < \varepsilon.$$

Поэтому ввиду (15) запишем

$$(E_k + E_k^0)(x^0 - x^*) = E_k(x^0 - x^*) - \delta_k \leqslant [E_k(x^0 - x^*)]^+ - \delta_k < 0, \quad k \in N_s.$$

В результате получаем, что для любого числа $\varepsilon > \varphi$ существует такая возмущающая матрица $E^0 \in \Omega_p(\varepsilon)$, что портфель $x^0 \in P^s(E)$ перестает быть парето-оптимальным портфелем возмущённой задачи $Z_B^s(E + E^0)$. Это значит, что $\rho^s(x^0, p, 1) \leqslant \varphi$. Следовательно, в силу теоремы 1 радиус устойчивости парето-оптимального портфеля задачи $Z_B^s(E)$ равен $\varphi = \varphi^s(x^0, p, 1)$. ■

4. Достижимость нижней оценки (при $m \geqslant 2$)

Теорема 2. При любых $\varphi > 0$, $m \geqslant 2$, $1 \leqslant p \leqslant \infty$ существует такой класс векторных инвестиционных задач $Z^s(E)$, $s \in \mathbb{N}$, что для радиуса устойчивости портфеля $x^0 \in P^s(E)$ любой задачи из этого класса справедлива формула

$$\rho^s(x^0, p, m) = \varphi = \varphi^s(x^0, p, m).$$

Доказательство. Пусть портфель $x^* \neq x^0$ таков, что выполняется равенство (14). Тогда при $\varepsilon > \varphi$ очевидно, что существует вектор $\delta = (\delta_1, \delta_2, \ldots, \delta_s) \in \mathbb{R}^s$, компоненты которого удовлетворяют неравенствам (5) и $\varphi < \|\delta\|_p < \varepsilon$. Далее будем предполагать, что существует индекс $l \in N_n$ с условием $x_l^0 = 1$, $x_l^* = 0$.

Рассмотрим возмущающую матрицу $E^0 = [e_{ijk}^0] \in \mathbb{R}^{m \times n \times s}$, элементы любого k-го сечения E_k^0, $k \in N_s$, которой зададим по правилу

$$e_{ijk}^0 = \begin{cases} -\delta_k, & \text{если } i = i(k),\ j = l, \\ 0 & \text{в остальных случаях,} \end{cases}$$

где $i(k) = \arg\min\{E_{ik}x^0 : \ i \in N_m\}$. Тогда для каждого индекса $k \in N_s$ очевидны соотношения

$$E_{i(k)k}^0 x^0 = -\delta_k;$$
$$E_{ik}^0 x^0 = 0, \quad i \in N_m \setminus \{i(k)\};$$
$$E_{ik}^0 x^* = 0, \quad i \in N_m;$$
$$\|E_k^0\|_{11} = \delta_k; \quad \varphi < \|E^0\|_{11p} = \|\delta\|_p < \varepsilon.$$

Отсюда с учётом неравенств (5) получаем

$$g_k(x^0, x^*, E_k + E_k^0) = \min_{i \in N_m} (E_{ik} + E_{ik}^0)x^0 - \min_{i \in N_m} (E_{ik} + E_{ik}^0)x^* =$$
$$= f_k(x^0, E) - \delta_k - f_k(x^0, E_k) = g_k(x^0, x^*, E_k) - \delta_k \leqslant g_k^+(x^0, x^*, E_k) - \delta_k < 0, \quad k \in N_s.$$

Следовательно, для каждого индекса $k \in N_s$ верно неравенство (6).

В результате получаем, что для любого числа $\varepsilon > \varphi$ существует такая возмущающая матрица $E^0 \in \Omega_p(\varepsilon)$, что портфель $x^0 \in P^s(E)$ перестает быть парето-оптимальным портфелем возмущённой задачи $Z^s(E + E^0)$. Это значит, что $\rho^s(x^0, p, m) \leqslant \varphi$. Следовательно, в силу теоремы 1 радиус устойчивости парето-оптимального портфеля любой задачи введенного класса равен $\varphi = \varphi^s(x^0, p, m)$. ■

Приведем числовой пример, свидетельствующий о существовании задач того класса, который указан в доказательстве теоремы 2.

Пример 1. Пусть $m = 3$, $n = 3$, $s = 2$, $X = \{x^0, x^*\}$, $x^0 = (1, 1, 0)^T$, $x^* = (0, 1, 1)^T$, $E \in \mathbb{R}^{3\times3\times2}$ — матрица с сечениями

$$E_1 = \begin{pmatrix} 2 & 1 & 1 \\ 3 & 1 & 3 \\ 4 & 2 & 4 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 3 & 1 & 3 \\ 2 & 1 & 1 \\ 4 & 2 & 4 \end{pmatrix}.$$

Тогда $f(x^0, E) = (3, 3)$, $f(x^*, E) = (2, 2)$, $x^0 \in P^2(E)$, $l = 1$,

$$\varphi^2(x^0, p, 3) = \|g^+(x^0, x^*, E)\|_p = \|(1, 1)\|_p = 2^{1/p}.$$

Поэтому, согласно теореме 2, при любом числе $p \in [1, \infty]$ имеем

$$\rho^2(x^0, p, 3) = \|g^+(x^0, x^*, E)\|_p = 2^{1/p}.$$

5. Достижимость верхней оценки

Теорема 3. При любых $\varphi > 0$, $m \geqslant 2$ и $1 \leqslant p \leqslant \infty$ существует такой класс векторных инвестиционных задач $Z^s(E)$, $s \in \mathbb{N}$, что для радиуса устойчивости портфеля $x^0 \in P^s(E)$ любой задачи из этого класса справедлива формула

$$\rho^s(x^0, p, m) = 2\varphi^s(x^0, p, m).$$

Доказательство. Пусть $x^0 \in P^s(E)$, $\varphi > 0$ и $m \geqslant 2$. Согласно теореме 1, достаточно построить класс задач $Z^s(E)$ с условием $\rho^s(x^0, p, m) \geqslant 2\varphi$. Покажем, что такой класс существует при $X = \{x^0, x^*\}$, где $x^0 \in P^s(E)$, $x^0 \leqslant x^*$, $x^0 \neq x^*$. Непосредственно из определения числа φ следует равенство (14).

Далее будем предполагать, что все строки E_{ik}, $i \in N_m$, любого сечения E_k, $k \in N_s$, матрицы $E \in \mathbb{R}^{m\times n\times s}$ одинаковы. Обозначив такую строку через e, будем считать, что $E_{ik}(x^0 - x^*) = e(x^0 - x^*) > 0$, $i \in N_m$, $k \in N_s$. Тогда имеем

$$g_k(x^0, x^*, E_k) = f_k(x^0, E_k) - f_k(x^*, E_k) = e(x^0 - x^*) > 0, \quad k \in N_s. \tag{16}$$

Учитывая это, из (14) получаем

$$e(x^0 - x^*) = \varphi/s^{1/p}. \tag{17}$$

Пусть теперь $E' \in \mathbb{R}^{m\times n\times s}$ — произвольная матрица с сечениями E'_k, $k \in N_s$. Тогда из равенств (16) и (17) для любого индекса $k \in N_s$ вытекают равенства

$$g_k(x^0, x^*, E_k + E'_k) = \min_{i\in N_m}(e - E'_{ik})x^0 - \min_{i\in N_m}(e - E'_{ik})x^* = e(x^0 - x^*) - \zeta_k = \varphi/s^{1/p} - \zeta_k,$$

где

$$\zeta_k = \min_{i\in N_m} E'_{ik}(x^0 + \widehat{x}) - \min_{i\in N_m} E'_{ik}x^0, \quad k \in N_s; \tag{18}$$

$$\widehat{x} = x^* - x^0. \tag{19}$$

Заметим, что $\widehat{x} \in \mathbf{E}^n$ и $\widehat{x} \neq 0_{(n)}$ в силу неравенств $x^* \geqslant x^0$ и $x^* \neq x^0$.

Пусть теперь возмущающая матрица $E' = [e'_{ijk}] \in \Omega_p(2\varphi)$. Тогда существует хотя бы один такой индекс $l \in N_s$, что для l-го сечения $E'_l = [e'_{ijl}] \in \mathbb{R}^{m\times n}$ матрицы E' справедливо неравенство $\|E'_l\|_{11} < 2\varphi/s^{1/p}$. Рассмотрим матрицу $W = [u, v] \in \mathbb{R}^{m\times2}$ со столбцами $u = E'_l x^0$ и $v = E'_l \widehat{x}$. Далее, введя для портфеля $x = (x_1, x_2, \ldots, x_n)^T$

обозначение $N(x) = \{j \in N_n : x_j = 1\}$, убеждаемся (ввиду (19)) в справедливости равенства $N(x^0) \cap N(\widehat{x}) = \varnothing$. Отсюда получаем

$$\|W\|_{11} = \|E'_l x^0\|_1 + \|E'_l \widehat{x}\|_1 = \sum_{i \in N_m} \left| \sum_{j \in N(x^0)} e'_{ijl} \right| + \sum_{i \in N_m} \left| \sum_{j \in N(\widehat{x})} e'_{ijl} \right| \leqslant$$
$$\leqslant \sum_{i \in N_m} \sum_{j \in N(x^*)} |e'_{ijl}| \leqslant \|E'_l\|_{11} < 2\varphi / s^{1/p}.$$

Поэтому благодаря лемме 4 (применение этой леммы возможно, так как $m \geqslant 2$ по условию теоремы 3) матрица W является $\varphi/s^{1/p}$-особой, т. е., согласно (18), выполняется неравенство $\zeta_l < \varphi/s^{1/p}$, которое вместе с (5) дает $g_l(x^0, x^*, E_l + E'_l) > 0$.

Следовательно, на основании леммы 2 заключаем, что при всякой возмущающей матрице $E' \in \Omega_p(2\varphi)$ выполняется включение $x^0 \in P^s(E + E')$, т. е. $\rho^s(x^0, p, m) \geqslant 2\varphi^s(x^0, p, m)$. ■

Следующий пример свидетельствует, что существуют задачи, принадлежащие классу, указанному в доказательстве теоремы 3.

Пример 2. Пусть $m = 3$, $n = 3$, $s = 2$, $X = \{x^0, x^*\}$, $x^0 = (0, 1, 1)^T$, $x^* = (1, 1, 1)^T$, $E \in \mathbb{R}^{3\times3\times2}$ — матрица с сечениями

$$E_1 = \begin{pmatrix} -1 & 1 & -2 \\ -1 & 1 & -2 \\ -1 & 1 & -2 \end{pmatrix}, \quad E_2 = \begin{pmatrix} -1 & 1 & -2 \\ -1 & 1 & -2 \\ -1 & 1 & -2 \end{pmatrix}.$$

Тогда $x^0 \leqslant x^*$, $x^0 \neq x^*$, $f(x^0, E) = (-1, -1)$, $f(x^*, E) = (-2, -2)$. Поэтому $x^0 \in P^2(E)$, $e = (-1, 1, -2)$, $g_k(x^0, x^*, E_k) = e(x^0 - x^*) = 1$, $k \in N_2$. Отсюда $\varphi^2(x^0, p, 3) = \|(1, 1)\|_p = 2^{1/p}$. Следовательно, согласно теореме 3, для любого числа $p \in [1, \infty]$ имеем $\rho^2(x^0, p, 3) = 2\varphi^2(x^0, p, 3) = 2 \cdot 2^{1/p}$.

Замечание 3. Из теорем 2 и 3 следует, что оценки радиуса устойчивости (13) векторной задачи $Z^s(E)$ являются достижимыми при любых числах $m \geqslant 2$ и $p \in [1, \infty]$. Ранее такой результат был известен лишь при $p = 1$ [18].

Заключение

В настоящей работе на базе портфельной теории Марковица сформулирована векторная (многокритериальная) булева задача выбора парето-оптимальных инвестиционных портфелей, состоящая в максимизации различных показателей эффективности принимаемых решений. При этом непредсказуемость состояния финансового рынка, присущая рыночной экономике, учитывается путём использования классических критериев теории игр [19, 20] — максиминных критериев Вальда, а учёт неточности и некорректности исходных числовых параметров (оценок экономической эффективности инвестиционных проектов), характерных для реальных инвестиционных задач, основан на проведении параметрического постоптимального анализа устойчивости парето-оптимального инвестиционного портфеля к возмущению этих параметров в случае, когда в критериальном пространстве задана любая метрика Гельдера l_p, $1 \leqslant p \leqslant \infty$. Получены нижняя и верхняя оценки (границы) радиуса устойчивости, под которым, как обычно, понимается предельный уровень изменений параметров, сохраняющих оптимальность портфеля. Построение конкретных классов векторных инвестиционных задач показало неулучшаемость этих оценок. Использование полученных здесь результатов позволяет указать границы надёжности решений, принимаемых инвестором при

формировании инвестиционного портфеля, оптимального по нескольким максиминным критериями экономической эффективности Вальда.

ЛИТЕРАТУРА

1. *Markowitz H.* Portfolio selection // J. Finance. 1952. V. 7. No. 1. P. 77–91.
2. *Markowitz H. M.* Portfolio Selection: Efficient Diversification of Investments. New York: Willey, 1991. 400 p.
3. *Шарп У. Ф., Александер Г. Дж., Бейли Д. В.* Инвестиции. М.: Инфра-М, 2003. 1028 с.
4. *Емеличев В. А., Кузьмин К. Г.* О радиусе устойчивости эффективного решения векторной задачи целочисленного линейного программирования в метрике Гёльдера // Кибернетика и системный анализ. 2006. № 4. С. 175–181.
5. *Емеличев В. А., Кузьмин К. Г.* Об одном типе устойчивости многокритериальной задачи целочисленного линейного программирования в случае монотонной нормы // Известия РАН. Теория и системы управления. 2007. № 5. С. 45–51.
6. *Емеличев В. А., Карелкина О.В.* Конечные коалиционные игры: параметризация концепции равновесия (от Парето до Нэша) и устойчивость эффективной ситуации в метрике Гельдера // Дискретная математика. 2009. Т. 21. Вып. 2. С. 43–50.
7. *Emelichev V. and Podkopaev D.* Quantitative stability analysis for vector problems of 0-1 programming // Discrete Optimization. 2010. V. 7. No. 1-2. P. 48–63.
8. *Емеличев В. А., Коротков В. В.* Оценки радиуса устойчивости лексикографического оптимума векторной булевой задачи с критериями рисков Сэвиджа // Дискрет. анализ и исслед. операций. 2011. Т. 18. № 2. С. 41–50.
9. *Емеличев В. А., Коротков В. В., Кузьмин К. Г.* Многокритериальная инвестиционная задача в условиях неопределенности и риска // Известия РАН. Теория и системы управления. 2011. № 6. С. 157–164.
10. *Емеличев В. А., Коротков В. В.* О радиусе устойчивости эффективного решения многокритериальной задачи портфельной оптимизации с критериями Сэвиджа // Дискретная математика. 2011. Т. 23. Вып. 4. С. 33–38.
11. *Емеличев В. А., Коротков В. В.* Постоптимальный анализ многокритериальной инвестиционной задачи Марковица // Информатика. 2011. № 4. С. 5–14.
12. *Emelichev V. and Korotkov V.* On stability radius of the multicriteria variant of Markowitz's investment portfolio problem // Bull. Acad. Sci. Moldova. Mathematics. 2011. No. 1. P. 83–94.
13. Portfolio Decision Analysis: Improved Methods for Resource Allocation (International Series in Operations Research and Management Science) / eds. A. Salo, J. Keisler, A. Morton. New York: Springer, 2011. 424 p.
14. *Бронштейн Е. М., Качкаева М. М., Тулупова Е. В.* Управление портфелем ценных бумаг на основе комплексных квантильных мер риска // Известия РАН. Теория и системы управления. 2011. № 1. С. 178–183.
15. *Царев В. В.* Оценка экономической эффективности инвестиций. СПб.: Питер, 2004. 464 с.
16. *Виленский П. Л., Лившиц В. Н., Смоляк С. А.* Оценка эффективности инвестиционных проектов: теория и практика. М.: Дело, 2008. 1104 с.
17. *Wald A.* Statistical Decision Functions. New York: Wiley, 1950. 179 p.
18. *Emelichev V. and Korotkov V.* Post-optimal analysis of investment problem with Wald's ordered maximin criteria // Bull. Acad. Sci. Moldova. Mathematics. 2012. No. 1. P. 59–69.
19. *Петросян Л. А., Зенкевич Н. А., Семина Е. А.* Теория игр. М.: Высшая школа, 1998.
20. *Фон Нейман Дж., Моргенштерн О.* Теория игр и экономическое поведение. М.: Наука, 1970. 707 с.

DOI 10.17223/20710410/18/6
УДК 519.68

РАЗВИТИЕ МЕТОДА НЕПРЕРЫВНЫХ АСИНХРОННЫХ КЛЕТОЧНЫХ АВТОМАТОВ ДЛЯ МОДЕЛИРОВАНИЯ ТУРБУЛЕНТНЫХ ПОТОКОВ

Г. Д. Тимчук, В. В. Жихаревич

Национальный технический университет «Харьковский политехнический институт», Черновицкий факультет, г. Черновцы, Украина

E-mail: galtym@meta.ua, vzhikhar@mail.ru

Представлен метод непрерывных асинхронных клеточных автоматов, моделирующих турбулентные потоки вещества. Предлагается его модификация, которая состоит в реализации вероятностного механизма передвижения клеточных автоматов вдоль компонент векторов скоростей. При этом моделирование процесса переноса вещества осуществляется путём направленного дублирования содержания соседних ячеек. Приведены результаты вычислительного эксперимента по наблюдению турбулентной динамики на примере потока вещества в трубе, которое имеет препятствия.

Ключевые слова: *клеточный автомат, компьютерное моделирование, турбулентность, уравнения Навье — Стокса.*

Введение

Проблема моделирования турбулентных потоков является актуальной уже более века. Общепринятым подходом в этом отношении считается численное решение уравнения Навье — Стокса и его различных модификаций. При этом возникают трудности, связанные с вычислительной сложностью, что, в свою очередь, стимулирует поиск альтернативных методов, адаптированных для компьютерной реализации.

Последнее время довольно распространёнными становятся клеточно-автоматные методы моделирования [1], которые привлекают своей простотой, универсальностью и естественным параллелизмом. В частности, в работе [2] продемонстрированы возможности метода непрерывных асинхронных клеточных автоматов по моделированию различных процессов, в том числе и волновой динамики, которая, как известно, является одним из решений уравнения Навье — Стокса [3]. При этом модель не предусматривает перемещения вещества, а наблюдение явления турбулентности невозможно.

Для устранения указанного недостатка и построения модели, которая даст возможность исследовать турбулентность, предложена модификация, суть которой состоит в реализации вероятностного механизма передвижения клеточных автоматов вдоль компонент векторов скоростей. Под передвижением в нашем случае следует понимать дублирование содержания соседних ячеек при осуществлении перемещения. Введение такого подхода определяется необходимостью моделирования сплошного непрерывного потока, а не потока отдельных дискретных частиц.

1. Постановка задачи

Как известно, турбулентное течение отличается от ламинарного вихревой динамикой, при которой имеет место вращательно-колебательный характер движения потоков вещества (рис. 1) [4]. Турбулентность может возникать в газах, жидкостях или сыпучих

средах за счёт существования сил внутреннего трения — динамической вязкости (η). Кроме вязкости, для образования турбулентного течения существенными параметрами являются скорость (υ), плотность вещества (ρ) и характерные размеры потока (L). Соотношение $\rho L\upsilon/\eta$ или же $L\upsilon/\nu$, где $\nu = \eta/\rho$ — кинематическая вязкость, называют числом Рейнольдса (Re) [5]. Превышение числом Рейнольдса некоторого критического значения $\mathrm{Re}_{\text{кр}}$ определяет возможность возникновения турбулентной динамики. Величина $\mathrm{Re}_{\text{кр}}$ зависит от конкретного вида течения.

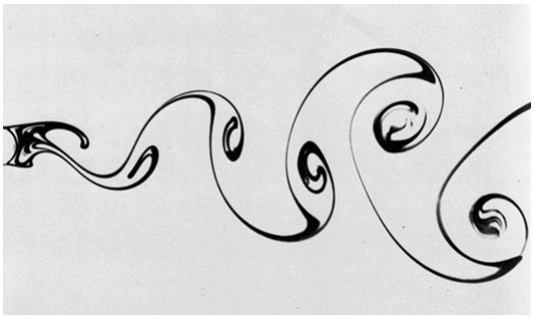

Рис. 1. Пример турбулентного потока (вихревая дорожка Кармана)

В общем случае как ламинарные, так и турбулентные потоки вещества можно описать уравнениями Навье — Стокса, т. е. системой нелинейных дифференциальных уравнений в частных производных [6]:

$$\frac{\partial \overrightarrow{v}}{\partial t} + (\overrightarrow{v} \cdot \nabla)\overrightarrow{v} = -\frac{1}{\rho}\nabla p + \nu\Delta\overrightarrow{v} + \overrightarrow{f}(\overrightarrow{x}, t); \tag{1}$$

$$\frac{\partial \rho}{\partial t} + \nabla(\rho\overrightarrow{v}) = 0, \tag{2}$$

где $\overrightarrow{v}(\overrightarrow{x}, t)$ — вектор скорости вещества; $p(\overrightarrow{x}, t)$ — давление; $\nu > 0$ — кинематическая вязкость; ρ — удельная плотность; $\overrightarrow{f}(\overrightarrow{x}, t)$ — внешняя сила; ∇ — оператор Гамильтона; Δ — оператор Лапласа. Уравнение (2) отображает закон сохранения массы. Неизвестными величинами являются скорость $\overrightarrow{v}(\overrightarrow{x}, t)$ и давление $p(\overrightarrow{x}, t)$.

В рамках этой работы предлагается клеточно-автоматная аппроксимация уравнения Навье — Стокса. Таким образом, динамическая картина, полученная в результате клеточно-автоматных взаимодействий, будет альтернативой численному решению уравнения Навье — Стокса. Основная задача данной работы — демонстрация принципиальной возможности построения модели турбулентных потоков на основе непрерывных вероятностных асинхронных клеточных автоматов.

2. Описание клеточно-автоматной модели

Опишем структуру клеточно-автоматного поля в случае моделирования двумерных потоков жидкости (рис. 2). Поле содержит три слоя: 1 — слой давления P, 2 — слой X-компоненты скорости V_x, 3 — слой Y-компоненты скорости V_y. Ячейки поля принимают вещественные непрерывные значения.

Площадь ячейки определяется размерностью клеточно-автоматного поля в соотношении к геометрическим размерам фрагмента моделируемой системы.

Процесс моделирования представляет собой итерационный цикл клеточно-автоматных взаимодействий с использованием асинхронной схемы. Данная схема предусматривает циклическое выполнение трех типичных шагов:

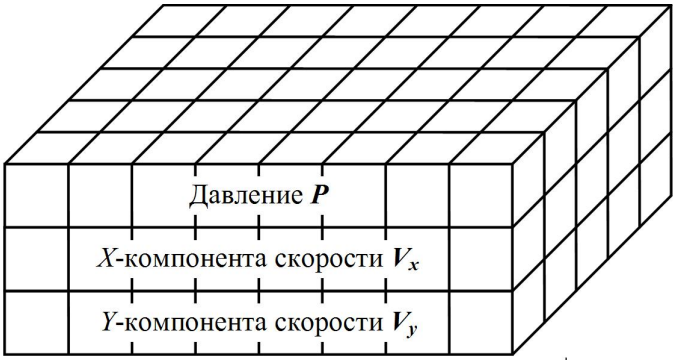

Рис. 2. Структура клеточно-автоматного поля двумерной модели потока

1. На клеточно-автоматном поле случайным образом выбирается некоторая клетка ($i = 1$) с целочисленными координатами x^1, y^1. При этом все клетки выбираются равновероятно.

2. Случайным равновероятным образом выбирается некоторая соседняя клетка ($i = 2$) с целочисленными координатами x^2, y^2. В качестве схемы соседства принята окрестность Неймана, т. е. у клетки есть только четыре соседа (рис. 3).

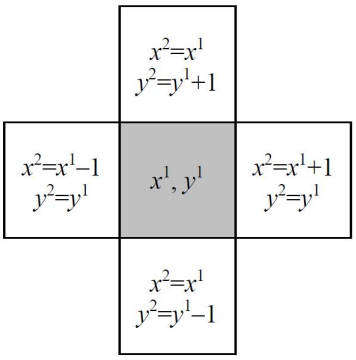

Рис. 3. Окрестность Неймана и координаты клеток

3. Происходит клеточно-автоматное взаимодействие между двумя клетками, суть которого заключается в модификации непрерывных значений соответствующих слоёв клеток согласно следующей системе уравнений:

$$\begin{cases} c_1^{i\prime} = c_1^i + k_1((x^1 - x^2)(c_2^2 - c_2^1) + (y^1 - y^2)(c_3^2 - c_3^1)), \\ c_2^{i\prime} = c_2^i + k_2(x^1 - x^2)(c_1^2 - c_1^1) + k_3(3 - 2i)(c_2^2 - c_2^1), \\ c_3^{i\prime} = c_3^i + k_2(y^1 - y^2)(c_1^2 - c_1^1) + k_3(3 - 2i)(c_3^2 - c_3^1). \end{cases} \tag{3}$$

Здесь $i = 1, 2$ — значение индекса, задающее выбранную и соседнюю клетки с координатами (x^1, y^1) и (x^2, y^2) соответственно; c_j^i и $c_j^{i\prime}$ — значения ячеек в моменты времени t и $t + 1$ соответственно: $c_1 \equiv P$, $c_2 \equiv V_x$, $c_3 \equiv V_y$; $k_1, k_2, k_3 > 0$ — коэффициенты пропорциональности, которые отражают пространственно-временные параметры клеточно-автоматной модели, а также удельную плотность и кинематическую вязкость. В частности, смысл коэффициента k_1 состоит в определении интенсивности изменения давления при различных значениях скорости потока вещества во взаимодействующих клетках. Коэффициент k_2 определяет интенсивность изменения компонентов векторов скоростей пропорционально соответствующему градиенту давления в двух соседних

клетках. Коэффициент k_3 определяет интенсивность «диффузии скорости», то есть является клеточно-автоматным отображением кинематической вязкости. Если выразить все величины в системе Си, то размерность коэффициента k_1 — Па·с/м, коэффициента k_2 — обратная величина м/(Па·с), а коэффициент k_3 является безразмерным параметром. Тут следует подчеркнуть, что разность координат двух соседних клеток $(x^1 - x^2)$ или $(y^1 - y^2)$ в системе (3) необходимо воспринимать как одно из значений $-1, 0, +1$, а не как некоторое расстояние.

Система уравнений (3) описывает изменение значений соответствующих ячеек во время одного элементарного взаимодействия клеточных автоматов и является своеобразной аппроксимацией численного решения уравнения Навье — Стокса (1), (2). Систему (3) можно представить в виде $c_j^{i\prime} = c_j^i + \Delta c_j^i$. Совершенно очевидно, что для обеспечения адекватности процесса моделирования прирост или уменьшение некоторого значения ячейки Δc_j^i должны быть как можно меньшей величиной, регулируемой коэффициентами k_1, k_2, k_3, при этом размер клеточно-автоматного поля должен быть как можно больше. С другой стороны, это неизбежно приведёт к слишком долгому процессу моделирования. Здесь по аналогии с различными многочисленными схемами решения возникает проблема поиска компромисса между точностью решения и временем, необходимым для его получения. Количественный анализ точности описываемого подхода не рассматривается и является предметом дальнейших научных исследований. Основной целью данной работы является построение качественной клеточно-автоматной модели турбулентной динамики.

Объясним вид системы уравнений (3), рассмотрев для простоты и наглядности одномерный случай ($y^1 = y^2$) без учета вязкости ($k_3 = 0$). При этом система (3) примет вид

$$\begin{cases} c_1^{i\prime} = c_1^i + k_1(x^1 - x^2)(c_2^2 - c_2^1), \\ c_2^{i\prime} = c_2^i + k_2(x^1 - x^2)(c_1^2 - c_1^1). \end{cases} \tag{4}$$

Первое уравнение системы отображает модификацию давления P для двух взаимодействующих соседних клеток. Если рассматривать две клетки как некий микрофрагмент системы, то в первом приближении можно считать, что изменение давления ΔP пропорционально разности векторов скоростей. Для наглядности обратимся к рис. 4,*а*. Пусть выбранная клетка ($i = 1$) с координатой x^1 находится слева, а соседняя клетка ($i = 2$) с координатой $x^2 = x^1 + 1$ — справа. Пусть векторы скоростей направлены вправо, причем $V_1 > V_2 > 0$. Тогда как для избранной, так и для соседней клеток прирост давления составляет $\Delta P = \Delta c_1^i = k_1(x^1 - x^2)(c_2^2 - c_2^1) = k(-1)(V_2 - V_1)$. Так как $V_1 > V_2 > 0$, то $\Delta P > 0$, что и видно на рис. 4,*а*. Если поменять местами выбранную клетку ($i = 1$) и соседнюю ($i = 2$), картина не изменится, поскольку $\Delta P = k_1(+1)(V_2 - V_1)$, но в этом случае $V_2 > V_1$, значит, $\Delta P > 0$. Можно проанализировать и другие случаи (рис. 4,*б*–*г*), причём все они должны отражать физику моделируемого явления, то есть давление должно увеличиваться, когда приток вещества превышает отток, и наоборот.

В частности, на рис. 4,*б* показан случай, когда $V_2 > V_1 > 0$, следовательно, при этом $\Delta P = k_1(-1)(V_2 - V_1) < 0$. На рис. 4,*в*,*г* показаны случаи, когда векторы скоростей направлены влево, то есть имеют отрицательные значения. При этом рис. 4,*в* соответствует случаю $V_1 < V_2 < 0$, и здесь результат $\Delta P < 0$ получается аналогично изображенному на рис. 4,*б*. Рис. 4,*г* соответствует случаю $V_2 < V_1 < 0$, и здесь результат $\Delta P > 0$ получается аналогично изображенному на рис. 4,*а*.

Второе уравнение системы (4) отражает изменение вектора скорости микрофрагмента вещества под действием градиента давления. Как можно видеть, оно полностью

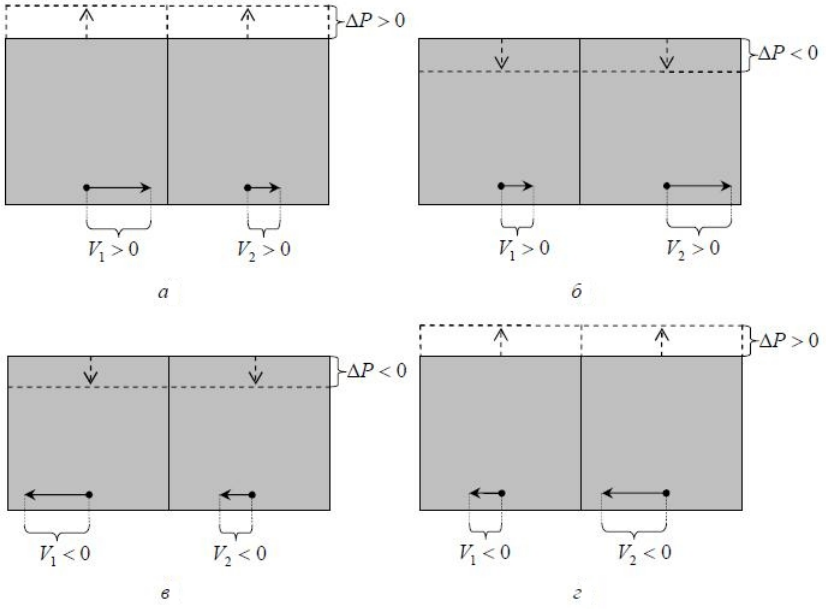

Рис. 4. Демонстрация правил клеточно-автоматных взаимодействий в случае изменения давления

аналогично первому уравнению системы. Для объяснения обратимся к рис. 5. Здесь в упрощенном виде показана модификация векторов скоростей двух взаимодействующих клеток под действием градиента давления. Если сравнить рис. 4,*а*,*б* с рис. 5 и отметить, что давление всегда является положительной величиной, то можно увидеть прямую аналогию между приращением или уменьшением скорости за счет разности давлений (рис. 5) и соответствующим приращением или уменьшением давления, обусловленным разностью скоростей в двух соседних клетках (рис. 4,*а*,*б*).

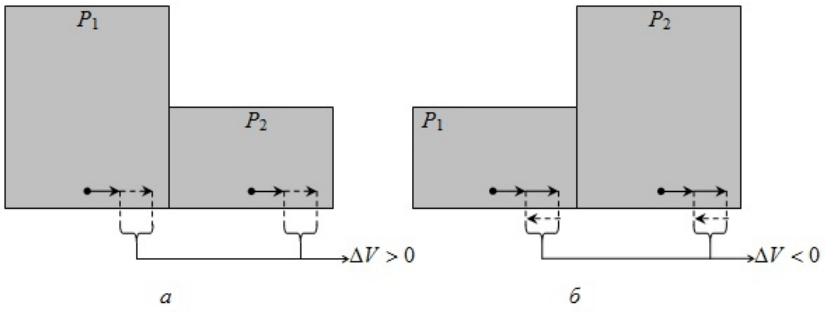

Рис. 5. Демонстрация правил клеточно-автоматных взаимодействий в случае модификации векторов скорости

Здесь следует заметить, что изменение вектора скорости за единицу времени (ускорение) пропорционально не только градиенту давления, но и массе вещества в элементе объёма, которая, в свою очередь, является функцией плотности, зависящей от давления сжимаемой среды. Но мы, в первом приближении, пренебрегаем этой зависимостью.

Рассмотрим слагаемые в системе (3), содержащие коэффициент пропорциональности k_3. Они отражают вязкость (трение соседних слоев вещества) и по сути пред-

ставляют собой диффузионную составляющую компонентов векторов скорости. Эти слагаемые уравновешивают значения векторов скорости в соседних клетках.

Проиллюстрируем этот процесс с помощью рис. 6. Пусть в момент времени t взаимодействуют две клетки: выбранная ($i = 1$) с вектором скорости V_1 и соседняя ($i = 2$) с вектором скорости V_2, причем $V_1 > V_2$. Проанализируем динамику изменения скорости. Для выбранной клетки $\Delta V_1 = k_3(3-2)(V_2 - V_1) = k_3(V_2 - V_1) < 0$, а для соседней $\Delta V_2 = k_3(3-4)(V_2 - V_1) = k_3(-1)(V_2 - V_1) > 0$, что видно из рис. 6.

Если поменять местами выбранную клетку с соседней, результат остаётся без изменений — компоненты векторов скоростей в следующий момент времени $t+1$ стремятся к усреднённому значению.

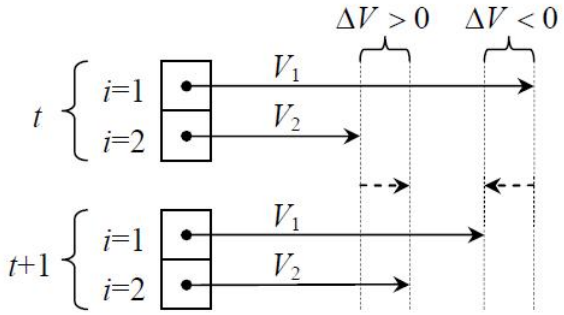

Рис. 6. Иллюстрация влияния составляющей системы (3), которая учитывает вязкость вещества — векторы скорости двух соседних взаимодействующих клеток стремятся к усреднённому значению

До сих пор мы рассматривали «микровзаимодействия» на уровне отдельных клеток. Если запустить асинхронный итерационный цикл взаимодействия на множестве клеточных автоматов (клеточно-автоматном поле), который описывается системой (3), то при отклонении от состояния равновесия можно наблюдать колебательную динамику, как это схематически показано на рис. 7 для одномерного случая.

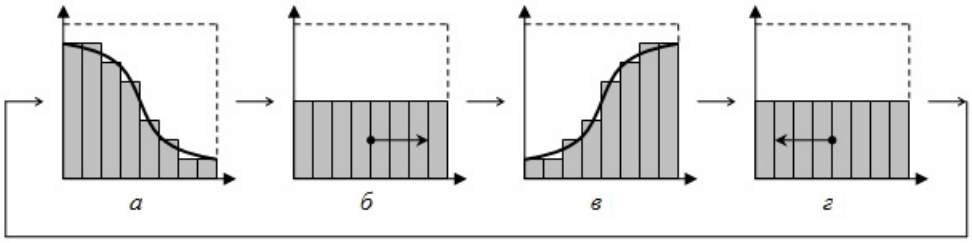

Рис. 7. Демонстрация примера клеточно-автоматной колебательной динамики

В то же время такое поведение системы клеточных автоматов никак не проявляет турбулентную динамику. Это связано с тем, что модель не предусматривает действительного перемещения вещества вместе с моментом импульса, а описывает лишь некую «упругую» среду. Для устранения этого недостатка дополним описанную выше систему итерационных функций (3) функцией перемещения, которая представляет собой реализацию вероятностного механизма дублирования соседней клетки. Для объяснения сути дополнения обратимся к иллюстрации перемещения отдельной частицы на

клеточно-автоматном поле. Пусть имеем элементарное поле размером 5×5 клеток, как это показано на рис. 8. Предположим наличие некоторой дискретной частицы, которая в начальный момент времени находится в нижнем левом углу поля. Заставим частицу передвигаться по полю вдоль вектора V, который приведен на рис. 8,*а*.

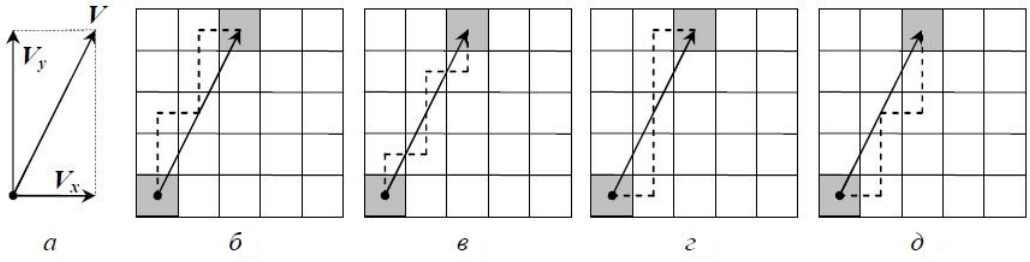

Рис. 8. Демонстрация движения отдельной частицы на клеточно-автоматном поле: *а* — вектор скорости; *б*–*д* — возможные варианты траектории движения частицы

Для этого организуем вероятностный механизм передвижения частицы. Используя метод Монте-Карло, будем определять вероятность перехода частицы в соседнюю клетку. При этом свяжем вероятность перехода с длиной соответствующей компоненты вектора скорости (V_x и V_y). Таким образом, если длина компоненты вектора скорости V_y в 2 раза больше длины V_x, то в среднем частица будет переходить в верхние соседние клетки в 2 раза чаще, чем в клетки, расположенные справа от частицы. Следовательно, глобальная динамика поведения частицы — движение вдоль вектора скорости V, как показано на рис. 8,*б*–*д*. Кроме того, привязав максимальную величину векторов скорости к единичной вероятности осуществления перехода, можно организовать движение частиц с различными скоростями.

Подобным же образом введём описанный подход в нашей модели; существенным отличием здесь является не перемещение частиц в смысле обмена местами в клетках поля, а дублирование содержания соседних ячеек при осуществлении перемещения, как показано на рис. 9. Введение дублирования вместо обмена содержанием соседних клеток при перемещении определяется, в нашем случае, моделированием сплошного непрерывного потока, а не потока отдельных дискретных частиц.

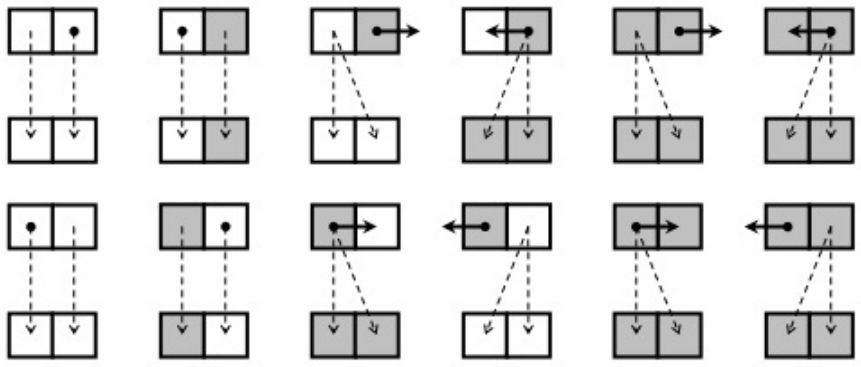

Рис. 9. Правила клеточно-автоматных взаимодействий в случае перемещения вещества в пределах сплошного потока (дублирование при перемещении)

Несмотря на нарушение законов сохранения на микроуровне (во время локальных микровзаимодействий клеточных автоматов), глобальная макродинамика такой системы вполне адекватна, что можно проиллюстрировать с помощью рис. 10, где показан пример асинхронного вероятностного перемещения фрагмента сплошного вещества в виде некоторой совокупности частиц.

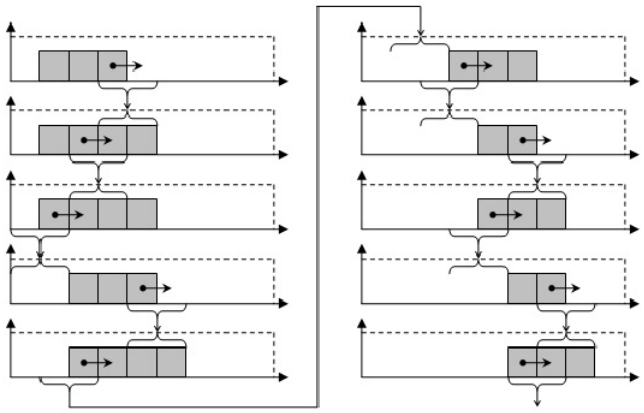

Рис. 10. Демонстрация перемещения вещества

3. Результаты вычислительного эксперимента

Для апробации предложенной в данной работе модели реализован вычислительный эксперимент по наблюдению турбулентной динамики на примере потока вещества в трубе, которая имеет препятствие (рис. 11, 12).

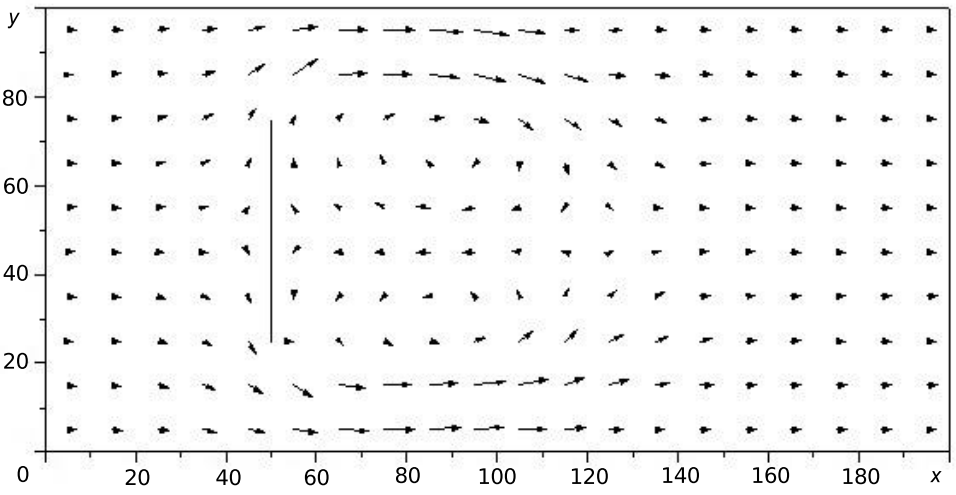

Рис. 11. Векторное поле скоростей

На рис. 11 и 12 приведён пример результата моделирования явления турбулентности на поле клеточного автомата размера 100×200. В частности, приведены векторное поле скоростей (рис. 11) и распределение давления (рис. 12).

Значения коэффициентов системы (3): $k_1 = 100; k_2 = 0{,}00001; k_3 = 0{,}1$.

Граничные условия:

1) левая граница: $P = 100; V_x = 0{,}01$;

2) верхняя и нижняя границы: $V_y = 0$;

Рис. 12. Распределение давления (черный цвет — максимальное давление, белый — минимальное)

3) препятствие (с обеих сторон): $V_x = 0$;

4) правая граница — «прозрачная стенка», то есть тут $P(x_\text{п}, y) = (x_\text{п}-1, y)$, $V_x(x_\text{п}, y) = V_x(x_\text{п} - 1, y)$, $V_y(x_\text{п}, y) = V_y(x_\text{п} - 1, y)$, где $x_\text{п}$ — координата клетки, находящейся на правой границе.

Вероятность перемещения клетки (дублирования содержимого соседней клетки) определялась методом Монте-Карло. Если неравенство $\zeta \leqslant V_{x,y}$ выполнялось, где $\zeta \in [0, 1]$ — некоторая случайная величина, а $V_{x,y}$ — X- или Y-компонента вектора скорости, то перемещение клетки происходило.

Заключение

Предложена клеточно-автоматная аппроксимация уравнения Навье — Стокса, которое описывает динамику вещества в сплошных средах. Реализован вычислительный эксперимент, позволяющий исследовать турбулентную динамику на примере потока вещества в трубе с препятствием. Приведены векторное поле скорости и распределение давления для двумерного случая. Количественный анализ предложенной клеточно-автоматной модели — предмет дальнейших научных исследований.

ЛИТЕРАТУРА

1. *Бандман О. Л.* Клеточно-автоматные модели пространственной динамики // Системная информатика. 2005. № 10. С. 57–113.
2. *Жихаревич В. В., Остапов С. Э.* Моделирование процессов самоорганизации и эволюции систем методом непрерывных асинхронных клеточных автоматов // Компьютинг. 2009. Т. 8. № 3. С. 61–71.
3. *Темам Р.* Уравнения Навье — Стокса. Теория и численный анализ. 2-е изд. М.: Мир, 1981. 408 с.
4. `http://ru.wikipedia.org/wiki/Турбулентность`
5. `http://ru.wikipedia.org/wiki/Число_Рейнольдса`
6. `http://ru.wikipedia.org/wiki/Существование_и_гладкость_решений_уравнений_Навье_-_Стокса`

ИСТОРИЧЕСКИЕ ОЧЕРКИ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЁ ПРИЛОЖЕНИЯМ

DOI 10.17223/20710410/18/7

УДК 519.7

ОБ ИСТОРИИ КРИПТОГРАФИИ В РОССИИ[1]

Н. Н. Токарева

Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск

E-mail: tokareva@math.nsc.ru

Представлен материал по истории криптографии в России. До сих пор она остаётся мало изученной и во многом засекреченной; в то же время к ней наблюдается повышенный интерес. Кратко рассмотрен период с середины XVI века до настоящего времени. Иногда хронологический порядок изложения нарушается, внимание обращается к отдельным событиям и людям, повлиявшим на ход истории криптографии или своеобразно его отразившим.

Ключевые слова: *криптография, криптоанализ, история России, П. Л. Шиллинг, В. И. Кривош-Неманич, Г. И. Бокий, В. А. Котельников.*

1. Появление криптографии в России

Первые профессиональные криптографы на Руси появились при Иване Грозном (1530–1584). Они находились на службе в Посольском приказе, созданном им в 1549 г. и отвечавшем за внешнюю политику страны. Криптографы разрабатывали так называемые «азбуки», «цифири», «цифры» или шифры, как они стали называться позднее. Сначала это были простые шифры замены.

Но всё-таки, как отмечает в своей книге [43] исследователь истории шифровального дела Т. А. Соболева, первым из российских государей, осознавшим всю важность криптографии для безопасности страны, стал Пётр I (1672–1725). Он поставил шифровальную службу действительно на профессиональную основу. С 1700 г. вся работа по созданию шифров, шифрованию и расшифрованию велась в цифирном отделении Посольского приказа, а позднее, с 1709 г., — в Посольской канцелярии. Криптографическая служба в это время находилась под постоянным и непосредственным контролем государственного канцлера Гавриила Ивановича Головкина и вице-канцлера Петра Павловича Шафирова. Ими же заслушивались отчеты о перехваченных иностранных шифрах, что может свидетельствовать и о начале криптоаналитической деятельности. Затем криптографическая работа велась в Первой экспедиции Коллегии иностранных дел, где она стала строго регламентироваться и засекречиваться.

Типичным шифром того времени был шифр простой замены: каждая буква алфавита заменялась новым знаком, буквой или сочетанием букв. Кроме того, добавлялись «пустышки» — незначащие символы, а также вводились специальные обозначения для

[1]Исследование выполнено при поддержке РФФИ (проекты № 10-01-00424, 11-01-00997, 12-01-31097) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 02.740.11.0429).

часто употребимых в определённом контексте слов или словосочетаний (такой словарь назывался «суплемент»). Авторство некоторых цифирей принадлежало лично Петру I.

У Петра I имелся даже специальный блокнот с шестью шифрами, которыми он активно пользовался. Однако в переписке случались и некоторые казусы. В книге [43] приводится такой пример. Пётр I часто употреблял французские шифры. В одном из писем фельдмаршал Г. Б. Огильви жаловался Головкину: «Французские цифирные грамотки нихто читать не может, тако не знаю, что на них ответствовать...» и писал напрямую Петру I: «...никого здесь нет, который бы французское ваше мог разуметь, понеже Рен ключ от того потерял... Изволте ко мне через цифирь мою писать, чтоб я мог разуметь...», на что Пётр I отвечал: «Французскою азбукою к вам писали для того, что иной не было. А которую вы перво прислали, и та не годна, понеже так, как простое письмо, честь можно. А когда другую прислал, то от тех пор ею, а не французскою к вам пишем. А и французской ключ послан». Кажется, что потеря ключа в то время не сильно озадачивала переписчиков. Однако позднее к Огильви был приставлен А. И. Репнин, доверенное лицо Петра I, которому было поручено наблюдать за действиями фельдмаршала.

Методы шифрования и сама шифрованная переписка петровской эпохи наиболее полно представлены в многотомном издании «Письма и бумаги императора Петра Великого» (под редакцией А. Ф. Бычкова и И. А. Бычкова).

2. Чёрные кабинеты

Криптографическую службу России продолжал курировать вице-канцлер. С 1725 г. этот пост занимал Андрей Иванович Остерман. При нём шифры становятся неалфавитными — кодируются уже комбинации букв, а в качестве шифробозначений теперь используются исключительно цифры. В 1741 г. с приходом к власти Елизаветы Петровны (1709–1761) вице-канцлером и главным директором почт назначается Алексей Петрович Бестужев-Рюмин. С его именем связано появление в России службы перлюстрации (тайного вскрытия почты). Осуществляется эта деятельность в «чёрных кабинетах» — тайных комнатах, имевшихся во всех крупных почтовых отделениях.

Вскрывать письма было непросто. Нужна была необыкновенная аккуратность и изобретательность. А иной раз ничего и не выходило. Например, об одной своей неудаче сообщал перлюстратор Ф. Аш в письме к Бестужеву-Рюмину: «...на письмах нитка таким образом утверждена была, что оный клей от пара кипятка, над чем письма я несколько часов держал, никак распуститься и отстать не мог. Да и тот клей, который под печатями находился (кои я хотя искусно снял), однако ж не распустился. Следовательно же я к превеликому моему соболезнованию никакой возможности не нашел оных писем распечатать без совершенного разодрания кувертов. И тако я оные паки запечатал и стафету в ея дорогу отправить принуждён был...» [43]. Со временем в чёрных кабинетах появился целый штат сотрудников: одни вскрывали и запечатывали письма, другие прошивали их ниткой и подделывали печати, третьи копировали содержимое, четвёртые переводили, пятые занимались дешифрованием и т. д. Их деятельность держалась в строгом секрете.

Государственные интересы оказывались выше доводов морали. И не только в России. Надо сказать, что в европейских странах чёрные кабинеты начали свою работу лет на сто раньше.

В 1742 г. на «особливую должность» в Коллегию иностранных дел был принят первый профессиональный криптоаналитик. Им стал математик Христиан Гольдбах (1690–1764), получивший через год первые успехи на новом поприще. Он дешифро-

вал ряд французских дипломатических шифров. Позднее криптоанализом занимались математики Ф. Эпинус и И. Тауберт; русские криптографы братья Ерофей и Фёдор Коржавины и другие [36].

3. Первая половина XIX века

С начала XIX века вся криптографическая деятельность, а также руководство службой перлюстрации осуществляются в Канцелярии только что созданного (1802 г.) Министерства иностранных дел. Непосредственно руководит Канцелярией (с 1810 г.) статс-секретарь Карл Васильевич Нессельроде, позднее ставший министром иностранных дел и государственным канцлером.

К числу ярких успехов того времени относится дешифрование военной переписки Наполеона. Этот факт сыграл важную роль в исходе Отечественной войны 1812 г. и поражении наполеоновской армии.

— Нам очень сильно помогло то, что мы всегда знали намерения вашего императора из его же собственных депеш <...>

— Я считаю очень странным, что Вы смогли их прочесть. Кто-нибудь, наверное, выдал Вам ключ?

— Отнюдь нет! Я даю Вам честное слово, что ничего подобного не имело места. Мы просто дешифровали их.

(Из разговора, состоявшегося после войны между императором Александром I и командующим одним из корпусов армии Наполеона маршалом Макдональдом.)

Интересно, что выдающийся русский учёный Павел Львович Шиллинг (1786–1837) — электротехник, изобретатель первого электромагнитного телеграфа[2] и электрической мины, собиратель ценнейших коллекций китайских и японских рукописей, учёный-востоковед, отважный военный, участвовавший в сражениях Отечественной войны 1812 г. и награждённый одной из самых почётных наград — саблей с надписью «За храбрость», блестящий игрок в шахматы, «весельчак, отличный говорун» и, кстати, петербургский знакомый А. С. Пушкина и К. Н. Батюшкова — был, кроме того, одним из крупнейших криптографов XIX века! И эта особая сторона его многогранной деятельности долгое время оставалась засекреченной. Даже сейчас она ещё не исследована должным образом.

Рис. 1. П. Л. Шиллинг. Портрет и мини-потрет на советской марке

[2]Получивший распространение телеграф С. Морзе был запатентован в 1837 г. — спустя пять лет после изобретения П. Л. Шиллинга.

Известно, что с 1803 г. П. Л. Шиллинг работал в МИД, в которое он вернулся и после окончания Отечественной войны. Именно он организовал министерскую литографию — способ плоской печати, только что входивший в употребление в Европе. До этого шифрдокументы копировались от руки. С 1818 г. барон Шиллинг стал заведующим цифирной экспедицией Канцелярии МИД, занимающейся разработкой шифров. Ему принадлежит изобретение биграммного шифра, в котором шифровались не отдельные буквы, а их двойные сочетания, биграммы. При этом некоторые статистические зависимости снимались за счёт того, что в биграммы объединялись буквы, находящиеся друг от друга на большом расстоянии [43].

4. Шифры второй половины XIX века

Во второй половине XIX века криптографическая служба России перестала быть привилегией МИД и была создана ещё в двух ведомствах: военном и Министерстве внутренних дел. Тем самым существенно расширялись сферы использования криптографии, её значение в жизни государства неуклонно росло. Появилась классификация шифров по их назначению и области применения. Были выделены шифры военного ведомства (включая императорские), шифры жандармерии, гражданские шифры (например, Министерства финансов), агентурные шифры, предназначенные для связи с разведчиками.

Активно использовались биграммные шифры, введённые бароном Шиллингом; биклавные шифры — шифры многозначной замены, определяемой двумя ключами (автор — барон Н. Ф. Дризен); шифровальные коды — шифры, использовавшие цифры в качестве шифралфавита; коды с перешифровкой.

Термины «шифр» и «ключ» тогда ещё были синонимами. Ключом назывался, по сути, принцип шифрования сообщения, его алгоритм. Раскрытие ключа было равносильно гибели всей криптографической системы. Не так будет обстоять дело в XX веке, когда ключ станет сменной частью сложной криптосистемы. Раскрытие ключа не будет приводить к краху шифра, а будет означать лишь то, что ключ необходимо поменять.

Цифирный комитет устанавливал предельный срок действия каждого шифра в среднем от трёх до шести лет. Но любопытно, что многие шифры использовались и по истечении их «срока годности», что, несомненно, сказывалось на тайне переписки. Кроме того, имели место серьёзные нарушения. Так, представлялось возможным снова использовать скомпрометированные шифры в других регионах или спустя некоторое время. Например, русский биграммный ключ № 356 использовался почти 25 лет! История его такова. Он был введен в действие в 1869 г. «в консульствах на Востоке». В 1888 г. его экземпляр был украден из Российской миссии в Пекине. Вследствие этого шифр был выведен из употребления, но лишь на некоторое время. Несмотря на очевидность компрометации, в начале 90-х годов XIX века шифр вновь ввели в действие, но уже в другом регионе. Он был направлен в Амстердам, Гаагу, Берн, Женеву, Стокгольм и другие города. В 1898 г. произошла ещё одна компрометация этого шифра: один его экземпляр был потерян начальником Адриатической эскадры. Вероятно, именно это событие, как пишет Т. А. Соболева [43], наконец заставило руководителей шифрслужбы окончательно изъять ключ № 356 из употребления. В соответствующем заключении было указано: «вследствие почти 1/4-векового всемирного использования». Лучше и не скажешь.

Но в целом криптографическая служба России в то время находилась на достаточно высоком профессиональном уровне. Очень быстро и эффективно работали чёрные

кабинеты. «Сохранить тайну шифра в Петербурге особенно трудно», — отмечал канцлер Германской империи Отто фон Бисмарк [13].

Один из бывших сотрудников спецслужбы перлюстратор С. Майский вспоминал: «Иностранная дипломатическая переписка попадала в руки российских специалистов практически полностью. „Чёрные кабинеты“, разумеется, существовали везде, даже в самых демократических республиках Америки и Старого Света. Но справедливость требует сказать, что нигде в мире „чёрный кабинет“ не работал так чисто, как в России, и в особенности в Петрограде» [13].

Интересно, что император Александр III в течение всего своего правления отказывался читать выписки из писем, добытые в чёрном кабинете. После вступления на престол и знакомства со службой перлюстрации он заявил: «Мне этого не нужно». Не так поступали другие императоры.

В Военном ведомстве второй половины XIX века чаще всего использовались «словарные ключи». Работали они так. Составлялся словарь небольшого объёма (до 1 000 словарных величин), каждому слову которого соответствовал код — трёх- или четырёхзначное число. Шифрование велось непосредственной заменой по словарю. Такие «военные ключи» действовали длительное время, при этом относительно часто менялся словарь.

Подобными (словарными) шифрами пользовался и Николай II. Примечательно, что словари Его Императорского Величества, предназначенные для деловой переписки, содержали множество слов с эмоциональной окраской. Например, такие: «бескорыстный», «безотрадный», «благородный», «болезненный», «ни под каким видом», «молва», «нелепый», «неправдоподобный» и др. [43].

Особое положение занимали *агентурные шифры*, использовавшиеся разведчиками и агентами царской охранки. Одним из основных требований, предъявляемых к таким шифрам, была «скрываемость», «безуликовость» их документации. Ключ должен был запоминаться или легко извлекаться из «окружающих предметов» (например, распространённых книг), наличие которых никак не компрометировало агента. Сам процесс шифрования должен был быть быстрым и простым. К числу таких шифров относились варианты шифра Цезаря, книжные шифры, шифры перестановок.

Книжный шифр при правильном использовании мог быть действительно очень надёжным и безуликовым. Выбиралась определённая книга, в которой номера страниц, строк и букв в строках служили шифробозначениями для шифруемых букв. Подобные шифры массово использовались и в русском подполье конца XIX века. Однако сотрудники «чёрных кабинетов» обнаружили несколько «зацепок» к раскрытию таких шифров. Оказалось, что корреспонденты предпочитали находить в книгах буквы, стоящие неподалеку от начала строки или страницы. Так, подсчёт номера буквы занимал меньше времени, да и риск ошибки был ниже. А вот редкие буквы обычно имели большие номера, так как в начале строк они попросту не попадались. Другой «зацепкой» было изъятие и внимательное изучение личной библиотеки каждого подозреваемого.

Подробнее о российской криптографии XIX века и начала XX века можно прочитать в [6 – 10, 14 – 21].

5. Криптограф-соловчанин

В 1898 г. сотрудник российской криптографической службы, коллежский регистратор Владимир Иванович Кривош (1865–1942) был послан в Париж для изучения иностранного опыта в делах перлюстрации. В том числе устройства местного чёрного кабинета.

Любопытно описание этого учреждения, которое приведём по книге [43]. «Парижский чёрный кабинет был устроен аналогично петербургскому. Эта „секретная часть“ находилась в частном доме. Официальная вывеска на нём гласила, что здесь располагается землемерный институт. Один из служащих „секретной части“ действительно знал толк в лесоводстве, и если какой-то частный человек туда забредал, то ему давалась вполне квалифицированная справка. В передней комнате, куда мог прийти с улицы кто угодно, на стенах висели карты, планы земельных участков, а на столах лежали свежие газеты и письменные принадлежности. Из этой комнаты была дверь в следующую, в которой также не было ничего секретного, но был шкаф, служивший дверью в третью комнату. Таким образом, чтобы пройти в действительно секретную часть, необходимо было идти через шкаф, зная, как его открыть (наступить одновременно на две дощечки на полу и нажать одно из украшений шкафа). Дверь автоматически сама запиралась за прошедшим через неё. В следующей комнате была перлюстрационная часть, имевшая сообщение пневматической почтой с главным почтамтом. Все прибывающие в Париж дипломатические пост-пакеты прежде всего отправлялись сюда. Здесь проводилась их регистрация и передача в кабинеты дешифровальщикам, занимавшимся с ними по двое. После дешифрования и фотографирования письма вновь заклеивались и отправлялись по той же трубе пневматическим способом на почтамт. Для президента ежедневно выпускался „листок“ со всеми полученными за сутки сведениями — нечто вроде дипломатической газеты».

Поездка не прошла даром. Вместе с французскими специалистами были раскрыты шифры, использовавшиеся Японией, Англией и Германией. В. И. Кривош, словак по происхождению, стал одним из ведущих российских криптографов. За предложенные им усовершенствования российской криптографической службы он получил орден Святого Владимира 4-й степени из рук П. А. Столыпина. Владимир Иванович постоянно приглашался для ведения заседаний государственных комиссий различного уровня секретности.

Удивительна судьба этого человека. В. И. Кривош родился в одной из деревень Австро-Венгерской монархии. Он рос вблизи строящейся железной дороги и мечтал: когда дорога будет достроена, он уедет в далёкие края. Какими же суровыми и фантастическими они оказались...

Его родители были мелкими предпринимателями, которым хватило средств отправить на учёбу только одного сына, Владимира. Его одарённость открыла ему поистине удивительные перспективы. Сначала были гимназии: немецко-словацко-венгерская и итальянско-хорватская. Потом с поразительной быстротой — Королевская Ориентальная Академия, Петербургский университет, парижская Сорбонна. В 1890 г. Владимиру Ивановичу 25 лет. Он блестяще образован, изучил математику и статистику, владеет пятнадцатью языками (к концу его жизни это число достигнет сорока!), написал диссертацию по арабской литературе и уже стал незаменимым российским специалистом в области криптографии и стенографии. Вскоре он становится Главным цензором газет и журналов Российской империи и занимает множество «особых» и «сверхсекретных» должностей. Царское правительство использует его талант в самых разных областях.

Однако в 1915 г. он попадает под подозрение в шпионаже. За этим следует разжалование и ссылка в Сибирь. И возвращение в революционный Петербург в 1917-м. Встреча и работа с В. И. Лениным, который зачисляет В. И. Кривоша в состав наркомата иностранных дел. Так начинается новый, советский, период его жизни.

А дальше, как пишет Любомир Гузи [23], исследователь жизни и творчества выдающегося криптографа, «жизненный путь этого человека напоминает шутку потерявше-

го всякую объективность биографа-графомана». Кривоша арестовывают: его прошлое дискредитирует советскую власть. Но расстрелять лучшего специалиста не решаются. Из тюрьмы он переводится на службу в разведку, потом становится переводчиком-дешифровальщиком Особого отдела ВЧК. Новый арест. И последовавший затем перевод в Спецотдел на разработку сложнейших шифров и их дешифрование. Вскоре «за принятие мер к выезду из страны» Кривош арестовывается и приговаривается к расстрелу. Но снова помилован. В мае 1922 г. — очередное освобождение и очередное назначение в контрразведку. Год спустя — опять арест «за несанкционированные контакты с представителями чехословацкой миссии». В тюрьме он ожидает то расстрела, то ссылки в лагерь. Кривош временно теряет зрение, но, когда оно возвращается, с радостью читает тюремную библиотеку и занимается переводами. Он приговаривается к 10-летнему заключению в концлагере, который ему разрешают выбрать самому — выбирает Соловки[3]. Главным образом потому, что первую волну заключённых составили преимущественно интеллектуалы бывшего режима.

На Соловках Кривош выбирает псевдоним «Тот, у которого ничего нет», что по-словацки звучит как «Нема нич». Он работает ботаником, зоологом, орнитологом, переводчиком, преподаёт иностранные языки, основывает оркестр, становится председателем научной комиссии по фауне и флоре Севера России.

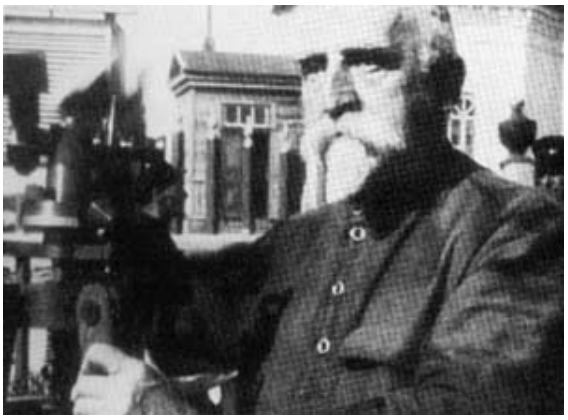

Рис. 2. В. И. Кривош-Неманич, узник СЛОНа

В 1928 г. Кривош-Неманич выходит на свободу. Дома его встречает жена, которая не отказалась от мужа во время всех преследований. До 1936 г. этот удивительный человек (принявший фамилию Кирпичников) работает в Министерстве иностранных дел, но вернуться на словацкую родину ему не удается. Во время войны он живет в эвакуации в Уфе, где преподаёт иностранные языки. Умер Кривош-Неманич в августе 1942 г. Хоронил его сын, однако через несколько лет останки выдающегося криптографа царской и советской России были перемещены в братскую могилу, следы которой затерялись [45]...

6. Первая мировая война

Общий недостаточный уровень подготовки России к войне отразился и на работе криптографической службы.

[3]Соловки, или СЛОН, — Соловецкий лагерь особого назначения — первый концентрационный лагерь Советской России. Организован в 1923 г. на базе древнего Соловецкого монастыря, расформирован в 1933 г.

В то время в российской армии практически отсутствовала надёжная проволочная телеграфная связь, поэтому основное взаимодействие между частями велось по радиосвязи. Но никакого отлаженного механизма использования шифрованной радиосвязи не было. Вследствие беспорядка с распределением и согласованием шифров радиостанции часто «не понимали» друг друга. Им приходилось передавать свои сообщения открытым текстом...

«Такое легкомыслие очень облегчало нам ведение войны на Востоке, иногда лишь благодаря ему и вообще возможно было вести операции», — вспоминал немецкий военачальник М. Гофман, позднее — командующий германскими войсками на Восточном фронте.

«Русские пользовались своими аппаратами так легкомысленно, как если бы они не предполагали, что в распоряжении австрийцев имеются такие же приемники, которые без труда настраивались на соответствующую волну. Австрийцы пользовались своими радиостанциями гораздо экономнее и осторожнее и, главным образом, для подслушивания, что им с успехом удавалось. Иногда расшифровка удавалась путём догадок, а иногда при помощи прямых запросов по радио во время радиопередачи. Русские охотно помогали „своим“, как они считали, коллегам» — из отзыва М. Ронге — начальника разведывательного бюро австрийского генштаба (см. [13]).

Всё это очень грустно.

Ошибка с передачей специального военного шифра сыграла определённую роль в поражении армии А. В. Самсонова на Мазурских островах у Танненберга [43]. Во время восточно-прусской операции в августе 1914 г. две армии (Самсонова и Ренненкампфа), выступив до завершения мобилизации, должны были оттянуть на себя часть немецких сил, тем самым сорвав основное наступление Германии против Франции. Но сценарий реализовался другой. При взаимодействии двух армий оказалось, что в армии П. К. Ренненкампфа новый шифр уже получен, а старый уничтожен, а в армии Самсонова ещё действовал старый шифр. Поэтому радиопереговоры между ними велись в открытую, чем не могло не воспользоваться немецкое командование. Кроме того, армия Самсонова не имела запасов телеграфной проволоки, командованию и разведке приходилось использовать для связи даже телефоны местных жителей. В то же время посылаемые приказы командующего фронтом о своевременном отходе армий к определённым рубежам просто не доходили до Самсонова. Его армия попала в окружение и героически сражалась, оставшись без какой-либо поддержки. К ней на помощь должна была прийти армия Ренненкампфа, но не пришла: по оценкам историков, это было фактическое предательство. В результате армия Самсонова была уничтожена. Потери составили десятки тысяч убитыми, ранеными и пленными [43]...

В сентябре 1914 г. российскому командованию всё-таки удалось обеспечить войска шифровальными средствами. Однако новый шифр был без труда раскрыт дешифровальной службой Австро-Венгрии уже через пять дней после его введения! Наши противники бесперебойно читали шифрпереписку русской армии. Потом они настолько привыкли к этому, что даже не отдавали приказов до тех пор, пока не получали очередной порции информации от своих дешифровальщиков.

В целом «войну в эфире» мы проиграли. Причинами этого послужили плохая организация шифрованной радиосвязи царских армий, слабость российских шифров и нарушения в их использовании. К этому необходимо добавить и то, что до войны в России не существовало военных дешифровальных отделений (они были только у Франции и Австро-Венгрии). Когда такие отделения были созданы, им не хватало со-

ответствующих специалистов и оборудования — например радиостанций пеленгации и перехвата.

Отметим и ряд успехов нашей криптографической службы. Перед войной и во время войны дешифровальная служба МИД работала довольно результативно. Ею читалась переписка многих иностранных государств (в первую очередь Австрии, Германии, Болгарии, Италии, Турции и др.). Позднее число перехваченных и дешифрованных телеграмм снизилось в связи с тем, что Германия и Австро-Венгрия стали чаще использовать телеграф, а не радиосвязь. В недавно созданных военных дешифровальных отделениях достаточно быстро вскрывались ключи немецкого морского шифра, что позволяло читать немецкие сообщения и приказы.

К числу успешных относится и операция по захвату кодовых книг с затонувшего немецкого крейсера «Магдебург» в 1914 г.

Приведём эту историю, следуя книге [13]. «В августе 1914 года наскочил на мель в восточной части Балтийского моря у острова Оденсхольм лёгкий немецкий крейсер „Магдебург“. Русские моряки сумели достать с этого крейсера кодовые книги ВМС Германии. Для того чтобы скрыть факт захвата кодовых книг с „Магдебурга“ от немцев, русские провели следующую операцию. Немцы не знали, что командир „Магдебурга“ Хабенихт при аварии был тяжело ранен и умирал в госпитале. В операции было решено использовать двойника командира немецкого крейсера. В Шлиссельбурге под охраной жил офицер русского флота И. И. Ренгартен. Он свободно говорил по-немецки и был внешне похож на Хабенихта. Как и рассчитывало русское командование Балтфлотом, немцы сумели выйти с ним на связь. Это было сделано с помощью немецких газет, которые „командир“ заказывал в шведском посольстве. Над буквами одной из статей Ренгартен обнаружил еле видные точки. Помеченные буквы складывались в следующий текст: «Где книги? Если уничтожили их, сообщите так: если утопили, попросите журнал „Иллюстрированные новости“, если сожгли, то „Шахматный журнал Кагана“ — номер, соответствующий номеру котла на „Магдебурге“». Ренгартен заказал „Шахматный журнал Кагана“ номер 14. Именно в этом котле крейсера русскими были сожжены фальшивые кодовые книги и подлинные обложки в свинцовом переплёте. На следующий день к сидящему на камнях „Магдебургу“ подошла немецкая подводная лодка. Высадившаяся из неё на крейсер группа извлекла пепел от „сгоревших кодовых книг“, остатки переплёта и кожи от обложек. Русские подводную лодку „не заметили“. Так немцы убедились в том, что кодовые книги с „Магдебурга“ уничтожены. В результате свой код они не сменили» [13].

Для России это был большой успех. Захваченными шифрами русские поделились с англичанами. Уинстон Черчиль, получивший доступ к этим документам, назвал их «бесценными». Англичане эффективно использовали русский подарок. Они не только дешифровывали ценные телеграммы, но и посылали сообщения от имени германского командования. Одно из таких сообщений привело к крупной победе англичан на море: была уничтожена немецкая эскадра под командованием генерала Шпее осенью 1914 г. недалеко от Южной Америки.

7. «На грани крушения»

Глубокий кризис, который переживала российская криптографическая служба, особенно остро ощущался самими криптографами. Многие из них искренно переживали за судьбу не только своей службы, но и России в целом. Юрий Александрович Колемин, управляющий шифровальной частью МИД, писал в своей докладной записке министру иностранных дел С. Д. Сазонову о необходимости немедленной реорганиза-

ции криптографической службы, находящейся, по его словам, «на грани крушения». Он писал о ничтожных окладах её сотрудников, об их «второсортном положении», а по сути об их ненужности государству. «На каком именно основании, — пишет Колемин, — они должны чувствовать солидарность с интересами своего дела?», ведь «добросовестность нельзя безнаказанно эксплуатировать». В его записке встречаются такие слова, как «крах», «безнадёжность», «банкротство»... Пользуясь активной поддержкой своих служащих, он предлагает организацию нового Отделения, детально разрабатывает принципы его устройства, вкладывает в это дело «всю свою душу»! Но этим планам не суждено было реализоваться. На пороге стоял 1917 год. И история начиналась совсем другая.

8. Глеб Бокий и начало советской криптографии

> По ночам Самбикин долго не мог заснуть от воображения труда на советской земле, освещённого сейчас электричеством. Он вставал с кровати, зажигал свет и ходил в волнении, желая предпринять что-либо немедленно. Он включал радио и слышал, что музыка уже не играет, но пространство гудит в своей тревоге, будто безлюдная дорога, по которой хотелось уйти.
>
> *А. Платонов. Счастливая Москва*

Пятого мая 1921 г. при ВЧК был создан Спецотдел, заведовавший криптографическими делами. Отдел находился на особом положении: его действия координировались непосредственно Политбюро. Распоряжения Спецотдела по всем вопросам шифрования были обязательными к исполнению всеми ведомствами РСФСР. Возглавил новую криптографическую службу Глеб Иванович Бокий (1879–1937), соратник В. И. Ленина.

Об этом человеке трудно найти какую-либо информацию. Особенно непротиворечивую. Историк Т. А. Соболева в своей книге [43] пишет: «Даже в моём собственном окружении, в той самой службе КГБ, которая была детищем Бокия и которую он возглавлял 17 лет, о нём почти никто ничего не знал».

Рис. 3. Г. И. Бокий

Дворянин Г. И. Бокий вступил в Российскую социал-демократическую рабочую партию (РСДРП) в 1900 г. Кстати, его партийный билет был номер 7. «Бокий, как и Сталин, в предреволюционный и революционный период входил в ядро, руководящую верхушку большевистской партии» [43]. На протяжении 20 лет (с 1897 по

1917 г.) он являлся одним из руководителей петербургского большевистского подполья. За это время Бокий двенадцать раз подвергался арестам, провёл полтора года в одиночной камере, два с половиной года — в сибирской ссылке, от побоев в тюрьме получил травматический туберкулёз [37]. Параллельно с революционной деятельностью он учился в Петербургском горном институте, работал гидротехником и горным инженером. Основательно изучал философию и политэкономию. «Работал над своим образованием настолько упорно, что позволял себе спать не более четырёх часов в сутки» [43].

Максим Горький писал о нём так: «Человек из породы революционеров-большевиков старого, несокрушимого закала. Я знаю почти всю его жизнь, всю работу и мне хотелось бы сказать ему о моём уважении к людям его типа, о симпатии лично к нему. Он, вероятно, отнёсся бы к такому „излиянию чувств“ недоумённо, оценил бы это как излишнюю и, пожалуй, смешную сентиментальность» [22].

В советский период Г. И. Бокий не только руководил Спецотделом, но и был членом ВЧК, затем коллегии ОГПУ и НКВД, входил в состав «троек» ОГПУ. Он был одним из активных создателей системы ГУЛАГ, в частности уже упоминавшегося Соловецкого лагеря. Именем Бокия был назван пароход, в трюме которого в Соловки привозили новых заключённых. Известный советский учёный-филолог Дмитрий Сергеевич Лихачёв, узник Соловков, вспоминал свою поездку на пароходе так: «Вывели нас на пристань с вещами, построили, пересчитали. Потом стали выносить трупы задохшихся в трюме или тяжело заболевших: стиснутых до перелома костей, до кровавого поноса...» [33]. А однажды на пароходе прибыл и сам «куратор Соловков». Но это был его рабочий визит. Заключённые лагеря сочинили тогда такие строки [45]:

«В волненье все, но я спокоен.
Весь шум мне кажется нелеп:
Уедет так же, как приехал,
На „Глебе Боком“ — Бокий Глеб».

На службе у Бокия работали некоторые криптографы царской России. Был здесь В. И. Кривош-Неманич, И. А. Зыбин, дешифровавший в своё время переписку Ленина, И. М. Ямченко, бывший начальник врангелевской радиостанции. В создании службы участвовали и люди, ранее не работавшие в области шифрования. Зять Бокия, писатель Лев Разгон, вспоминал: «В спецотделе работало множество самого разного народа, так как криптографический талант — талант от Бога. Были старые дамы с аристократическим прошлым, был немец с бородой почти до ступней» и множество других непонятных людей.

К работе на Спецотдел Бокий привлек и учёного-мистика А. Барченко, исследовавшего биоэлектрические явления в жизни клетки, в работе мозга и в живом организме в целом. Свои лабораторные опыты Барченко совмещал с должностью эксперта Бокия по психологии и парапсихологии. В частности, им разрабатывалась методика выявления лиц, склонных к криптографической работе. Учёный выступал консультантом при обследовании всевозможных знахарей, шаманов, гипнотизёров и прочих людей, утверждавших, что они общаются с призраками. С конца 1920-х годов Спецотдел активно использовал их в своей работе. Как отмечается в книге [37], исследования и методика Барченко применялись и в особенно сложных случаях дешифрования вражеских сообщений — в таких ситуациях проводились сеансы связи с духами.

Первый успех новой криптографической службы относится к 1921 г.: был раскрыт немецкий дипломатический код. С этого времени и вплоть до 1933 г. контролировалась переписка многих линий дипломатической связи Германии и её консульств в СССР.

С 1921 г. читалась переписка внутренних линий связи Турции. В 1924 г. были вскрыты два шифра польского разведотдела генерального штаба, которые использовались для связи с военными атташе в Москве, Париже, Лондоне, Вашингтоне и Токио. В 1927 г. началось чтение японской переписки, в 1930 г. — переписки некоторых линий связи США. Разрабатывались коды и других стран.

Одновременно со «взломом» чужих шифров шла напряжённая работа по созданию своих. В 1924 г. на основе 52 различных шифров был создан так называемый «русский код», дешифровать который не удалось никому. В литературе по истории криптографии об этом коде нет информации. По одним источникам, «на десятилетия он стал основным шифром для всех служб СССР», по другим — такого кода никогда не было.

Несмотря на большой спектр решаемых задач, спецотдел в ВЧК, а затем в ОГПУ был в их структуре самым засекреченным. Его сотрудникам запрещалось даже родным говорить, где они работают.

В 30-е годы руководство криптографической службой сменилось, а Глеб Бокий был расстрелян.

Его жизнь окружена множеством легенд. Кто-то их подтверждает, кто-то яростно опровергает. Часто говорится о связи Г. И. Бокия с представителями тайных обществ, о его поисках Шамбалы — страны вечных мудрецов, по преданию, затерянной где-то в Азии. В 1925 г. он даже планировал туда научную экспедицию, но запретило Политбюро.

Одни считали Бокия «страшным человеком», устраивавшим тайные оргии на своей даче. Вспоминали, что некоторые сотрудники спецотдела, принимавшие в них участие, потом заканчивали жизни самоубийством. Атмосферу созданной им «дачной коммуны» сравнивали с атмосферой Великого бала у сатаны в романе его современника М. А. Булгакова «Мастер и Маргарита». Только в действительности, вспоминали очевидцы, было ещё страшнее. Другие с возмущением отвергали подобные «байки», считая их «версией, которую пустили в обиход после ареста Бокия». Эти люди вспоминали Бокия как «интеллигентного и весьма скромного человека, никогда и никому не пожимавшего руки и отказывавшегося от всех привилегий». Как человека, который «на сделку с совестью не шёл никогда».

9. Секретная связь во время Великой Отечественной войны

В этом и следующих разделах речь пойдёт о методах секретной связи и криптографии в СССР во время Великой Отечественной войны и в период подготовки к ней. Это и секретная телефонная связь, и радиосвязь, и создание текстовых шифраторов.

Первые разработки аппаратов секретного телефонирования в СССР относятся к 1927–1928 гг., когда в Научно-исследовательском институте связи РККА были изготовлены для погранохраны и войск ОГПУ шесть телефонных аппаратов ГЭС (конструктор Н. Г. Суэтин). В 1930-х годах в области секретной телефонии вели работы семь организаций: НИИ НКПиТ (наркомата почт и телеграфа), НИИС РККА, завод имени Коминтерна, завод «Красная Заря», НИИ связи и телемеханики ВМФ, НИИ № 20 Наркомата электропромышленности (НКЭП), лаборатория НКВД.

ВЧ-связь. В 1930 г. заработали первые линии междугородной правительственной высокочастотной связи (ВЧ-связи) Москва — Ленинград и Москва — Харьков. Отметим, что сама технология ВЧ-связи без применения аппаратуры шифрования была совершенно ненадёжна и могла защитить только от прямого прослушивания. В 1935–1936 гг. на заводе «Красная Заря» было создано устройство автоматического засекречивания телефонных переговоров — *инвертор ЕС* (названный по фамилиям разра-

ботчиков К. П. Егорова и Г. В. Старицына) — и налажен его выпуск для каналов телефонной ВЧ-связи. Практически на всём протяжении Великой Отечественной войны и позднее для организации ВЧ-связи успешно использовались устройства этого типа. К 1941 г. в СССР функционировало 116 ВЧ-станций и 39 трансляционных пунктов, а число абонентов высшего партийного и государственного руководства достигло 720.

К первому периоду войны относится разработка портативной, исполненной в виде чемодана, засекречивающей аппаратуры СИ-15 («Синица») и САУ-16 («Снегирь»), которая использовалась в основном при выездах высшего командного состава в пункты, не имевшие ВЧ-станций.

В 1938–1939 гг. в Центральном научно-исследовательском институте связи были созданы две лаборатории по засекречиванию телеграфной и телефонной информации. Возглавил их выдающийся учёный Владимир Александрович Котельников. Это человек, сыгравший ключевую роль в организации надёжной секретной связи самого высокого уровня во время Великой Отечественной войны и после неё.

Секретная телеграфная связь. В. А. Котельниковым впервые в СССР были разработаны принципы построения телеграфной засекречивающей аппаратуры путём наложения на сообщение знаков гаммы (аппаратура «Москва»).

Как приводится в работе [11], «Сам шифратор, сконструированный на электромеханических узлах, был сложным и громоздким. В основе конструкции лежал барабан, заполненный шариками. При вращении барабана через систему штырей из щелей шарики случайным образом скатывались по шести вертикальным трубкам на две движущиеся телеграфные ленты, которые были наложены одна на другую через „копирку“. В результате на обеих лентах получался одинаковый рисунок — „дорожки“ из случайно расположенных пятен. Затем по этим меткам ленты перфорировались. Эти ленты образовывали случайный ключ и рассылались на пункты установки аппаратуры».

Сама схема наложения гаммы на открытый текст была уже хорошо известна к тому времени благодаря изобретению Гильберта Вернама 1917 г. Она оказалась очень привлекательной и долгое время использовалась в аппаратуре последующих поколений.

Секретная телефонная связь. В 1939 г. В. А. Котельникову было поручено решение важной государственной задачи — создание шифратора для засекречивания речевых сигналов с повышенной стойкостью к дешифрованию.

В лаборатории Котельникова было установлено, что для хорошей маскировки речевого сигнала необходимо использовать *частотные преобразования* и *временные перестановки* отрезков речи одновременно [12]. Эти принципы легли в основу новой разработанной под руководством Котельникова сложной засекречивающей аппаратуры С-1 («Соболь») [28], которая стала широко использоваться в действующей армии. Несмотря на все трудности, уже к осени 1942 г. сотрудники лаборатории Котельникова изготовили несколько образцов оборудования «Соболь-П». Согласно работе [11], это была самая сложная аппаратура засекречивания информации, не имевшая аналогов в мире. «Соболь-П» использовался для обеспечения секретной связи самого высокого уровня (Ставки Верховного Главнокомандующего со штабами фронтов), причём впервые такая связь осуществлялась с помощью радиоканала. Заменить относительно безопасный проводной канал связи на радиоканал для связи такого уровня оказалось возможно только благодаря *исключительной стойкости* использованного шифрования.

Как вспоминали ветераны ВОВ, применение шифраторов Котельникова в ходе решающих боев на Курской дуге в значительной степени определило успешный исход битвы [11]. По сведениям советской разведки, Гитлер заявлял, что за одного крип-

тоаналитика, способного «взломать» советскую радиосвязь, он не пожалел бы трёх отборных дивизий.

Уже в то время В. А. Котельников понимал, что для обеспечения высокой стойкости и уровня маскировки речевого сигнала необходимо сначала проводить сжатие речи [12]. Поэтому параллельно с разработкой «Соболя-П» В. А. Котельников проводил работы по созданию *вокодера* — устройства, обеспечивавшего компрессию спектра речи примерно в 10 раз. К октябрю 1941 г. вокодер начал «говорить». В ноябре 1941 г. лаборатория продолжила свою работу в Уфе, куда была эвакуирована.

За создание шифраторов В. А. Котельников и его коллеги по лаборатории (И. С. Нейман, Д. П. Горелов, А. М. Трахтман, Н. Н. Найдёнов) получили в марте 1943 г. Сталинские премии I степени. Все разработки были жёстко засекречены. Сотрудник лаборатории Е. В. Руднев передает атмосферу секретности в своих стихах-воспоминаниях [39]:

«В 43-м весною, по радио
Мы узнали — трудились не зря.
Золотыми нагрудными знаками
Удостоена эта работа была.
Первый том был написан В. А.
Мой четвёртый — последний,
Между ними два тома Д. Б. и Ю. С.
Все четыре — под грифом С. С.»

Аппаратура «Соболь-П» очень активно использовалась в дальнейшем. После окончания Второй мировой войны она получила применение и на дипломатических линиях связи Москвы с Хельсинки, Парижем и Веной при проведении переговоров по заключению мирных договоров, а также при проведении Тегеранской, Ялтинской и Потсдамской конференций и для связи с Москвой нашей делегации во время принятия капитуляции Германии в мае 1945 г. За дальнейшие разработки в области шифраторов Котельникову и его группе в 1946 г. была повторно присуждена Сталинская премия I степени.

Одновременно с созданием аппаратуры засекречивания в СССР проводились и работы по её дешифрованию. Было установлено, что аналоговая аппаратура шифрования мозаичного типа теоретически дешифруема. Для того чтобы получить недешифруемую аппаратуру засекречивания телефонных переговоров, речь необходимо переводить в *цифровую форму*.

В 1941 г. Владимир Александрович доказал, что можно создать *математически недешифруемую систему* засекречивания, если каждый знак сообщения будет засекречиваться выбираемым случайно и равновероятно знаком гаммы. Параллельно и независимо к этим идеям пришёл выдающийся американский учёный Клод Шеннон. Подобные системы он стал называть *совершенно секретными шифрами*. Такие системы, как показал В. А. Котельников, должны быть цифровыми, а преобразование аналогового сигнала в цифровую форму должно основываться на доказанной им *теореме отсчётов* (другое название — *теорема дискретизации*). Эта теорема, как и другие результаты В. А. Котельникова, прочно вошла в Золотой фонд классических результатов современной теории информации.

Теорема Котельникова. Если аналоговый сигнал $s(t)$ имеет ограниченный спектр, то он может быть восстановлен однозначно и без потерь по своим дискретным отсчётам, взятым с частотой не менее удвоенной максимальной частоты спектра.

Другими словами, теорема говорит о возможности восстановления непрерывных функций с ограниченным спектром по их значениям через определённые интервалы времени. Заслуга Котельникова состоит в том, что он первый осознал возможности приложений этого математического факта и осуществил удачный выбор класса функций для дискретизации. В зарубежной литературе эта теорема более известна как теорема Найквиста — Шеннона.

С этих результатов В. А. Котельникова, представленных в секретной научной работе «Основные положения автоматической шифровки» (1941) и независимо полученных К. Шенноном в 1945 г., и началась криптография как наука. Для криптографических методов впервые за всю историю их развития был разработан строгий математический аппарат.

Необходимо отметить, что результаты К. Шеннона были опубликованы в открытой печати, тогда как работы В. А. Котельникова долгое время оставались засекреченными. Поэтому приоритет в этой области по праву закреплён за К. Шенноном.

После войны, 21 января 1948 г., была создана секретная Марфинская лаборатория [28] для работы над следующими проблемами:

- дискретизация непрерывного речевого сигнала;
- увеличение скорости передачи двоичных сигналов;
- разработка высокоскоростного шифратора;
- создание нового направления — криптографического анализа.

Однако В. А. Котельников отказался возглавить лабораторию; он только её курировал. В это время он продолжал работать в Московском энергетическом институте (МЭИ). Руководил Марфинской лабораторией А. М. Васильев.

В новой лаборатории вместе с вольными работали заключённые спецтюрьмы № 16 МГБ СССР. На проведение всех работ руководство страны поставило сверхкороткий срок — полтора года! Атмосфера была очень напряжённой. Марфинская криптографическая лаборатория описана в романе А. И. Солженицына «В круге первом». Правда, как вспоминал в 2003 г. В. А. Котельников, «Солженицын не слишком правильно описал атмосферу в лаборатории. „Вольным“ приходилось работать больше, чем заключённым, и кормили их много хуже. Усложняла работу и обстановка излишней секретности. Закрытость и секретность вообще много вреда принесли нашей науке» [26].

10. В. А. Котельников

Владимир Александрович Котельников (1908–2005) родился в Казани, в семье университетского профессора — известного математика Александра Петровича Котельникова. Его дед, Пётр Иванович Котельников, также всю жизнь проработал математиком в Казанском университете и, между прочим, был первым математиком, который открыто поддержал смелые работы Н. И. Лобачевского о неевклидовой геометрии.

В 1926 г. Владимир Александрович поступил в Московское высшее техническое училище им. Баумана, на последних курсах перешел в отделившийся от училища Московский энергетический институт, который и окончил в 1930 г., получив звание инженера-электрика. Однако научная деятельность В. А. Котельникова началась раньше — в 1930 г. в НИИ связи Красной Армии, куда он был зачислен в качестве инженера. Одновременно с научной деятельностью с 1931 по 1941 г. В. А. Котельников преподавал на кафедре радиотехники МЭИ. В конце 30-х годов и в годы войны Владимир Александрович занимался разработкой специальной шифровальной аппаратуры связи. Достигнутые им криптографические успехи без преувеличения внесли огромный

вклад в нашу победу, а сам В. А. Котельников снискал себе негласный титул «патриарха секретной телефонии».

В конце 40-х годов Владимир Александрович организовал Особое конструкторское бюро МЭИ, ставшее впоследствии одним из ведущих предприятий в области космической техники. С 1954 г. В. А. Котельников возглавил недавно созданный Институт радиотехники и электроники (ИРЭ), получивший при нём мощное развитие.

В 90-е годы В. А. Котельников был одним из шести основателей Академии криптографии. Он принимал активное участие в работе её советов и комиссий.

Обширные научные интересы Владимира Александровича включали в себя общую и прикладную физику; радиофизику, радиотехнику и электронику; теорию информации, в частности — методы защиты информации от помех в системах радиосвязи и криптографию, практические вопросы разработки специальной аппаратуры связи; исследования космоса, в особенности созданное им направление планетной радиолокации и многое, многое другое. Во всех этих областях В. А. Котельников получил существенные результаты.

В. А. Котельников — лауреат Ленинской премии, дважды лауреат Государственной премии СССР, дважды Герой Социалистического труда. Он награждён шестью орденами Ленина, орденом «За заслуги перед Отечеством» I степени, другими орденами и медалями, в частности орденом «За заслуги перед Москвой». Хоть и с большим опозданием, его научные заслуги были признаны во всем мире. В 1999 г. ему были присуждены высшие международные награды — премия Э. Рейна и Золотая медаль А. Белла. Решением Международного астрономического союза астероид № 2726 носит имя «Kotelnikov». Президент Международного института электронной и электрической инженерии Брюс Эйзенштейн (США) признавал самый существенный вклад Котельникова в развитие радиосвязи и криптографии, он говорил: «Over the years the West had its Shannon; and the East had its Kotelnikov».

Рис. 4. В. А. Котельников

Полученные звания и награды не стали препятствием основному делу его жизни: Владимир Александрович сохранил научную активность до самого последнего времени. Его творческий и земной путь завершился на 97-м году жизни почти законченной, но не опубликованной работой «Модельная квантовая механика».

Коллеги В. А. Котельникова отмечали его выдающиеся личные качества. «Прежде всего, это необычайная серьёзность в подходе к решению любого вопроса, будь то государственная проблема или личная проблема сотрудника. Далее, неизменная доброжелательность, обязательность в выполнении обещанного, стремление всегда решить

вопрос, не откладывая на завтра, — вот те замечательные качества, которые характеризовали Владимира Александровича как руководителя и как человека» (директор ИРЭ академик Ю. В. Гуляев) [24].

На работе и в жизни Владимир Александрович был скромен и прост. Он умел видеть главное и быть требовательным. Читая воспоминания [30] тех, кому посчастливилось работать с ним, отмечаешь, что в присутствии Владимира Александровича людям неожиданно становилось... стыдно. За себя, за недостатки в своей работе. И они старались работать лучше, не позволяя себе «халтуры», и сами менялись к лучшему.

11. Немного о советских шифрмашинах

Когда речь заходит о шифровальной технике времён Второй мировой войны, то, как правило, вспоминают знаменитую немецкую шифровальную машину «Энигма» — изобретение инженера Артура Шербиуса 1918 г. Этим дисковым шифратором с 1926 г. стали оснащаться вооружённые силы и спецслужбы Германии. Наиболее востребованной «Энигма» стала после прихода к власти Гитлера и особенно во время войны. По некоторым оценкам, для вооружения немецкой армии было выпущено до 100 000 её экземпляров.

Вспоминают тайную работу по дешифрованию «Энигмы», которая велась в разных странах и увенчалась успехом. На протяжении войны немецкие сообщения тайно читались англичанами, американцами, русскими и др.

Первый математический аппарат для дешифрования «Энигмы» разработали выпускники Познаньского университета (Польша) Мариан Раевский, Генрих Зыгальский и Ежи Розицкий (см. подробнее [13, 29, 42]). В 2008 г. в Познани о них был снят документальный фильм [46]. Результатами польских криптоаналитиков воспользовались англичане. Ими была спланирована масштабная операция «Ультра», нацеленная как на аналитическое дешифрование сообщений «Энигмы», так и на захват её действующих кодовых книг. Об этой успешной операции и её главном криптографическом центре в Блетчли-парке написано довольно много. Большой объём сведений можно найти и о самой «Энигме».

А какими были советские шифрмашины?

До последнего времени информации о них практически не было.

«...кто возьмет в плен русского шифровальщика, либо захватит русскую шифровальную технику, будет награждён Железным крестом, отпуском на родину и обеспечен работой в Берлине, а после окончания войны — поместьем в Крыму».

«Эти проклятые русские шифровальные машины, мы никак не можем их расколоть!»

Многое дают понять эти слова Гитлера. Он инициировал настоящую охоту за советскими шифровальщиками. Однако немцам так и не удалось дешифровать сообщения, зашифрованные с помощью советской техники. С 1942 г. эти сообщения перестали перехватывать. Благодаря разработанной перед войной шифровальной технике Советскому Союзу удалось скрыть свои стратегические планы. Это был огромный успех нашей шифровальной службы!

В подтверждение приведём несколько цитат.

«Ни одно донесение о готовящихся военно-стратегических операциях нашей армии не стало достоянием фашистских разведок» (начальник Генштаба Маршал Советского Союза А. М. Василевский).

«Хорошая работа шифровальщиков помогла выиграть не одно сражение» (зам. Верховного Главнокомандующего Маршал Советского Союза Г. К. Жуков).

В своих показаниях начальник штаба при ставке верховного главнокомандования немецких вооружённых сил генерал-полковник А. Йодль сообщал: «Радиоразведка играла особую роль в самом начале войны, но и до последнего времени не теряла своего значения. Правда, нам никогда не удавалось перехватить и расшифровать радиограммы вашей ставки, штабов фронтов и армий. Радиоразведка, как и все прочие виды разведок, ограничивалась только тактической зоной» [32].

Первая попытка создать текстовый электромеханический шифратор в СССР была предпринята в 1923 г. в Особом техническом бюро по военным изобретениям специального назначения. Найти какую-либо информацию об этой попытке достаточно трудно.

В 30-е годы образцы советской шифровальной техники создавались под руководством талантливого инженера Ивана Павловича Волоска. Шифрмашины того времени реализовывали наложение случайной последовательности (гаммы) на открытое текстовое сообщение. Даже сейчас такой подход абсолютно современный и при выполнении некоторых условий может обеспечивать гарантированную стойкость шифрования.

В-4, М-100 — одни из первых советских шифрмашин, реализующих шифры гаммирования. В 1938 г. началось их серийное производство.

«Шифровальная машина М-100 состояла из трёх основных узлов: клавиатуры с контактными группами, лентопротяжного механизма с трансмиттером и приспособления, устанавливаемого на клавиатуру пишущей машинки, и семи дополнительных блоков. Общий вес комплекта достигал 141 кг. Только одни аккумуляторы для автономного питания электрической части машины весили 32 кг. Тем не менее данная техника выпускалась серийно и в 1938 г. была успешно испытана в боевых условиях во время гражданской войны в Испании (1936–1939 гг.), на Халхин-Голе (1939), во время советско-финской войны (1939–1940 гг.). Шифрованная связь в этих военных конфликтах осуществлялась в звене Генеральный штаб — Штаб армии» [11].

Позднее появились и более компактные машины, например К-37 («Кристалл»), М-101 («Изумруд») и другие. Наряду с шифрами гаммирования применялись и шифры многоалфавитной замены. После войны в СССР использовались такие шифрмашины, как М-105 «Агат», М-125 «Фиалка» и др.

Широко использовалось и ручное шифрование. Телеграммы отправлялись с помощью лёгких, весом в три килограмма, радиостанций «Север», или «Северок», как их ласково называли военные связисты. Эта техника, быстро завоевавшая симпатии наших разведчиков и партизан, выпускалась в блокадном Ленинграде.

На машинную шифросвязь в годы войны легла основная нагрузка при передаче секретных телеграмм. И с этой нагрузкой, как уже отмечалось выше, наша шифровальная служба справилась блестяще. Только в 8-м Управлении Красной Армии за период с 1941 по 1945 г. было обработано свыше 1,6 миллионов шифротелеграмм.

Не будем забывать про эти успехи.

Известно много примеров героического поведения наших шифровальщиков на войне [32]. Офицеры спецсвязи на грани жизни и смерти, часто с тяжелейшими ранениями уничтожали шифровальные документы перед приходом врага. В большинстве случаев это было то последнее, что они успевали сделать перед смертью. Советские шифровальщики под страшными пытками не выдавали ни наших кодовых таблиц, ни особенностей использования нашей шифровальной техники. Без этого личного героизма секретная работа даже самой надёжной шифровальной техники была бы невозможна.

Успехи нашей дешифровальной службы во время войны требуют отдельного исследования. Приведём лишь один пример. Как отмечает в своём интервью Н. Н. Андреев,

бывший руководителем 8-го Главного Управления КГБ, с 1992 по 1998 г. — президент Академии криптографии РФ, «во время войны мы читали японскую дипломатическую переписку, анализ которой позволил сделать вывод о том, что Япония не намерена начинать военные действия против СССР, что дало возможность перебросить значительные силы на германский фронт» [27].

12. После войны

О том, как развивалась отечественная криптография после войны, есть только обрывочные сведения.

Ещё с 1 сентября 1939 г. в СССР велась подготовка военных криптографов. С момента образования Спецотдела ВЧК и вплоть до Великой Отечественной войны каких-либо стационарных учебных заведений (кроме краткосрочных курсов и школ) для подготовки профессионалов-криптографов не было. В эти годы основы криптографии преподавались в Военно-инженерной академии имени В. В. Куйбышева и в Военной академии связи в Ленинграде.

В Спецотделе разрабатывались и первые учебники по криптографии. Среди них — пособие «Шифры и их применение» (1933), учебник «Криптография (шифрование и дешифрование)» (авторы А. И. Копытцев, С. Г. Андреев, С. С. Толстой, Б. А. Аронский, 1939). В эти же годы был подготовлен, а в 1951 г. издан учебник «Введение в криптографию» (автор М. С. Одноробов). Учебник состоял из четырёх частей (общим объёмом 737 страниц), содержал большое количество примеров, построенных на реальных материалах (подробнее см. [38]).

В 1940 г. при ОГПУ была создана криптографическая школа особого назначения (ШОН), которая с началом войны перебазировалась в Уфу. Именно там, в криптографической школе, преподавал иностранные языки удивительный В. И. Кривош-Неманич. Кстати, языковой подготовке в СССР уделялось очень большое внимание. Считалось, что каждому криптографу следует владеть хотя бы одним иностранным языком.

В начале 1946 г. при Высшей школе НКГБ были организованы криптографические курсы, которые позднее послужили основой подготовки криптографов на закрытом отделении механико-математического факультета МГУ. Такое отделение было создано в 1949 г. и просуществовало до 1957 г.; его возглавлял Георгий Иванович Пондопуло (1910–1996).

Как вспоминает выпускник закрытого отделения мехмата В. Н. Сачков, «в послевоенные годы в связи с резким увеличением информационного обмена и необходимостью его надёжной защиты, а также с целью повышения эффективности дешифровальной работы возникла потребность существенного усиления криптографических служб ведущих держав. С этой целью в Советском Союзе в 1949 г. было создано Главное управление специальной службы (ГУСС), а в США в 1952 г. — Агентство национальной безопасности (АНБ). Деятельность как ГУСС, так и АНБ протекала в условиях строгой секретности» [41].

19 октября 1949 г., в год четырёхсотлетия российской криптографической службы, были созданы Главное управление Специальной службы и *Высшая школа криптографов* (ВШК). ВШК стала первым и единственным в стране высшим учебным заведением такого профиля. Впоследствии она была преобразована в Высшую школу криптографов 8-го Управления МВД СССР, затем — в Высшую школу криптографов КГБ при Совете Министров СССР, затем — в технический факультет Высшей школы 8-го Главного управления КГБ при СМ СССР, а в 1992 г. — в *Институт крипто-*

графии, связи и информатики (ИКСИ). Все эти годы днём рождения ИКСИ и его предшественников считается 19 октября [38].

Позволим небольшое отступление от хронологии: 19 октября — это день рождения ещё одного учебного заведения — Царскосельского лицея, особо почитаемый его первыми выпускниками. Помните у А. С. Пушкина:

«Кому ж из нас под старость день лицея
Торжествовать придется одному?»

«Торжествовать» пришлось Александру Михайловичу Горчакову (1798–1883), российскому дипломату, министру иностранных дел России с 1856 по 1882 г. Любопытно вспомнить его здесь как человека, на самом высоком уровне причастного к криптографической деятельности. Ведь именно министр иностранных дел в XIX веке контролировал шифровальную службу.

С 40-х годов XX века криптографические задачи стали существенно сложнее и математичнее. В ряде институтов, таких, как Математический институт им. В. А. Стеклова, были созданы закрытые отделы для их решения. Например, в терминах теории вероятностей и математической статистики решалась задача о критерии открытого текста. Она заключалась в том, чтобы из всевозможных «хаотических» вариантов, которые получаются при дешифровании перехваченного сообщения, выделить единственный верный вариант. Для этого нужно было очень тонко учитывать статистические особенности, присущие неизвестному «правильному» тексту, составленному на том или ином языке.

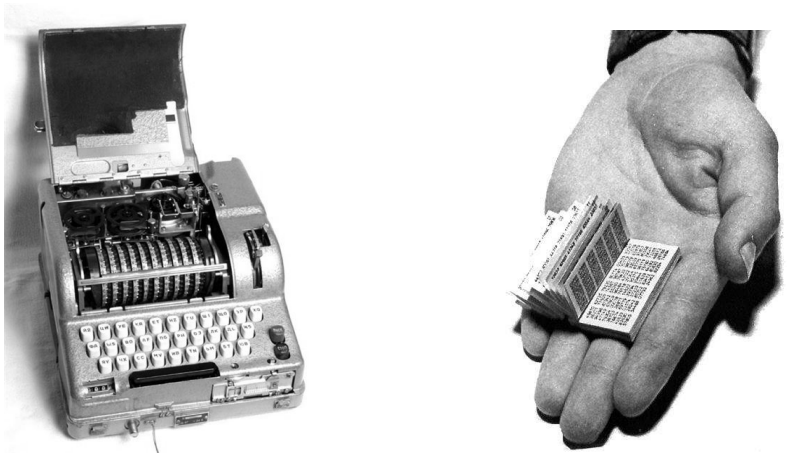

Рис. 5. Шифрмашина М-125 «Фиалка»; кодовая книга советского разведчика (одноразовый блокнот)

Как отмечается в книге [38], в 50-е годы в Высшей школе активизировалась работа по подготовке специалистов-криптографов. В 1955 г. в ВШ был создан учёный совет, стали готовиться научные работы и диссертации. Большой творческий вклад в подготовку научных кадров внёс член-корреспондент Академии наук СССР Владимир Яковлевич Козлов (1914–2007) — им подготовлено более 25 кандидатов и докторов наук [4]. Забота о становлении, развитии и укреплении дневного отделения подготовки криптографов (создано в 1962 г.) легла на плечи Ивана Яковлевича Верченко (1907–1995), очень уважаемого студентами преподавателя, декана технического факультета Высшей школы КГБ [40].

По заказам оборонных предприятий криптографические исследования проводились во многих вузах страны (см., например, [2]). Результаты исследований публи-

ковались в закрытых сборниках, о которых и сейчас мало информации. Попытки опубликовать криптографические результаты в открытой печати, предпринимавшиеся отдельными исследователями, были безуспешны. Так, рукопись А. Д. Закревского «Метод автоматической шифрации сообщений» 1959 г. была не принята к печати из-за её высокой секретности; автору пришлось сменить область своих исследований. Спустя 50 лет рукопись была опубликована в журнале «Прикладная дискретная математика» [25].

В целом, специалисты-криптографы высоко оценивали работу нашей шифровальной службы послевоенного времени. Американский криптограф Дэвид Кан так описывает криптографические успехи СССР 50–60-х годов: «Россия сама по себе остаётся загадкой, овеянной тайной из тайн. То же самое касается и её средств связи. Одноразовые шифрблокноты обеспечивают надёжную защиту для сообщений российских разведчиков, военных, дипломатов и работников тайной политической полиции. Грамотно сконструированные шифраторы навечно сохраняют в секрете от врагов России её наиболее важную дипломатическую, агентурную и военную переписку. В период „холодной войны“ русские сумели вскрыть шифры американского посольства в Москве. Такие подвиги свидетельствуют об их осведомлённости, базирующейся на глубоком понимании шифровального дела и криптоанализа. Так или иначе русские вознесли достижения своей страны в криптологии до высоты полёта её космических спутников» [29].

Однако не всё было гладко. С начала 40-х годов и вплоть до 1 октября 1980 г. в контрразведке США действовал проект Venona, направленный на дешифрование советских сообщений. Успехи американцев привели к раскрытию нескольких советских разведчиков и утечке секретных сведений. Официально проект был рассекречен в США в 1995 г.

В отличие от других стран, в СССР все исследования по криптографии были сильно засекречены. Почти вплоть до распада Союза «упоминание слова „криптография“ в открытой печати даже в невинном контексте часто вызывало в инстанциях резкие возражения и обычно под тем или иным предлогом приводило к запрещению этого упоминания» [31].

До сих пор большинство архивов по истории российских спецслужб (в том числе по истории криптографии) остаются закрытыми. Более того, как отмечается в книге А. Солдатова и И. Бороган [44], «некоторые архивы, открытые в 1990-е, были вновь засекречены в недавнее время».

13. Современность

«Остановиться бы тогда, в конце 80-х годов, снять с глаз тёмные очки и оглядеться вокруг на окружающую действительность. Была же ведь реальная возможность побороться за мировые рынки сбыта наукоёмкой криптографической продукции, программ и алгоритмов, была возможность даже в каком-то смысле стать законодателями криптографической моды. Были и идеи, и отличные молодые специалисты...», — так рассуждает в своей книге «Криптография и свобода» [34] криптограф М. Е. Масленников, выпускник 4-го факультета Высшей школы, с 1979 по 1993 г. сотрудник 8-го Главного управления КГБ, ныне — свободный житель Южной Кореи.

Но возможность была упущена. Тогда, в конце 80-х, криптографическая служба России была не готова к переменам. Как в далёком 1917 году, она переживала тяжёлые времена.

И всё же они миновали. Страна выдержала. Выдержала и обновилась криптографическая служба. Начиная с 90-х годов в России стала развиваться гражданская криптография. Теперь криптография изучается в гражданских вузах, многие статьи и книги по криптографии публикуются в открытой печати, широко используются криптографические средства защиты информации.

Отметим лишь некоторые события последних десятилетий в области российской криптографии и защиты информации.

В 70–80-х годах был разработан блочный шифр ГОСТ 28147-89, ставший с 1990 г. государственным стандартом России. Он был рассекречен в 1994 г.

В 1991 г. было создано Федеральное агентство правительственной связи и информации при Президенте РФ (ФАПСИ). Упразднено в 2003 г.

В 1992 г. в России была создана Академия криптографии. Её первым президентом стал Н. Н. Андреев. Идею создания Академии поддержали академики и члены-корреспонденты РАН: В. А. Котельников, Ю. В. Прохоров, В. Я. Козлов, В. К. Левин, Б. А. Севастьянов. Академия решает задачи государственной важности по обеспечению национальной безопасности и обороноспособности страны [27].

В 90-е и 2000-е годы защиту информации и криптографию начали изучать в гражданских вузах страны.

В 1995 г. был издан Указ Президента РФ от 03.04.1995 г. № 334 о мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации. Согласно Указу, был наложен запрет на использование, разработку, производство, реализацию и эксплуатацию шифровальных средств юридическими и физическими лицами без наличия лицензий ФАПСИ.

В настоящее время криптографическая деятельность в России также подлежит обязательному лицензированию (см. Приказ ФСБ России от 09.02.2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение пкз-2005)», Постановление Правительства РФ от 29.12.2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»).

В 1997 г. была образована «Лаборатория Касперского». Её возглавляет Евгений Касперский — выпускник 1987 г. технического факультета Высшей школы КГБ СССР. Сейчас компания является одним из мировых лидеров в сфере программных решений для информационной защиты конечных пользователей.

В 1999 г. Институт криптографии, связи и информатики отметил своё 50-летие. Ко дню рождения вышла книга [38] об истории ИКСИ, ставшая библиографической редкостью.

В 1999 г. была создана Российская криптографическая ассоциация «РусКрипто», аналог международной организации IACR.

В 2003 г. на базе ФАПСИ была создана Служба специальной связи и информации Федеральной службы охраны РФ (Спецсвязь России).

В 2010 г. шифр ГОСТ был заявлен в качестве участника конкурса Международной организации по стандартизации (ISO) на приобретение статуса Всемирного стандарта шифрования (Worldwide Industrial Encryption Standard).

В апреле 2011 г. вступил в силу Закон об электронной подписи в РФ, согласно которому каждый гражданин России может завести себе электронную подпись.

В 2013 г. в 15-й и соответственно в 12-й раз пройдут российские конференции Рус-Крипто и SIBECRYPT по криптографии.

Вместо заключения

О советской криптографии сняты несколько документально-публицистических фильмов. Среди них:

• «Открытая закрытая связь» (режиссёр Д. Скворцов, 2006) — фильм об истории создания секретной телефонной связи в СССР.

• «Код Верченко» (режиссёр А. Трофимов, 2007) — фильм о советском криптографе И. Я. Верченко (1907–1995), сотруднике Марфинской лаборатории, позднее — декане технического факультета Высшей школы КГБ.

Для более глубокого знакомства с историей криптографии в России можно рекомендовать книги Т. А. Соболевой «История шифровального дела в России» [43], Ю. И. Гольева, Д. А. Ларина, А. Е. Тришина, Г. П. Шанкина «Криптография: страницы истории тайных операций» [13], А. В. Бабаша, Г. П. Шанкина «История криптографии» (часть 1) [5], Д. Кана «Взломщики кодов» [29], С. Сингха «Книга шифров. Тайная история шифров и их расшифровки» [42], главы по истории в книгах А. П. Алфёрова, А. Ю. Зубова, А. С. Кузьмина, А. В. Черёмушкина [3], В. И. Нечаева [35], В. М. Фомичёва [47]. Российской криптографии XIX века и начала XX века посвящены статьи А. В. Бабаша, Ю. И. Гольева, Д. А. Ларина, А. Е. Тришина, Г. П. Шанкина [6 – 10, 14 – 21]. О вкладе Х. Гольдбаха и Ф. Эпинуса в российскую криптографию можно прочитать в работе В. К. Новика [36]. Дополнительно о В. И. Кривоше-Неманиче см. публикации [23, 45]. О криптографии во время Великой Отечественной войны, В. А. Котельникове, Марфинской лаборатории можно прочитать в статье Д. А. Ларина [32], сборнике «В. А. Котельников. Судьба, охватившая век» [30], книге К. Ф. Калачёва [28]. О криптографии в XX веке — в сборнике об истории ИКСИ [38], статьях и интервью Н. Н. Андреева [4, 27], В. А. Котельникова [26], В. Н. Сачкова [41], А. Д. Закревского [25], Г. П. Агибалова [2], сайте фонда им. И. Я. Верченко [40], публикациях сайта [1], отчёте лаборатории МГУ [31], книге [34] и других. На английском языке истории российской криптографии посвящены некоторые публикации журнала «Cryptologia», среди них — статьи T. R. Hammant [49 – 51], D. Kahn [52], D. Schimmelpenninck [54], J. Bury [48], Z. J. Карега [53] и другие.

Автор выражает глубокую благодарность В. М. Фомичёву за ценные замечания и обсуждения.

ЛИТЕРАТУРА

1. Агентура.ру. Российский интернет-ресурс, посвященный проблемам спецслужб, разведки и борьбы с терроризмом // `www.agentura.ru`.
2. *Агибалов Г. П.* 50 лет криптографии в Томском государственном университете // Прикладная дискретная математика. 2009. № 2. С. 104–126.
3. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черёмушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2005. 480 с.
4. *Андреев Н. Н., Зубков А. М., Ивченко Г. И. и др.* Владимир Яковлевич Козлов (к девяностолетию со дня рождения) // Дискретная математика. 2004. Т. 16. № 2. С. 3–6.
5. *Бабаш А. В., Шанкин Г. П.* История криптографии. Ч. 1. М.: Гелиос АРВ, 2002. 240 с.

6. *Бабаш А. В., Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* О развитии криптографии в XIX веке // Защита информации. Конфидент. 2003. № 5. С. 90–96.
7. *Бабаш А. В., Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Криптографические идеи XIX века // Защита информации. Конфидент. 2004. № 1. С. 88–95; 2004. № 2. С. 92–96.
8. *Бабаш А. В., Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Криптографические идеи XIX века. Русская Криптография // Защита информации. Конфидент. 2004. № 3. С. 90–96.
9. *Бабаш А. В., Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Шифры революционного подполья России XIX века // Защита информации. Конфидент. 2004. № 4. С. 82–87.
10. *Бабаш А. В., Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Криптография в XIX веке // Информатика. 2004. Т. 466. № 33. С. 17–23.
11. *Бабиевский В. В., Бутырский Л. С., Ларин Д. А., Шанкин Г. П.* Советская шифровальная служба: 1920–40-е // `http://www.agentura.ru`
12. *Букашкин С. А.* В. А. Котельников — основоположник секретной телефонии // Сб. «В. А. Котельников. Судьба, охватившая век». Т. 1. Воспоминания коллег. М.: Физматлит, 2011. С. 21–24.
13. *Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П.* Криптография: страницы истории тайных операций. М.: Гелиос АРВ, 2008. 288 с.
14. *Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П.* Криптографическая деятельность в период наполеоновских войн // Защита информации. Конфидент. 2004. № 5. С. 90–95.
15. *Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П.* Научно-технический прогресс и криптографическая деятельность в России XIX века // Защита информации. INSIDE. 2005. № 2. С. 67–75.
16. *Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П.* Начало войны в эфире // Защита информации. INSIDE. 2005. № 3. С. 89–96.
17. *Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П.* Криптографическая деятельность во время Гражданской войны в России // Защита информации. INSIDE. 2005. № 4. С. 89–96.
18. *Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П.* Криптографическая деятельность революционеров в 20–70-х годах XIX века в России: успехи и неудачи // Защита информации. INSIDE. 2005. № 5. С. 90–96.
19. *Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Криптографическая деятельность организаций «Земля и воля» и «Народная воля» в России в 1876–1881 годах // Защита информации. INSIDE. 2005. № 6. С. 80–87.
20. *Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Криптографическая деятельность революционеров в России. 1881–1887 годы: агония «Народной воли» // Защита информации. INSIDE. 2006. № 2. С. 88–96.
21. *Гольев Ю. И., Ларин Д. А., Шанкин Г. П.* Криптографическая деятельность революционеров в России в 90-е годы XIX века // Защита информации. INSIDE. 2006. № 4. С. 84–91.
22. *Горький М.* По союзу советов. Очерк V. Соловки // Собрание сочинений в тридцати томах. Т. 17. М.: ГИХЛ, 1952. С. 201–220.
23. *Гузи Л.* Узник Соловецких островов Владимир Кривош-Неманич // Кафедра русистики, ФФ ПУ Прешов. Словакия. Специально для «Соловки Энциклопедия». 15.11.2005. Доступно по адресу `http://www.solovki.ca/camp\_20/scientists.php`.
24. *Гуляев Ю. В.* Краткая научная биография академика В. А. Котельникова. `www.cplire.ru/alt/Kotelnikov/index.html`.
25. *Закревский А. Д.* Метод автоматической шифрации сообщений // Прикладная дискретная математика. 2009. № 2. С. 127–137.

26. Интервью: «Владимир Котельников: „Радио — главное открытие XX века“» // С. Лесков. http://fbm2000.ru/tp/in/rd.htm.
27. Интервью: «Н. Н. Андреев: Россия остаётся в числе лидеров мировой криптографии» // http://www.ssl.stu.neva.ru/psw/crypto/Andreev23.html.
28. *Калачев К. Ф.* В круге третьем: Воспоминания и размышления о работе Марфинской лаборатории в 1948–1951 годах. М.: Машмир, 2001. 129 с.
29. *Кан Д.* Взломщики кодов. М.: Центрполиграф, 2000. Перевод книги *Kahn D.* The codebreakers. 1967.
30. В. А. Котельников. Судьба, охватившая век. В 2 т. / сост. Н. В. Котельникова. М.: Физматлит, 2011. 312 с.
31. Лаборатория МГУ по математическим проблемам криптографии 1990–2000. Материалы к заседанию межведомственного междисциплинарного семинара по научным проблемам информационной безопасности 30 ноября 2000 г. М.: МГУ, 2000. 48 с.
32. *Ларин Д. А.* Советская шифровальная служба в годы Великой Отечественной войны // Изв. УрФУ. Сер. 1: Проблемы образования, науки и культуры. 2011. Т. 86. № 1. С. 69–80. http://proceedings.usu.ru/
33. *Лихачёв Д. С.* Избранное: Великое наследие. Заметки о русском. СПб.: Logos, 1998. 560 с.
34. *Масленников М. Е.* Криптография и свобода. http://lib.rus.ec/b/145611
35. *Нечаев В. И.* Элементы криптографии (Основы теории защиты информации). М.: Высшая школа, 1999. 109 с.
36. *Новик В. К.* Христиан Гольдбах и Франц Эпинус (из истории шифровальных служб России XVIII века) // Математика и безопасность информационных технологий. Материалы конф. в МГУ 23–24 октября 2003 г. М.: МЦНМО, 2004. С. 87–110.
37. *Первушин А. И.* Оккультный Сталин. М.: Яуза, 2006.
38. Пятьдесят лет Институту криптографии, связи и информатики. Исторический очерк / под ред. Б. А. Погорелова. М., 1999. 272 с.
39. *Руднев Е. В.* О нашей юности и сверстнике моём // Сб. В. А. Котельников. Судьба, охватившая век: в 2 т. М.: Физматлит, 2011. Т. 1. Воспоминания коллег. С. 19–20.
40. Сайт благотворительного фонда им. И. Я. Верченко. www.verchenko.ru
41. *Сачков В. Н.* Вклад выпускников МГУ в развитие теоретической криптографии в России во второй половине XX века // Московский университет и развитие криптографии в России. Материалы конф. в МГУ 17–18 октября 2002 г. М.: МЦНМО, 2003. С. 250–257.
42. *Сингх С.* Книга шифров. Тайная история шифров и их расшифровки. М.: АСТ Астрель, 2006. 447 с.
43. *Соболева Т. А.* История шифровального дела в России. М.: ОЛМА-ПРЕСС, 2002. 512 с.
44. *Солдатов А., Бороган И.* Новое дворянство: Очерки истории ФСБ. М.: ООО «Юнайтед Пресс», 2011. 298 с.
45. Соловки-энциклопедия. Digest project. www.solovki.ca.
46. ENIGMA. Poznan mathematicians success. Познаньский университет, Польша. Фильм, 2008. Реж. J. Malinowska.
47. *Фомичёв В. М.* Из истории развития шифров. Раздел в учеб. пособии «Математические основы современной криптологии». М.: Финансовый университет при Правительстве РФ, 2013 (в печати).
48. *Bury J.* Operation Stonka. An Ultimate Deception Spy Game // Cryptologia. 2011. V. 35. No. 4. P. 297–327.
49. *Hammant T. R.* Russian and Soviet cryptology I — Some communications intelligence in tsarist Russia // Cryptologia. 2000. V. 24. No. 3. P. 235–249.

50. *Hammant T. R.* Russian and Soviet cryptology II — The Magdeburg incident: the Russian view // Cryptologia. 2000. V. 24. No. 4. P. 333–338.
51. *Hammant T. R.* Russian and Soviet cryptology III — Soviet Comint and the Civil War, 1918–1921 // Cryptologia. 2001. V. 25. No. 1. P. 50–60.
52. *Kahn D.* Soviet Comint in the Cold War // Cryptologia. 1998. V. 22. No. 1. P. 1–24.
53. *Kapera Z. J.* Summary Report of the State of the Soviet Military Sigint in November 1942 Noticing "ENIGMA" // Cryptologia. 2011. V. 35. No. 3. P. 247–256.
54. *Schimmelpenninck van der Oye D.* Tsarist Codebreaking some Background and some examples // Cryptologia. 1998. V. 22. No. 4. P. 342–353.

АНАЛИТИЧЕСКИЕ ОБЗОРЫ

DOI 10.17223/20710410/18/8

УДК 519.7

SIBECRYPT'12. ОБЗОР ДОКЛАДОВ

Г. П. Агибалов, И. А. Панкратова

Национальный исследовательский Томский государственный университет, г. Томск, Россия

E-mail: agibalov@isc.tsu.ru, pank@isc.tsu.ru

Приводится аналитический обзор лекций и докладов, представленных на Sibecrypt'12 — XI Всероссийской конференции «Сибирская научная школа-семинар с международным участием „Компьютерная безопасность и криптография“», состоявшейся 3 – 8 сентября 2012 г. в Институте динамики систем и теории управления СО РАН (г. Иркутск).

Ключевые слова: *прикладная дискретная математика, криптография, компьютерная безопасность, защита информации.*

Введение

Sibecrypt — это Всероссийская конференция под названием «Сибирская научная школа-семинар с международным участием „Компьютерная безопасность и криптография“». Её ежегодно, начиная с 2002 г., организует и в первой трети сентября проводит кафедра защиты информации и криптографии Национального исследовательского Томского государственного университета в сотрудничестве с кафедрой программирования и компьютерной безопасности Института криптографии, связи и информатики (ИКСИ, г. Москва) на базе того или иного вуза или научного учреждения Сибири.

Конференция посвящена одному из важнейших направлений в области информационной безопасности — математическому и программному обеспечению компьютерной безопасности (КБ). В последние годы в этом направлении наблюдается высокая активность исследовательской работы молодых ученых, и возникает настоятельная необходимость в организации их научного общения друг с другом и с известными специалистами в данной области. Именно эту цель и преследует школа-семинар, имея в виду, в первую очередь, интересы молодых ученых Сибири и крупных учёных европейской части России, Беларуси, Украины. Цель достигается путём организации и проведения обсуждений на её заседаниях фундаментальных проблем защиты информации в компьютерных системах и сетях и обмена научными результатами по их решению методами прикладной дискретной математики (ПДМ).

Кроме докладов, на конференции Sibecrypt для её участников, а также для сотрудников и студентов принимающей организации (вуза, НИИ) ведущими специалистами в данной области (из числа участников конференции) читаются лекции по математическим проблемам компьютерной безопасности, защиты информации, информатики и криптографии. Материалы конференции публикуются в приложении к журналу «Прикладная дискретная математика», ставшем с 2012 г. самостоятельным журналом «Прикладная дискретная математика. Приложение».

В 2012 г. конференция состоялась в 11-й раз — с аббревиатурой Sibecrypt'12, на этот раз — 3–8 сентября в Иркутске на базе Института динамики систем и теории управления СО РАН. Тезисы докладов, представленных в её программу, опубликованы в [1]. Аналитический обзор в форме аннотаций их содержания, а также содержания лекций, прочитанных на конференции, является целью данной статьи. В соответствии с тематикой Sibecrypt'12 аннотации докладов разбиты по следующим её направлениям: теоретические основы ПДМ, математические методы криптографии и стеганографии, математические основы КБ, прикладная теория графов, математические основы информатики и программирования, вычислительные методы в дискретной математике.

1. Лекции по криптографии и информатике

О содержании понятия «электронная подпись» в Директиве 1999/93/ЕС от 1999 г. (далее Директива) и в Федеральном законе РФ от 2011 г. (далее ФЗ), регламентирующих порядок использования электронных подписей в Европейском сообществе и в России соответственно, рассказано в лекции А. В. Черёмушкина. Основные выводы докладчика следующие: 1) имеются принципиальные отличия определений основных понятий и систем технических требований в Директивах и ФЗ; 2) определения электронной подписи в Директивах и ФЗ ориентированы в основном на применение в юридической сфере и расходятся с математическим определением этого понятия. Полностью доклад опубликован в [2].

Обстоятельный обзор применения латинских квадратов в криптографии для построения шифров, схем аутентификации, однонаправленных функций, схем разделения секрета, криптографических хеш-функций и протоколов с нулевым разглашением представлен в лекции М. Э. Тужилина. Полностью текст опубликован в [3].

Одной из важнейших научных проблем, если не самой важной проблемой, современной теоретической информатики и компьютерной математики, будь то алгебра, теория чисел, дискретная математика, криптография или информационная безопасность, является сложность алгоритмов решения NP-трудных задач. Её математическое исследование предполагает построение подходящей модели вычислительной сложности и решение в рамках этой модели задач анализа и синтеза алгоритмов. В ряду первых важное место занимают задачи классификации алгоритмов по вычислительной сложности и построения для алгоритмов точных, рекуррентных или асимптотических оценок сложности. Важны также задачи разработки алгоритмов, решающих те или иные NP-трудные задачи с как можно меньшей сложностью.

Именно о решении этих задач шла речь на конференции в лекции В. В. Быковой. В ней за сложность алгоритма принята его эластичность, а точнее, эластичность функции его временной сложности от размера входных данных и, возможно, параметра задачи [4]. Так назван предел отношения относительного приращения этой функции к относительному приращению аргумента. Он характеризует коэффициент пропорциональности между темпами роста его временной сложности и размера входных данных или параметра задачи. Понятие эластичности заимствовано из экономики, где оно относится к производственным функциям. Это не единственный пример полезного заимствования математикой понятий из других областей науки. Достаточно вспомнить понятие энтропии состояния информационной системы по Шеннону как аналога энтропии состояния физической системы. Свойства эластичности алгоритма в теории сложности оказались столь же продуктивными, сколь и свойства энтропии в теории информации. И это открытие не может не восхищать математиков. Эластичность алгоритма легко вычисляется и выражается более простой формулой, чем

соответствующая логарифмически-экспоненциальная функция временной сложности, а построенная классификация по ней алгоритмов — от субполиномиальных до гиперэкспоненциальных — более прозрачна, нежели её прообраз.

В части, касающейся анализа алгоритмов, в лекции построены нижние и верхние асимптотические оценки временной сложности рекурсивных алгоритмов, решающих задачи путём последовательного уменьшения размера входных данных на некоторую константу. Из этих оценок следует, что такие алгоритмы могут быть только субполиномиальные, полиномиальные и экспоненциальные. Первые возможны лишь при одной подзадаче и беззатратном рекурсивном переходе, вторые — лишь в случае полиномиальной сводимости задачи к одной подзадаче меньшего размера, а третьи — всегда при числе подзадач больше 1 и только.

Параметризация задач — самый «молодой» из известных подходов к преодолению проблемы вычислительной сложности. Несмотря на его сравнительно малую изученность, его перспективность доказана в исследованиях многих зарубежных и отечественных учёных, в том числе и В. В. Быковой [4, 5]. В её лекции дана исчерпывающая двумерная классификация параметризированных и, в частности, FPT-алгоритмов по эластичности от размера данных и параметра задачи; в терминах эластичностей охарактеризованы параметризированные алгоритмы с низкой, равносильной и доминирующей зависимостями от параметра и установлены альтернативные формы характеризации FPT-разрешимости — аддитивная и смешанная, равносильные исходной — мультипликативной. Кроме того, рассказано о технологии построения FPT-алгоритмов для решения задач выбора (поиска и оптимизации в конечной области) методом динамического программирования на графах и гиперграфах с ограниченной древовидной шириной. В частности, осуществлена алгоритмизация этого метода на базе бинарного сепараторного дерева декомпозиции, позволившего решить присущую ему проблему памяти. Продемонстрированы FPT-алгоритмы решения задач SAT и о наименьшем вершинном покрытии графа, построенные на этой базе, и полиномиальные алгоритмы вычисления верхних и нижних оценок древовидной ширины графа и гиперграфа. Использование сепараторного дерева декомпозиции позволило для вычисления таблиц динамического программирования привлечь аппарат реляционной алгебры и ациклических баз данных и тем самым существенно снизить теоретическую и практическую сложность получаемых FPT-алгоритмов.

2 ноября 2012 г. В. В. Быкова успешно защитила докторскую диссертацию на тему «Методы анализа и разработки параметризированных алгоритмов» в совете Сибирского федерального университета по теоретическим основам информатики. От имени участников школы-семинара Sibecrypt поздравляем Валентину Владимировну с этим замечательным событием в её научной жизни и желаем ей дальнейших успехов в нашем общем деле.

В лекции А. А. Евдокимова рассмотрены свойства дискретных метрических пространств и метрик, которые возникают в исследовании вложений конечных пространств и графов. Отображения, в классе которых исследуются вложения, являются изометрическими, локально изометрическими и параметрическим семейством отображений ограниченного искажения. Последние при малых значениях параметров могут рассматриваться как дискретные аналоги непрерывных отображений, сохраняющих метрические свойства близости и отделимости элементов [6, 7]. Свойство k-продолжения метрики для связных графов с обычной метрикой пути означает, что любые две вершины графа, расстояние между которыми меньше k, принадлежат некоторой кратчайшей цепи длины k. Второе свойство связано с характеризацией комбинаторной

структуры шаров в графе, когда их радиусы последовательно возрастают от единицы до диаметра графа (раздувающиеся шары). Точнее, свойство r-разнообразия шаров означает, что шары одного радиуса с центрами в любых двух вершинах графа не равны (как множества вершин), если этот радиус не превосходит r (значение r не больше эсцентриситета графа). Приведены теоремы о значении рассмотренных свойств в вопросах вложений и классификации графов, а также некоторые нерешённые задачи.

Лекция А. А. Семенова посвящена основам структурной теории сложности алгоритмов и использованию различных формальных вычислительных моделей для определения классов двоичных языков, распознаваемых этими моделями. Рассмотрены: полиномиальная детерминированная машина Тьюринга и класс P, полиномиальная недетерминированная машина Тьюринга и класс NP, полиномиальная вероятностная машина Тьюринга и определяемые с её помощью классы (RP, co-RP, BPP), а также класс P/poly, образованный языками, распознаваемыми при помощи семейств схем полиномиальной сложности. Кроме этого, рассмотрена полиномиальная иерархия (иерархия Стокмейера), образованная языками, для определения которых используется оракульная машина Тьюринга. Приведены результаты, касающиеся аргументации сложности задач обращения ряда криптографических функций, базирующиеся на принятых предположениях относительно взаимосвязи между основными сложностными классами. В частности, в краткой форме приведено известное доказательство У. Шенинга того факта, что задача определения изоморфности пары простых графов не может быть NP-полной в предположении, что полиномиальная иерархия не стабилизируется на третьем уровне.

2. Теоретические основы прикладной дискретной математики

Дискретные функции по-прежнему находятся в центре внимания теоретических исследований, ориентированных на криптографические приложения.

В докладе А. М. Зубкова и А. А. Серова построены нижние и верхние оценки числа булевых функций, отстоящих по Хэммингу от аффинных и квадратичных функций на ограниченном расстоянии. Оценки получены с использованием формул включения-исключения и оценок хвостов биномиального распределения. Приведены условия, при которых они асимптотически эквивалентны.

Н. А. Коломеец доказал, что нелинейность всякой булевой функции от чётного числа n переменных, равной 0 (1) на наборах веса меньше (больше) $n/2$, не превосходит $2^{n-1} - \binom{n-1}{n/2}$, и эта оценка точная. Примечательно, что все эти функции обладают максимально возможной алгебраической иммунностью $n/2$, но их нелинейность, как видим, заметно отличается от максимально возможной $2^{n-1} - 2^{n/2-1}$.

Продолжая представление результатов исследования по проблеме статистической независимости суперпозиций булевых функций, начатое на предыдущей школе-семинаре, О. Л. Колчева и И. А. Панкратова на этот раз показали, что 1) если функции $f_1(x, y)$, $f_2(x, y)$ и $f_1(x, y) \oplus f_2(x, y)$ статистически не зависят от переменных в x, то этим свойством обладает и любая суперпозиция вида $g(f_1(x, y), f_2(x, y), z)$, и 2) если $f(x, y)$ статистически не зависит от переменных в x, то $f(x, y) \oplus g(x)$ тоже обладает этим свойством тогда и только тогда, когда f уравновешена или $g = \text{const}$. В этих утверждениях x, y, z — произвольные наборы значений булевых переменных.

Булева функция называется *почти уравновешенной*, если в любой грани области её определения количество элементов, на которых она равна 1, отличается от половины мощности грани не более чем на 1. В своём докладе В. Н. Потапов предложил

некоторые конструкции почти уравновешенных функций и установил некоторые свойства этих функций и нижнюю границу их числа. Он показал, в частности, что класс почти уравновешенных булевых функций является наследственным (содержит вместе с любой функцией и все её подфункции) с бесконечным набором минимальных запретов (функций не из класса, все подфункции которых принадлежат классу) и что булева функция f почти уравновешена, если и только если $f - h \in B_0$, где h — булева функция со значением 1 на всех наборах нечётного веса (и только) и $g \in B_0$, если $g : \{0,1\}^n \to \{-1,0,1\}$, $g^{-1}(1)$ и $g^{-1}(-1)$ — подмножества наборов соответственно чётного и нечётного веса и абсолютная величина суммы значений g на любой грани области её определения не превышает 1.

В текущем году С. В. Смышляев доказал гипотезу Голича о перестановочности (линейности) по первой или последней существенной переменной любой сильно совершенно уравновешенной булевой функции. В докладе на школе-семинаре он представил обобщение этой гипотезы как условие Голича в формулировке: «Сильная совершенная уравновешенность в P_k (для любого $k \geqslant 2$) эквивалентна перестановочности по первой или последней существенной переменной» и в свою очередь выдвинул гипотезу: «Условие Голича выполнено тогда и только тогда, когда k простое», доказав её в части необходимости простоты k и установив некоторые утверждения, косвенно подтверждающие эту гипотезу и в части достаточности.

В своё время, в 2011 г., Н. Н. Токарева сформулировала гипотезу о возможности разложения любой булевой функции от чётного числа n переменных степени не более $n/2$ в сумму двух бент-функций от n переменных. В докладе на школе-семинаре она доказала ослабленный вариант этой гипотезы, показав, что при чётном n любая булева функция от n переменных степени $d \leqslant n/2$ может быть представлена суммой не более чем $2\binom{2b}{b}$ бент-функций от n переменных, где b — наименьшее целое, такое, что $b \geqslant d$ и $(2b)|n$.

Булева функция f от чётного числа переменных n называется *функцией Касами*, если для некоторого $\lambda \in \mathrm{GF}(2^n)$ и любого $\beta \in \mathrm{GF}(2^n)$ имеет место $f(\beta) = \mathrm{tr}(\lambda\beta^k)$, где $k = 2^{2d} - 2^d + 1$, $(n,d) = 1$, $0 < d < n$. При λ, не равном кубу элемента в $\mathrm{GF}(2^n)$, она является бент-функцией. Булева функция *s-существенно зависима*, если любое произведение s её переменных входит в моном её АНФ. В докладе А. А. Фроловой показано, что для любого чётного $n \geqslant 8$ функция Касами степени t является s-существенно зависимой, а её кратная производная по s линейно независимым направлениям не равна тождественно 0, если $s = t - 3$, $4 \leqslant t \leqslant n/2$, или $s = t - 2$, $4 \leqslant t \leqslant (n+3)/3$. Кроме того, она 2-существенно зависима, если $t \geqslant 4$.

В докладе К. Л. Глуско и С. С. Титова предложен метод решения квадратного уравнения $x^2 + x = a$ в поле $\mathrm{GF}(2^n)$ путём разложения его в систему булевых уравнений $x_{i-1}^2 + x_i + a_i = 0$, $i = 0, 1, \ldots, n-1$, связывающих компоненты векторов x^2, x и a.

В докладе В. А. Едемского и О. В. Антоновой предложен метод анализа линейной сложности последовательностей с периодом $2^m p^n$, построенных на основе обобщённых циклотомических классов. Метод позволяет для рассматриваемых последовательностей вычислять линейную сложность, получать её оценки, строить минимальный многочлен и определять последовательности с заведомо высокой линейной сложностью. Эти возможности метода продемонстрированы на ряде последовательностей, построенных на основе классов квадратичных и биквадратичных вычетов. Полностью доклад опубликован в [8].

Формулы для среднего и дисперсии числа векторов веса s или не больше s в случайном линейном двоичном (N, k)-коде, имеющем равномерное распределение на множестве всех таких кодов, выведены в докладе А. М. Зубкова и В. И. Круглова. Приведены формулы для среднего и дисперсии веса w покомпонентной суммы по модулю 2 двух независимых случайных булевых векторов длины N, имеющих вес s и t соответственно и равномерные распределения на множествах таких векторов, а также для вероятности равенства $w = m$. Дана также оценка сверху для вероятности линейной зависимости n независимых случайных булевых векторов длины N и веса s, имеющих равномерное распределение на множестве таких векторов.

В докладе А. С. Кузнецовой и К. В. Сафонова указано решение комбинаторной задачи, в которой для последовательности первых n натуральных чисел, записанных в произвольном порядке по окружности, требуется вычислить наименьшее число d транспозиций соседних чисел, чтобы все числа в окружности оказались записанными в естественном порядке: $1, 2, \ldots, n-1, n$, и приведены значения d для $n = 2, 3, \ldots, 12$.

Свойства наборов натуральных чисел с наибольшим общим делителем 1 изучены и алгоритм их перечисления предложен в докладе С. Н. Кяжина и В. М. Фомичёва. Полностью доклад опубликован в [9].

Вектор a из различных натуральных чисел, упорядоченных по возрастанию, называется *инъективным*, если для любого натурального числа α существует не более одного подмножества компонент этого вектора, сумма которых равна α. Вектор a *сверхрастущий*, если любая его компонента больше суммы всех предыдущих его компонент. Говорят также, что вектор $b = b_1 b_2 \ldots b_n$ получен из вектора $a = a_1 a_2 \ldots a_n$ операцией *сильного модульного умножения* относительно модуля m и множителя t, если m больше суммы компонент в a и $b_i = a_i t \bmod m$, $i = 1, 2, \ldots, n$. В докладе Д. М. Мурина показано, что количества инъективных векторов и сверхрастущих векторов с числом компонент (размерностью) n и наибольшим значением компоненты M ведут себя как полиномы степени $n-1$ от M, а пределы их отношений к числу всех векторов с теми же параметрами n и M при $M \to \infty$ и фиксированном n существуют, конечны и не равны 0. На основании результатов компьютерных экспериментов установлено, что при фиксированном натуральном n и значениях натурального M, близких к 2^{2n}, отношение количества различных инъективных векторов размерности n, полученных из сверхрастущих векторов размерности n с наибольшей компонентой меньше M с помощью сильного модульного умножения относительно модуля $m \leqslant \min(M, 2\sum_{i=1}^{n} a_i)$ и всевозможных значений множителя $t = 2, 3, \ldots, m-1$, к числу всех инъективных векторов размерности n с наибольшей компонентой меньше M достигает величины 0,9 и что операция сильного модульного умножения в применении к сверхрастущим векторам приводит чаще всего к векторам с малой евклидовой длиной.

Множество мобильных точек подстановки $G \in S_N$ обозначается $\Gamma(G)$, а множество всех подстановок с q мобильными точками — $\Gamma_N(q)$. Здесь $\Gamma(G) \subseteq \{1, \ldots, N\}$, $2 \leqslant q \leqslant N$. В докладе А. Б. Пичкура доказано, что если $N \geqslant 8$, $3 \leqslant q \leqslant N/2$ и $1 < |\Gamma(G)| < 2q-1$ или $N > 10$, $2 \leqslant t < N-2$, $2 \leqslant q < (N-t)/2+1$ и $t \leqslant |\Gamma(G)| \leqslant 2q+t-2$, то существуют подстановки $H_1 \in \Gamma_N(q)$, $H_2 \in \Gamma_N(q+1)$ или $H_1 \in \Gamma_N(q)$, $H_2 \in \Gamma_N(q+t)$ соответственно, такие, что $G = H_1 \cdot H_2$. Показано также, что при $N \geqslant 4$, $2 \leqslant q < N/2$ подстановка из $\Gamma_N(2q+1)$ принадлежит множеству $\Gamma_N(q) \cdot \Gamma_N(q+1)$, если и только если среди её неединичных циклов есть такие, сумма длин которых равна q, а при $N \geqslant 4$, $2 \leqslant q \leqslant N/2$ подстановка из $\Gamma_N(2q)$ принадлежит множеству $\Gamma_N(q) \cdot \Gamma_N(q+1)$, если и только если среди её неединичных циклов есть цикл длины $m_0 > 2$ и циклы длин

$m_1, \ldots, m_k$, таких, что $q - m_1 + \ldots + m_k \in \{2, \ldots, m_0 - 1\}$. Аналогичные характеризации имеются для подстановок из $\Gamma_N(2q + t - 1)$ и из $\Gamma_N(2q + t)$, принадлежащих произведению $\Gamma_N(q) \cdot \Gamma_N(q + t)$.

В совместном докладе Б. А. Погорелова с М. А. Пудовкиной и в отдельном докладе М. А. Пудовкиной изучены свойства групп преобразований векторного пространства над полем GF(2), порождённых парами операций, в которых одна операция — наложение вектора, а вторая — соответственно линейное преобразование и замена вектора по блокам.

Декомпозиции и аппроксимации недоопределённых данных посвящён доклад Л. А. Шоломова. Первая заключается в представлении, а вторая в реализации каждого недоопределённого символа набором символов 0, 1, * (неопределённость). Доказаны теоремы их существования и алгоритмов их эффективного построения для любого источника недоопределённых данных. Показана также возможность эффективного построения безызбыточных (тупиковых) декомпозиций и аппроксимаций и эффективной проверки равносильности двух разложений; построена полная система равносильных преобразований различных разложений недоопределённого источника.

Алгоритм с субэкспоненциальной сложностью для вычисления изогений (алгебраических морфизмов, являющихся групповыми гомоморфизмами) большой степени между эллиптическими кривыми предложен в устном докладе В. Г. Сухарева. Он построен по схеме алгоритма BCL (Broker — Charles — Lauter), в котором для более быстрой факторизации идеала в кольце изогений кривой используются идеи из субэкспоненциального алгоритма дискретного логарифмирования в классических группах (Hafner and McLurley).

3. Математические методы криптографии и стеганографии

В докладе А. В. Волгина и А. В. Иванова рассматривается генератор, порождающий последовательность $u_0u_1\ldots$ над полем $P = \mathrm{GF}(p^s)$ по рекуррентному соотношению $u_{n+1} = au_n + b$, $n \geqslant 0$, усложнённый маской $(e_0e_1\ldots e_s) \in P^{s+1}$, где все e_i представимы линейными комбинациями одних и тех же k элементов базиса поля P и $k < s$. Известно, что при известных разностях $u_i - e_i$, $i = 0, \ldots, t-1$, для $k+1 \geqslant t > 2$ и известных параметрах a, b, где a не принадлежит фиксированному подмножеству в P мощности меньше $2p^{\sigma_t} + \binom{k}{t-2} p^{2k-t+2}$ (σ_t — наибольший из делителей s, меньших t), значение u_0 находится с полиномиальной сложностью. Утверждается, что это верно и при неизвестном b и прежних остальных условиях.

В 2001 г. М. М. Глухов-мл. построил класс алгебро-геометрических кодов $\{C_r : [768, 3r - 57, 768 - 3r]_{256}, 39 \leqslant r \leqslant 255\}$ на кривой, заданной над $P = \mathrm{GF}(2^8)$ уравнением $y^3 = x^{60} + x^{57} + x^{54} + \ldots + x^3 + 1$. Из каждого кода C_r путём вычёркивания в его порождающей матрице любых $(768 - m)$ столбцов можно получить код $C'_{r,m}$, который при условии $114 < 3r < m \leqslant 768$ будет $[m, 3r - 57, m - 3r]$-кодом. В своём докладе на школе-семинаре автор этих кодов показал, что при $r \leqslant 127$ и фиксированном m число различных кодов $C'_{r,m}$ равно $\dfrac{1}{18}\binom{768}{m}$. Доказательство утверждения конструктивно и даёт возможность выбора столбцов порождающей матрицы так, чтобы все получаемые коды были различны. Этим результатом фактически заявлена новая идея образования порождающей матрицы кода в кодовых криптосистемах с открытым ключом. Изучены также условия на выбор столбцов в порождающей матрице кода C_r для получения кода $C'_{r,m}$ с тривиальной группой автоморфизмов. Доказано, что если композиция ав-

томорфизма и покомпонентного умножения всех кодовых векторов кода $C'_{r,m}$ на вектор $k \in P^m$ является автоморфизмом этого кода, то все компоненты в k одинаковы.

В докладе А. А. Камаевой рассматриваются упрощённые варианты хэш-функции Whirpool, в которых блочный шифр последней усечён до одного (двух) раундов, и показывается, что наибольшая вероятность найти коллизию для них равна 2^{-115} (2^{-225}).

Г. А. Карпунин и Е. З. Ермолаева результатами компьютерного эксперимента показывают, что трудоёмкость известного алгоритма построения коллизии для хэш-функции RIPEMD в квадрат раз выше заявленной его авторами (X. Wang, X. Lai, D. Feng, et al.).

В докладе Д. С. Ковалёва сообщается об аппаратной реализации на базе ПЛИС шифра FAPKC-4 и о его программных реализациях на языках Perl и PHP. Приведены результаты экспериментов с этими реализациями. Показано в частности, что в среднем ПЛИС-реализация на Virtex-5 XCVLX330T работает в 1,34 раза быстрее, чем PHP-реализация на компьютере с процессором Intel Core i5-2300, которая, в свою очередь, в 2,6 раза быстрее, чем Perl-реализация на том же компьютере.

В докладе К. Г. Когоса и В. М. Фомичёва обсуждается хорошо известная проблема разложения системы дискретных уравнений путём фиксации значений некоторых переменных на подсистемы, обладающие полезными свойствами (линейность, треугольность и т. п.), облегчающими их решение. Полностью доклад опубликован в [10].

В докладе А. М. Кореневой и В. М. Фомичёва описан итеративный блочный шифр, построенный путём конкретизации параметров обобщённой схемы Фейстеля, рассматриваемой как регистр сдвига длины m над множеством n-мерных булевых векторов с обратной связью — функцией от раундового ключа и компонент регистра. Шифр представлен как иллюстрация к этому обобщению схемы Фейстеля. В нём $m = 4$, $n = 16$ и функция обратной связи регистра выбрана так, что шифру обеспечивается свойство инволютивности.

В докладе С. Д. Лошкарёва с целью выяснения влияния булевых функций и констант циклических сдвигов в MD5 на стойкость этой хэш-функции к дифференциальному анализу построены разностное уравнение для каждого шага преобразования в ней и формула для среднего значения вероятности угадать решение этого уравнения при случайном и равновероятном выборе значений переменных и различных фиксациях значений параметров. Путём сравнения этих значений для разных булевых функций или разных величин циклических сдвигов можно сравнивать последние по степени их влияния на исследуемую стойкость MD5. Так, показано, что использование функции XOR в MD5 оптимально с точки зрения устойчивости MD5 к дифференциальной атаке и что для каждой булевой функции в MD5 все значения циклических сдвигов с этой точки зрения эквивалентны.

В связи с возможностью задания структур доступа, реализуемых в совершенных идеальных схемах разделения секрета, матроидами в докладе Н. В. Медведева и С. С. Титова вводится понятие *почти порогового* матроида. В нём все циклы имеют некоторую одну и ту же мощность n, но возможны подмножества мощности n, которые не являются циклами. Утверждается, что для $n = 1, 2, 3$ связного почти порогового, но не порогового матроида не существует. Матроид называется *разделяющим*, если для любых двух его элементов в нём есть цикл с одним из этих элементов, не содержащий другого. Утверждается, что бинарные (в $\mathrm{GF}(2^m)$) связные разделяющие почти пороговые матроиды исчерпываются кодами Рида — Маллера первого порядка.

В докладе Е. Л. Столова предложена последовательностная схема генератора случайных чисел, состоящая из конечного числа одинаковых комбинационных блоков,

работающих асинхронно и реализующих функцию 3-значной логики от двух переменных. Утверждается, что последовательность состояний схемы является марковским процессом с единственным финальным распределением вероятностей и с равномерным распределением на выходе каждого блока.

Один из видов цифровой подписи — *кольцевая* — позволяет любому участнику группы подписать сообщение от имени всей группы, а проверяющему убедиться, что подпись сделана участником действительно этой группы, но кем именно — ему не дано знать. В докладе Г. О. Чикишева кольцевая подпись наделяется свойством одноразовости: при подписании двух сообщений одним и тем же участником группы его личность становится известной. Это свойство требуется во многих приложениях, в том числе для электронного голосования, для обеспечения неотслеживаемости платежей в системах электронных денег и др. В предложенной кольцевой подписи оно достигается благодаря тому, что каждый участник имеет две пары (открытый ключ, закрытый ключ), и подписывающий использует оба закрытых ключа так, что повторное применение второго из них приводит к некоторому одному и тому же значению одной из компонент в разных кольцевых подписях, указывающему на соответствующие два открытых ключа и тем самым идентифицирующему подписавшего.

В докладе Г. И. Шушуева утверждается, что уравнение $(a, x_0) \oplus (a, x_5) = (c, k_4) \oplus \oplus (c, k_5)$, где x_0 — блок открытого текста, x_i и k_i для $i > 0$ — соответственно блок шифртекста на выходе i-го раунда и раундовый ключ этого раунда, $a = (0^{32}, 0^{32}, 0^{32}, c)$ и $c = \texttt{0x0011ffba}$, является оптимальным линейным приближением пяти раундов SMS4 (стандарта блочного шифра КНР для беспроводных сетей). Утверждается также, что минимальная трудоёмкость линейного криптоанализа девяти раундов SMS4 составляет 2^{115} операций зашифрования.

Результат обнаружения цифровых водяных знаков на основе модифицированной контрольной карты Хотеллинга существенно зависит от содержимого обучающей выборки. Опыт показывает, что лучшие результаты получаются, когда значения соответствующих пикселей изображений обучающей выборки и тестируемого контейнера близки, или, говоря другими словами, изображения в выборке и контейнере подобные. Задача автоматизации поиска подобных изображений решается в докладе Б. Б. Борисенко, предложившего считать изображение I более подобным изображению I_1, чем изображению I_2, если для некоторой хэш-функции h значение $h(I)$ ближе к $h(I_1)$, чем к $h(I_2)$, в некоторой метрике. В качестве h предложено использовать вейвлет-преобразование Хаара, последний уровень в котором определяется как первый из тех, на которых хотя бы один из размеров матрицы коэффициентов аппроксимации не превышает 32.

4. Математические основы компьютерной безопасности

Как и прежде на школе-семинаре, в проблематике этого направления важнейшее место занимают разработка и исследование математических моделей безопасности компьютерных систем (КС).

В докладе Д. М. Бречки представлен алгоритм поиска мостов в графе доступов модели Take-Grant между известными островами графа. Алгоритм основан на поиске в глубину, имеет полиномиальную сложность, предназначен для применения в анализе безопасности КС.

Достаточные условия для реализации информационного потока по памяти в операционных системах (ОС) семейства Linux сформулированы в докладе П. Н. Девянина.

Их проверка заключается в установлении истинности некоторого предиката ролевой ДП-модели управления доступом и информационными потоками в таких ОС.

Нередко реализация запрещённых информационных потоков по времени в ОС осуществляется с использованием интерфейса сокетов: наличие или отсутствие слушающего сокета на некотором порту может служить посылкой одного бита информации — соответственно 1 или 0. Некоторые известные методы предотвращения подобных информационных потоков проанализированы в докладе А. Н. Долгих. Предложен механизм регистрации событий с целью идентификации таких потоков.

В известных ролевых моделях управления доступом (RBAC и др.) отсутствуют средства задания и контроля прав доступов, учитывающие иерархию сущностей в КС. Модель иерархического ролевого управления доступом, RBAC-H, предложена в докладе Д. Н. Колегова. В ней, кроме всего прочего, введены типы сущностей, верхняя полурешётка $(L, \geqslant)$ уровней иерархии сущностей, функция f_e, задающая для каждой сущности её уровень в этой полурешётке, и предикат, истинный для тех и только тех субъект-сессий s, сущностей e и прав доступа p, для которых $f_e(e) \leqslant f_e(s)$ и право доступа p к сущности типа e принадлежит множеству прав доступа ролей субъект-сессии s. Это существенно расширяет класс компьютерных систем, в которых ролевое управление доступом адекватно выражается в математической модели.

Ещё одно расширение языковых средств ДП-моделей предложено в докладе П. Ю. Свиридова с целью адекватного описания мандатных и ролевых механизмов системы управления доступом RSBAC в ОС GNU/Lunux. А именно, в ДП-модель вводятся: множества атрибутов, ассоциируемых с сущностями и учитываемых при проверке прав доступа к последним; новые права и виды доступа и типы сущностей, характерные для RSBAC — право доступа на создание (клонирование) процесса, доступ для изменения рабочей директории, тип сущностей межпроцессорного обмена и т. п.; вместо линейной — произвольная решётка уровней доступа; множество прав доступа к сущностям определённого типа и функция прав доступа ролей к таким сущностям, как в RBAC-H.

Для анализа безопасности систем управления базами данных В. Ю. Смольянинов построил СУБД ДП-модель как модификацию известной РОСЛ ДП-модели и сформулировал в ней достаточные условия похищения прав доступа.

В докладе Н. О. Ткаченко показывается, как в СУБД MySQL (с дискреционным управлением доступом) может быть реализовано мандатное управление доступом путём использования механизма расширения безопасности системы SELinux. Для этого надо для каждой сущности СУБД MySQL задать контекст безопасности в виде набора атрибутов — пользователя, роли, типа и уровня безопасности, создать модуль политики безопасности средствами системы SELinux и разработать для СУБД MySQL компоненту с функциями Object Manager. Сообщается, как это сделано в конкретной реализации данного метода.

Обзор шести публикаций последних лет, посвящённых моделям атрибутного управления доступом в КС, дан в докладе Д. В. Чернова, сделавшего попытку изложить их основные свойства в терминах языка ДП-моделей.

Информация о лабораторном практикуме «Основы построения защищённых компьютерных сетей» на платформе Cisco Packet Tracer содержится в докладе Д. Н. Колегова и Б. Ш. Хасанова. Его целью является привлечение студентов к исследовательской работе по разработке архитектуры и методов проектирования защищённых компьютерных сетей, планированию и построению подсистем защиты информационных технологий, настройке механизмов и средств защиты сетевой инфраструк-

туры, поиску и устранению неисправностей в системах защиты компьютерных сетей. Кроме традиционной формы обучения практикум позволяет проводить многопользовательские и ролевые игры студентов по проектированию и анализу защищённых компьютерных сетей.

5. Прикладная теория графов

Много докладов на школе-семинаре было посвящено приложениям теории графов к синтезу отказоустойчивых управляющих и вычислительных систем. Традиционно сильно в данном направлении выступает Саратовская научная школа, от которой в этом году было представлено 6 докладов.

В 1995 г. Ф. Харари и М. Хурум высказали утверждение о том, что минимальное вершинное 1-расширение сверхстройного дерева с k цепями и p сложными вершинами содержит в точности $k+p+1$ дополнительных ребер, и предложили метод построения такого расширения. Здесь вершина сверхстройного дерева T, расположенная на ярусе $j>1$ в цепи длины m, называется *сложной*, если в T нет концевых вершин на $(j-1)$-м и $(m-j)$-м ярусах. В докладе М. Б. Абросимова и Д. Д. Комарова отмечается, что в общем случае построенное 1-расширение не обязательно является минимальным; приводятся примеры сверхстройных деревьев, имеющих 1-расширения с меньшим, чем $k+p+1$, числом дополнительных рёбер.

В докладе М. Б. Абросимова и Н. А. Кузнецова сообщается о вычислительном эксперименте с использованием распределённых вычислений, в рамках которого удалось построить все минимальные вершинные (MB-1P) и рёберные (MP-1P) 1-расширения циклов с числом вершин до 17; приводятся данные о количестве таких расширений.

В докладе М. Б. Абросимова и О. В. Моденовой изучаются орграфы, имеющие минимальные вершинные 1-расширения с одной и двумя дополнительными дугами; доказано, что 1) объединения нескольких двухвершинных цепей с одной или более изолированными вершинами, и только они, имеют MB-1P с одной дополнительной дугой; 2) среди связных орграфов гамильтоновы цепи, и только они, имеют MB-1P с двумя дополнительными дугами; 3) среди несвязных орграфов без изолированных вершин только орграфы, являющиеся объединением гамильтоновой цепи P_n с несколькими контурами C_{n+1} при $n>2$, имеют в своём MB-1P две дополнительных дуги; при $n=2$ добавляется ещё один случай: вместо контура C_3 можно взять транзитивную тройку. Представлен вид всех этих расширений.

Расширения неориентированных графов, вершинам которых могут быть приписаны различные типы, рассматриваются в докладе П. П. Бондаренко. Описаны все MB-1P и MP-1P цепей P_n, концевые вершины которых считаются принадлежащими одному типу, а неконцевые — другому. Доказано, что MB-1P таких цепей имеют $3k$ рёбер при $n=2k$ и $3k+2$ рёбер при $n=2k+1$, а MP-1P имеют $3k-1$ рёбер при $n=2k$ и $3k+1$ рёбер при $n=2k+1$.

Индексом состояния динамической системы называется расстояние от этого состояния до аттрактора. В докладе А. В. Жарковой предложен алгоритм вычисления индекса состояния динамической системы булевых векторов (B^n,θ), где для вектора v в B^n, рассматриваемого как цикл, в котором первая компонента следует за последней, $\theta(v)$ получается заменой в векторе v каждой биграммы 10 биграммой 01. Доказано, что максимальный индекс состояния в такой системе равен $(n-1)/2-1$ для нечётного n и $n/2-1$ для чётного.

В докладе Е. О. Кармановой рассматриваются *конгруэнции цепей*, т. е. такие отношения эквивалентности на множестве вершин цепи, все классы которых являются

независимыми множествами. Доказано, что количество конгруэнций m-рёберной цепи равно количеству эквивалентностей на m-элементном множестве; найдена длина кратчайшей цепи, фактор-графом которой является данный граф G; она равна $m + l - k$, где m — количество рёбер G, l — количество рёбер в минимальном цепном паросочетании на множестве вершин нечётной степени и k — максимальная из длин цепей в таких паросочетаниях.

Авторы И. С. Грунский и С. В. Сапунов рассматривают задачу разметки блуждающим агентом вершин графа так, чтобы в окрестности радиуса 2 каждой вершины все вершины были размечены разными метками. Предложены алгоритмы выполнения такой разметки агентом, наблюдающим из каждой вершины её окрестность радиуса 3, и агентом, наблюдающим только окрестность радиуса 2, но способным ставить метки двух типов; доказана вычислительная эквивалентность этих агентов.

Интервальной рёберной раскраской графа называется правильная раскраска его рёбер, при которой для каждой вершины графа рёбра, инцидентные ей, окрашены в последовательные цвета. Известно, что задача об интервальной рёберной раскраске NP-полна. В докладе А. М. Магомедова сформулирована теорема о том, что задача об интервальной рёберной раскраске остаётся NP-полной и для двудольных мультиграфов $G = (X, Y, E)$ с $|X| = 2$.

Разбиение множества рёбер двудольного графа $G = (X, Y, E)$ на паросочетания E_1, E_2, ... называется *непрерывным*, если любое ребро, инцидентное вершине x степени d из X, включено в одно из первых d паросочетаний. В докладе Т. А. Магомедова представлен алгоритм поиска такого разбиения, состоящий в последовательном удалении из графа минимальных паросочетаний, насыщающих все вершины максимальной степени. Доказано, что последний элемент разбиения является полным паросочетанием X с Y.

Задача построения графа, изоморфного заданному графу G, при помощи блуждающего по G агента A рассмотрена в докладе Е. А. Татаринова. Ранее автором был предложен базовый алгоритм решения этой задачи со сложностью $O(n + qt)$, где n — количество вершин графа, q — его цикломатическое число и t — длина максимального простого цикла в G. Наибольшего времени при этом требует проход по так называемому «красному пути» — пути, состоящему из уже пройденных вершин, для которых не все инцидентные им рёбра восстановлены. Здесь предложена модификация базового алгоритма, состоящая в том, что в помощь агенту A придаются ещё j агентов, располагающихся вдоль красного пути и способных передавать информацию (в частности, о расстоянии от агента до начала или конца красного пути) по цепочке. Тем самым сложность алгоритма понижена до $O(n + qt/j)$ в случае, если вспомогательные агенты поддерживают равные расстояния между собой.

В докладе Л. И. Сенниковой и А. А. Кочкарова рассмотрены предфрактальные графы, т. е. графы, полученные из связного графа-затравки за конечное число итераций, где каждая итерация состоит в замене в графе каждой вершины графом-затравкой и каждого ребра — ребром между произвольными вершинами соответствующих его концам графов-затравок. Предложен параллельный алгоритм поиска остовного дерева минимального веса (ОДМВ) на взвешенном предфрактальном графе. Алгоритм применяет стратегию «разделяй и властвуй»: ОДМВ отыскиваются (алгоритмом Прима) на подграф-затравках, изоморфных исходной затравке, затем результаты объединяются. Сложность алгоритма равна $O(n^{L+2})$, где n — количество вершин затравки и L — количество итераций. Заметим, что если алгоритм Прима применить к предфрактальному графу целиком, то получим сложность $O(n^{2L})$.

6. Математические основы информатики и программирования

В докладе А. Ю. Бернштейна и Н. В. Шилова исследуется задача о роботах в пространстве, которые, зная собственные координаты и координаты всех укрытий и имея возможность попарного общения и обмена укрытиями друг с другом, хотят перераспределить укрытия между собой так, чтобы пути от них к своим укрытиям не пересекались. Утверждается, что в случае бесконечного пространства не существует протокола решения этой задачи, если роботы обмениваются ограниченным числом бит информации, и что в случае конечного пространства существует протокол, который позволяет роботам, обмениваясь ограниченной информацией, узнать, пересекаются или нет их пути к своим укрытиям, не раскрывая своих координат другим.

В настоящее время существует множество распределённых СУБД со свойством масштабируемости, большая часть которых не использует реляционных схем данных. В работе И. Н. Глотова, С. В. Овсянникова и В. Н. Тренькаева предлагаются принципы построения системы управления реляционной MySQL-совместимой распределённой базой данных со свойствами масштабируемости и отказоустойчивости. За основу взята открытая СУБД MariaDB (ветка MySQL), которая изначально ориентирована на управление локальными данными. Особенностью предлагаемого решения является разделение сервера MariaDB на две части: ядро и движок. При этом движок вынесен на удалённый узел, который по сети принимает запросы от ядра. Для реализации данной схемы разработаны дополнительные модули для сервера MariaDB: виртуальный движок и виртуальное ядро, а также протокол VSVD сетевого взаимодействия этих модулей.

Проект добровольных вычислений SAT@home, созданный ИДСТУ СО РАН и ИСА РАН и предназначенный для решения задачи о выполнимости КНФ, представлен в докладе О. С. Заикина, М. А. Посыпкина и А. А. Семенова. Распределённое приложение проекта состоит из управляющей и расчётной частей. Управляющая часть отвечает за создание заданий в базе данных проекта и обработку результатов их выполнения. Основу расчётной части составляют SAT-решатели minisat-1.14.1 и minisat-2.0, модифицированные с учётом особенностей КНФ, кодирующих задачи обращения дискретных функций. На момент представления доклада в проекте SAT@home принимали участие более тысячи активных добровольцев и были задействованы более двух тысяч активно работающих ПК; успешно решены 9 из 10 тестов по криптоанализу генератора ключевого потока A5/1, не поддающихся анализу с использованием радужных таблиц. Средняя производительность проекта за весь период работы составляет 1,7 терафлопс.

В докладе А. Г. Банных рассматривается проблема выполнения массовых операций на многомерных массивах данных. Доказаны утверждения, позволяющие свести задачу с массовыми обновлениями к хорошо изученной задаче с единичными обновлениями, которую можно решать с использованием любых существующих структур данных. Это свойство позволяет выбирать оптимальную структуру данных для каждой задачи отдельно.

Большое внимание на школе-семинаре было уделено проблеме анализа программного обеспечения с целью восстановления алгоритма по тексту программы, исполняемому или объектному файлу. А. С. Бурлаков в своём докладе представил разрабатываемую им систему динамического анализа исполняемых файлов, которая эмулирует оперативную память и устройства ввода/вывода и может настраиваться на разные типы процессоров и компиляторов. Семантика машинных команд описывается на искусственном языке, разработанном автором; эмулятор при запуске читает описание

семантики, инициализируется должным образом и затем может дизассемблировать программы, скомпилированные для данного процессора, и выполнять их пошаговую отладку.

Проблеме декомпиляции объектных файлов DelphiB посвящён доклад А. А. Михайлова. С помощью разработанных автором структур данных, предназначенных для описания семантики машинных команд процессоров семейства Intel x86, решаются задачи извлечения имён вызываемых виртуальных методов, распространения констант, подстановки имён используемых переменных и т. д., которые существенно ускоряют восстановление алгоритма исследуемой программы.

В докладе А. М. Сауха рассматривается задача синтаксического и семантического анализа программ на языках высокого уровня, лексика которых задаётся с помощью регулярных выражений, синтаксис — контекстно-свободной грамматикой. Целью такого анализа является построение таблицы идентификаторов и выявление областей их использования. В результате получается абстрактное представление разбираемой программы, не зависящее от языка программирования и доступное для семантического анализа. В настоящее время в терминах системы формально описан язык C#; в дальнейшем предполагается расширить список языков.

7. Вычислительные методы в дискретной математике

Алгоритмы решения задач построения инволюции по её номеру и вычисления номера инволюции (в лексикографическом порядке) предложены в докладе Л. Н. Андреевой и В. А. Потеряевой. Приводятся результаты испытаний алгоритмов для инволюций порядков от 25 до 31.

Авторы Ю. Л. Зачёсов и А. М. Гришин, проведя (по опубликованным данным) сравнение оценки производительности метода решета числового поля факторизации чисел с экстраполированными оценками производительности самых мощных суперкомпьютеров из списка Top500, пришли к выводу, что трудоёмкость алгоритма факторизации при прогнозируемом увеличении размеров чисел, используемых в качестве параметров криптосистем, будет возрастать быстрее, чем производительность суперкомпьютеров.

Два доклада посвящены проблеме построения и исследования параллельных алгоритмов решения комбинаторных задач. В докладе А. В. Медведева сообщается об опыте реализации на видеокарте с использованием технологии CUDA алгоритма поиска совершенной нелинейности (т. е. расстояния до класса функций с линейной структурой) булевой функции, которая оказалась быстрее, чем последовательный алгоритм, примерно в 106 раз, а в сравнении с параллельной реализацией на центральном процессоре — примерно в 26,5 раз. Значительное увеличение производительности алгоритмов приведения базиса целочисленных решёток за счёт замены рекуррентного алгоритма Грама — Шмидта параллельными алгоритмами ортогонализации экспериментально продемонстрировано в работе В. С. Усатюка.

Для построения статистических критериев с заданными вероятностями ошибок требуется знание распределений используемых в этих критериях статистик. Вместо точных формул (которые зачастую слишком громоздки с вычислительной точки зрения) в качестве приближений часто используют формулы из соответствующих предельных теорем, относящихся к случаям, когда объём выборки неограниченно возрастает. Представляют интерес методы точного вычисления распределений статистик для выборок умеренного объёма. В докладе А. М. Зубкова и М. В. Филиной обсуждается такой способ точного вычисления распределений разделимых статистик с помощью

аппарата неоднородных по времени цепей Маркова и результаты численного исследования распределений статистики Пирсона для схем с числом исходов до нескольких сотен и числом испытаний до нескольких тысяч.

Авторами А. А. Семеновым и А. С. Игнатьевым ранее был предложен алгоритм гибридного SAT+ROBDD-логического вывода, решающий задачу обращения дискретной функции с помощью сведения её к задаче выполнимости КНФ. В представленном на школе-семинаре докладе строго доказана сходимость этого алгоритма.

ЛИТЕРАТУРА

1. Тезисы докл. Всерос. конф. «XI Сибирская научная школа-семинар с международным участием „Компьютерная безопасность и криптография“» — Sibecrypt'12 (Иркутск, 3–8 сентября 2012 г.) // Прикладная дискретная математика. Приложение. 2012. № 5. 135 с.
2. *Черёмушкин А. В.* О содержании понятия «электронная подпись» // Прикладная дискретная математика. 2012. № 3(17). С. 53–69.
3. *Туэжилин М. Э.* Латинские квадраты и их применение в криптографии // Прикладная дискретная математика. 2012. № 3(17). С. 47–52.
4. *Быкова В. В.* FPT-алгоритмы и их классификация на основе эластичности // Прикладная дискретная математика. 2011. № 2(12). С. 40–48.
5. *Быкова В. В.* FPT-алгоритмы на графах ограниченной древовидной ширины // Прикладная дискретная математика. 2012. № 2(16). С. 65–78.
6. *Евдокимов А. А.* Вложения графов в n-мерный булев куб и интервальное кодирование табло // Вестник Томского госуниверситета. Приложение. 2006. № 17. С. 15–19.
7. *Евдокимов А. А.* Вложения в классе параметрических отображений ограниченного искажения // Ученые записки Казанского госуниверситета. Сер. Физико-математические науки. 2009. Т. 151. № 2. С. 72–80.
8. *Едемский В. А., Антонова О. В.* Линейная сложность обобщённых циклотомических последовательностей с периодом $2^n p^m$ // Прикладная дискретная математика. 2012. № 3(17). С. 5–12.
9. *Кяжин С. Н., Фомичёв В. М.* О примитивных наборах натуральных чисел // Прикладная дискретная математика. 2012. № 2(16). С. 5–14.
10. *Когос К. Г., Фомичёв В. М.* О разветвлениях криптографических функций на преобразования с заданным признаком // Прикладная дискретная математика. 2012. № 1(15). С. 50–54.

СВЕДЕНИЯ ОБ АВТОРАХ

АГИБАЛОВ Геннадий Петрович — профессор, доктор технических наук, заведующий кафедрой защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: **agibalov@isc.tsu.ru**

ГРИБОВ Алексей Викторович — аспирант Московского государственного университета им. М. В. Ломоносова, г. Москва. E-mail: **alexey.gribov@yandex.ru**

ЕМЕЛИЧЕВ Владимир Алексеевич — профессор, доктор физико-математических наук, профессор кафедры математической кибернетики Белорусского государственного университета, г. Минск. E-mail: **emelichev@bsu.by**

ЖИХАРЕВИЧ Владимир Викторович — кандидат физико-математических наук, доцент Черновицкого факультета Национального технического университета «Харьковский политехнический институт», г. Черновцы. E-mail: **vzhikhar@mail.ru**

ЗОЛОТЫХ Павел Андреевич — аспирант Московского государственного университета им. М. В. Ломоносова, г. Москва. E-mail: **pzolotykh@gmail.com**

КОГОС Константин Григорьевич — студент факультета кибернетики и информационной безопасности Национального исследовательского ядерного университета (МИФИ), г. Москва. E-mail: **k.kogos@mail.ru**

КОРОТКОВ Владимир Владимирович — аспирант кафедры математической кибернетики Белорусского государственного университета, г. Минск.
E-mail: **wladko@tut.by**

МАРКОВ Виктор Тимофеевич — кандидат физико-математических наук, доцент Московского государственного университета им. М. В. Ломоносова, г. Москва.
E-mail: **markov@mech.math.msu.su**

МИХАЛЕВ Александр Васильевич — доктор физико-математических наук, профессор Московского государственного университета им. М. В. Ломоносова, г. Москва.

ПАНКОВ Константин Николаевич — старший преподаватель кафедры информационной безопасности Московского государственного технического университета радиотехники, электроники и автоматики, г. Москва. E-mail: **k.n.pankov@gmail.com**

ПАНКРАТОВА Ирина Анатольевна — доцент, кандидат физико-математических наук, доцент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **pank@isc.tsu.ru**

ПЕСТУНОВ Андрей Игоревич — научный сотрудник Института вычислительных технологий СО РАН, г. Новосибирск. E-mail: **pestunov@gmail.com**

СКАЖЕНИК Сергей Сергеевич — аспирант Московского государственного университета им. М. В. Ломоносова, г. Москва. E-mail: **sergey_skazhenik@hotmail.com**

ТИМЧУК Галина Дмитриевна — ассистент Черновицкого факультета Национального технического университета «Харьковский политехнический институт», г. Черновцы. E-mail: **galtym@meta.ua**

ТОКАРЕВА Наталья Николаевна — кандидат физико-математических наук, старший научный сотрудник Института математики им. С. Л. Соболева СО РАН, г. Новосибирск. E-mail: **tokareva@math.nsc.ru**

ФОМИЧЕВ Владимир Михайлович — старший научный сотрудник, доцент, доктор физико-математических наук, профессор кафедры математики Финансового университета при Правительстве Российской Федерации, г. Москва.
E-mail: **fomichev@nm.ru**

АННОТАЦИИ СТАТЕЙ НА АНГЛИЙСКОМ ЯЗЫКЕ

Kogos K. G., Fomichev V. M. **POSITIVE PROPERTIES OF NON-NEGATIVE MATRICES.** Some results of graph (non-negative matrice) primitiveness research are reviewed and some generalizations of them are considered. Estimates for exponents of graphs and systems of graphs (matrices and systems of matrices) are pointed.
Keywords: *primitive graphs, primitive matrices, exponent, subexponent.*

Pankov K. N. **SPEEDS OF CONVERGENCE IN LIMIT THEOREMS FOR JOINT DISTRIBUTIONS OF SOME RANDOM BINARY MAPPINGS CHARACTERISTICS.** For linear combinations of coordinate functions of random binary mappings, the limit joint distributions of some their autocorrelation and spectral coefficients and subfunction weights along with the speeds of convergence are obtained. Also, it is proved that these vectors satisfy some congruences.
Keywords: *random binary mapping, local limit theorem, law of large numbers, autocorrelation coefficients, spectral coefficients, weights of subfunction.*

Markov V. T., Mikhalev A. V., Gribov A. V., Zolotykh P. A., Skazhenik S. S. **QUASIGROUPS AND RINGS IN CODING THEORY AND CRYPTOGRAPHY.** Cryptoschemes and codes over associative and nonassociative algebraic structures are studied. A cryptoscheme over graded ring, a cryptoscheme over Moufang loop, a key agreement protocol, and linearly optimal codes are constructed.
Keywords: *nonassociative algebraic structure, graded ring, quasigroup ring, Moufang loop, commutator quasigroup, cryptoschemes, linearly optimal code.*

Pestunov A. I. **ON PROBABILITY OF ONE-BIT DIFFERENCE PROPAGATION THROUGH MODULO ADDITION AND SUBTRACTION.** In this paper, a proof is given for the fact that the probability of one-bit difference propagation through modulo addition and subtraction is equal to 1 if the bit is the most significant one, and 1/2 otherwise. This theoretical fact is verified too with the experimental data.
Keywords: *block cipher, differential cryptanalysis, difference propagation.*

Emelichev V. A., Korotkov V. V. **INVESTIGATION OF THE SOLUTION STABILITY OF VECTOR INVESTMENT BOOLEAN PROBLEM IN THE CASE OF HÖLDER METRIC IN A CRITERIA SPACE.** The stability of a Pareto-optimal portfolio in the multicriteria discrete variant of Markowitz's investment problem with the Wald's maximin efficiency criteria is analysed. The lower and upper bounds for the stability radius of such a portfolio are obtained in the case of the Hölder metric l_p, $1 \leqslant p \leqslant \infty$, in the criteria space of the problem parameters.
Keywords: *vector investment problem, Pareto-optimal investment portfolio, Wald's efficiency criteria, stability radius of portfolio, the Hölder metric.*

Tymchyk G. D., Zhikharevich V. V. **DEVELOPMENT OF A CONTINUOUS ASYNCHRONOUS CELLULAR AUTOMATA METHOD FOR SIMULATING TURBULENT FLOWS.** A method for simulating turbulent flows of the matter based on the continuous asynchronous cellular automata is presented, and a modification of it is proposed. The modification includes the implementation of a probabilistic mechanism

in the cellular automaton movement along the components of the velocity vectors, and the modeling the substance transfer process by the directional state duplication of the neighbour cells. The results of numerical experiments are given for the dynamic of turbulent matter flow in a tube with obstacles.
Keywords: *cellular automaton, computer simulation, turbulence, the Navier — Stokes equation.*

Tokareva N. N. **ON THE HISTORY OF CRYPTOGRAPHY IN RUSSIA.** In this paper, the historical survey of the cryptography in Russia is given. The period from the middle of XVI century up to date is considered.
Keywords: *cryptography, cryptanalysis, history of Russia, P. L. Shilling, V. I. Krivosh-Nemanich, G. I. Bokii, V. A. Kotelnikov.*

Agibalov G. P., Pankratova I. A. **SIBECRYPT'12 REVIEW.** This is a survey of papers and lectures presented and delivered at 11th Siberian Workshop SIBECRYPT devoted to mathematical problems in computer security and cryptography and held on September 3rd – 8th, 2012, in Irkutsk, Russia.
Keywords: *applied discrete mathematics, computer security, cryptography.*

Микони С. В.
Дискретная математика для бакалавра: множества, отношения, функции, графы: учебное пособие. 1-е изд. Рекомендовано НМС по математике вузов Северо-Западного региона России в качестве учебного пособия для студентов инженерных специальностей и направлений вузов. СПб.: Лань, 2012. 192 с. Тираж 1500. Формат 12,8×20 см. Переплёт твёрдый.
ISBN 978-5-8114-1386-7

Определяется множество, его виды (чёткое, нечёткое и мультимножество) и способы задания. Устанавливается связь между прямым (декартовым) произведением множеств, бинарным и функциональным отношениями. Приводятся формы представления бинарного отношения, показывается его связь с графом. Излагаются алгебры с различным числом операций как конкретизации алгебраической системы. Алгебры логики, множеств и отношений рассматриваются как частные случаи алгебры с тремя операциями. Особое внимание уделено алгебре бинарных отношений. Её операции иллюстрируются в трёх формах — множественной (перечислительной), матричной и графовой, что показывает изоморфизм соответствующих алгебр. Рассматриваются элементарные и неэлементарные свойства бинарных отношений. Центральное место в книге отведено графам, их свойствам и типовым задачам, решаемым на графах. На невзвешенных графах решаются задачи анализа структур, а на взвешенных — оптимизационные. Приводятся основные сведения из комбинаторики и теории сложности вычислений, иллюстрируемые на графах.

Целью книги является изложение языка дискретных моделей, широко применяемых в компьютерном моделировании. Книга рассчитана на бакалавров инженерных и экономических специальностей и преподавателей вузов.

Рецензенты:

В. Г. Дегтярев — доктор технических наук, профессор кафедры математики и моделирования Санкт-Петербургского государственного университета путей сообщения, заслуженный деятель науки РФ;

Б. А. Кулик — доктор физико-математических наук, ведущий научный сотрудник Института проблем машиноведения РАН.

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*
- *Математические основы информатики и программирования*
- *Вычислительные методы в дискретной математике*
- *Прикладная теория кодирования*
- *Прикладная теория автоматов*
- *Прикладная теория графов*
- *Логическое проектирование дискретных автоматов*
- *Дискретные модели реальных процессов*
- *Математические основы интеллектуальных систем*
- *Исторические очерки по дискретной математике и её приложениям*