МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М. В. ЛОМОНОСОВА

**Факультет
вычислительной математики
и кибернетики**

Сборник статей молодых ученых факультета ВМК МГУ

Выпуск 8

МОСКВА — 2011

УДК 517.9+519.6+519.7
ББК 22
С23

Составители:
И. Г. ШЕВЦОВА, А. В. ПОЗДНЕЕВ

Технический редактор:
А. В. ПОЗДНЕЕВ

С23 **Сборник статей молодых ученых факультета ВМК МГУ** / Ред. совет: Ложкин С. А. и др. — М.: Издательский отдел факультета ВМК МГУ (лицензия ИД № 05899 от 24.09.2001), 2011. — Выпуск 8. — 147 стр.

В настоящий сборник вошли статьи, написанные молодыми учеными факультета вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова в 2010–2011 гг.

517.9+519.6+519.7
ББК 22

ISBN 978-5-89407-451-1

Данный выпуск посвящается
300-летию М. В. Ломоносова —
первого русского
ученого-естествоиспытателя
и
50-летию первого полета
человека в космос

СОДЕРЖАНИЕ

ГРАНИЧНОЕ УПРАВЛЕНИЕ ПРОЦЕССОМ КОЛЕБАНИЙ, ОПИСЫВАЕМЫМ НЕОДНОРОДНЫМ ВОЛНОВЫМ УРАВНЕНИЕМ, ЗА МИНИМАЛЬНЫЙ ПРОМЕЖУТОК ВРЕМЕНИ
М. Ф. Абдукаримов 5

ОБ АТАКЕ НА ФИЛЬТРУЮЩИЙ ГЕНЕРАТОР С ФУНКЦИЕЙ УСЛОЖНЕНИЯ БЛИЗКОЙ К АЛГЕБРАИЧЕСКИ ВЫРОЖДЕННОЙ
Е. К. Алексеев 19

ЭРГОДИЧНОСТЬ ВРЕМЕННОГО РЯДА ОБОБЩЕННОГО ПОКАЗАТЕЛЯ ЛИКВИДНОСТИ
Н. А. Андреев, В. А. Лапшин, В. В. Науменко 33

ОЦЕНКИ ВРЕМЕНИ СУЩЕСТВОВАНИЯ ОБОБЩЕННЫХ РЕШЕНИЙ НАЧАЛЬНО-КРАЕВОЙ ЗАДАЧИ ДЛЯ ОДНОГО НЕЛИНЕЙНОГО УРАВНЕНИЯ СОБОЛЕВСКОГО ТИПА
А. И. Аристов 42

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ТРАНСПОРТНЫХ ПОТОКОВ НА КОЛЬЦЕВОЙ АВТОСТРАДЕ
Е. Г. Дорогуш 54

РАСШИРЕНИЕ ОБЛАСТИ СЕКРЕТНОСТИ ПРОТОКОЛА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ФАЗОВО-ВРЕМЕННЫМ КОДИРОВАНИЕМ
Д. А. Кронберг 69

ОЦЕНКА РАДИУСА ПОКРЫТИЯ МНОГОМЕРНОЙ ЕДИНИЧНОЙ СФЕРЫ МЕТРИЧЕСКОЙ СЕТЬЮ, ПОРОЖДЕННОЙ СФЕРИЧЕСКОЙ СИСТЕМОЙ КООРДИНАТ
Т. С. Майская 83

О КРИПТОАНАЛИЗЕ LILI-128, ОСНОВАННОМ НА ЧАСТИЧНОМ ОПРОБОВАНИИ И МОНОМИАЛЬНОЙ СОВМЕСТНОСТИ СИСТЕМ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ
А. С. Мелузов 99

МЕТОД БРОЙДЕНА ДЛЯ РЕШЕНИЯ ЗАДАЧ РАВНОВЕСНОГО ПРОГРАММИРОВАНИЯ
А. В. Ничипорчук 108

ПРИМЕНЕНИЕ УСЛОВИЙ ВТОРОГО ПОРЯДКА В ИССЛЕДОВАНИИ ЛОКАЛЬНОЙ ОПТИМАЛЬНОСТИ НЕКОТОРЫХ ТРАЕКТОРИЙ В ЗАДАЧЕ РИДСА-ШЕППА
И. А. Самыловский 117

МАКСИМАЛЬНАЯ МОЩНОСТЬ (k, l)-МНОЖЕСТВА, СВОБОДНОГО ОТ СУММ В ЦИКЛИЧЕСКОЙ ГРУППЕ
В. Г. Саргсян 123

СОЗДАНИЕ ПРОГРАММНОЙ СРЕДЫ ДЛЯ СТАТИСТИЧЕСКОЙ ОБРАБОТКИ ДАННЫХ БИОИМПЕДАНСНЫХ ИЗМЕРЕНИЙ
О. А. Старунова 129

БЕСПОВТОРНЫЕ ФУНКЦИИ НАИМЕНЬШЕЙ ТЕСТОВОЙ СЛОЖНОСТИ
Д. В. Чистиков 135

РЕФЕРАТЫ 145

УДК 517.984.5

ГРАНИЧНОЕ УПРАВЛЕНИЕ ПРОЦЕССОМ КОЛЕБАНИЙ, ОПИСЫВАЕМЫМ НЕОДНОРОДНЫМ ВОЛНОВЫМ УРАВНЕНИЕМ, ЗА МИНИМАЛЬНЫЙ ПРОМЕЖУТОК ВРЕМЕНИ

© 2011 г. М. Ф. Абдукаримов

mahmadsalim_86@mail.ru

Кафедра общей математики

Введение. С задачей граничного управления связаны многие практические задачи, в частности, задачи акустики. Ввиду этого изучение таких задач является одной из актуальных для настоящего времени.

В 1988 году Ж. Л. Лионс начал изучение граничного управления колебаниями в форме смешанных задач для волнового уравнения. В его работах изучалось задача успокоения с граничными условиями типа смещения. Им же в работе [1] с помощью метода гильбертовых пространств была доказана неединственность решения полученной задачи при $T > 2l$ в терминах обобщенного решения из класса L_2.

В монографии А. Г. Бутковского [2] задача граничного управления была исследована с помощью метода Фурье и метода моментов, который был применен для построения искомого граничного управления в виде ряда Фурье.

В работе А. Е. Егорова [3] для конструктивного решения задачи граничного управления был использован метод падающих и отраженных волн.

В статье Ф. П. Васильева [4] была предложена трактовка основ теории двойственности в линейных задачах управления и наблюдения. Конструктивному решению задачи о граничном управлении процессом колебаний посвящены также его совместные с учениками работы [5, 6], в которых построены эффективные численные алгоритмы нахождения искомого граничного управления.

Отметим, что в упомянутых работах теорема существования искомого граничного управления доказывается лишь для промежутка времени T, строго большего $2l$, и явного аналитического выражения для этого управления не устанавливается.

В работе В. А. Ильина [8] впервые для любого T из интервала $0 < T \leqslant l$ установлены необходимые и достаточные условия существования и явный вид граничных управлений на двух концах, а для случая $T > l$ (точнее, для случая $l < T \leqslant 2l$) приведен самый общий вид граничных управлений, включающих две произвольные постоянные и четыре функции из класса W_2^2 на сегменте длины $l - T$, которые обеспечивают переход колебательного процесса, описываемого однородным волновым уравнением, из произвольного начального состояния в наперед заданное финальное состояние. В этой работе при изучении задачи большую роль играет класс $\widehat{W}_2^2[0 \leqslant x \leqslant l] \times [0 \leqslant t \leqslant T]$, впервые введенный В. А. Ильиным в работе [7] (определение этого класса будет дано ниже).

По теме теории граничного управления колебаниями, описываемыми волновым и телеграфным уравнением, как в форме локальных, так и нелокальных смешанных задач, В. А. Ильиным, Е. И. Моисеевым и их учениками опубликован ряд работ.

Данная работа является продолжением этих работ, где рассматривается этот же вопрос для неоднородного волнового уравнения. Иными словами, изучим проблему отыскания на концах $x = 0$ и $x = l$ таких граничных управлений $\mu(t)$ и $\nu(t)$ из класса $W_2^2[0, T]$, которые за минимальный промежуток времени T приводят начальные смещение $\varphi(x) \in W_2^2[0, l]$ и скорость $\psi(x) \in W_2^1[0, l]$ соответственно к двум наперед заданным функциям $\varphi_1(x) \in W_2^2[0, l]$ и $\psi_1(x) \in$ $\in W_2^1[0, l]$ в случае, когда на колебательную систему влияет внешняя сила $f(x, t)$.

1^0. **Постановка смешанных задач и определение класса их решений.** Рассмотрим следующие три задачи для неоднородного волнового уравнения в прямоугольнике $Q_T = [0 \leqslant x \leqslant l] \times [0 \leqslant t \leqslant T]$.

Смешанная задача I:

$$u_{tt}(x,t) - u_{xx}(x,t) = f(x,t) \quad \text{в} \quad Q_T, \tag{1}$$
$$u(0,t) = \mu(t), \quad u(l,t) = \nu(t) \quad \text{при} \quad 0 \leqslant t \leqslant T, \tag{2}$$
$$u(x,0) = \varphi(x), \quad u_t(x,0) = \psi(x) \quad \text{при} \quad 0 \leqslant x \leqslant l, \tag{3}$$

в которой $\mu(t)$, $\nu(t) \in W_2^2[0,T]$, $\varphi(x) \in W_2^2[0,l]$, $\psi(x) \in W_2^1[0,l]$, $f(x,t) \in W_2^1(Q_T)$ и выполнены условия согласования

$$\mu(0) = \varphi(0), \quad \nu(0) = \varphi(l), \quad \mu'(0) = \psi(0), \quad \nu'(0) = \psi(l). \tag{4}$$

Смешанная задача II:

$$u_{tt}(x,t) - u_{xx}(x,t) = f(x,t) \quad \text{в} \quad Q_T, \tag{5}$$
$$u(0,t) = \mu(t), \quad u(l,t) = \nu(t) \quad \text{при} \quad 0 \leqslant t \leqslant T, \tag{6}$$
$$u(x,T) = \varphi_1(x), \quad u_t(x,T) = \psi_1(x) \quad \text{при} \quad 0 \leqslant x \leqslant l, \tag{7}$$

в которой $\mu(t)$, $\nu(t) \in W_2^2[0,T]$, $\varphi_1(x) \in W_2^2[0,l]$, $\psi_1(x) \in W_2^1[0,l]$, $f(x,t) \in W_2^1(Q_T)$ и выполнены условия согласования

$$\mu(T) = \varphi_1(0), \quad \nu(T) = \varphi_1(l), \quad \mu'(T) = \psi_1(0), \quad \nu'(T) = \psi_1(l). \tag{8}$$

Задача III:

$$u_{tt}(x,t) - u_{xx}(x,t) = f(x,t) \quad \text{в} \quad Q_T, \tag{9}$$
$$u(x,0) = \varphi(x), \quad u_t(x,0) = \psi(x) \quad \text{при} \quad 0 \leqslant x \leqslant l, \tag{10}$$
$$u(x,T) = \varphi_1(x), \quad u_t(x,T) = \psi_1(x) \quad \text{при} \quad 0 \leqslant x \leqslant l, \tag{11}$$

в которой $\varphi(x)$ и $\varphi_1(x) \in W_2^2[0,l]$, $\psi(x)$, $\psi_1(x) \in W_2^1[0,l]$ и $f(x,t) \in W_2^1(Q_T)$.

Решение поставленных задач будем искать в классе $\widehat{W_2^2}(Q_T)$.

Определение 1. Будем говорить, что функция двух переменных $u(x,t)$ *принадлежит классу* $\widehat{W_2^2}(Q_T)$, если сама функция $u(x,t)$ и ее частные производные первого порядка непрерывны в замкнутом прямоугольнике $\overline{Q_T}$ и если у этой функции существуют все обобщенные частные производные второго порядка, каждая из которых принадлежит классу $L_2[0 \leqslant x \leqslant l]$ при любом $t \in [0,T]$ и принадлежит классу $L_2[0 \leqslant t \leqslant T]$ при любом $x \in [0,l]$.

Определение 2. Будем говорить, что функция одной переменной $\mu(t)$ *принадлежит классу* $\underline{W}_2^2[0,T]$ (соответственно *классу* $\overline{W}_2^2[0,T]$), если эта функция принадлежит классу $W_2^2[0,T]$ и, кроме того, удовлетворяет условиям $\mu(0) = 0$, $\mu'(0) = 0$, $\mu(t) \equiv 0$ при $t \leqslant 0$ (соответственно удовлетворяет условиям $\mu(T) = 0$, $\mu'(T) = 0$, $\mu(t) \equiv 0$ при $t \geqslant T$).

Из определения 2 следует, что функция $\mu(t)$, принадлежащая классу $\underline{W}_2^2[0,T]$, принадлежит классу $W_2^2[-A,T]$ при любом $A > 0$, а функция $\mu(t)$, принадлежащая классу $\overline{W}_2^2[0,T]$, принадлежит классу $W_2^2[0,A]$ при любом $A > T$.

Теперь дадим определения решений поставленных задач I–III.

Определение 3. *Решением из* $\widehat{W_2^2}(Q_T)$ *смешанной задачи I* (соответственно *смешанной задачи II*) называется такая функция $u(x,t)$, которая удовлетворяет уравнению $u_{tt}(x,t) - u_{xx}(x,t) = f(x,t)$ для любого $t \in [0,T]$ и для почти всех $x \in [0,l]$, а также для любого $x \in [0,l]$ и для почти всех $t \in [0,T]$ и, кроме того, удовлетворяет в классическом смысле краевым условиям (2) и начальным условиям (3) (соответственно краевым условиям (6) и условиям (7)).

Определение 4. *Решением из* $\widehat{W_2^2}(Q_T)$ *задачи III* называется такая функция $u(x,t)$ из этого класса, которая удовлетворяет уравнению $u_{tt}(x,t) - u_{xx}(x,t) = f(x,t)$ для любого $t \in [0,T]$ и для почти всех $x \in [0,l]$, а также для любого $x \in [0,l]$ и для почти всех $t \in [0,T]$ и, кроме того, удовлетворяет в классическом смысле условиям (10) и (11).

Заметим, что функция $u(x,t)$, являющаяся решением из класса $\widehat{W_2^2}(Q_T)$ задачи III, по определению этого класса имеет при $x = 0$ и $x = l$ краевые значения $u(0,t) = \mu(t)$ и $u(l,t) = \nu(t)$, каждое из которых обладает обобщенной производной второго порядка $u_{tt}(0,t) = \mu''(t)$ и $u_{tt}(l,t) = \nu''(t)$, принадлежащей классу $L_2[0 \leqslant t \leqslant T]$, то есть каждое из краевых значений $u(0,t) = \mu(t)$ и $u(l,t) = \nu(t)$ принадлежит классу $W_2^2[0,T]$. Эти краевые значения в силу определения класса $\widehat{W_2^2}(Q_T)$ должны быть согласованы с функциями $\varphi(x)$, $\psi(x)$, $\varphi_1(x)$ и $\psi_1(x)$, стоящими в условиях (10) и (11), то есть для краевых значений $\mu(t)$ и $\nu(t)$ должны быть выполнены как четыре условия согласования (4), так и четыре условия согласования (8).

2^0. **Утверждения о единственности решения.** В этом пункте приведем два утверждения о единственности решения поставленных задач. Доказательства этих утверждений полностью аналогичны приведенным для однородного уравнения в [8].

Утверждение 1. *Для любого T может существовать только одно решение из класса* $\widehat{W_2^2}(Q_T)$ *как смешанной задачи I, так и смешанной задачи II.*

Утверждение 2. *Для любого $T \leqslant l$ может существовать только одно решение из класса* $\widehat{W_2^2}(Q_T)$ *задачи III.*

3^0. **Необходимые условия существования решения из** $\widehat{W_2^2}(Q_l)$ **задачи III.** В этом пункте мы установим необходимые условия существования решения из $\widehat{W_2^2}(Q_l)$ задачи III при условии, что $T = l$. Имеет место следующее утверждение.

Утверждение 3. *Если $T = l$ и для произвольных пяти функций $\varphi(x) \in W_2^2[0,l]$, $\psi(x) \in W_2^1[0,l]$, $\varphi_1(x) \in W_2^2[0,l]$, $\psi_1(x) \in W_2^1[0,l]$ и $f(x,t) \in W_2^1(Q_l)$ существует решение из класса* $\widehat{W_2^2}(Q_l)$ *задачи III, то оно удовлетворяет следующим трем требованиям:*

$$u_t(0,0) - u_x(0,0) - u_t(l,l) + u_x(l,l) + \int_0^l f(\tau,\tau)\,d\tau = 0, \tag{12}$$

$$u_t(l,0) + u_x(l,0) - u_t(0,l) - u_x(0,l) + \int_0^l f(l-\tau,\tau)\,d\tau = 0, \tag{13}$$

$$\int_0^l u_t(x,0)\,dx + u(0,0) + u(l,0) + \int_0^l u_t(x,l)\,dx - u(0,l) - u(l,l) - \int_0^l \int_{l-\tau}^{\tau} f(\xi,\tau)\,d\xi\,d\tau = 0. \tag{14}$$

Доказательство. Сначала докажем это утверждение для частного случая $u(x,0) = \varphi(x) \equiv 0$ и $u_t(x,0) = \psi(x) \equiv 0$ при $0 \leqslant x \leqslant l$, то есть докажем, что для этого частного случая решение из класса $\widehat{W_2^2}(Q_l)$ задачи III удовлетворяет трем требованиям:

$$u_x(l,l) - u_t(l,l) + \int_0^l f(\tau,\tau)\,d\tau = 0, \tag{12*}$$

$$u_t(0,l) + u_x(0,l) - \int_0^l f(l-\tau,\tau)\,d\tau = 0, \tag{13*}$$

$$\int_0^l u_t(x,l)dx - u(0,l) - u(l,l) - \int_0^l \int_{l-\tau}^{\tau} f(\xi,\tau)\,d\xi\,d\tau = 0. \tag{14*}$$

Так как граничные значения $u(0,t)=\mu(t)$, $u(l,t)=\nu(t)$ решения $u(x,t)$ из класса $\widehat{W_2^2}(Q_l)$ задачи III принадлежат по t классу $W_2^2[0,l]$ и при $t=0$ удовлетворяют условиям согласования с $\varphi(x)\equiv 0$ и $\psi(x)\equiv 0$, то

$$\mu(0)=0,\quad \nu(0)=0,\quad \mu'(0)=0,\quad \nu'(0)=0. \tag{15}$$

Продолжив граничные значения $\mu(t)$ и $\nu(t)$ тождественным нулем на значения $t<0$, мы в силу условий (15) получим, что так продолженные функции (обозначим их символами $\underline{\mu}(t)$ и $\underline{\nu}(t)$) будут принадлежать классу $\underline{W}_2^2[0,l]$.

Продолжим также функцию $f(x,t)$ по первой переменной нечетно относительно точек $x=0$ и $x=l$ на $[-l,0]$ и $[l,2l]$ (так продолженные функции принадлежат классам $W_2^1[(-l\leqslant x\leqslant 0)\times(0\leqslant t\leqslant l)]$ и $W_2^1[(l\leqslant x\leqslant 2l)\times(0\leqslant t\leqslant l)]$). Без труда проверяется, что единственное решение (в силу утверждения 1) из класса $\widehat{W_2^2}(Q_l)$ смешанной задачи (1)–(3) при $\varphi(x)\equiv 0$ и $\psi(x)\equiv 0$ имеет следующий вид:

$$u(x,t)=\underline{\mu}(t-x)+\underline{\nu}(t+x-l)+\frac{1}{2}\int\limits_0^t\int\limits_{x-t+\tau}^{x+t-\tau} f(\xi,\tau)\,d\xi\,d\tau. \tag{16}$$

Дифференцируя (16) по t и по x, после этого полагая $t=l$, получим для всех $x\in[0,l]$:

$$u_t(x,l)=\underline{\mu}'(l-x)+\underline{\nu}'(x)+\frac{1}{2}\int\limits_0^l [f(x+l-\tau,\tau)+f(x-l+\tau,\tau)]\,d\tau, \tag{17}$$

$$u_x(x,l)=-\underline{\mu}'(l-x)+\underline{\nu}'(x)+\frac{1}{2}\int\limits_0^l [f(x+l-\tau,\tau)-f(x-l+\tau,\tau)]\,d\tau. \tag{18}$$

Полагая в (17) и (18) сначала $x=0$, а затем $x=l$ и используя равенства (15), найдем:

$$u_t(0,l)=\underline{\mu}'(l)+\frac{1}{2}\int\limits_0^l [f(l-\tau,\tau)+f(\tau-l,\tau)]\,d\tau, \tag{19}$$

$$u_x(0,l)=-\underline{\mu}'(l)+\frac{1}{2}\int\limits_0^l [f(l-\tau,\tau)-f(\tau-l,\tau)]\,d\tau, \tag{20}$$

$$u_t(l,l)=\underline{\nu}'(l)+\frac{1}{2}\int\limits_0^l [f(2l-\tau,\tau)+f(\tau,\tau)]\,d\tau, \tag{21}$$

$$u_x(l,l)=\underline{\nu}'(l)+\frac{1}{2}\int\limits_0^l [f(2l-\tau,\tau)-f(\tau,\tau)]\,d\tau. \tag{22}$$

Складывая почленно (19) и (20), получим равенство (13*), а вычитая из (21) равенство (22), — равенство (12*). Для доказательства равенства (14*) проинтегрируем соотношения (17) и (18) по x от нуля до l и снова воспользуемся равенствами (15). Имеем:

$$\int\limits_0^l u_t(x,l)\,dx=\int\limits_0^l [\underline{\mu}'(l-x)+\underline{\nu}'(x)]\,dx+\frac{1}{2}\int\limits_0^l\int\limits_0^l [f(x+l-\tau,\tau)+f(x-l+\tau,\tau)]\,d\tau\,dx=$$

$$= \underline{\mu}(l) - \underline{\mu}(0) + \underline{\nu}(l) - \underline{\nu}(0) + \frac{1}{2}\int_0^l\int_0^l [f(x+l-\tau,\tau) + f(x-l+\tau,\tau)]\,d\tau\,dx =$$

$$= u(0,l) + u(l,l) + \frac{1}{2}\int_0^l\int_0^l f(x+l-\tau,\tau)\,d\tau\,dx + \frac{1}{2}\int_0^l\int_0^l f(x-l+\tau,\tau)\,d\tau\,dx, \quad (23)$$

$$\int_0^l u_x(x,l)\,dx = \int_0^l [-\underline{\mu}'(l-x) + \underline{\nu}'(x)]\,dx + \frac{1}{2}\int_0^l\int_0^l [f(x+l-\tau,\tau) - f(x-l+\tau,\tau)]\,d\tau\,dx,$$

$$u(l,l) - u(0,l) =$$

$$= \underline{\mu}(0) - \underline{\mu}(l) + \underline{\nu}(l) - \underline{\nu}(0) + \frac{1}{2}\int_0^l\int_0^l f(x+l-\tau,\tau)\,d\tau\,dx - \frac{1}{2}\int_0^l\int_0^l f(x-l+\tau,\tau)\,d\tau\,dx.$$

Из последнего равенства придем к соотношению

$$\int_0^l\int_0^l f(x+l-\tau,\tau)\,d\tau\,dx = \int_0^l\int_0^l f(x-l+\tau,\tau)\,d\tau\,dx. \quad (24)$$

Сопоставляя равенства (23) и (24), получим равенство (14*). Тем самым, для частного случая $\varphi(x) \equiv 0$ и $\psi(x) \equiv 0$ утверждение 3 доказано.

Пусть теперь $u(x,t)$ — решение из класса $\widehat{W_2^2}(Q_l)$ общей задачи III с произвольными $\varphi(x)$ и $\psi(x)$. Продолжим функции $\varphi(x)$ и $\psi(x)$ на сегменты $[-l,0]$ и $[l,2l]$ так, чтобы продолженные функции $\varphi(x)$ и $\psi(x)$ принадлежали классам $W_2^2[-l,2l]$ и $W_2^1[-l,2l]$ соответственно. Продолжим также функцию $f(x,t)$ нечетно по первой переменной относительно точек $x=0$ и $x=l$ на сегменты $-l \leqslant x \leqslant 0$ и $l \leqslant x \leqslant 2l$.

Теперь рассмотрим функцию $v(x,t)$ с так продолженными функциями $\varphi(x)$, $\psi(x)$ и $f(x,t)$ вида

$$v(x,t) = \frac{1}{2}[\varphi(x+t) + \varphi(x-t)] + \frac{1}{2}\int_{x-t}^{x+t}\psi(\xi)\,d\xi + \frac{1}{2}\int_0^t\int_{x-t+\tau}^{x+t-\tau} f(\xi,\tau)\,d\xi\,d\tau. \quad (25)$$

Эта функция заведомо принадлежит классу $\widehat{W_2^2}(Q_l)$ и удовлетворяет начальным условиям при $t=0$:

$$v(x,0) = \varphi(x), \quad v_t(x,0) = \psi(x) \quad \text{при} \quad 0 \leqslant x \leqslant l. \quad (26)$$

Дифференцируя равенство (25) по t и по x и после этого полагая $t=l$, получим:

$$v_t(x,l) = \frac{1}{2}[\varphi'(x+l) - \varphi'(x-l)] + \frac{1}{2}[\psi(x+l) + \psi(x-l)] +$$

$$+ \frac{1}{2}\int_0^l [f(x+l-\tau,\tau) + f(x-l+\tau,\tau)]\,d\tau, \quad (27)$$

$$v_x(x,l) = \frac{1}{2}[\varphi'(x+l) + \varphi'(x-l)] + \frac{1}{2}[\psi(x+l) - \psi(x-l)] +$$

$$+ \frac{1}{2}\int_0^l [f(x+l-\tau,\tau) - f(x-l+\tau,\tau)]\,d\tau. \quad (28)$$

Заметим теперь, что в силу равенств (26) разность $u(x,t)-v(x,t)$ является решением из класса $\widehat{W_2^2}(Q_l)$ задачи Коши для неоднородного волнового уравнения с нулевыми начальными условиями при $t=0$ и с нулевой правой частью $f(x,t)\equiv 0$. Поэтому для этой разности в силу рассмотренного выше частного случая выполнены три требования вида (12*)–(14*):

$$-[u_t(l,l)-v_t(l,l)]+[u_x(l,l)-v_x(l,l)]=0, \tag{29}$$

$$[u_t(0,l)-v_t(0,l)]+[u_x(0,l)-v_x(0,l)]=0, \tag{30}$$

$$\int_0^l [u_t(x,l)-v_t(x,l)]\,dx-[u(0,l)-v(0,l)]-[u(l,l)-v(l,l)]=0. \tag{31}$$

Полагая в равенствах (27) и (28) $x=l$, получим из этих равенств, что

$$v_t(l,l)-v_x(l,l)=\psi(0)-\varphi'(0)+\int_0^l f(\tau,\tau)\,d\tau=u_t(0,0)-u_x(0,0)+\int_0^l f(\tau,\tau)\,d\tau. \tag{32}$$

Из (29) и (32) вытекает требование (12).
Далее, полагая в равенствах (27) и (28) $x=0$, находим, что

$$-v_t(0,l)-v_x(0,l)=-\psi(l)-\varphi'(l)-\int_0^l f(l-\tau,\tau)\,d\tau=$$

$$=-u_t(l,0)-u_x(l,0)-\int_0^l f(l-\tau,\tau)\,d\tau. \tag{33}$$

Из равенств (30) и (33) вытекает требование (13).
Наконец, из соотношений (25) и (27) следует, что

$$-\int_0^l v_t(x,l)\,dx+v(0,l)+v(l,l)=-\frac{1}{2}\int_0^l[\varphi'(x+l)-\varphi'(x-l)]\,dx-$$

$$-\frac{1}{2}\int_0^l[\psi(x+l)+\psi(x-l)]\,dx-\frac{1}{2}\int_0^l\int_0^l[f(x+l-\tau,\tau)+f(x-l+\tau,\tau)]\,d\tau\,dx+$$

$$+\frac{1}{2}[\varphi(l)+\varphi(-l)]+\frac{1}{2}\int_{-l}^l\psi(y)\,dy+\frac{1}{2}[\varphi(2l)+\varphi(0)]+\frac{1}{2}\int_0^{2l}\psi(y)\,dy=$$

$$=\frac{1}{2}[-\varphi(2l)+\varphi(l)+\varphi(0)-\varphi(-l)]-\frac{1}{2}\int_l^{2l}\psi(y)\,dy-\frac{1}{2}\int_{-l}^0\psi(y)\,dy+$$

$$+\frac{1}{2}[\varphi(2l)+\varphi(l)+\varphi(0)+\varphi(-l)]+\frac{1}{2}\int_{-l}^l\psi(y)\,dy+\frac{1}{2}\int_0^{2l}\psi(y)\,dy-$$

$$-\frac{1}{2}\int_0^l\int_0^l[f(x+l-\tau,\tau)+f(x-l+\tau,\tau)]\,d\tau\,dx=$$

$$= \int_0^l \psi(y)\,dy + \varphi(0) + \varphi(l) - \frac{1}{2}\int_0^l\int_0^l [f(x+l-\tau,\tau) + f(x-l+\tau,\tau)]\,d\tau\,dx =$$

$$= \int_0^l u_t(x,0)\,dx + u(0,0) + u(l,0) - \frac{1}{2}\int_0^l\int_0^l [f(x+l-\tau,\tau) + f(x-l+\tau,\tau)]\,d\tau\,dx, \quad (34)$$

а из соотношений (25) и (28) —

$$\int_0^l v_x(x,l)\,dx - v(l,l) + v(0,l) = \frac{1}{2}\int_0^l [\varphi'(x+l) + \varphi'(x-l)]\,dx +$$

$$+ \frac{1}{2}\int_0^l [\psi(x+l) - \psi(x-l)]\,dx + \frac{1}{2}\int_0^l\int_0^l [f(x+l-\tau,\tau) - f(x-l+\tau,\tau)]\,d\tau\,dx -$$

$$- \frac{1}{2}[\varphi(2l) + \varphi(0)] - \frac{1}{2}\int_0^{2l} \psi(x)\,dx + \frac{1}{2}[\varphi(l) + \varphi(-l)] + \frac{1}{2}\int_{-l}^{l} \psi(x)\,dx,$$

что приводит к равенству

$$\int_0^l\int_0^l f(x+l-\tau,\tau)\,d\tau\,dx = \int_0^l\int_0^l f(x-l+\tau,\tau)\,d\tau\,dx.$$

Сопоставлением последнего равенства с (34) и (31) устанавливается справедливость требования (14). Утверждение 3 полностью доказано.

4^0. **Основной результат настоящей работы.** В настоящем пункте будет доказано центральное утверждение этой работы.

Теорема. *Для того чтобы при $T = l$ для наперед заданных пяти функций $\varphi(x) \in W_2^2[0,l]$, $\psi(x) \in W_2^1[0,l]$, $\varphi_1(x) \in W_2^2[0,l]$, $\psi_1(x) \in W_2^1[0,l]$ и $f(x,t) \in W_2^1(Q_T)$ существовали граничные управления $\mu(t)$ и $\nu(t)$ из класса $W_2^2[0,T]$, обеспечивающие удовлетворение решением из класса $\widehat{W_2^2}(Q_l)$ смешанной задачи (1)–(3), условиям (7) и подчиненные условиям согласования (4) и (8), необходимо и достаточно, чтобы выполнялись три требования:*

$$\psi(0) - \varphi'(0) - \psi_1(l) + \varphi_1'(l) + \int_0^l f(\tau,\tau)\,d\tau = 0, \quad (35)$$

$$\psi(l) + \varphi'(l) - \psi_1(0) - \varphi_1'(0) + \int_0^l f(l-\tau,\tau)\,d\tau = 0, \quad (36)$$

$$\int_0^l \psi(x)\,dx + \varphi(0) + \varphi(l) + \int_0^l \psi_1(x)\,dx - \varphi_1(0) - \varphi_1(l) - \int_0^l\int_{l-\tau}^{\tau} f(\xi,\tau)\,d\xi\,d\tau = 0. \quad (37)$$

При выполнении указанных трех требований искомые граничные управления $\mu(t)$ и $\nu(t)$

вычисляются по формулам:

$$\mu(t)=\frac{1}{2}\left[\int\limits_0^t \psi(x)\,dx+\varphi(t)+\varphi(0)+\int\limits_{l-t}^{l}\psi_1(x)\,dx+\varphi_1(l-t)-\varphi_1(l)-\right.$$
$$\left.-\int\limits_0^l\int\limits_{l-t}^{l} f(x-l+\tau,\tau)\,d\tau\,dx\right], \quad (*)$$

$$\nu(t)=\frac{1}{2}\left[\int\limits_0^t \psi_1(x)\,dx+\varphi_1(t)-\varphi_1(0)+\int\limits_{l-t}^{l}\psi(x)dx+\varphi(l-t)+\varphi(l)-\right.$$
$$\left.-\int\limits_0^l\int\limits_{0}^{t} f(x+l-\tau,\tau)\,d\tau\,dx\right]. \quad (**)$$

Доказательство. Необходимость трех требований (35)–(37) доказана в утверждении 3. Покажем, что при выполнении этих трех требований существуют в явном аналитическом виде граничные управления $\mu(t)$ и $\nu(t)$ из класса $W_2^2[0,T]$, обеспечивающие удовлетворение решением из класса $\widehat{W}_2^2(Q_l)$ задачи (1)–(3), условиям (7) и условиям согласования (4) и (8).

Будем искать решение из класса $\widehat{W}_2^2(Q_l)$ задачи III, рассматриваемой при $T=l$, то есть задачи

$$u_{tt}(x,t)-u_{xx}(x,t)=f(x,t) \quad \text{в} \quad Q_l, \tag{38}$$
$$u(x,0)=\varphi(x), \quad u_t(x,0)=\psi(x) \quad \text{при} \quad 0\leqslant x\leqslant l, \tag{39}$$
$$u(x,l)=\varphi_1(x), \quad u_t(x,l)=\psi_1(x) \quad \text{при} \quad 0\leqslant x\leqslant l, \tag{40}$$

в следующем виде

$$u(x,t)=F(x+t)+G(t+l-x)+\frac{1}{2}\int\limits_0^t\int\limits_{x-t+\tau}^{x+t-\tau} f(\xi,\tau)\,d\xi\,d\tau, \tag{41}$$

где $F(z)$ и $G(z)$ — две функции из класса $W_2^2[0,2l]$, подлежащие определению. Для того чтобы выразить функции $F(z)$ и $G(z)$ для всех значений $z\in[0,2l]$ через $\varphi(x)$, $\psi(x)$, $\varphi_1(x)$ и $\psi_1(x)$, продифференцируем (41) по t. Получим:

$$u_t(x,t)=F'(x+t)+G'(t+l-x)+\frac{1}{2}\int\limits_0^t [f(x+t-\tau,\tau)+f(x-t+\tau,\tau)]\,d\tau. \tag{42}$$

После этого положим в (41) и (42) сначала $t=0$, а затем $t=l$. Используя условия (39) и (40), придем к следующим соотношениям:

$$F(x)+G(l-x)=\varphi(x), \tag{43}$$
$$F'(x)+G'(l-x)=\psi(x), \tag{44}$$
$$F(l+x)+G(2l-x)+\frac{1}{2}\int\limits_0^l\int\limits_{x-l+\tau}^{x+l-\tau} f(\xi,\tau)\,d\xi\,d\tau=\varphi_1(x), \tag{45}$$
$$F'(l+x)+G'(2l-x)+\frac{1}{2}\int\limits_0^l [f(x+l-\tau,\tau)+f(x-l+\tau,\tau)]\,d\tau=\psi_1(x), \tag{46}$$

справедливым для всех x из сегмента $[0, l]$. Дифференцируя по x соотношения (43) и (45), получим:

$$F'(x) - G'(l - x) = \varphi'(x), \tag{47}$$

$$F'(l + x) - G'(2l - x) + \frac{1}{2}\int_0^l [f(x + l - \tau, \tau) - f(x - l + \tau, \tau)]\, d\tau = \varphi_1'(x). \tag{48}$$

Полусумма и полуразность (44) и (47) приводят к равенствам:

$$F'(x) = \frac{1}{2}\psi(x) + \frac{1}{2}\varphi'(x), \tag{49}$$

$$G'(l - x) = \frac{1}{2}\psi(x) - \frac{1}{2}\varphi'(x), \tag{50}$$

выражающим функции $F(z)$ и $G(z)$ на сегменте $[0, l]$ через функции $\varphi(x)$ и $\psi(x)$, а полусумма и полуразность соотношений (46) и (48) приводят к равенствам:

$$F'(l + x) = \frac{1}{2}\psi_1(x) + \frac{1}{2}\varphi_1'(x) - \frac{1}{2}\int_0^l f(x + l - \tau, \tau)\, d\tau, \tag{51}$$

$$G'(2l - x) = \frac{1}{2}\psi_1(x) - \frac{1}{2}\varphi_1'(x) - \frac{1}{2}\int_0^l f(x - l + \tau, \tau)\, d\tau, \tag{52}$$

выражающим функции $F(z)$ и $G(z)$ на сегменте $[l, 2l]$ через функции $\varphi_1(x)$ и $\psi_1(x)$.

Точнее, равенства (49) и (50) выражают производные функций $F(z)$ и $G(z)$ на сегменте $[0, l]$ через функции $\varphi(x)$ и $\psi(x)$, а равенства (51) и (52) выражают производные функции $F(z)$ и $G(z)$ на сегменте $[l, 2l]$ через функции $\varphi_1(x)$ и $\psi_1(x)$.

Установим теперь выражения для самих функций $F(z)$ и $G(z)$ на сегментах $0 \leqslant z \leqslant l$ и $l \leqslant z \leqslant 2l$.

Интегрируя (49) по x в пределах от нуля до z, получим для любого z из сегмента $[0, l]$:

$$F(z) = F(0) + \frac{1}{2}\int_0^z \psi(x)\, dx + \frac{1}{2}\varphi(z) - \frac{1}{2}\varphi(0), \tag{53}$$

а интегрируя (50) по x в пределах от $l - z$ до l, получим для любого z из сегмента $[0, l]$:

$$G(z) = G(0) + \frac{1}{2}\int_{l-z}^l \psi(x)\, dx - \frac{1}{2}\varphi(l) + \frac{1}{2}\varphi(l - z). \tag{54}$$

Интегрируя далее (51) по x в пределах от $z - l$ до l, имеем для любого z из сегмента $[l, 2l]$:

$$F(z) = F(2l) - \frac{1}{2}\int_{z-l}^l \psi_1(x)\, dx - \frac{1}{2}\varphi_1(l) + \frac{1}{2}\varphi_1(z - l) + \frac{1}{2}\int_{z-l}^l \int_0^l f(x + l - \tau, \tau)\, d\tau\, dx. \tag{55}$$

Наконец, интегрируя (52) по x в пределах от нуля до $2l - z$, найдем для любого z из сегмента $[l, 2l]$:

$$G(z) = G(2l) - \frac{1}{2}\int_0^{2l-z} \psi_1(x)\, dx + \frac{1}{2}\varphi_1(2l - z) - \frac{1}{2}\varphi_1(0) + \frac{1}{2}\int_0^{2l-z} \int_0^l f(x - l + \tau, \tau)\, d\tau\, dx. \tag{56}$$

Используя соотношения (43), выразим $G(0)$ через $F(0)$. Подставляя в (43) значения $F(x)$ и $G(l-x)$, определяемые из соотношений (53) и (54), найдем, что

$$F(0)+\frac{1}{2}\int\limits_0^x \psi(\xi)\,d\xi+\frac{1}{2}\varphi(x)-\frac{1}{2}\varphi(0)+G(0)+\frac{1}{2}\int\limits_x^l \psi(\xi)\,d\xi-\frac{1}{2}\varphi(l)+\frac{1}{2}\varphi(x)=\varphi(x),$$

откуда

$$G(0)=-F(0)+\frac{1}{2}\varphi(0)+\frac{1}{2}\varphi(l)-\frac{1}{2}\int\limits_0^l \psi(\xi)\,d\xi. \tag{57}$$

Теперь из условия непрерывности функции $G(z)$ в точке $z=l$, то есть из условия совпадения между собой значений $G(l)$, определяемых из соотношений (54) и (56), выразим $G(2l)$ через $F(0)$. Приравнивая правые части (54) и (56), взятые при $z=l$, получим:

$$G(2l)=-F(0)-\frac{1}{2}\varphi_1(l)+\frac{1}{2}\varphi_1(0)+\varphi(0)+\frac{1}{2}\int\limits_0^l \psi_1(\xi)\,d\xi-\frac{1}{2}\int\limits_0^l\int\limits_0^l f(\xi-l+\tau,\tau)\,d\tau\,d\xi. \tag{58}$$

Далее, из условия совпадения между собой значений $F(l)$, определяемых из соотношений (53) и (55), выразим $F(2l)$ через $F(0)$. Имеем:

$$F(0)+\frac{1}{2}\int\limits_0^l \psi(\xi)\,d\xi+\frac{1}{2}\varphi(l)-\frac{1}{2}\varphi(0)=$$

$$=F(2l)-\frac{1}{2}\int\limits_0^l \psi_1(\xi)\,d\xi-\frac{1}{2}\varphi_1(l)+\frac{1}{2}\varphi_1(0)+\frac{1}{2}\int\limits_0^l\int\limits_0^l f(\xi+l-\tau,\tau)\,d\tau\,d\xi.$$

Из последнего равенства и из соотношения (37) найдем, что

$$F(2l)=F(0)+\varphi_1(l)-\varphi(0). \tag{59}$$

Соотношения (57), (58) и (59) показывают, что все три постоянные $G(0)$, $G(2l)$ и $F(2l)$ линейно выражаются через $F(0)$. Очевидно, что при установленной нами связи между этими постоянными функции $F(z)$ и $G(z)$ являются непрерывным в точке $z=l$. А также значения $F'(z)$ в точке $z=l$ слева и справа, определяемые соответственно из равенств (49) и (51), совпадают между собой в силу соотношения (36), а значения $G'(z)$ в точке $z=l$ слева и справа, определяемые соответственно из (50) и (52), совпадают между собой в силу (35).

Теперь мы можем утверждать, что функции $F(z)$ и $G(z)$, определяемые соотношениями (53)–(56), при условии, что постоянные $G(0)$, $G(2l)$ и $F(2l)$ выражаются через $F(0)$ с помощью равенств (57)–(59) принадлежат классу $W_2^2[0,2l]$. Действительно, из соотношений (53) и (54) и из того, что $\varphi(x)\in W_2^2[0,l]$, $\psi(x)\in W_2^1[0,l]$, заключаем, что каждая из функций $F(z)$ и $G(z)$ принадлежит классу $W_2^2[0,l]$, а из соотношений (55) и (56) и из того, что $\varphi_1(x)\in W_2^2[0,l]$, $\psi_1(x)\in W_2^1[0,l]$, $f(x,t)\in W_2^1(Q_l)$, вытекает, что каждая из функций $F(z)$ и $G(z)$ принадлежит классу $W_2^2[l,2l]$. Принадлежность каждой из функций $F(z)$ и $G(z)$ классу $W_2^2[0,2l]$ на объединенном сегменте $[0,2l]$, следует из установленного нами равенства предельных значений $F(z)$ при $z\to l-0$ и $z\to l+0$, определяемых из соотношений (53) и (55), предельных значений $G(z)$ при $z\to l-0$ и $z\to l+0$, определяемых из соотношений (54) и (56), предельных значений $F'(z)$ при $z\to l-0$ и $z\to l+0$, определяемых из соотношений (49) и (51), и предельных значений $G'(z)$ при $z\to l-0$ и $z\to l+0$, определяемых из соотношений (50) и (52).

Из принадлежности функций $F(z)$ и $G(z)$ классу $W_2^2[0,2l]$ вытекает, что функция $u(x,t)$, определяемая равенством (41), является решением из $\widehat{W}_2^2(Q_l)$ задачи (38)–(40).

Для завершения доказательства теоремы вычислим в явном виде искомые граничные управления $\mu(t)$ и $\nu(t)$. Из равенства (41) имеем:

$$u(0,t) = \mu(t) = F(t) + G(l+t), \tag{60}$$
$$u(l,t) = \nu(t) = F(l+t) + G(t). \tag{61}$$

Подставляя в правую часть (60) значения $F(t)$ и $G(l+t)$, определяемые из равенств (53) и (56), и используя соотношение (58) для $G(2l)$, получим $(*)$.

Аналогично, подставляя в правую часть (61), значения $F(l+t)$ и $G(t)$, определяемые из равенств (54) и (55), имеем:

$$\nu(t) = F(2l) - \frac{1}{2}\int\limits_t^l \psi_1(x)\,dx - \frac{1}{2}\varphi_1(l) + \frac{1}{2}\varphi_1(t) + \frac{1}{2}\int\limits_t^l\int\limits_0^l f(x+l-\tau,\tau)\,d\tau\,dx + \\ + G(0) + \frac{1}{2}\int\limits_{l-t}^l \psi(x)\,dx - \frac{1}{2}\varphi(l) + \frac{1}{2}\varphi(l-t).$$

Используя в правой части последнего равенства соотношения (59) и (57) для $F(2l)$ и $G(0)$, найдем, что

$$\nu(t) = -\frac{1}{2}\int\limits_t^l \psi_1(x)\,dx + \frac{1}{2}\varphi_1(l) + \frac{1}{2}\varphi_1(t) - \frac{1}{2}\int\limits_0^{l-t} \psi(x)\,dx + \\ + \frac{1}{2}\varphi(l-t) - \frac{1}{2}\varphi(0) + \frac{1}{2}\int\limits_t^l\int\limits_0^l f(x+l-\tau,\tau)\,d\tau\,dx.$$

Добавляя к правой части последнего равенства половину равной нулю величины, стоящей в левой части соотношения (37), окончательно получим $(**)$.

Используя соотношения (35)–(37), без труда можно проверить, что найденные нами граничные управления $(*)$ и $(**)$ удовлетворяют при $t = 0$ условиям согласования (4), а при $t = l$ условиям согласования (8). Теорема полностью доказана.

5^0. Следствия из теоремы. Сформулируем два важных утверждения, первое из которых вытекает из теоремы при $\varphi_1(x) \equiv 0$ и $\psi_1(x) \equiv 0$, а второе — при $\varphi(x) \equiv 0$ и $\psi(x) \equiv 0$.

Теорема о полном успокоении колебательного процесса. *Для того чтобы для наперед заданных функций $\varphi(x) \in W_2^2[0,l]$, $\psi(x) \in W_2^1[0,l]$ и $f(x,t) \in W_2^1(Q_l)$ существовали граничные управления $\mu(t)$ и $\nu(t)$ из класса $\overline{W}_2^2[0,l]$, обеспечивающие удовлетворение решением $u(x,t)$ из класса $\widehat{W}_2^2(Q_l)$ смешанной задачи (1)–(3) условиям полного успокоения $u(x,l) \equiv 0$, $u_t(x,l) \equiv 0$ при $0 \leqslant x \leqslant l$ и подчиненные условиям согласования с функциями $\varphi(x)$ и $\psi(x)$ при $t = 0$, необходимо и достаточно, чтобы выполнялись три требования:*

$$\psi(0) - \varphi'(0) + \int\limits_0^l f(\tau,\tau)\,d\tau = 0,$$

$$\psi(l) + \varphi'(l) + \int\limits_0^l f(l-\tau,\tau)\,d\tau = 0,$$

$$\int\limits_0^l \psi(x)\,dx + \varphi(0) + \varphi(l) - \int\limits_0^l\int\limits_{l-\tau}^{\tau} f(\xi,\tau)\,d\xi\,d\tau = 0.$$

При выполнении указанных трех требований искомые граничные управления $\mu(t)$ *и* $\nu(t)$ *имеют вид:*

$$\mu(t)=\frac{1}{2}\int\limits_0^t\psi(x)\,dx+\frac{1}{2}\varphi(t)+\frac{1}{2}\varphi(0)-\frac{1}{2}\int\limits_0^l\int\limits_{l-t}^l f(x-l+\tau,\tau)\,d\tau\,dx,$$

$$\nu(t)=\frac{1}{2}\int\limits_{l-t}^l\psi(x)\,dx+\frac{1}{2}\varphi(l-t)+\frac{1}{2}\varphi(l)-\frac{1}{2}\int\limits_0^l\int\limits_0^t f(x+l-\tau,\tau)\,d\tau\,dx.$$

Теорема о приведении первоначально покоящейся системы в любое заданное состояние. *Для того чтобы для наперед заданных функций* $\varphi_1(x)\in W_2^2[0,l]$, $\psi_1(x)\in W_2^1[0,l]$ *и* $f(x,t)\in W_2^1(Q_l)$ *существовали граничные управления* $\mu(t)$ *и* $\nu(t)$ *из класса* $\underline{W}_2^2[0,l]$, *обеспечивающие удовлетворение решением* $u(x,t)$ *из класса* $\widehat{W}_2^2(Q_l)$ *смешанной задачи (1)–(3) с* $\varphi(x)\equiv 0$ *и* $\psi(x)\equiv 0$ *условиям* $u(x,l)=\varphi_1(x)$, $u_t(x,l)=\psi_1(x)$ *при* $0\leqslant x\leqslant l$ *и подчиненные условиям согласования с функциями* $\varphi_1(x)$ *и* $\psi_1(x)$ *при* $t=l$, *необходимо и достаточно, чтобы выполнялись три требования:*

$$\varphi_1'(l)-\psi_1(l)+\int\limits_0^l f(\tau,\tau)\,d\tau=0,$$

$$\varphi_1'(0)+\psi_1(0)-\int\limits_0^l f(l-\tau,\tau)\,d\tau=0,$$

$$\int\limits_0^l\psi_1(x)\,dx-\varphi_1(0)-\varphi_1(l)-\int\limits_0^l\int\limits_{l-\tau}^{\tau} f(\xi,\tau)\,d\xi\,d\tau=0.$$

При выполнении указанных трех требований искомые граничные управления $\mu(t)$ *и* $\nu(t)$ *имеют вид:*

$$\mu(t)=\frac{1}{2}\int\limits_{l-t}^l\psi_1(x)\,dx-\frac{1}{2}\varphi_1(l)+\frac{1}{2}\varphi_1(l-t)-\frac{1}{2}\int\limits_0^l\int\limits_{l-t}^l f(x-l+\tau,\tau)\,d\tau\,dx,$$

$$\nu(t)=\frac{1}{2}\int\limits_0^t\psi_1(x)\,dx+\frac{1}{2}\varphi_1(t)-\frac{1}{2}\varphi_1(0)-\frac{1}{2}\int\limits_0^l\int\limits_0^t f(x+l-\tau,\tau)\,d\tau\,dx.$$

6^0.**О минимальности промежутка времени** $T=l$**.** Мы доказали существование граничных управлений $\mu(t)$ и $\nu(t)$, обеспечивающих переход колебательной системы из одного состояния в другое состояние за промежуток времени T, равный длине l колебательной системы. При этом функции $\varphi'(x)$, $\psi(x)$, $\varphi_1'(x)$, $\psi_1(x)$ и $f(x,t)$ не предполагаются линейно зависимыми ни на одном содержащемся в $[0,l]$ сегменте положительной длины.

Естественно возникает вопрос о существовании граничных управлений, обеспечивающих указанный переход колебательной системы за промежуток времени T, меньший l, то есть вопрос о минимальности используемого нами промежутка времени $T=l$. Убедимся в том, что за промежуток времени T, меньший l, невозможно обеспечить переход от произвольного состояния, то есть от функций $\varphi(x)\in W_2^2[0,l]$ и $\psi(x)\in W_2^1[0,l]$, к произвольному состоянию, то есть к функциям $\varphi_1(x)\in W_2^2[0,l]$ и $\psi_1(x)\in W_2^1[0,l]$, без предположения о том, что функции $\varphi'(x)$, $\psi(x)$, $\varphi_1'(x)$, $\psi_1(x)$ и $f(x,t)$ являются линейно зависимыми на содержащихся в $[0,l]$ сегментах положительной длины.

Ради простоты рассмотрим задачу о возбуждении колебательной системы, то есть случай $\varphi(x) \equiv 0$ и $\psi(x) \equiv 0$.

В пункте 3 отмечено, что при любом T, удовлетворяющем условию $0 \leqslant T \leqslant l$, единственное решение из класса $\widehat{W}_2^2(Q_l)$ смешанной задачи (1)–(3) в случае $\varphi(x) \equiv 0$ и $\psi(x) \equiv 0$, при произвольных граничных функциях $\underline{\mu}(t)$ и $\underline{\nu}(t)$, принадлежащих классу $\underline{W}_2^2[0,T]$, представляется в виде

$$u(x,t) = \underline{\mu}(t-x) + \underline{\nu}(t+x-l) + \frac{1}{2}\int\limits_0^t \int\limits_{x-t+\tau}^{x+t-\tau} f(\xi,\tau)\,d\xi\,d\tau,$$

где $f(x,t)$ — произвольная функция из класса $W_2^1(Q_T)$, продолженная нечетно по первой переменной относительно точек $x = 0$ и $x = l$.

Так как при $t = T$ и при всех x из сегмента $[0,l]$ имеем:

$$u(x,T) = \underline{\mu}(T-x) + \underline{\nu}(T+x-l) + \frac{1}{2}\int\limits_0^T \int\limits_{x-T+\tau}^{x+T-\tau} f(\xi,\tau)\,d\xi\,d\tau = \varphi_1(x), \tag{62}$$

$$u_t(x,T) = \underline{\mu}'(T-x) + \underline{\nu}'(T+x-l) + \frac{1}{2}\int\limits_0^T [f(x+T-\tau,\tau) + f(x-T+\tau,\tau)]\,d\tau = \psi_1(x). \tag{63}$$

Из равенства (62) вытекает, что

$$u_x(x,T) = -\underline{\mu}'(T-x) + \underline{\nu}'(T+x-l) + \frac{1}{2}\int\limits_0^T [f(x+T-\tau,\tau) - f(x-T+\tau,\tau)]\,d\tau = \varphi_1'(x), \tag{64}$$

тогда из (63) и (64) следует, что для всех x из сегмента $[0,l]$

$$\psi_1(x) + \varphi_1'(x) - \int\limits_0^T f(x+T-\tau,\tau)\,d\tau = 2\underline{\nu}'(T+x-l),$$

$$\psi_1(x) - \varphi_1'(x) - \int\limits_0^T f(x-T+\tau,\tau)\,d\tau = 2\underline{\mu}'(T-x).$$

Так как $\underline{\mu}'(x) \equiv 0$ для всех $T \leqslant x$, а $\underline{\nu}'(x) \equiv 0$ для всех $x \leqslant l-T$, то из двух последних равенств получаем, что

$$\psi_1(x) + \varphi_1'(x) - \int\limits_0^T f(x+T-\tau,\tau)\,d\tau \equiv 0 \quad \text{на сегменте} \quad 0 \leqslant x \leqslant l-T$$

и

$$\psi_1(x) - \varphi_1'(x) - \int\limits_0^T f(x-T+\tau,\tau)\,d\tau \equiv 0 \quad \text{на сегменте} \quad T \leqslant x \leqslant l.$$

Таким образом, при любом $T < l$ функции $\varphi'(x)$, $\psi_1(x)$ и $f(x,t)$ являются линейно зависимыми на каждом из содержащихся в $[0,l]$ сегментов $[0,l-T]$ и $[T,l]$ положительной длины.

Автор выражает глубокую благодарность своему научному руководителю доценту Крицкову Л. В. за постоянное внимание и полезные обсуждения при выполнении этой работы.

Список литературы

[1] *Lions J. L.* Exact controllability, stabilization and perturbations for distributed systems // SIAM Review. — 1988. — Vol. 30, no. 1. — P. 1–68.

[2] *Бутковский А. Г.* Теория оптимального управления системами с распределенными параметрами. — М.: Наука, 1985.

[3] *Егоров А. И.* Управление упругими колебаниями // ДАН УССР, серия физ-мат. и техн. наук. — 1986. — № 5. — С. 60–63.

[4] *Васильев Ф. П.* О двойственности в линейных задачах управления и наблюдения // Дифференц. уравнения. — 1995. — Т. 31, № 11. — С. 1893–1900.

[5] *Васильев Ф. П., Куржанский М. А., Потапов М. А.* Метод прямых в задачах граничного управления и наблюдения для уравнений колебаний струны // Вестник МГУ, сер. 15, вычисл. матем. и киберн. — 1993. — № 3. — С. 8–15.

[6] *Васильев Ф. П., Куржанский М. А., Разгулин А. В.* О методе Фурье для решения одной задачи управления колебанием струны // Вестник МГУ, сер. 15, вычисл. матем. и киберн. — 1993. — № 2. — С. 3–8.

[7] *Ильин В. А., Тихомиров В. В.* Волновое уравнение с граничным управлением на двух концах и задача о полном успокоении колебательного процесса // Дифференц. уравнения. — 1999. — Т. 35, № 5. — С. 692–704.

[8] *Ильин В. А.* Волновое уравнение с граничным управлением на двух концах за произвольный промежуток времени // Дифференц. уравнения. — 1999. — Т. 35, № 11. — С. 1517–1534.

УДК 004.056.55

ОБ АТАКЕ НА ФИЛЬТРУЮЩИЙ ГЕНЕРАТОР С ФУНКЦИЕЙ УСЛОЖНЕНИЯ БЛИЗКОЙ К АЛГЕБРАИЧЕСКИ ВЫРОЖДЕННОЙ

© 2011 г. Е. К. Алексеев

alekseev@cs.msu.su

Кафедра математической кибернетики

1 Введение

Одним из существенных элементов в структуре ряда методов криптографического анализа являются математические модели аппроксимации криптографических булевых функций (отображений). Результатом применения этих методов является то, что удается свести решение исходной криптографической задачи (вскрытие зашифрованных данных, определение ключа и т. п.) к решению соответствующей математической задачи. Это сведение позволяет находить решение криптографической задачи наиболее эффективно. Как правило, криптографические функции аппроксимируются с помощью аффинных (линейных) функций. Данный вид аппроксимации используется в корреляционном [7] и линейном [4] методах криптографического анализа, а также в их комбинациях с другими методами (например, в линейно-дифференциальном методе).

В настоящей работе рассмотрен случай аппроксимации функции усложнения фильтрующего генератора с помощью алгебраически вырожденной функции. На основе этой аппроксимации строится алгоритм определения ключа фильтрующего генератора по его выходной последовательности. Расчитывается и обосновывается верхняя оценка для трудоемкости алгоритма.

Статья организована следующим образом. В следующем разделе рассматриваются основные определения, понятия и факты, которые понадобятся для дальнейшего изложения. В третьем разделе описывается алгоритм восстановления ключа фильтрующего генератора, который основан на аппроксимации функции усложнения с помощью алгебраически вырожденной функции. Четвертый раздел посвящен расчету верхней оценки трудоемкости алгоритма. В пятом разделе рассматривается некоторая модификация алгоритма, использующая методы математической статистики. В шестом разделе рассматриваются некоторые свойства тех аппроксимирующих функций, которые расположены на минимальном расстоянии от функции усложнения. В заключительном разделе приводятся некоторые примеры фильтрующих генераторов. Для них оценивается трудоемкость применения описанных ранее алгоритмов.

2 Основные определения и понятия

Пусть $\mathbb{F}_2$ — конечное поле из двух элементов. Пусть $V_n = \mathbb{F}_2^n$ — векторное пространство наборов длины n с компонентами из $\mathbb{F}_2$. *Булевой функцией* от n переменных будем называть отображение из V_n в $\mathbb{F}_2$. Множество всех булевых функций от n переменных будем обозначать $\mathcal{F}_n$. *Носителем* функции $f \in \mathcal{F}_n$ называется множество $1_f = \{x \in V_n \mid f(x) = 1\}$. *Весом* $\mathrm{wt}(f)$ булевой функции $f \in \mathcal{F}_n$ называется мощность ее носителя 1_f.

В дальнейшем будем придерживаться следующих обозначений: $x^{(i)}$ — i-ый вектор из некоторой совокупности векторов, а x_i — i-ая компонента вектора x. Если n — натуральное число, а $c \in \{0, 1\}$, то через c^n будем обозначать вектор длины n, все компоненты которого равны c. Константные булевы функции будем обозначать через $\overline{0}$ и $\overline{1}$.

Пусть L — подмножество пространства V_n. Тот факт, что L является подпространством пространства V_n, будем обозначать так: $L < V_n$. Для произвольного линейного подпространства $L < V_n$ через L^* будем обозначать множество $L \setminus \{0^n\}$.

Индикаторной функцией множества $S \subseteq V_n$ называется такая функция $I_S \in \mathcal{F}_n$, что $I_S(x) = 1$ тогда и только тогда, когда $x \in S$.

Для булевой функции f от n переменных и вектора $u \in V_n$ будем обозначать через f^u функцию $f^u\colon x \to f(x \oplus u)$. *Производной булевой функции* f по направлению $u \in V_n^*$ называется функция $D_u f = f \oplus f^u$. Через $J(f)$ будем обозначать подпространство $\{u \in V_n \mid f^u = f\}$ пространства V_n. Ограничением функции $f \in \mathcal{F}_n$ на множестве $S \subseteq V_n$ называется такая функция $f|_S\colon S \to \mathbb{F}_2$, что $f|_S(x) = f(x)$ для любого $x \in S$.

Пусть A — $(n \times k)$-матрица над $\mathbb{F}_2$, а g — булева функция от k переменных. Через g^A будем обозначать функцию от n переменных, определенную следующим образом: $g^A\colon x \to g(xA)$.

Утверждение 1 (Алексеев [2])**.** Любая функция $f \in \mathcal{F}_n$ представима в виде

$$f = \bigoplus_{i=1}^{2^{n-\dim J(f)}} \varepsilon_i I_{J(f) \oplus z^{(i)}}, \quad \text{где} \quad \varepsilon_i \in \{0,1\}, \quad z^{(i)} \in V_n.$$

Определение 1 (Dawson, Wu [3])**.** *Порядком алгебраической вырожденности* $\mathrm{AD}(f)$ булевой функции $f \in \mathcal{F}_n$ называется максимально возможное значение $n-k$, где целое число $0 \leqslant k \leqslant n$ таково, что существуют такие функция $g \in \mathcal{F}_k$ и $(n \times k)$-матрица D над $\mathbb{F}_2$, что выполнено равенство $f = g^D$. Функции, для которых $\mathrm{AD}(f) > 0$, называются *алгебраически вырожденными*. Множество всех алгебраически вырожденных функций от n переменных обозначим через

$$\mathrm{DG}(n) = \{f \in \mathcal{F}_n \mid \mathrm{AD}(f) > 0\}.$$

Утверждение 2 (Алексеев [5])**.** Для любой булевой функции $f \in \mathcal{F}_n$ справедливо равенство

$$\mathrm{AD}(f) = \dim J(f).$$

Утверждение 3. Пусть $n = k \cdot s$ и $t = \frac{2^n-1}{2^k-1}$. Пусть $A\colon V_n \to V_n$ — линейное преобразование пространства V_n, характеристический многочлен которого примитивен. Тогда для любого вектора $u \in V_n^*$ множество $L = \{0^n, u, A^t u, \ldots, A^{(2^k-2)\cdot t} u\}$ является подпространством пространства V_n и выполнено соотношение $A^t L = L$.

Доказательство. Пусть u — произвольный ненулевой вектор пространства V_n. Поскольку характеристический многочлен оператора A является примитивным, то векторы u, Au, A^2u, …, $A^{n-1}u$ линейно независимы и являются базисом пространства V_n. Пусть ξ — примитивный элемент поля $\mathrm{GF}(2^n)$. Рассмотрим изоморфизм φ пространств V_n и $\mathrm{GF}(2^n)$, определенный следующим образом: $\varphi(A^i u) = \xi^i$ для $i = 0, 1, \ldots, n-1$. Образом $\varphi(L)$ множества L относительно отображения φ является подполе $\mathrm{GF}(2^k)$ поля $\mathrm{GF}(2^n)$. Поскольку множество $\mathrm{GF}(2^k)$ является подпространством пространства $\mathrm{GF}(2^n)$, то и множество L является подпространством пространства V_n. Тот факт, что $A^t L = L$ следует из определения множества L и из соотношения $A^t(A^{(2^k-2)\cdot t} u) = A^{2^n-1} u = u$. □

В дальнейшем основным объектом исследований является такой криптографический примитив, как *фильтрующий генератор* (рисунок 1), построенный с помощью линейных преобразований $A\colon V_n \to V_n$, $B\colon V_n \to V_m$ и фильтрующей функции $f \in \mathcal{F}_n$, обозначаемый $\mathrm{LFSR}(A, B, f)$. Фильтрующий генератор используется в качестве генератора псевдослучайной последовательности. Бит z_i, порожденный с помощью вектора начального заполнения $u^{(0)} \in V_n$ на такте с номером $i \geqslant 0$, удовлетворяет соотношению $z_i = f(BA^i u^{(0)})$.

3 Восстановление ключа фильтрующего генератора

Рассмотрим задачу восстановления начального состояния (ключа) фильтрующего генератора по его выходной последовательности, математически описывающую атаку по открытому и шифрованному текстам на соответствующий потоковый шифр с угрозой вскрытия ключа.

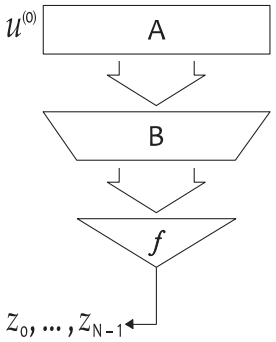


Рис. 1. LFSR(A, B, f).

Пусть невырожденное линейное преобразование $A\colon V_n \to V_n$, где $n = k \cdot s$ и $1 < k < n$, имеет примитивный характеристический многочлен. Пусть $t = \frac{2^n-1}{2^k-1}$, тогда из утверждения 3 следует, что существует такое подпространство $L \subset V_n$ размерности k, что $A^t(L) = L$. Пусть линейное отображение $B\colon V_n \to V_m$ сюръективно, а фильтрующая функция $f \in \mathcal{F}_m$ является алгебраически невырожденной. В таком случае, i-ый бит z_i выходной последовательности, полученный с помощью вектора начального заполнения $u^{(0)}$, удовлетворяет соотношению

$$z_i = f(BA^i u^{(0)}).$$

Будем считать, что не существует двух различных векторов u, $v \in V_n$, для которых равенство $f(BA^i u) = f(BA^i v)$ выполнено для любого значения $i = 0, 1, \ldots, n-1$.

Пусть нам известны N первых бит $z_0 \ldots z_{N-1}$ выходной последовательности фильтрующего генератора. Требуется определить начальное состояние (ключ) $u^{(0)}$ фильтрующего генератора, используя систему N булевых уравнений

$$f(BA^i u^{(0)}) = z_i, \quad i = 0, 1, \ldots, N-1.$$

Пусть $l = \dim(L \cap \ker B)$, тогда $\dim B(L) = k - l$.

Пусть g — некоторая функция из $\mathcal{F}_m$, удовлетворяющая условиям

$$B(L) \subseteq J(g) \quad \text{и} \quad |1_{f \oplus g} \cap (B(L) \oplus y))| \leqslant 2^{\dim B(L)-1}, \quad y \in V_m.$$

Заметим, что если заданы функция $f \in \mathcal{F}_m$ и подпространство M пространства V_m, где $\dim M = k$, то носитель функции g, удовлетворяющей указанным условиям, можно представить в следующем виде

$$1_g = \bigcup_{y \in V_m\colon |1_f \cap (M \oplus y)| \geqslant 2^{k-1}} M \oplus y.$$

Для таким образом определенной функции g справедливо соотношение

$$\operatorname{dist}(f, g) = \min_{g' \in \mathcal{F}_m\colon M \subseteq J(g')} \operatorname{dist}(f, g').$$

Будем считать, что множества $\{y \in B(L) \oplus v \mid f(y) \neq g(y)\}$ вычислены для любого вектора $v \in V_m$.

Пусть $\{u^{(1)}, \ldots, u^{(k)}\}$ — произвольный базис пространства L, а $\{v^{(1)}, \ldots, v^{(n-k)}\}$ — произвольное дополнение базиса пространства L до базиса всего пространства V_n.

Тогда ключ $u^{(0)}$ представим в виде

$$u^{(0)} = \underbrace{x_1 u^{(1)} \oplus \ldots \oplus x_k u^{(k)}}_{\in L} \oplus \underbrace{y_1 v^{(1)} \oplus \ldots \oplus y_{n-k} v^{(n-k)}}_{v^{(0)}}.$$

Для любого такта с номером вида $t \cdot i$ справедливо $A^{t \cdot i}(u^{(0)}) \in L \oplus A^{t \cdot i}(v^{(0)})$, то есть то, в каком смежном классе по L лежит вектор $A^{t \cdot i}(u^{(0)})$, определяется лишь вектором $v^{(0)}$.

Опишем алгоритм $\mathcal{K}$, который позволяет по значению выходной последовательности восстановить истинное значение ключа $u^{(0)}$. Для этого фиксируем натуральный параметр $d \in \mathbb{N}$ (число проверок для смежных классов) и обозначим через $\widetilde{L}$ подпространство, порожденное векторами $\{v^{(1)}, \ldots, v^{(n-k)}\}$.

Описание алгоритма $\mathcal{K}$.

1. Выберем произвольный вектор $v \in \widetilde{L}$ и присвоим $\widetilde{L} := \widetilde{L} \setminus \{v\}$.
2. Если равенство $g(BA^{t \cdot i}v) = z_{t \cdot i}$ выполнено для всех $i \in \{0, \ldots, d-1\}$, то положим $Y := L \oplus v$ и переходим к пункту 4.
3. Положим $Y := \{y \in L \oplus v \mid f(BA^{t \cdot i}y) \neq g(BA^{t \cdot i}y)\}$, для произвольного $i \in \{0, \ldots, d-1\}$ такого, что $g(BA^{t \cdot i}v) \neq z_{t \cdot i}$.
4. Если $Y = \emptyset$, то переходим к пункту 1, иначе выберем некоторый вектор $u \in Y$, присвоим $Y := Y \setminus \{u\}$.
5. Если равенство $f(BA^j u) = z_j$ выполнено для всех $j \in \{0, \ldots, n-1\}$, то возвращаем вектор u в качестве результата и заканчиваем работу. Иначе переходим к пункту 4.

Учитывая сделанные ранее предположения, справедлива следующая основная теорема.

Теорема 1. Алгоритм $\mathcal{K}$ всегда останавливается и возвращает истинное значение ключа $u^{(0)}$.

Доказательство. Поскольку перебор происходит по конечному множеству смежных классов $L \oplus v$, а для каждого смежного класса необходимо перебрать конечное число векторов, то алгоритм $\mathcal{K}$ всегда останавливается.

Для любого вектора u из смежного класса $L \oplus v \neq L \oplus v^{(0)}$ существует такой номер $0 \leqslant j \leqslant n-1$, что $f(BA^j u) \neq z_j$. Таким образом, никакой вектор из смежного класса $L \oplus v \neq L \oplus v^{(0)}$ не может быть возвращен в качестве результата.

Рассмотрим смежный класс $L \oplus v^{(0)}$. Если равенства $g(BA^{t \cdot i}v^{(0)}) = z_{t \cdot i}$ выполнены для всех значений $i = 0, 1, \ldots, d-1$, то после перебора по всему смежному классу $L \oplus v^{(0)}$ в качестве результата будет возвращено истинное значение ключа $u^{(0)}$.

Если же на некотором такте i выполнено неравенство $g(BA^{t \cdot i}v^{(0)}) \neq z_{t \cdot i}$, то выполнено включение $A^{t \cdot i}u^{(0)} \in \{y \in L \oplus A^{t \cdot i}v^{(0)} \mid f(By) \neq g(By)\}$ или, что тоже самое,

$$u^{(0)} \in \{y \in L \oplus v^{(0)} \mid f(BA^{t \cdot i}y) \neq g(BA^{t \cdot i}y)\}.$$

Из описания пункта 3 видно, что именно из этого множества будут выбираться векторы u в пункте 4. Поэтому в качестве результата будет возвращено истинное значение ключа $u^{(0)}$. $\square$

4 Оценка трудоемкости алгоритма

Для $v \in V_n$ через $D_v(i)$ обозначим множество $D_v(i) = \{y \in A^{t \cdot i}v \oplus L \mid f(By) \neq g(By)\}$. Заметим, что выполнено соотношение $|D_v(i)| = 2^l \cdot \mathrm{wt}(f \oplus g)|_{B(L \oplus A^{t \cdot i}v)}$. Справедлива следующая

Лемма 1. Для любого фиксированного значения $i = 0, 1, \ldots, 2^k - 2$ справедливо соотношение

$$\sum_{v \in \widetilde{L}} |D_v(i)| = 2^{n-m} \cdot \mathrm{dist}(f, g).$$

Доказательство. Подпространство $\ker B$ обозначим через K. Заметим, что образы подпространств $L + K$ и L относительно оператора B совпадают. Пусть подпространство M пространства V_n таково, что $M \cap (L + K) = \{0^n\}$ и $M + (L + K) = V_n$. Справедливы следующие

соотношения

$$\sum_{v\in\widetilde{L}}|D_v(i)| = \frac{1}{2^{\dim L}}\sum_{v\in V_n}|D_v(i)| = \frac{1}{2^k}\sum_{u\in M}\sum_{v\in(L+K)\oplus u}|D_v(i)| =$$

$$= \frac{1}{2^k}\sum_{u\in M}2^{n-m+k-l}\cdot|D_u(i)| = \frac{2^l\cdot 2^{n-m+k-l}}{2^k}\cdot\operatorname{dist}(f,g) = 2^{n-m}\cdot\operatorname{dist}(f,g). \quad \square$$

Для расчета параметров алгоритма $\mathcal{K}$ будем использовать следующую вероятностную модель.

При случайном выборе векторов v, $u^{(0)}$ из V_n так, что $v\notin L\oplus u^{(0)}$, будем считать, что события $\{g(BA^{t\cdot i}v) = f(BA^{t\cdot i}u^{(0)})\}$, где $i = 0, 1, \ldots, d-1$, являются независимыми в совокупности, а также выполнено соотношение

$$\Pr\left[g(BA^{t\cdot i}v) = f(BA^{t\cdot i}u^{(0)}) \mid v\notin L\oplus u^{(0)}\right] = \frac{1}{2},$$

для любого $i = 0, 1, \ldots, d-1$. Также будем считать, что при случайном выборе различных u, $u^{(0)}\in V_n$ события $\{f(BA^ju) = f(BA^ju^{(0)})\}$, где $j = 0, 1, \ldots, n-1$, независимы в совокупности и

$$\Pr\left[f(BA^ju) = f(BA^ju^{(0)}) \mid u\neq u^{(0)}\right] = \frac{1}{2},$$

для любого $j = 0, 1, \ldots, n-1$. Также будем считать, что события $\{g(BA^{t\cdot i}u^{(0)}) = f(BA^{t\cdot i}u^{(0)})\}$, где $i = 0, 1, \ldots, d-1$, независимы в совокупности, причем

$$\Pr\left[g(BA^{t\cdot i}u^{(0)}) = f(BA^{t\cdot i}u^{(0)})\right] = \left(1-\frac{|D_{u^{(0)}}(i)|}{2^k}\right)$$

для любого целого $i\geqslant 0$.

Под одним шагом алгоритма будем понимать вычисление значений $g(BA^{t\cdot i}v)$ для фиксированного вектора v и для всех номеров $i = 0, 1, \ldots, d-1$ и проверку равенств, предусмотренных пунктом 2 алгоритма $\mathcal{K}$. Также будем считать за один шаг алгоритма вычисление значений $f(BA^ju)$ для фиксированного вектора u и для всех номеров $j = 0, 1, \ldots, n-1$ и проверку равенств, предусмотренных пунктом 5.

Определим семейство дискретных случайных величин $\{\xi^v_{v^{(0)}} \mid v, v^{(0)}\in\widetilde{L}\}$, отражающих трудоемкость алгоритма $\mathcal{K}$ на разных этапах его работы. Опишем распределение случайных величин из этого семейства. Если $v\neq v^{(0)}$, то

$$\Pr\left[\xi^v_{v^{(0)}} = 1+2^k\right] = \frac{1}{2^d},$$

$$\Pr\left[\xi^v_{v^{(0)}} = 1+s_v(i)\right] = \frac{1}{2^{i+1}} \quad \text{для любого номера } i = 0, 1, \ldots, d-1.$$

Если же $v = v^{(0)}$, то

$$\Pr\left[\xi^{v^{(0)}}_{v^{(0)}} = 1+2^k\right] = \prod_{j=0}^{d-1}\left(1-\frac{|D_v(j)|}{2^k}\right),$$

$$\Pr\left[\xi^{v^{(0)}}_{v^{(0)}} = 1+s_v(i)\right] = \frac{|D_v(i)|}{2^k}\prod_{j=0}^{i-1}\left(1-\frac{|D_v(j)|}{2^k}\right) \quad \text{для любого номера } i = 0, 1, \ldots, d-1.$$

Заметим, что случайная величина $\xi^v_{v^{(0)}}$ при $v\neq v^{(0)}$ отражает то количество шагов, которое проделывает алгоритм $\mathcal{K}$, начиная с пункта 1, на котором выбирается вектор v, до возвращения к этому же пункту для выбора нового вектора. При этом истинный ключ принадлежит

смежному классу $L \oplus v^{(0)}$. Если же $v = v^{(0)}$, то случайная величина $\xi_{v^{(0)}}^{v^{(0)}}$ отражает количество шагов, которое проделывает алгоритм $\mathcal{K}$ от выбора в пункте 1 вектора $v = v^{(0)}$ до возвращения истинного ключа в пункте 5.

Случайная величина $\xi_{v^{(0)}}$, отражающая трудоемкость определения ключа $u^{(0)} \in L \oplus v^{(0)}$ в «худшем» случае, то есть когда вектор $v \in L \oplus v^{(0)}$ выбирается в пункте 1 из множества $\widetilde{L}$ последним, определяется равенством

$$\xi_{v^{(0)}} = \sum_{v \in \widetilde{L}} \xi_{v^{(0)}}^{v}.$$

Поскольку истинный ключ может находиться в любом смежном классе по L с вероятностью $\frac{1}{2^{n-k}}$, то средняя трудоемкость алгоритма $\mathcal{K}$ не превосходит значения

$$\frac{1}{2^{n-k}} \sum_{v^{(0)} \in \widetilde{L}} \mathbf{M}\xi_{v^{(0)}}.$$

Обозначим это значение через $S_{\mathcal{K}}$. Справедлива следующая

Теорема 2. Справедливо неравенство

$$S_{\mathcal{K}} \leqslant 2^k + 2^{n-k} + 2^{n-d} + 2^{n-m} \cdot \operatorname{dist}(f, g).$$

Доказательство. Заметим, что $\mathbf{M}\xi_{v^{(0)}}^{v^{(0)}} \leqslant 2^k$, и при любом $v \neq v^{(0)}$ справедливо равенство

$$\mathbf{M}\xi_{v^{(0)}}^{v} = 1 + \sum_{i=0}^{d-2} \frac{|D_v(i)|}{2^{i+1}} + 2^{k-d}.$$

Пусть v' — некоторый ненулевой вектор из $\widetilde{L}$. Для $S_{\mathcal{K}}$ справедливо соотношение

$$S_{\mathcal{K}} = \frac{1}{2^{n-k}} \sum_{v^{(0)} \in \widetilde{L}} \sum_{v \in \widetilde{L}} \mathbf{M}\xi_{v^{(0)}}^{v} = \frac{1}{2^{n-k}} \sum_{v \in \widetilde{L}} \left[\mathbf{M}\xi_{v}^{v} + (2^{n-k} - 1)\mathbf{M}\xi_{v}^{v \oplus v'} \right] \leqslant 2^k + \sum_{v \in \widetilde{L}} \mathbf{M}\xi_{v}^{v \oplus v'}.$$

Преобразуем полученную сумму, учитывая соотношения для соответствующего математического ожидания.

$$\sum_{v \in \widetilde{L}} \mathbf{M}\xi_{v}^{v \oplus v'} = \sum_{v \in \widetilde{L}} \left[1 + \sum_{i=0}^{d-2} \frac{|D_v(i)|}{2^{i+1}} + 2^{k-d} \right] = 2^{n-k} + 2^{n-d} + \sum_{v \in \widetilde{L}} \sum_{i=0}^{d-2} \frac{|D_v(i)|}{2^{i+1}} =$$

$$= 2^{n-k} + 2^{n-d} + \sum_{i=0}^{d-2} \frac{1}{2^{i+1}} \sum_{v \in \widetilde{L}} |D_v(i)| \leqslant 2^{n-k} + 2^{n-d} + 2^{n-m} \cdot \operatorname{dist}(f, g).$$

Учитывая это, получаем необходимое соотношение. □

Рассмотрим подробнее смысл тех параметров, которые участвуют в полученной верхней оценке трудоемкости алгоритма $\mathcal{K}$. Параметр d определяет необходимый для атаки объем шифртекста и открытого текста. Действительно, при работе алгоритма используются значения z_0, z_t, z_{2t}, …, $z_{t\cdot(d-1)}$ для определения смежного класса, содержащего ключ, и биты z_0, z_1, …, z_{n-1} для определения самого ключа. Таким образом, необходимо не более $d + n - 1$ битов гаммы. Однако, максимальный номер необходимого бита равен $t \cdot (d-1)$, поэтому в «худшем случае» для осуществления атаки необходимо $t \cdot (d-1) + 1 = (d-1) \cdot \frac{2^n - 1}{2^k - 1} + 1$ битов гаммы.

Параметры k и $\operatorname{dist}(f, g)$ отражают качество аппроксимации функции f алгебраически вырожденной функцией g. Значение $\operatorname{dist}(f, g)$ также отражает тот объем памяти, который необходим для атаки. Действительно, нам необходимо хранить в памяти все различные множества вида $\{y \in B(L) \oplus v \mid f(y) \neq g(y)\}$ для всех $v \in V_m$. Различные множества такого вида не пересекаются и сумма их мощностей равна $\operatorname{dist}(f, g)$.

5 Вероятностный алгоритм определения ключа

Перед описанием алгоритма $\mathcal{K}$ было сделано предположение о том, что для любого вектора $v \in V_m$ множество $\{y \in B(L) \oplus v \mid f(y) \neq g(y)\}$ вычислено. Однако в том случае, когда число m велико, вычисление этих множеств само по себе может быть достаточно трудоемкой задачей. В данном разделе исследуется возможность применения методов математической статистики для определения ключа в том случае, когда предварительное вычисление множеств $\{y \in B(L) \oplus v \mid f(y) \neq g(y)\}$ невозможно.

Для удобства дальнейших рассуждений в схеме фильтрующего генератора под функцией f будем понимать совокупность преобразований B и f. То есть будем считать, что бит z_i, выработанный фильтрующим генератором на i-ом такте с помощью вектора начального заполнения $u^{(0)}$, удовлетворяет соотношению $z_i = f'(A^i u^{(0)})$, где $f' = f^B \colon x \to f(Bx)$. Далее функцию f' будем обозначать просто f. Аппроксимирующая функция g строится с помощью подпространства L по схеме аналогичной той, которая была описана ранее (разница в рассуждениях заключается в том, что теперь мы считаем преобразование B тождественным).

Идея вероятностного алгоритма, который будет подробно описан далее, состоит в следующем. Исходя из той вероятностной модели, которая была описана при оценке параметров алгоритма $\mathcal{K}$, в том случае, когда векторы v, $v^{(0)}$ лежат в разных смежных классах по подпространству L, при достаточно большом значении параметра d вес вектора

$$w = \Big(g(A^{0\cdot t}v) \oplus f(A^{0\cdot t}v^{(0)}), \ldots, g(A^{(d-1)\cdot t}v) \oplus f(A^{(d-1)\cdot t}v^{(0)})\Big)$$

будет близок к значению $\frac{d}{2}$. Если же векторы v и $v^{(0)}$ лежат в одном смежном классе по L, то вес вектора w будет отличаться от $\frac{d}{2}$, причем степень отклонения от этого значения будет тем больше, чем лучше функция g аппроксимирует функцию f. Для того, чтобы различить эти два случая, будут использоваться методы математической статистики.

Описание и оценку параметров вероятностного алгоритма определения ключа будем проводить в предположении, что $\operatorname{dist}(f,g) \ll 2^{n-1}$. Мы будем исходить из следующих рассуждений о распределении векторов из носителя функции $f \oplus g$ по пространству V_n. Поскольку подпространство L не зависит от фильтрующей функции f, то будем считать, что векторы из носителя функции $f \oplus g$, то есть векторы, на которых значения функций f и g не совпадают, распределены по пространству V_n случайно. Распределение векторов из $1_{f\oplus g}$ по смежным классам по пространству L представим в виде случайного бросания $\operatorname{dist}(f,g)$ шаров в 2^{n-k} урн. Поскольку $\operatorname{dist}(f,g) \ll 2^{n-1}$, будем считать, что вероятность попадания вектора в произвольный смежный класс $L \oplus z$ при любом по счету бросании равна $\frac{1}{2^{n-k}}$. В таком случае, случайная величина X_z, отражающая количество попаданий в смежный класс $L \oplus z$, представима в виде $X_z = \xi_1 + \ldots + \xi_{\operatorname{dist}(f,g)}$, где $\xi_i \in \{0,1\}$ и $\Pr[\xi_i = 1] = \frac{1}{2^{n-k}}$ для любого $i \in \{1, \ldots, \operatorname{dist}(f,g)\}$. Тогда

$$\mathbf{M}X_z = \sum_{i=1}^{\operatorname{dist}(f,g)} \mathbf{M}\xi_i = \frac{\operatorname{dist}(f,g)}{2^{n-k}}.$$

Определим случайную величину Y_z, которая принимает значение 0 и 1, причем $Y_z = 1$, если значения функций f и g на случайно выбранном векторе из смежного класса $L \oplus z$ различны. Пусть R — случайная величина, равномерно распределенная на сегменте $[0,1]$. Тогда Y_z может быть представлена следующим образом:

$$Y_z = \begin{cases} 1, & \text{если } R \leqslant \frac{X_z}{2^k}, \\ 0, & \text{иначе.} \end{cases}$$

Вычислим $\Pr[Y_z = 1]$, воспользовавшись формулой полной вероятности:

$$\Pr[Y_z = 1] = \Pr[X_z = 0] \cdot \Pr[R \leqslant 0] + \ldots + \Pr[X_z = 2^{k-1}] \cdot \Pr[R \leqslant \frac{2^{k-1}}{2^k}] =$$
$$= \frac{1}{2^k} \sum_{t=0}^{2^{k-1}} t \cdot \Pr[X_z = t] \leqslant \frac{1}{2^k} \mathbf{M} X_z = \frac{\operatorname{dist}(f,g)}{2^n} \ll \frac{1}{2}.$$

Трудоемкость алгоритма будет тем меньше, чем меньше будет вероятность того, что на произвольном смежном классе по L функции f и g различаются, то есть чем меньше значение $\Pr[Y_z = 1]$. Таким образом, верхняя оценка трудоемкости алгоритма может быть получена путем замены вероятности $\Pr[Y_z = 1]$ на ее верхнюю оценку. Далее будем считать, что для любого смежного класса эта вероятность равна $\frac{\operatorname{dist}(f,g)}{2^n}$.

Опишем алгоритм $\mathcal{K}_{\Pr}$, с помощью которого будет определяться ключ. Напомним, что истинный ключ представим в виде $u^{(0)} = x_1 u^{(1)} \oplus \ldots \oplus x_k u^{(k)} \oplus y_1 v^{(1)} \oplus \ldots \oplus y_{n-k} v^{(n-k)}$. Пусть $\widetilde{L}$ — подпространство, порожденное векторами $\{v^{(1)}, \ldots, v^{(n-k)}\}$, а C — некоторая константа, значение которой будет вычислено далее. Необходимый для работы алгоритма объем d шифрующей последовательности также будет вычислен далее.

Описание алгоритма $\mathcal{K}_{\Pr}$.

1. Если множество $\widetilde{L}$ пусто, то заканчиваем работу, ничего не возвращая в качестве результата. В противном случае выберем произвольный вектор $v \in \widetilde{L}$ и присвоим $\widetilde{L} := \widetilde{L} \setminus \{v\}$.
2. Пусть вектор $w \in V_d$ таков, что $w_i = g(A^{t \cdot i} v) \oplus z_{t \cdot i}$. Если $\operatorname{wt}(w) \geqslant C$, то положим $Y := L \oplus v$ и переходим к пункту 3, иначе переходим к пункту 1.
3. Если $Y = \emptyset$, то переходим к пункту 1, иначе выберем некоторый вектор $u \in Y$, присвоим $Y := Y \setminus \{u\}$.
4. Если равенство $f(A^j u) = z_j$ выполнено для всех $j \in \{0, \ldots, n-1\}$, то возвращаем вектор u в качестве результата и заканчиваем работу. Иначе переходим к пункту 3.

Для расчета параметров алгоритма нам потребуется следующая вероятностная модель (рисунок 2). Пусть $\{Z_{t \cdot i}^{(0)}\}$, $\{X_{t \cdot i}^{(1)}\}$, $\ldots$, $\{X_{t \cdot i}^{(n)}\}$, $i = 0, 1, \ldots, N-1$, — независимые в совокупности

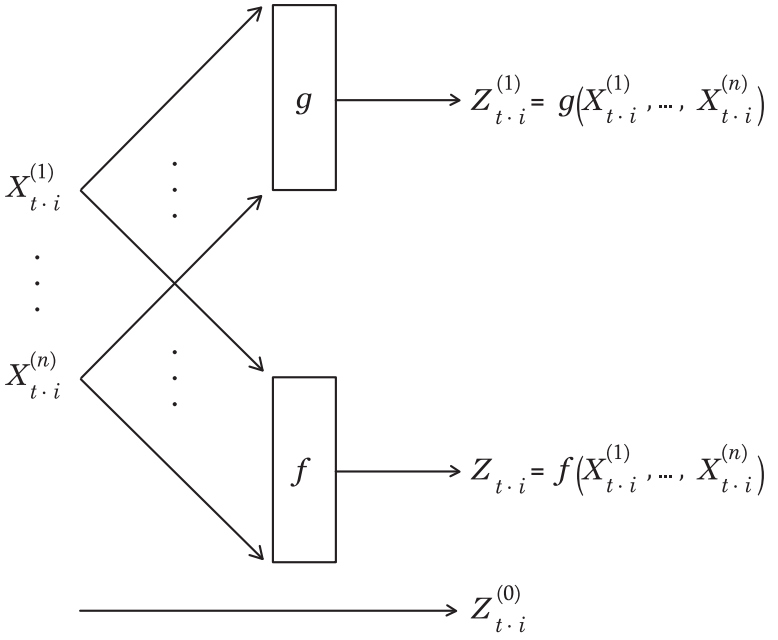


Рис. 2. Вероятностная модель.

и одинаково распределенные случайные величины с распределением $\Pr[X_{t\cdot i}^{(j)} = 0] = \Pr[X_{t\cdot i}^{(j)} = 1]$ и $\Pr[Z_{t\cdot i}^{(0)} = 0] = \Pr[Z_{t\cdot i}^{(0)} = 1]$ для $j = 1, 2, \ldots, n$, $i = 0, 1, \ldots, N-1$. Следовательно, случайный вектор $\left(X_{t\cdot i}^{(1)}, \ldots, X_{t\cdot i}^{(n)}\right)$ при любом i имеет распределение

$$\Pr\left[(X_{t\cdot i}^{(1)}, \ldots, X_{t\cdot i}^{(n)}) = u\right] = 2^{-n}$$

для любого $u \in V_n$. Поскольку функция f является уравновешенной, то случайные величины

$$Z_{t\cdot i} = f(X_{t\cdot i}^{(1)}, \ldots, X_{t\cdot i}^{(n)}), \quad i = 0, 1, \ldots, N-1,$$

имеют одинаковое распределение при любом i, а именно $\Pr[Z_{t\cdot i} = 0] = \Pr[Z_{t\cdot i} = 1]$, $i = 0, 1, \ldots, N$. В силу предположений о случайных величинах $\{X_{t\cdot i}^{(1)}\}, \ldots, \{X_{t\cdot i}^{(n)}\}$ случайные величины $Z_{t\cdot 0}, \ldots, Z_{t\cdot(N-1)}$ независимы. Случайные величины

$$Z_{t\cdot i}^{(1)} = g(X_{t\cdot i}^{(1)}, \ldots, X_{t\cdot i}^{(n)}), \quad i = 0, 1, \ldots, N,$$

также независимы и одинаково распределены. Справедливо соотношение

$$\Pr\left[Z_{t\cdot i}^{(1)} = Z_{t\cdot i}\right] = \Pr\left[(f \oplus g)(X_{t\cdot i}^{(1)}, \ldots, X_{t\cdot i}^{(n)}) = 0\right] = 1 - \frac{\operatorname{dist}(f, g)}{2^n} = q_1 > \frac{1}{2}.$$

Кроме того, поскольку $Z_{t\cdot i}^{(0)}$ и $Z_{t\cdot i}$ в силу наших предположений являются независимыми случайными величинами для $i = 0, 1, \ldots, N-1$, то

$$\Pr\left[Z_{t\cdot i}^{(0)} = Z_{t\cdot i}\right] = q_0 = \frac{1}{2}.$$

Учитывая все это, имеем

$$\Pr\left[Z_{t\cdot i}^{(1)} \oplus Z_{t\cdot i} \oplus 1 = 1\right] = q_1 > \frac{1}{2},$$
$$\Pr\left[Z_{t\cdot i}^{(0)} \oplus Z_{t\cdot i} \oplus 1 = 1\right] = q_0 = \frac{1}{2}.$$

Рассмотрим случайную величину ξ, характеризующую корреляцию между последовательностями $Z_{t\cdot 0}, \ldots, Z_{t\cdot(d-1)}$ и $Z_{t\cdot 0}^{(j)}, \ldots, Z_{t\cdot(d-1)}^{(j)}$, $j = 0, 1$, и определяемую следующим соотношением

$$\xi = \sum_{i=0}^{d-1} \left(Z_{t\cdot i}^{(j)} \oplus Z_{t\cdot i} \oplus 1\right).$$

Таким образом мы можем рассмотреть две простые гипотезы:

- H_1 — выбранный вектор v является представителем того же смежного класса, что и истинный ключ $u^{(0)}$. Этот случай соответствует ξ, отражающей корреляцию $\{Z_{t\cdot i}^{(1)}\}$ и $\{Z_{t\cdot i}\}$.
- H_0 — выбранный вектор v и истинный ключ $u^{(0)}$ лежат в разных смежных классах по подпространству L. Этот случай соответствует ξ, отражающей корреляцию $\{Z_{t\cdot i}\}$ и $\{Z_{t\cdot i}^{(0)}\}$.

Для случайной величины ξ справедливы соотношения:

$$\Pr_{\xi|H_0}(r) = \Pr_0(\xi = r) = \binom{d}{r} q_0^r (1 - q_0)^{d-r},$$
$$\Pr_{\xi|H_1}(r) = \Pr_1(\xi = r) = \binom{d}{r} q_1^r (1 - q_1)^{d-r},$$

$r = 0, 1, \ldots, d$. Как известно [6], оптимальный критерий для проверки гипотезы H_0 против конкурирующей гипотезы H_1 строится, исходя из неравенства (следствие леммы Неймана-Пирсона) $r \geqslant C$, где C — некоторая константа. При выполнении этого неравенства гипотеза H_0 отвергается, а в остальных случаях — принимается.

Через u_γ будем обозначать квантиль стандартного нормального распределения, для которой $1 - \Phi(u_\gamma) = \gamma$. Выбрав вероятности ошибок первого (вероятность отвергнуть гипотезу H_0, когда она верна) и второго (вероятность принять H_0, когда верна H_1) рода (α и β), получаем для заданных α и β границу

$$C \approx dq_0 + u_\alpha \sqrt{dq_0(1-q_0)} \approx dq_1 - u_\beta \sqrt{dq_1(1-q_1)}.$$

Эти соотношения дают также приблизительно необходимое количество битов d шифрующей последовательности для реализации статистического критерия

$$d \approx \frac{\left(u_\alpha \sqrt{q_0(1-q_0)} + u_\beta \sqrt{q_1(1-q_1)}\right)^2}{(q_0 - q_1)^2}.$$

Под одним шагом алгоритма будем понимать вычисление значений $g(A^{t \cdot i} v)$ для фиксированного вектора v и для всех номеров $i = 0, 1, \ldots, d-1$ и проверку неравенства, предусмотренного пунктом 2 алгоритма $\mathcal{K}_{\mathrm{Pr}}$. Также будем считать за один шаг алгоритма вычисление значений $f(A^j u)$ для фиксированного вектора u и для всех номеров $j = 0, 1, \ldots, n-1$ и проверку равенств, предусмотренных пунктом 4.

Таким образом, нам необходимо проверить 2^{n-k} векторов v из множества $\widetilde{L}$. Для тех векторов v, для которых выполнено неравенство в пункте 2, необходимо проверить 2^k векторов из смежного класса $L \oplus v$. Выберем вероятность ошибки первого рода α (вероятность того, что для вектора $v \notin L \oplus u^{(0)}$ неравенство в пункте 2 выполнено) и вероятность ошибки второго рода β (вероятность того, что для $v \in L \oplus u^{(0)}$ неравенство в пункте 2 не выполняется). В таком случае не более чем через $2^{n-k} + \alpha \cdot 2^{n-k} \cdot 2^k = 2^{n-k} + \alpha \cdot 2^n$ шагов мы определим истинный ключ с надежностью $1 - \beta$.

6 Об одном классе аппроксимирующих функций

В этом разделе рассмотрен класс аппроксимирующих функций, которые находятся на минимально возможном расстоянии от функции усложнения f. Такие функции g интересны именно тем, что для них параметр $\mathrm{dist}(f, g)$, который участвует в верхней оценке трудоемкости алгоритма $\mathcal{K}$, принимает минимально возможное значение.

Качество аппроксимации функции усложнения f играет важную роль при оценке трудоемкости алгоритма $\mathcal{K}$. Под «качеством» подразумевается не только значение расстояния $\mathrm{dist}(f, g)$, но и порядок алгебраической вырожденности аппроксимирующей функции g (размерность пространства $B(L)$). Далее будет приведен пример фильтрующих генераторов, для которых трудоемкость применения алгоритма $\mathcal{K}$ вообще не зависит от функции усложнения f. Однако, существует широкий класс генераторов, для которых качество аппроксимации выходит на первый план (например, когда преобразование B тождественно).

Нижней границей для расстояния между функцией f и аппроксимирующей функцией g является значение такого параметра, как невырожденность функции f.

Определение 2 (Алексеев [5])**.** *Невырожденностью* булевой функции $f \in \mathcal{F}_n$ называется расстояние $\rho(f) = \mathrm{dist}(f, \mathrm{DG}(n))$.

Параметр $\pi_\rho(f)$ отражает максимально возможное значение порядка алгебраической вырожденности тех функций, которые находятся от f на расстоянии $\rho(f)$ [5]:

$$\pi_\rho(f) = \max_{g \in \mathrm{DG}(n):\ \mathrm{dist}(f,g) = \rho(f)} \mathrm{AD}(g).$$

Таким образом, для функций g, находящихся от f на расстоянии $\rho(f)$, верхней границей для порядка их алгебраической вырожденности служит значение параметра $\pi_\rho(f)$. Соотношение между параметрами $\rho(f)$ и $\pi_\rho(f)$ отражено в следующей теореме.

Теорема 3 (Алексеев [5]). Для любой булевой функции $f \in \mathcal{F}_n$, для которой $\rho(f) > 0$, справедливо соотношение $\log_2 \rho(f) + \pi_\rho(f) \leqslant n$.

Множество функций g, находящихся на расстоянии $\rho(f)$ от функции f, обозначим через $\mathrm{DG}(f) = \{g \in \mathrm{DG}(n) \mid \mathrm{dist}(f, g) = \rho(f)\}$.

Для того, чтобы с помощью аппроксимирующей функции g такой, что $\mathrm{dist}(f, g) = \rho(f)$, нельзя было эффективно применить алгоритм $\mathcal{K}$, необходимо, чтобы значение $\rho(f)$ было велико, а $\pi_\rho(f)$ — мало. Из предыдущей теоремы видно, что при увеличении значения $\rho(f)$ параметр $\pi_\rho(f)$ автоматически будет уменьшаться. Такая ситуация с взаимным поведением криптографических параметров $\rho(f)$ и $\pi_\rho(f)$ отличается от той, которая имеет место, например, для порядка корреляционной-иммунности $\mathrm{cor}(f)$ и алгебраической степени $\deg(f)$ функции f. Для этих параметров также существует неравенство, связывающее их значения: $\mathrm{cor}(f)+\deg(f) \leqslant n$ (неравенство Зигенталера), однако в данном случае с точки зрения стойкости криптографических примитивов необходимо максимизировать оба значения.

В заключении рассмотрим вопрос построения множеств $\{y \in B(L) \oplus v \mid f(y) \neq g(y)\}$ для функции $g \in \mathrm{DG}(f)$ такой, что $B(L) \subseteq J(g)$. В работе [5] показано, что функции f и g отличаются друг от друга на любом смежном классе вида $B(L) \oplus v$ не более чем в одной точке. Таким образом, нужные нам множества состоят не более чем из одного вектора. Вычисление этих множеств можно проводить по следующей схеме. Произведем аффинную замену переменных функции $f \oplus g$ так, чтобы смежный класс $B(L) \oplus v$ перешел в подпространство M, имеющее стандартный базис. Рассмотрим получившуюся после замены переменных функцию h на подпространстве M. Для нее выполнено неравенство $\mathrm{wt}(h) \leqslant 1$. Таким образом, полином функции h будет либо нулевым, либо будет соответствовать функции веса 1. Рассмотрим задачу определения вектора u, для которого $h(u) = 1$, по полиному Жегалкина функции h при условии $\mathrm{wt}(h) = 1$. Для определения тех переменных, значения которых равны 1 для вектора u, построим конъюнкцию всех мономов полинома функции h. Таким образом мы определим те переменные, которые присутствуют в каждом мономе полинома Жегалкина функции h. Эти переменные и определяют все те позиции вектора u, в которых стоят значения 1.

7 Примеры

В данном разделе рассматриваются некоторые примеры фильтрующих генераторов, для которых применимы описанные ранее алгоритмы.

Далее векторы $x \in V_n$ будем представлять в виде $x = (x_{n-1}x_{n-2}\ldots x_1x_0)$.

Пример 1. Линейное преобразование $A\colon V_{16} \to V_{16}$ действует на векторы $x \in V_{16}$ следующим образом: $A(x) = y$, где $y_{15} = x_5 \oplus x_3 \oplus x_2 \oplus x_0$ и $y_i = x_{i+1}$ для всех $i = 0, 1, \ldots, 14$. Регистр сдвига, определенный с помощью преобразования A, имеет максимально возможный период $2^{16} - 1$.

Преобразование B тождественно.

Опишем функцию усложнения $f \in \mathcal{F}_{16}$. Для этого нам понадобятся некоторые вспомогательные множества.

Подпространство P пространства V_{16} имеет базис

(0000000010000000), (0000000001000000), (0000000000100000), (0000000000010000),
(0000000000001000), (0000000000000100), (0000000000000010), (0000000000000001).

Подпространство L пространства V_{16} имеет следующий базис

(1000000001010000), (0100000010000100), (0010000001001111), (0001000010111111),
(0000100011011000), (0000010010100010), (0000001010000001), (0000000110101100).

Множество $M \subset V_{16}$ состоит из четырех векторов:

(0010111100011000), (1101000001101011), (1010111011100100), (0101000110010111).

Векторы множества $S \subset P$ представим в виде десятичных чисел, двоичное представление которых соответствует векторам из P (число 13 соответствует вектору $(0 \dots 01101) \in V_{16}$):

0,	1,	3,	4,	6,	10,	13,	17,
20,	21,	22,	25,	26,	29,	30,	34,
36,	39,	43,	47,	50,	51,	55,	56,
57,	58,	60,	61,	62,	63,	65,	66,
67,	68,	70,	71,	72,	73,	74,	78,
80,	81,	84,	86,	87,	88,	90,	93,
94,	96,	97,	98,	107,	108,	113,	116,
117,	120,	121,	122,	123,	128,	129,	132,
135,	136,	139,	140,	143,	144,	145,	146,
148,	149,	150,	154,	155,	156,	157,	162,
163,	165,	166,	167,	168,	170,	171,	173,
174,	176,	179,	180,	182,	183,	184,	185,
186,	192,	193,	195,	196,	197,	199,	202,
209,	210,	211,	213,	214,	215,	217,	219,
220,	223,	224,	226,	230,	231,	232,	233,
235,	237,	238,	241,	242,	244,	251,	254.

Подпространство L удовлетворяет соотношению $A^t(L) = L$ при $t = \frac{2^{16}-1}{2^8-1} = 257$. Заметим, что прямая сумма $L \oplus P$ подпространств L и P совпадает с V_{16}.

Функция $f \in \mathcal{F}_{16}$ определяется следующим равенством:

$$f = g \oplus h \quad \text{где} \quad g = \bigoplus_{u \in S} I_{L \oplus u} \quad \text{и} \quad h = \bigoplus_{u \in M} I_{P \oplus u}.$$

Справедливы соотношения $\mathrm{wt}(h) = 1024$, $J(g) = L$, причем

$$\mathrm{dist}(f, g) = \mathrm{wt}(h) = 1024 = \min_{g' \colon J(g') = L} \mathrm{dist}(f, g').$$

Функция f является уравновешенной и для нее выполнены следующие соотношения

$$\mathrm{cor}(f) = 1, \quad \mathrm{nl}(f) = 27312, \quad \deg(f) = 7.$$

Оценим трудоемкость применения алгоритма $\mathcal{K}$ для определения ключа фильтрующего генератора $\mathrm{LFSR}(A, f)$. Положим $d = 16$. В таком случае средняя трудоемкость не провосходит $2^{\dim L} + 2^{16-\dim L} + 2^{16-d} + 2^0 \cdot \mathrm{dist}(f, g) = 1537$ шагов. При этом нам потребуется в худшем случае $16 \cdot t = 4112$ бит шифрующей последовательнсоти. Средняя трудоемкость полного перебора для такого фильтрующего генератора равна $2^{15} = 32768$.

Пример 2. Опишем класс фильтрующих генераторов, для которых истинный ключ с помощью алгоритма $\mathcal{K}$ может быть определен за порядка $2^{\frac{n}{2}}$ шагов. Особенностью этого класса является то, что трудоемкость определения ключа не зависит от выбора функции усложнения.

Такая особенность возникает вследствие того, что подпространство L пространства V_n, с помощью которого далее строится аппроксимирующая функция g, оказывается подпространством пространства $\ker B$.

Пусть линейное преобразование $A \colon V_{32} \to V_{32}$ действует на векторы $x \in V_{32}$ следующим образом: $A(x) = y$, где $y_{32} = x_{30} \oplus x_{25} \oplus x_{16} \oplus x_0$ и $y_i = x_{i+1}$ для всех $i = 0, 1, \dots, 30$. Регистр сдвига, определенный с помощью преобразования A, имеет максимально возможный период $2^{32} - 1$.

Преобразование $B\colon V_{32} \to V_8$ определяется следующими соотношениями:

$$
\begin{aligned}
&B(x) = y, \quad \text{где}\\
&y_0 = x_1 \oplus x_6 \oplus x_{12} \oplus x_{26} \oplus x_{31},\\
&y_1 = x_0 \oplus x_7 \oplus x_{19} \oplus x_{22} \oplus x_{27},\\
&y_2 = x_8 \oplus x_{12} \oplus x_{14} \oplus x_{26} \oplus x_{27},\\
&y_3 = x_5 \oplus x_{11} \oplus x_{15} \oplus x_{18} \oplus x_{25},\\
&y_4 = x_{15} \oplus x_{16} \oplus x_{18} \oplus x_{24} \oplus x_{27},\\
&y_5 = x_4 \oplus x_{16} \oplus x_{21} \oplus x_{25} \oplus x_{31},\\
&y_6 = x_0 \oplus x_{14} \oplus x_{15} \oplus x_{17} \oplus x_{20},\\
&y_7 = x_1 \oplus x_{11} \oplus x_{14} \oplus x_{19} \oplus x_{23}.
\end{aligned}
$$

Базис подпространства L пространства V_{32} состоит из следующих 16-ти векторов:

$$
\begin{array}{ll}
(10000000000000100000101010111011), & (01000000000010000000100010101100),\\
(00100000000000000101101011100001), & (00010000000010000001000110001010),\\
(00001000000000001000101101001111), & (00000100000010100000100101101001),\\
(00000010000010100100000110110100), & (00000001000000101000000000101100),\\
(00000000100010100101001010001010), & (00000000010010100100001100000000),\\
(00000000001010100000100000110101), & (00000000000110000101101010100010),\\
(00000000000001101001001101001000), & (00000000000000001100000101011010 1),\\
(00000000000000000010101001101110), & (00000000000000000000010000000000).
\end{array}
$$

При $t = \frac{2^{32}-1}{2^{16}-1}$ справедливы соотношения $A^t(L) = L$ и $B(L) = \{0^8\}$.

Трудоемкость применения алгоритма $\mathcal{K}$ для получения ключа такого фильтрующего генератора не зависит от выбора функции усложнения f, поскольку аппроксимирующая функция g должна удовлетворять условию $B(L) = \{0^8\} \subseteq J(g)$, а этому условию удовлетворяет любая функция из $\mathcal{F}_8$. Поэтому мы можем положить $g = f$ и получить $\operatorname{dist}(f, g) = 0$.

Таким образом, средняя трудоемкость поиска ключа с помощью алгоритма $\mathcal{K}$ не превосходит $2^{16} + 2^{16} + 2^{32-d}$ шагов. Если $d = 16$, то получаем $3 \cdot 2^{16}$, тогда как трудоемкость полного перебора составляет в среднем 2^{31} шагов.

8 Заключение

В работе описаны новые алгоритмы восстановления ключа фильтрующего генератора, основанные на аппроксимации функции усложнения с помощью алгебраически вырожденной функции. В естественных криптографических предположениях расчитаны параметры указанных алгоритмов и предложены некоторые методы оптимизации этих параметров.

Автор выражает глубокую благодарность своему научному руководителю кандидату физико-математических наук Логачеву Олегу Алексеевичу за поддержку и помощь при работе над статьей. Также автор выражает благодарность кандидату физико-математических наук Чиликову Алексею за ценные советы и конструктивную критику.

Работа поддержана Российским фондом фундаментальных исследований (номер проекта 09-01-00653-а).

Список литературы

[1] *Логачев О.А., Сальников А.А., Ященко В.В.* Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004. — 470 с. — ISBN 5-94057-117-4.

[2] *Алексеев Е.К.* О некоторых алгебраических и комбинаторных свойствах корреляционно-иммунных булевых функций // Дискретная математика. — М.: Наука, 2010. — Т. 22, вып. 3. — С. 110.

[3] *Dawson E., Wu C.K.* Construction of Correlation Immune Boolean Functions // Information and Communications Security, LNCS 1334, Y.Han, T.Okamoto, S.Qing (Eds), Springer-Verlag, 1997. — Pp. 170–180.

[4] *Matsui M.* Linear cryptanalysis method for DES cipher // Advances in Cryptology. — EUROCRYPT'93. — Pp. 386–397.

[5] *Алексеев Е.К.* О некоторых мерах нелинейности булевых функций // Прикладная дискретная математика. — 2011. — Т. 2.

[6] *Севастьянов Б.А.* Курс теории вероятностей и математической статистики. — М.: Наука. Главная редакция физико-математической литературы, 1982. — 256 с.

[7] *Siegenthaler T.* Decrypting a Class of Stream Chipher Using Ciphertext Only // IEEE Trans. on Computers C. — 1985. — Vol. 34, no. 1. — Pp. 81–85.

УДК 519.248

ЭРГОДИЧНОСТЬ ВРЕМЕННОГО РЯДА ОБОБЩЕННОГО ПОКАЗАТЕЛЯ ЛИКВИДНОСТИ

© 2011 г. Н. А. Андреев, В. А. Лапшин, В. В. Науменко

nandreev@cs.msu.su, vlapshin@cs.msu.su, vnaumenko@hse.ru

Кафедра системного анализа факультета ВМК МГУ, Лаборатория по финансовой инженерии и риск-менеджменту НИУ ВШЭ

1 Релаксация рынка и эргодичность

Определение оптимальной ликвидационной стоимости портфеля эквивалентно, по сути, выбору оптимальной стратегии ликвидации портфеля при фиксировании ряда параметров, например, количества временных интервалов, в течение которых должна быть закрыта позиция, и уровня несклонности к риску, отражающего предпочтения инвестора относительно агрессивности торговли [3]. Получаемая на выходе модели ликвидации портфеля стратегия представляет собой вектор, выражающий объемы актива, которые должны быть куплены (проданы) в каждый из временных интервалов.

В любой из этих моментов времени при продаже (покупке) определенного объема актива путем выставления соответствующей рыночной заявки цена актива упадет (вырастет) после ее исполнения. При этом, чем больше объем такой заявки, тем сильнее может измениться цена в неблагоприятном для нас направлении. Если продолжать выставлять рыночные заявки на продажу (покупку), то можно ускорить дальнейшее движение цены. Более того, любое движение цены в ту или иную сторону может быть усилено (получить дополнительный импульс) путем исполнения выставленных другими участниками стоп-лоссов. Однако в соответствии с теорией микроструктуры рынка, если возмущение рынка актива вызвано неинформационным шоком (не подкреплено никакой относящейся к активу — релевантной — информацией), то он должен вернуться в нормальное состояние. Данное свойство рынка Альберт Кайл назвал релаксацией рынка [1].

Таким образом, для того чтобы определить длину временных интервалов (расстояние между точками входа в рынок), нужно оценить время релаксации рынка [2]. В настоящей статье представлена попытка подойти к оценке времени релаксации рынка определенного актива через понятие эргодичности — «свойства динамической системы, позволяющей ввести однозначно определенную инвариантную меру» [4]. Данная концепция была введена в 1887 году австрийским физиком Людвигом Больцманом для обоснования статистической физики и термодинамики. Эргодическая гипотеза в статистической физике — предположение, что средние по времени (time-series) значения физических величин, характеризующих систему, равны их средним статистическим (по ансамблю, cross-section) [5].

Аналогия со статистической физикой и термодинамикой, на наш взгляд, вполне уместна не только из соображений, что ее математический аппарат для описания равновесных систем взят на вооружение экономической наукой со времен опубликования Полом Самуэльсоном своего фундаментального труда [6]. Разумно полагать, что рынок отдельного актива можно рассматривать как динамическую систему, состоящую из множества элементов — участников рынка, выставляющих заявки на покупку/продажу (по аналогии с моделью идеального газа в термодинамике). Следовательно, можно попробовать использовать инструментарий, применяемый в статистической физике.

Однако, «в контексте термодинамики и статистической физики, эргодичность обеспечивает возможность обращаться с равновесными ансамблями и определять постоянные по времени усредненные характеристики систем, но не позволяет рассматривать процесс релаксации системы к равновесному состоянию» [4]. В то же время известно, что «свойство перемешивания

Исследование осуществлено в рамках программы фундаментальных исследований ГУ-ВШЭ в 2010 году.

считается принципиальным для статистической физики в плане объяснения релаксации систем к термодинамическому равновесию» [4]. «Перемешивание (в фазовом пространстве) — свойство потока траекторий консервативной динамической системы, достаточное для перехода этой системы в процессе ее временной эволюции к стохастическому поведению» [7].

Релаксация рынка в понимаемом нами смысле — возвращение некоторого процесса к «обычному» состоянию после возникшего шока, причем не обязательно неинформационного. В этом смысле мы несколько отходим от определения Кайла [1], по сути оценивая некоторую условную релаксацию рынка, что связано с трудностями определения характера шоков: информационного или вызванного мотивом ликвидности (в смысле желания продать актив для получения денег).

В рамках данного определения можно показать, что релаксация как свойство случайного процесса может быть формализована в терминах свойства перемешивания, смысл которого в том, что любые два события в процессе являются все более независимыми по мере удаления друг от друга во времени. Таким образом, наблюдается в некотором роде «забывание» процессом своей предыстории, что тесно связано с пониманием релаксации в рамках данного подхода. Время релаксации при этом можно измерять как скорость данного «забывания».

Доказано, что для класса общих стохастических процессов из перемешивания следует эргодичность системы, однако обратное утверждение неверно. «Эргодичность обеспечивает допустимость использования статистических средних лишь в смысле среднего по времени, тогда как при перемешивании это справедливо и асимптотически. Эргодичность (без перемешивания) соответствует регулярному квазипериодическому заполнению фазового пространства траекториями, перемешивание — хаотическому» [7].

Мы предполагаем, что рассматриваемый нами процесс — марковский. Известно, что в классе марковских процессов из перемешивания с экспоненциальной скоростью следует сильная эргодичность (распределение процесса стремится к некоторому инвариантному распределению, то есть не зависящему от начального распределения) при условии, что процесс не «разбалтывается», то есть представляет собой стационарный режим. Более того, в случае марковского процесса справедливо, что сильная эргодичность является достаточным условием для перемешивания. Нет оснований полагать, что стационарного режима у рассматриваемых процессов нет, поэтому утверждение полагается верным.

Так как свойство перемешивания проверяется достаточно тяжело, имеет смысл убедиться в целесообразности развития данного направления исследований, проверив косвенный признак наличия данного свойства. В нашем случае — сильную эргодичность. Отсутствие таковой говорит (в силу утверждения) об отсутствии свойства перемешивания.

Для исследования релаксации рынка — процесса его возврата после шока к нормальному состоянию — мы рассмотрим вопрос о его эргодичности. Если процесс эргодичен, то после экзогенного шока, вызванного, например, большой сделкой, он будет вновь сходиться к стационарному распределению. И характеристики этого стремления к стационарному распределению, такие как скорость сходимости, можно исследовать при помощи математического аппарата эргодической теории. Неэргодичность же может означать, что после шока поведение цен может качественно измениться ввиду перехода траектории процесса в другой эргодический подкласс. В этом случае постановка задачи оценки времени релаксации рынка таким способом невозможна.

Отметим также, что наше предположение об эргодичности процесса, характеризующего ликвидность рынка, не противоречит размышлениям Дугласа Норта о неэргодическом характере экономики [8]. Объяснением служит то, что мы работаем с высокочастотными данными о ходе торговли ценными бумагами, охватывающими периоды от нескольких часов до нескольких дней. Предполагается, что за такое время маловероятны (если и есть, то их можно отследить: внедрение новых информационных систем, правил торговли, условий регулирования рынка и т. д.) резкие институциональные изменения, которые могут привести к переходу системы в другой, качественно новый режим функционирования. При этом с точки зрения математической статистики, данных достаточно для формирования статистических гипотез.

Общепринято считать, что об эргодичности процесса невозможно судить по одной его реализации сколь угодно большой длины (за некоторыми специальными исключениями). Метод, предлагаемый в [9], по сути, подразумевает генерацию множества реализаций траекторий при помощи оценки переходного ядра. Соответственно, вопрос о возможности суждения об эрго-

дичности сводится к вопросу о возможности оценки переходного ядра по одной реализации траектории процесса. Это, в свою очередь, возможно только в том случае, если процесс является эргодическим. В [9] приведены достаточные условия, при которых одна реализация траектории процесса содержит достаточно информации для вывода не только об отсутствии (неудача процедуры оценки переходного ядра или получение неэргодичного переходного ядра, очевидно, свидетельствуют о неэргодичности исходного процесса, в то время, как обратное неверно), но и о наличии эргодичности.

Мы применим их методологию для исследования эргодичности случайного процесса цены акции по отдельным реализациям.

В данной работе приведены результаты исследования эргодичности финансовых рядов на примере динамики одной из характеристик ликвидности на рынке акций ММВБ за один торговый день. В качестве характеристики ликвидности взята Xetra Liquidity Measure (XLM) — средние издержки при покупке и продаже определенного объема актива в один и тот же момент времени. В данном исследовании величина объема устанавливалась, исходя из принципа соответствия средним издержкам за рассматриваемый период времени. Расчеты производились для акций ОАО «Лукойл» за январь 2006 года.

2 Исследование эргодических свойств показателя ликвидности

Можно привести ряд признаков, свидетельствующих об эргодическом поведении процесса на основании одной его траектории. Разумеется, тем самым будет нельзя подтвердить наличие эргодичности. Тем не менее, простой тест, свидетельствующий об отсутствии данного свойства, избавляет от необходимости применения более сложных проверочных методов. Тем самым, в начале исследования имеет смысл проверять признаки эргодичности ряда. В качестве примера было проведено моделирование траектории XLM_t на основе метода, требующего слабой эргодичности процесса*.

1. Пусть $(x_1, x_2, \ldots, x_T)$ — траектория слабо эргодического марковского процесса с дискретным временем. Рассмотрим выборку размера $T-1$, элементами которой являются двумерные векторы вида (x_{i-1}, x_i), $i = 2, 3, \ldots, T$.

2. По построенной выборке методом ядерного оценивания в двумерном случае получаем функцию, которая в силу слабой эргодичности процесса будет являться оценкой переходного ядра процесса.

3. Пользуясь полученной оценкой переходного ядра, последовательно моделируем траекторию, выходящую из точки $\tilde{x}_t$, для моментов $t+1$, $t+2$, ...

На рисунке 1 приведен результат моделирования на период с 12 ч 26 мин 13 с до 12 ч 31 мин 40 с; для сравнения приведена также и реальная траектория за данный период. Смоделированная траектория дает достаточно хорошее приближение истинной примерно на 2 минуты вперед, а также отражает общую динамику на всем периоде прогнозирования. Таким образом, в задаче прогнозирования рассмотренным методом XLM_t может считаться обладающим эргодическими свойствами.

2.1 Базовые понятия и определения

Рассматривается одномерный марковский процесс на $\mathbb{R}$ с переходным ядром $p(x, A)$, где $x \in \mathbb{R}$, $A \in B(\mathbb{R})$, $B(\mathbb{R})$ — борелевская σ-алгебра над $\mathbb{R}$. Исходя из известного распределения $p_0(x, A)$ в начальный момент времени, можно выразить вероятность попадания в любое борелевское множество A в момент времени s как

$$\mathbb{P}(x_s \in A) = \int_A p_0(\xi) p^{(s)}(\xi, d\eta), \tag{1}$$

*Слабая эргодичность процесса (эргодичность в понимании Больцмана) следует из сильной эргодичности, исследуемой в данной работе, и неформально формулируется как поведение, при котором «среднее по времени равно среднему по ансамблю».

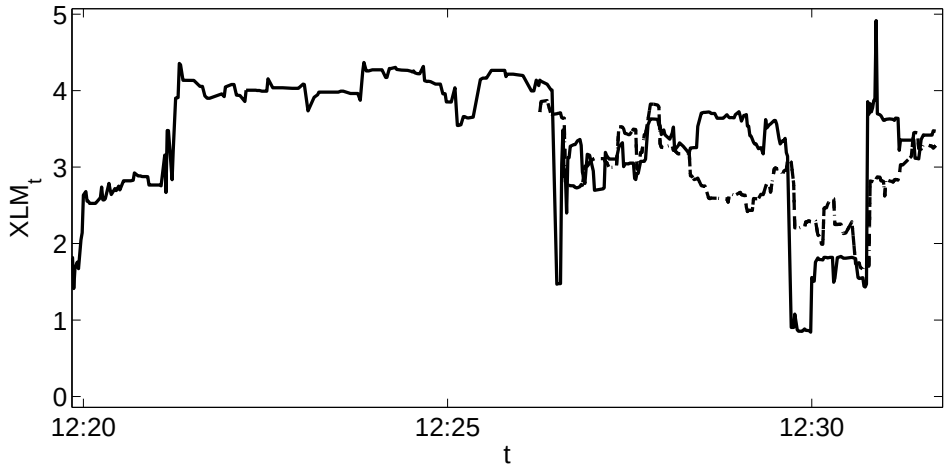


Рис. 1. Часть исходной траектории (сплошная линия) и результат моделирования (пунктирная линия).

где $p^{(s)}(x, A)$ — s-шаговое переходное ядро, определяемое рекурсивно:

$$p^{(s)}(x, A) = \int_{\mathbb{R}} p^{(s-1)}(x, d\eta)p(\eta, A).$$

Таким образом, на пространстве вероятностных плотностей $D(\mathbb{R})$ можно задать оператор $P^s\colon D(\mathbb{R}) \to D(\mathbb{R})$. Процесс называется *эргодическим*, если существует плотность $\pi(\cdot) \in D(\mathbb{R})$ такая, что для любого $x \in \mathbb{R}$ и для любой допустимой плотности $g(\cdot) \in D(\mathbb{R})$ выполнено

$$\lim_{s\to\infty} \frac{1}{s} \sum_{i=0}^{s-1} P^s g(x) = \pi(x) \tag{2}$$

или, в эквивалентной формулировке, если для любого $x \in \mathbb{R}$ и для любых допустимых плотностей $g_1(\cdot), g_2(\cdot) \in D(\mathbb{R})$ верно, что

$$\lim_{s\to\infty} \left| \frac{1}{s} \sum_{i=0}^{s-1} (P^s g_1(x) - P^s g_2(x)) \right| = 0 \tag{3}$$

Дальнейшее исследование основано на применении теста на эргодичность, предложенного в [9]. Используемая методика основана на предположении, что каждый временной ряд может быть представлен как траектория процесса X_t, состоящего из двух компонент:

- систематической, для которой плотность распределения x_{t+1} задается с помощью переходного ядра $p(x_t, \cdot|s_{t+1})$, зависящего от предыдущего значения x_t, а также от значения переменной состояния в текущий момент времени s_{t+1};
- «шума», определяемого плотностью распределения $\nu(\cdot)$.

Предполагается, что случайный процесс $s_t \in \{1, \ldots, n\}$ имеет стационарное распределение, определяющее долю времени нахождения в каждом из состояний, и независим от процесса X_t. Переходное ядро $\tilde{p}(x_t, \cdot|s_{t+1})$ исходного процесса, в рамках модели, может быть записано в виде

$$\tilde{p}(x_t, \cdot|s_{t+1}) = \begin{cases} p(x_t, \cdot|s_{t+1}), & \text{если } \mathrm{shock}_t = 0, \\ p(x_t, \cdot|s_{t+1}) + \alpha\nu, & \text{если } \mathrm{shock}_t = 1. \end{cases} \tag{4}$$

где $\alpha \in (0, 1)$, а shock_t — двоичный процесс, не зависящий от X_t и s_t.

Для обеспечения относительно небольшого воздействия зашумления на систематическую составляющую, накладываются определенные ограничения на интенсивность шоковых состояний:

(A.1) $\sum_{t=0}^{T-1} \mathrm{shock}_t \xrightarrow[T\to\infty]{} \infty$ почти наверное;

(A.2) $\frac{1}{T}\sum_{t=0}^{T-1} \mathrm{shock}_t \xrightarrow[T\to\infty]{} 0$ почти наверное.

На практике переходное ядро $p(x, A)$ неизвестно, но может быть оценено, исходя из наблюдаемой траектории. В данной работе с помощью стандартной процедуры ядерного оценивания была построена оценка переходной плотности $f(x, y)$, а также состоятельная оценка $f(x, A) = \int_A f(x, y)\, dy$ ядра $p(x, A)$. Далее, используя алгоритмы, представленные в [9], была проведена серия попарных сравнений распределений вида $\lim\limits_{s\to\infty} \frac{1}{s}\sum_{i=0}^{s-1} P^s g(x)$ с помощью критерия Колмогорова-Смирнова равенства двух распределений по выборке. При условии, что гипотеза об эргодичности ряда X_t верна, выборка из полученных значений доверительной вероятности (*p-value*) должна соответствовать равномерному распределению на отрезке $[0, 1]$. Отметим также, что при сделанных предположениях верно и обратное утверждение.

2.2 Применение метода тестирования для выявления эргодических свойств процесса

Прежде чем иметь возможность применять вышеизложенную методику к реальным данным (в рассмотренном примере — траектория процесса XLM_t), необходимо убедиться в верности всех предположений модели динамики подлежащего процесса. В то время как большинство из них являются достаточно общими, предположения (A.1) и (A.2) об интенсивности возникновения шоков требуют проверки. Для этого к исходным данным была применена методика выявления шоковых состояний, которая будет подробно изложенная в другой работе (краткое изложение метода см. в разделе 4). На рисунке 2 представлена часть траектории процесса XLM_t, соответствующая 30 минутам из середины торгового дня.

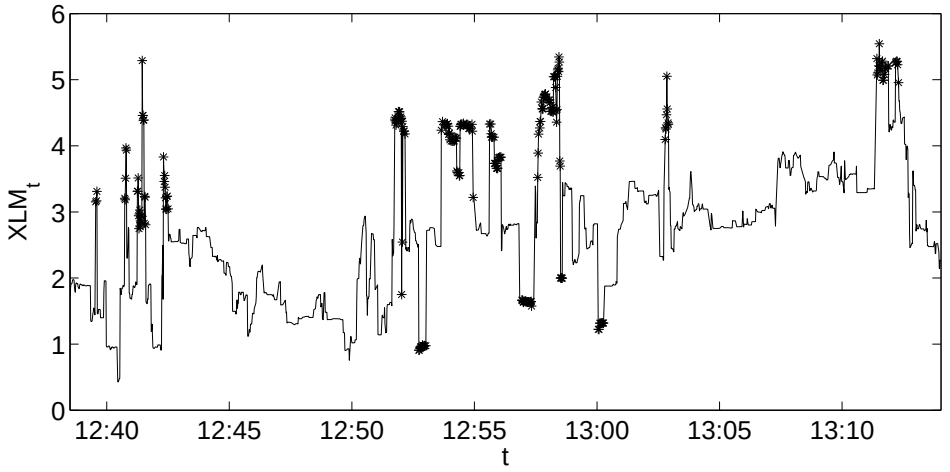


Рис. 2. Часть траектории процесса XLM_t с выделенными моментами шокового состояния.

Результатом является полное восстановление траектории процесса shock_t, на основе которой возможно проверить выполнение свойств (A.1) и, в особенности, (A.2), рассмотрев предельное поведение частичных сумм $S_1(T) = \sum_{t=0}^{T-1} \mathrm{shock}_t$ и $S_2(T) = \frac{1}{T}\sum_{t=0}^{T-1} \mathrm{shock}_t$ на бесконечности. Для рассматриваемого примера графики $S_1(T)$ и $S_2(T)$ приведены на рисунках 3 и 4.

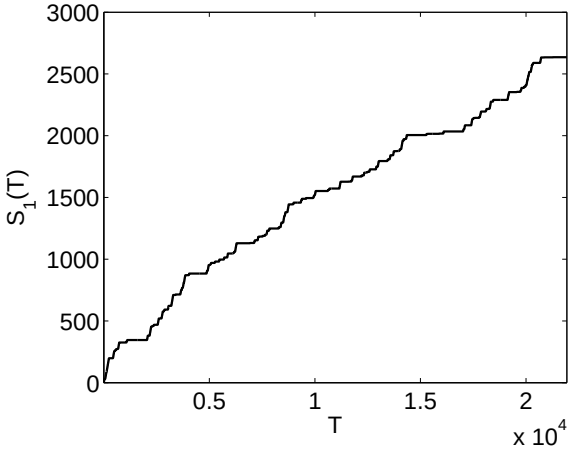
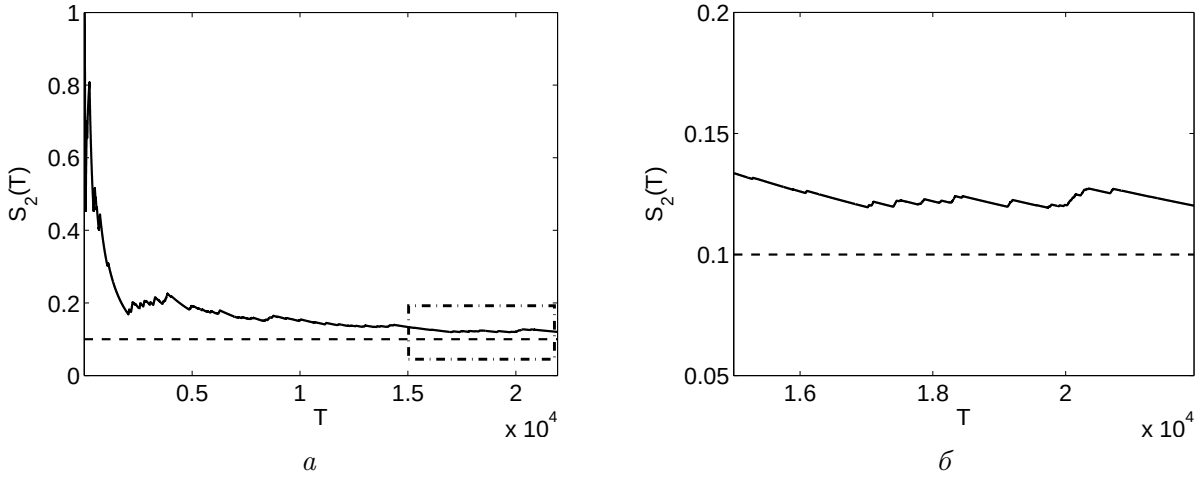


Рис. 3. Поведение частичной суммы $S_1(T)$ на всей области рассмотрения (один торговый день).



а *б*

Рис. 4. Поведение $S_2(T)$ на всей области рассмотрения ($а$) и приближение дальнего конца графика ($б$).

Графики наглядно иллюстрируют выполнение свойства (A.1) и дают основание считать, что (A.2) не выполняется. Хотя на основе реальных данных можно рассмотреть не само значение предела $S_2(T)$, а лишь его приближенное значение на достаточно большом горизонте, есть все основания предполагать, что $\frac{1}{T}\sum_{t=0}^{T-1} \text{shock}_t \xrightarrow[T\to\infty]{} \text{const} \neq 0$, что говорит о том, что возникновение шоковых состояний соответствует пуассоновскому потоку однородных событий, достигая противоречия с (A.2). В таком случае, применив метод тестирования напрямую, нельзя удостовериться в состоятельности полученных результатов.

В качестве решения данной проблемы предлагается использовать полученную информацию о траектории shock_t и при оценивании переходной плотности не использовать данные, соответствующие моментам шока ($\text{shock}_t = 1$). В таком случае задача, по сути, сводится к описанной в [9], где указанный алгоритм был предложен впервые. Подробнее об алгоритме распознавания шоковых состояний процесса рассказано ниже. На рисунке 5 приведена плотность распределения, оцененная по выборке значений доверительной вероятности величиной 10 000.

При условии эргодичности процесса плотность должна соответствовать равномерному распределению на отрезке $[0, 1]$, в противном случае должна наблюдаться большая концентрация элементов выборки в области малых значений, что в некоторой степени можно наблюдать в данном случае. В силу неоднозначности вида оценки плотности более точный анализ можно

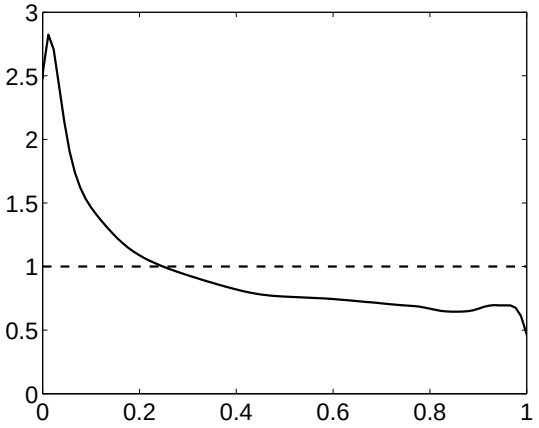


Рис. 5. Плотность распределения вероятностей для величины доверительной вероятности на основе 10 000 экспериментов.

провести на основании частот появления малых значений, приведенных в таблице 1.

Таблица 1. Частота появления малых значений p-value.

Величина значения p-value	**Процент**
Меньше 0,05	18 %
Меньше 0,1	24 %

Подобные результаты были рассмотрены в [9] и были расценены как недостаточные для отвержения гипотезы об эргодичности (процент небольших значений достаточно мал). К сожалению, формального критерия близости полученного эмпирического распределения доверительных вероятностей к равномерному пока не существует из-за слишком большого количества источников погрешностей (конечный размер исходной выборки, приближенная природа оценки переходного ядра, конечный размер набора генерируемых траекторий и т. д.). Тем не менее, можно считать, что рассматриваемый процесс XLM_t по своим свойствам близок к эргодическому, то есть может считаться эргодическим применительно к задаче, не требующей высокой точности вычислений и не зависящей жестко от эргодических свойств процесса.

3 Определение моментов нерегулярного поведения (шоковых состояний) временного ряда

В данном разделе приведен алгоритм для определения моментов «шока» у временного ряда. Под «шоком» понимается отклонение наблюдаемой траектории $Y(t)$ от ее типичного поведения. Предлагаемый подход состоит из трех шагов:

1. определение общего направления динамики временного ряда (тренда);
2. построение характеристической функции на основе исходных данных;
3. выявление участков нерегулярности на основе анализа характеристической функции.

3.1 Определение тренда

Для корректной оценки величины отклонения $Y(t)$ естественно учитывать эффекты, наложенные общей динамикой (рост, осциллирование и т. д.). Для определения функции $f_0(t)$, характеризующей тренд, предлагается метод сглаживания для наблюдений

$$(y_0, y_1, \ldots, y_n) = (Y(t_0), Y(t_1), \ldots, Y(t_n)), \quad t_0 < t_1 < \ldots < t_n \leqslant T.$$

При таком подходе $f_0(t)$ на отрезке $[0,T]$ находится как решение задачи минимизации

$$\sum_{i=0}^{n} \alpha_i \left(f_0(t_i) - Y(t_i)\right)^2 + \varepsilon \int_0^T \left(f_0''(s)\right)^2 ds \to \inf_{f_0 \in W}, \tag{5}$$

где W — класс Соболева функций $f(t)$ таких, что $f(t)$, $f'(t)$ — абсолютно непрерывны на $[0,T]$, а $f''(t) \in L_2[0,T]$. Параметр ε положителен и задается априорно. Большие значения отвечают большей гладкости решения. Веса α_i выбираются по формуле $\alpha_i = \frac{c}{1+\left|X(t_i)-\overline{X}\right|}$, где константа c выбирается, исходя из условия нормировки $\alpha_0 + \alpha_1 + \ldots + \alpha_n = 1$.

3.2 Построение характеристической функции

Определим $f(t,\varepsilon)$ как решение задачи минимизации (5). Обозначим $g(t,\varepsilon) = f(t,\varepsilon) - f_0(t)$. Характеристическая функция временного ряда $Y(t)$ определяется как

$$\psi(t) = \lambda \int_0^{+\infty} e^{-\lambda\varepsilon} g^2(t,\varepsilon)\, d\varepsilon. \tag{6}$$

Полученная функция $\psi(t)$ имеет скачки в те моменты времени, для которых поведение временного ряда отличается от обычного, предсказуемого, что интерпретируется как шоковое состояние. Так как значение имеют только относительная величина скачка $\psi(t)$, то в дальнейшем для облегчения вычислений под $\psi(t)$ подразумевается ее нормированное значение.

3.3 Построение критерия шокового состояния

Пусть $(\psi_0, \psi_1, \ldots, \psi_k) = (\psi(t'_0), \psi(t'_1), \ldots, \psi(t'_k))$, где моменты t'_0, t'_1, $\ldots$, t'_k соответствуют всем неотрицательным значениям $\psi(t)$. Формально применив простой фильтр Калмана к временному ряду $(\psi_0, \psi_1, \ldots, \psi_k)$, считая, что наблюдаются незашумленные значения $(\psi_0, \psi_1, \ldots, \psi_k)$, получаем, что $\psi(t_{k+1}|t_k)$ можно считать нормально распределенной случайной величиной со средним $l(t_k)$ и дисперсией σ^2_ψ. «Среднюю» функцию $l(t)$ можно определить методами из первой части методики для наблюдений $(\psi_0, \psi_1, \ldots, \psi_k)$; в качестве σ^2_ψ логично брать выборочную дисперсию.

Получив оценку $\psi(t_{k+1}|t_k)$, можно для каждого момента времени t'_k определить верхнюю границу доверительного интервала для $\psi(t_{k+1}|t_k)$, уровень доверия при этом должен быть задан априорно. Искомая граница $m(t)$ определяется теперь следующим образом:

1. для моментов t'_0, t'_1, $\ldots$, t'_k величина $m(t)$ совпадает с найденным значением верхней границы доверительного интервала;

2. для остальных моментов времени граница доопределяется с помощью интерполяционных методов (например, линейной интерполяцией).

Критерием шокового состояния является выход $\psi(t)$ за границу стационарности $m(t)$. Формально,

$$\{\tau \text{ — момент шока}\} \qquad \Leftrightarrow \qquad \psi(\tau) > m(\tau). \tag{7}$$

Замечание. Во многих случаях выборочная дисперсия имеет слишком большое значение из-за большой амплитуды скачков $\psi(t)$, что ведет к завышению границы и неадекватным оценкам. Для решения данной проблемы рекомендуется произвести несколько предварительных итераций данного алгоритма, на каждой из которой необходимо исключить из текущего вектора наблюдений $(\psi_0, \psi_1, \ldots, \psi_k)$ те точки, которые на текущей итерации определяются как шоковые. Тем самым точки с большой амплитудой будут исключены и не повлияют на оценку дисперсии и построение границы.

4 Заключение

Мы сформулировали вопрос об эргодичности финансового ряда как неотъемлемую часть исследования процесса релаксации. Для конкретной постановки задачи, связанной с релаксацией после шока, мы описали процедуру, позволяющую проверить гипотезу об эргодичности. Проведенные эксперименты не позволяют отвергнуть гипотезу об эргодичности, следовательно, постановка задачи об исследовании релаксации цен имеет право на существование.

Наблюдаемые результаты позволяют нам считать, что делаемое предположение об эргодичности может не противоречить реальным данным. Что позволяет вести будущие исследования в терминах свойства перемешивания и инвариантной меры, оценивая сходимость процессов, характеризующих ликвидность, к стационарному режиму после шока, вызванного, например, сделкой значительного объема.

Невыполнение предположения об эргодичности, либо в силу отсутствия стационарной меры, либо в силу ее неединственности, влекло бы значительное усложнение модели ввиду необходимости рассмотрения нескольких ее устойчивых состояний (соответствующих подклассам эргодичности), притом шок, вызванный сделкой, мог бы приводить к переходу процесса из одного устойчивого состояния в другое, таким образом, понятие релаксации в нашей его нынешней интерпретации оказалось бы неприменимо к подобного рода модели.

Список литературы

[1] *Kyle A.* Continuous Auctions and Insider Trading // Econometrica. — 1985. — Vol. 53, no. 6. — Pp. 1315–1336.

[2] *Андреев Н.А., Лапшин В.А., Науменко В.В., Смирнов С.Н.* Определение ликвидационной стоимости портфеля акций с учетом особенностей микроструктуры рынка (на примере ММВБ). — 1,4 п.л. — (для публикации в журнале «Управление риском»).

[3] *Костов Т.В., Науменко В.В., Смирнов С.Н.* Измерение риска и управление портфелем в условиях низкой ликвидности // Управление риском. — М.: Изд-во Анкил, 2009. — № 3. — С. 66–71.

[4] *Кузнецов С.П.* Динамический хаос (курс лекций). — М.: Издательство физико-математической литературы, 2001. — 296 с.

[5] Физический энциклопедический словарь. — М.: Советская энциклопедия, 1983.

[6] *Samuelson P.* Foundations of Economic Analysis // Cambridge: Harvard University Press, 1947.

[7] Физическая энциклопедия. В 5-ти томах. — М.: Советская энциклопедия, 1988.

[8] *Норт Д.* Фундамент новой институциональной экономики // Center for International Private Enterprise (CIPE). — `http://developmentinstitute.org/north/north_ru_script.pdf`.

[9] *Domowitz I, El-Gamal M.A.* A consistent nonparametric test of ergodicity for time series with applications // Journal of Econometrics. — 2001. — Vol. 102, no. 2. — Pp. 365–398.

УДК 517.955.8

ОЦЕНКИ ВРЕМЕНИ СУЩЕСТВОВАНИЯ ОБОБЩЕННЫХ РЕШЕНИЙ НАЧАЛЬНО-КРАЕВОЙ ЗАДАЧИ ДЛЯ ОДНОГО НЕЛИНЕЙНОГО УРАВНЕНИЯ СОБОЛЕВСКОГО ТИПА

© 2011 г. А. И. Аристов

ai_aristov@mail.ru

Кафедра общей математики

1 Предварительные рассмотрения

Рассмотрим следующую начально-краевую задачу:

$$\begin{cases} \dfrac{\partial}{\partial t}\left(\Delta u - u\right) + \mu\left(x,t\right)|u|^{\sigma}u + \left(\lambda,\nabla\right)u^2 = 0, \\ u\left(x,0\right) = u_0\left(x\right), \\ u\left(x,t\right)|_{\partial\Omega} = 0. \end{cases} \tag{1}$$

Здесь $u \in \mathbb{R}$ — функция от времени $t > 0$ и вектора пространственных переменных $x \in \Omega$, где Ω — ограниченное подмножество $\mathbb{R}^3$ с границей $\partial\Omega \in C^{(2,\delta)}$, $\delta \in (0,1]$, $\sigma \in (1,2]$, $\lambda = (\lambda_1,\lambda_2,\lambda_3) \in \mathbb{R}^3$, $\mu\left(x,t\right) \in C\left[0;T;L_4\left(\Omega\right)\right)$ (смысл параметра $T > 0$ уточним позже), $u_0\left(x\right) \in H_0^1\left(\Omega\right)$.

Замечание. Условия $\mu\left(x,t\right) \in C\left[0;T;L_4\left(\Omega\right)\right)$ достаточно для доказательства теоремы об однозначной разрешимости задачи и для вывода нижней оценки времени разрушения решения; в теоремах о верхних оценках будут фигурировать более жесткие ограничения на коэффициент $\mu\left(\cdot\right)$.

Уравнения такого вида используются для описания нестационарных процессов в полупроводниках.

Систематическое изучение неклассических уравнений в частных производных, то есть не являющихся уравнениями типа Коши-Ковалевской, началось в середине XX века. Одним из первых трудов, посвященных неклассическим уравнениям, стала работа С. Л. Соболева, опубликованная в 1954 году [1]. В ней было выведено уравнение, описывающее малые колебания во вращающейся жидкости.

В [2] дано систематическое изложение методов функционального анализа, используемых для исследования уравнений в частных производных. Значительное внимание уделено неклассическим уравнениям.

В данной работе получают развитие идеи, использовавшиеся в [3] для изучения уравнения

$$\frac{\partial}{\partial t}\left(\Delta u - u\right) + u\frac{\partial u}{\partial x_1} + u^3 = 0$$

и уравнения Осколкова-Бенджамена-Бона-Махони-Бюргерса (ОББМБ):

$$\frac{\partial}{\partial t}\left(\Delta u - u\right) + \Delta u + u\frac{\partial u}{\partial x_1} + u^3 = 0.$$

В [3] были рассмотрены начально-краевые задачи для названных уравнений, исследована их глобальная и локальная по времени разрешимость, для случая локальной разрешимости найдены в виде явных формул двусторонние оценки времени разрушения решения.

В [4] была исследована глобальная и локальная разрешимость начально-краевой задачи для уравнения вида

$$\frac{\partial}{\partial t}\left(\Delta u - u\right) + a\left(\Delta u - u\right) + F\left(u\right) = 0,$$

где $a > 0$, а в качестве $F\left(u\right)$ были рассмотрены нелинейности с постоянными коэффициентами вида $\mu u^3 + \left(\lambda, \nabla\right) u^2$ и $\mu \left|u\right|^\sigma u$.

В [5] была рассмотрена аналогичная задача для уравнения

$$\frac{\partial}{\partial t}\left(\Delta u - u\right) + b\Delta u - au + \mu\left(x\right)\left|u\right|^\sigma u + \left(\lambda, \nabla\right) u^2 = 0. \tag{2}$$

При этом условия теоремы о нижней оценке времени разрушения при нетривиальных начальных данных допускали только строго положительные коэффициенты a и b. В теореме о верхней оценке фигурировало условие $b - a < 2 - 4/\sigma$, из которого следовало, что $b < a$, поскольку $1 < \sigma \leqslant 2$.

Данная работа дополняет исследование уравнения (2): здесь взяты коэффициенты $a = b = 0$, кроме того, введен в рассмотрение коэффициент $\mu\left(\cdot\right)$ более общего вида. Введено определение обобщенного решения задачи (1), исследована однозначная обобщенная разрешимость глобально и локально по времени, найдены верхние и нижние оценки времени существования решения в виде явных и квадратурных формул. Показано, что в случае зависимости μ от t решение может существовать глобально по времени не только при тривиальных $\mu\left(\cdot\right)$.

Введем классы $X_T = C^1\left[0; T; H_0^1\left(\Omega\right)\right)$, $0 < T \leqslant \infty$.

Определение 1. Обобщенным решением задачи (1) будем называть такое $u \in X_T$, что

$$\begin{cases} \int\limits_\Omega \left(\dfrac{\partial}{\partial t}\left(\Delta u - u\right) + \mu\left(x, t\right)\left|u\right|^\sigma u + \left(\lambda, \nabla\right) u^2\right) w\, dx = 0, \\ u\big|_{t=0} = u_0 \end{cases} \tag{3}$$

для любой функции $w \in H_0^1\left(\Omega\right)$ и для любого $t \in [0, T)$.

Определение 2. Говорят, что обобщенное решение задачи (1) разрушается за конечное время, если эта задача имеет решение $u \in X_T$ при некотором конечном $T > 0$, но не имеет решения из класса X_∞. В частности, говорят, что решение разрушается путем опрокидывания, если $\lim\limits_{t \to T-} \|u\|_{H_0^1(\Omega)} = \infty$.

Введем необходимые обозначения:

$$\begin{array}{lll} L_p = L_p\left(\Omega\right), \quad 1 \leqslant p \leqslant \infty, & H_0^1 = H_0^1\left(\Omega\right), & H^{-1} = H^{-1}\left(\Omega\right), \\ \|\cdot\| = \|\cdot\|_{L_2}, & \|\cdot\|_{+1} = \|\cdot\|_{H_0^1}, & \|\cdot\|_{-1} = \|\cdot\|_{H^{-1}}, \\ \Phi = \|u\|^2 + \|\nabla u\|^2. & & \end{array}$$

Штрихом будем обозначать производную по времени. Положим $W = \|u'\|^2 + \|\nabla u'\|^2$. Под нижним индексом «0» будем подразумевать, что выражение рассматривается при $t = 0$ (если не будет оговорено противное). C_p — оптимальная константа вложения H_0^1 в L_p (если существует), то есть

$$C_p = \inf\{C \mid \|w\|_{L_p} \leqslant C\|w\|_{H_0^1}\ \forall w \in H_0^1\}.$$

Через C будем обозначать положительные постоянные, возможно, различные.

Полагая в (3) $w = u$ и $w = u'$, после интегрирования по частям получим соответственно первое и второе энергетические тождества:

$$\begin{array}{ll} \text{I.} & \dfrac{\Phi'}{2} = \displaystyle\int\limits_\Omega \mu\left|u\right|^{\sigma+2}\, dx; \\ \text{II.} & W = \displaystyle\int\limits_\Omega \mu\left|u\right|^\sigma uu'\, dx + \int\limits_\Omega u'\left(\lambda, \nabla\right) u^2\, dx. \end{array} \tag{4}$$

Эти тождества будут использоваться для вывода оценок для параметра T.

Заметим, что Φ_0' можно однозначно выразить через начальные данные с помощью первого энергетического равенства. Очевидно, и Φ_0 однозначно определяется начальными данными. Поэтому в дальнейшем будем считать величины Φ_0 и Φ_0' данными.

2 Существование и единственность

Теорема 1. Пусть $\mu(\cdot) \in C[0;\ T;\ L_4)$. Тогда для любой функции $u_0(\cdot) \in H_0^1$ найдется $T > 0$ (возможно, $T = \infty$), для которого существует единственное обобщенное решение задачи (1). При этом если $T < \infty$, то $\lim\limits_{t \to T-} \|u\|_{H_0^1(\Omega)} = \infty$, то есть имеет место опрокидывание решения.

Доказательство аналогично доказательству соответствующего утверждения для уравнения Осколкова-Бенджамена-Бона-Махони-Бюргерса в [3]. Изложим его схематично.

Доказательство. Введем следующие операторы: $F_0 u = u - \Delta u$, $F_1 u = \mu(x,t)\,|u|^\sigma u$, $F_2 u = (\lambda, \nabla)\, u^2$. Заметим, что оператор $F_0 \colon H_0^1 \to H^{-1}$ имеет липшиц-непрерывный обратный. Поэтому в обобщенном смысле задача сводится к следующему уравнению:

$$u = Hu \equiv u_0 + \int\limits_0^t F_0^{-1}\left(F_1 u + F_2 u\right)\, d\tau \tag{5}$$

С помощью неравенства Гельдера и теоремы вложения H_0^1 в L_p можно доказать, что при $v_{1,2} \in H_0^1$

$$\|F_1 v_1 - F_1 v_2\|_{-1} \leqslant C\,\|\mu\|_{L_4} \max^\sigma\left(\|v_1\|_{+1}, \|v_2\|_{+1}\right) \|v_1 - v_2\|_{+1}.$$

Кроме того, заметим, что

$$\|F_2 v_1 - F_2 v_2\|_{-1} \leqslant C \max\left(\|v_1\|_{+1}, \|v_2\|_{+1}\right) \|v_1 - v_2\|_{+1}.$$

Рассмотрим шар $B_R = \left\{u \in L_\infty\left[0;T;H_0^1\right) \mid \|u\|_T \equiv \left\|\|u\|_{+1}\right\|_{L_\infty[0;T)} \leqslant R\right\}$.

Докажем, что оператор H переводит этот шар в себя. Пусть $u \in B_R$. В силу найденных оценок

$$\|Hu\|_T \leqslant \|u_0\|_{+1} + C \int\limits_0^T \|\mu\|_{L_4}\, d\tau \cdot R^{\sigma+1} + CTR^2$$

Пусть R достаточно велико, то есть $\|u_0\|_{+1} \leqslant R/2$. Пусть T достаточно мало, то есть

$$R^\sigma \int\limits_0^T \|\mu\|_{L_4}\, d\tau + RT \leqslant (2C)^{-1}.$$

Следовательно, и $Hu \in B_R$. Аналогично можно доказать, что оператор H является сжимающим. Таким образом, существует единственное решение уравнения (5) из класса $L_\infty\left[0;T;H_0^1\right)$.

Как и в [3], применим стандартный алгоритм продолжения решений интегральных уравнений с переменным верхним пределом. Получим, что существует некоторое максимальное $T \in (0;\infty]$, причем если T конечно, то $\lim\limits_{t \to T-} \|u\|_{+1} = \infty$.

Заметим, что в силу сглаживающих свойств оператора H интегральное уравнение однозначно разрешимо не только в классе $L_\infty\left[0;T;H_0^1\right)$, но и в $C^1\left[0;T;H_0^1\right)$. □

В дальнейшем будем рассматривать обобщенные решения задачи (1), соответствующие нетривиальным начальным данным.

3 Оценки времени существования решения

Лемма 1. Если $\nu(x) \in L_4,\ w(x) \in H_0^1$, то

$$\left| \int\limits_\Omega \nu |w|^{\sigma+2}\, dx \right| \leqslant C_4 C_{2\sigma+2}^{\sigma+1} \|\nu\|_{L_4} \left(\|w\|^2 + \|\nabla w\|^2 \right)^{\sigma/2+1}$$

Доказательство. Действительно,

$$\begin{aligned} \left| \int\limits_\Omega \nu |w|^{\sigma+2}\, dx \right| &\leqslant \sqrt{\int\limits_\Omega \nu^2 w^2\, dx \int\limits_\Omega |w|^{2\sigma+2}\, dx} \leqslant \\ &\leqslant \sqrt[4]{\int\limits_\Omega \nu^4\, dx \int\limits_\Omega w^4\, dx}\, \|w\|_{L_{2\sigma+2}}^{\sigma+1} = \|\nu\|_{L_4} \|w\|_{L_4} \|w\|_{L_{2\sigma+2}}^{\sigma+1} \leqslant \\ &\leqslant \|\nu\|_{L_4} \cdot C_4 \|\nabla w\|_{L_2} \cdot C_{2\sigma+2}^{\sigma+1} \|\nabla w\|_{L_2}^{\sigma+1} \leqslant \\ &\leqslant C_4 C_{2\sigma+2}^{\sigma+1} \|\nu\|_{L_4} \left(\|w\|^2 + \|\nabla w\|^2 \right)^{\sigma/2+1}. \end{aligned}$$

□

Лемма 2. $\Phi'^2/4 \leqslant \Phi W$.

Доказательство. Обозначим $y_k = \partial u/\partial x_k$, $k \in \{1,2,3\}$. С одной стороны, с помощью неравенств Коши-Буняковского-Шварца можно убедиться, что

$$\left(\|u\| \cdot \|u'\| + \sum_{k=1}^{3} \|y_k\| \cdot \|y_k'\| \right)^2 \leqslant \left(\|u\|^2 + \sum_{k=1}^{3} \|y_k\|^2 \right) \left(\|u'\|^2 + \sum_{k=1}^{3} \|y_k'\|^2 \right) = \Phi W.$$

С другой стороны,

$$\left(\|u\| \cdot \|u'\| + \sum_{k=1}^{3} \|y_k\| \cdot \|y_k'\| \right)^2 \geqslant \left(\int\limits_\Omega uu'\, dx + \sum_{k=1}^{3} \int\limits_\Omega y_k y_k'\, dx \right)^2 = \left(\frac{\Phi'}{2} \right)^2.$$

Следовательно, $(\Phi'/2)^2 \leqslant \Phi W$. □

Лемма 3. Пусть $0 < \gamma < 1$. Тогда $b = \gamma^{-\gamma}(1-\gamma)^{\gamma-1}$ — наибольшее значение константы b, при котором $v^\gamma \geqslant bv/(v+1)$ для любого $v \geqslant 0$.

Доказательство. Рассмотрим функцию $f(v) = k(v+1) - v^\beta$, где $\beta \in (0,1)$. Несложно убедиться, что $k = \beta^\beta (1-\beta)^{1-\beta}$ — оптимальная константа в неравенстве $f(v) \geqslant 0$. Положим $\beta = 1-\gamma$, где $\gamma \in (0,1)$. Тогда неравенство можно привести к виду

$$v^\gamma \geqslant \frac{1}{\gamma^\gamma (1-\gamma)^{1-\gamma}} \cdot \frac{v}{v+1}.$$

□

Теорема 2. Пусть $\mu(x,t) \in C[0;T;L_4)$. Положим

$$J = \frac{\Phi_0^{-\sigma/2}}{C_4 C_{2\sigma+2}^{\sigma+1} \sigma}$$

1. Если
$$\int_0^t \|\mu\|_{L_4}\, d\tau < J$$
при всех конечных t, то решение существует глобально по времени, то есть $T = \infty$.

2. Пусть уравнение
$$\int_0^t \|\mu\|_{L_4}\, d\tau = J$$
имеет корень $t = T_1 > 0$ (если положительных корней более одного, то T_1 — наименьший из них). Тогда для параметра T имеет место оценка $T \geqslant T_1$, то есть обобщенное решение задачи (1) гарантированно существует в классе $X_{T_1} \equiv C^1\left[0; T_1; H_0^1\right)$.

   В частности, если μ зависит только от x, то T_1 имеет явное выражение:
$$T_1 = \frac{J}{\|\mu\|_{L_4}}. \tag{6}$$

Доказательство. Рассмотрим первое энергетическое тождество. Оценим его правую часть с помощью леммы 1:
$$\frac{\Phi'}{2} = \int_\Omega \mu\,|u|^{\sigma+2}\, dx \leqslant C_4 C_{2\sigma+2}^{\sigma+1}\,\|\mu\|_{L_4}\,\Phi^{\sigma/2+1}.$$

Положим $g(t) = C_4 C_{2\sigma+2}^{\sigma+1}\,\|\mu\|_{L_4}\,\sigma$, $y = \Phi^{-\sigma/2}$, откуда $\Phi^{-\sigma/2-1}\Phi' = -2y'/\sigma$. Тогда неравенство легко привести к следующему виду:
$$y' + g(t) \geqslant 0.$$

Проинтегрируем неравенство от 0 до t:
$$y - y_0 + \int_0^t g(\tau)\, d\tau \geqslant 0.$$

Возвращаясь к первоначальным обозначениям, получим:
$$0 < \Phi \leqslant \left(\Phi_0^{-\sigma/2} - C_4 C_{2\sigma+2}^{\sigma+1}\sigma \int_0^t \|\mu\|_{L_4}\, d\tau\right)^{-2/\sigma}.$$

Из этой оценки видно, что решение гарантированно существует в окрестности нуля, границей которой является наименьшее значение t, при котором выражение в скобках обращается в нуль, то есть наименьший положительный корень уравнения
$$C_4 C_{2\sigma+2}^{\sigma+1}\sigma \int_0^t \|\mu\|_{L_4}\, d\tau = \Phi_0^{-\sigma/2} \tag{7}$$
(если оно разрешимо). Возможна ситуация, когда величина $\Phi_0^{-\sigma/2}$ настолько велика, что левая часть уравнения не достигает этого значения ни при каких конечных t. Тогда решение существует глобально по времени.

Если дополнительно предположить, что μ зависит только от x, то T_1 легко выразить из (7) явно. В этом случае придем к формуле (6). □

Для того чтобы оценить сверху время разрушения решения, наложим более жесткие требования на параметры, входящие в задачу (1).

Теорема 3. Пусть $\mu(x,t) \in C^1[0;T;L_4)$, $\lambda = (0,0,0)$.

Пусть уравнение

$$C_4 C_{2\sigma+2}^{\sigma+1}\sigma \int_0^t \int_0^\tau \|\mu'\|_{L_4}\, d\xi\, d\tau - \frac{\sigma}{2}\Phi_0^{-\sigma/2-1}\Phi_0' t + \Phi_0^{-\sigma/2} = 0 \tag{8}$$

имеет хотя бы один положительный корень $t = T_2$ (если положительных корней более одного, то T_2 — наименьший из них). Тогда решение задачи (1) разрушается за конечное время $T \leqslant T_2$.

В частности, если μ зависит только от x, то T_2 имеет явное выражение:

$$T_2 = \frac{2\Phi_0}{\sigma \Phi'_0}. \tag{9}$$

Замечание. Достаточным условием разрешимости уравнения (8), менее жестким, чем зависимость μ только от x, является, например, сходимость интеграла

$$\int_0^\infty \int_0^\tau \|\mu'\|_{L_4}\, d\xi\, d\tau.$$

Действительно, пусть этот интеграл равен положительной постоянной M. Тогда, обозначая левую часть уравнения через $F(t)$, а свободный член и множитель при t соответственно через A и B, получим:

$$A - Bt \leqslant F(t) \leqslant A - Bt + C_4 C_{2\sigma+2}^{\sigma+1}\sigma M$$

Из этой оценки видно, что при положительных A и B функция $F(t)$ положительна в некоторой окрестности нуля и равна нулю при $t = T_2 \in [A/B, \left(A + C_4 C_{2\sigma+2}^{\sigma+1}\sigma M\right)/B]$. В данном случае явной верхней оценкой для T, более грубой, чем T_2, может служить величина $\left(A + C_4 C_{2\sigma+2}^{\sigma+1}\sigma M\right)/B$.

Перейдем к доказательству теоремы.

Доказательство. Из первого энергетического равенства следует, что

$$\frac{\Phi''}{2} = \int_\Omega \mu' |u|^{\sigma+2}\, dx + (\sigma+2)\int_\Omega \mu |u|^\sigma u u'\, dx.$$

Поэтому второе энергетическое равенство можно переписать в следующем виде:

$$W = \frac{\Phi''}{2(\sigma+2)} - \frac{1}{\sigma+2}\int_\Omega \mu' |u|^{\sigma+2}\, dx.$$

Воспользуемся неравенством леммы 2:

$$\frac{\Phi'^2}{4} \leqslant \Phi W = \frac{\Phi\Phi''}{2(\sigma+2)} - \frac{\Phi}{\sigma+2}\int_\Omega \mu' |u|^{\sigma+2}\, dx.$$

Продолжим оценку с помощью леммы 1:

$$\frac{\Phi'^2}{4} \leqslant \frac{\Phi\Phi''}{2(\sigma+2)} + \frac{\Phi}{\sigma+2}\cdot C_4 C_{2\sigma+2}^{\sigma+1}\|\mu'\|_{L_4}\Phi^{\sigma/2+1},$$

откуда

$$\Phi\Phi'' - \left(1 + \frac{\sigma}{2}\right)\Phi'^2 + 2C_4C_{2\sigma+2}^{\sigma+1}\left\|\mu'\right\|_{L_4}\Phi^{\sigma/2+2} \geqslant 0.$$

Положим $\Phi = z^{-2/\sigma}$. После упрощений получим:

$$z'' \leqslant C_4C_{2\sigma+2}^{\sigma+1}\sigma\left\|\mu'\right\|_{L_4}.$$

Дважды проинтегрируем это неравенство от 0 до t:

$$z - z_0 - z_0't \leqslant C_4C_{2\sigma+2}^{\sigma+1}\sigma\int\limits_0^t\int\limits_0^\tau\left\|\mu'\right\|_{L_4}d\xi\,d\tau.$$

Вернемся к первоначальным обозначениям:

$$\Phi \geqslant \left(C_4C_{2\sigma+2}^{\sigma+1}\sigma\int\limits_0^t\int\limits_0^\tau\left\|\mu'\right\|_{L_4}d\xi\,d\tau - \frac{\sigma}{2}\Phi_0^{-\sigma/2-1}\Phi'_0t + \Phi_0^{-\sigma/2}\right)^{-2/\sigma}.$$

Φ'_0 можно выразить из первого энергетического равенства, а значит, эта величина однозначно определяется начальными данными. Таким образом, T_2 — наименьший положительный корень уравнения

$$C_4C_{2\sigma+2}^{\sigma+1}\sigma\int\limits_0^t\int\limits_0^\tau\left\|\mu'\right\|_{L_4}d\xi\,d\tau - \frac{\sigma}{2}\Phi_0^{-\sigma/2-1}\Phi'_0t + \Phi_0^{-\sigma/2} = 0. \tag{10}$$

Если дополнительно предположить, что μ зависит только от x, то T_2 легко выразить из (10) явно. В этом случае придем к формуле (9). □

Дополним список используемых обозначений. Пусть ε – некоторое фиксированное число. Формально положим

$$\Lambda = \frac{\max\limits_{1\leqslant k\leqslant 3}|\lambda_k|}{2},\quad \alpha = \frac{\sigma}{2} - \Lambda\varepsilon\left(\frac{\sigma}{2}+1\right),\quad \gamma = 2 - \frac{1}{\alpha},$$
$$b = \gamma^{-\gamma}(1-\gamma)^{\gamma-1},\quad A = \frac{6C_4^4\Lambda(\sigma+2)\alpha}{\varepsilon}.$$

Пусть, кроме того, $z = \Phi^{-\alpha}$, откуда $z' = -\alpha\Phi^{-\alpha-1}\Phi'$. Так как Φ_0 и Φ'_0 однозначно определяются начальными данными, то и величины z_0 и z'_0 при фиксированном α можно считать известными. Обозначим

$$B = \frac{\gamma}{2A}z'^2_0 - z_0^\gamma,\quad q = \frac{B}{B+b}.$$

Введем функцию

$$F(z) = \frac{1}{\sqrt{B+b}}\cdot\left(\sqrt{(z+q)(z+1)} + \operatorname{arch}\frac{2z+1+q}{1-q}\right).$$

Теорема 4. Пусть μ зависит только от x, причем $\mu(x) \in L_4$, $\mu > 0$ почти всюду на Ω, $\lambda \neq (0,0,0)$. Пусть

$$12C_4^4\Lambda^2(\sigma+2)^2\Phi_0^3 < (\sigma-1)\Phi'^2_0. \tag{11}$$

Положим

$$\varepsilon = \frac{\sigma}{2(\Lambda(\sigma+2))} - \sqrt{\frac{\sigma^2-2\sigma+2}{4\Lambda^2(\sigma+2)^2} - \frac{6C_4^4\Phi_0^3}{\Phi'^2_0}}.$$

Тогда решение задачи (1) разрушается за конечное время $T \leqslant T_3$, где

$$T_3 = \sqrt{\frac{\gamma}{2A}} \cdot \left(F\left(z_0\right) - F\left(0\right)\right).$$

Доказательство. Из первого энергетического равенства следует, что

$$\frac{\Phi''}{2\left(\sigma+2\right)} = \int\limits_\Omega \mu \left|u\right|^\sigma uu'\, dx.$$

С учетом этого соотношения преобразуем второе энергетическое равенство:

$$W = \frac{\Phi''}{2\left(\sigma+2\right)} + \int\limits_\Omega u'\left(\lambda, \nabla\right) u^2\, dx.$$

Оценим второе слагаемое в правой части:

$$\left|\int\limits_\Omega u'\left(\lambda,\nabla\right)u^2 dx\right| = \left|\int\limits_\Omega u^2\left(\lambda,\nabla\right)u'\, dx\right| \leqslant \max_{1\leqslant k\leqslant 3}\left|\lambda_k\right| \sum_{k=1}^{3}\left|\int\limits_\Omega u^2 \frac{\partial}{\partial x_k}u'\, dx\right| \leqslant$$

$$\leqslant \max_{1\leqslant k\leqslant 3}\left|\lambda_k\right| \cdot \frac{1}{2}\sum_{k=1}^{3}\left(\frac{1}{\varepsilon}\int\limits_\Omega u^4\, dx + \varepsilon\int\limits_\Omega\left(\frac{\partial}{\partial x_k}u'\right)^2 dx\right),$$

где $\varepsilon > 0$. Так как

$$\int\limits_\Omega u^4\, dx = \left\|u\right\|_{L_4}^4 \leqslant C_4^4 \left\|\nabla u\right\|^4 \leqslant C_4^4 \Phi^2$$

и

$$\sum_{k=1}^{3}\int\limits_\Omega\left(\frac{\partial u'}{\partial x_k}\right)^2 dx = \left\|\nabla u'\right\|^2 \leqslant W,$$

то

$$\left|\int\limits_\Omega u'\left(\lambda,\ \nabla\right)u^2\, dx\right| \leqslant \frac{\max\limits_{1\leqslant k\leqslant 3}\left|\lambda_k\right|}{2} \cdot \left(\frac{3C_4^4}{\varepsilon}\cdot\Phi^2 + \varepsilon W\right).$$

Следовательно,

$$W\left(1-\Lambda\varepsilon\right) \leqslant \frac{\Phi''}{2\left(\sigma+2\right)} + \frac{3C_4^4\Lambda}{\varepsilon}\cdot\Phi^2,$$

где $\Lambda = \max\limits_{1\leqslant k\leqslant 3}\left|\lambda_k\right|/2$. Пусть множитель при W положителен, то есть $0 < \varepsilon < 1/\Lambda$. Тогда из этой оценки и леммы 2 следует, что

$$\Phi'^2/4 \leqslant \frac{\Phi}{1-\Lambda\varepsilon}\cdot\left(\frac{\Phi''}{2\left(\sigma+2\right)} + \frac{3C_4^4\Lambda}{\varepsilon}\cdot\Phi^2\right),$$

откуда

$$\Phi\Phi'' - \left(1+\alpha\right)\Phi'^2 + \frac{6C_4^4\Lambda\left(\sigma+2\right)}{\varepsilon}\cdot\Phi^3 \geqslant 0,$$

где $\alpha = \left(1-\Lambda\varepsilon\right)\sigma/2 - \Lambda\varepsilon$. Пусть $\alpha > 0$. Положим $\Phi = z^{-1/\alpha}$. Тогда неравенство можно привести к следующему виду:

$$-\frac{1}{\alpha}z^{-2/\alpha-1}z'' + \frac{6C_4^4\Lambda\left(\sigma+2\right)}{\varepsilon}\cdot z^{-3/\alpha} \geqslant 0.$$

Таким образом,

$$z'' \leqslant Az^{-\beta},$$

где $A = 6C_4^4\Lambda(\sigma+2)\alpha/\varepsilon$, $\beta = 1/\alpha - 1$. Из первого энергетического равенства следует, что $\Phi' > 0$ для любого t, а значит, $z' = -\alpha\Phi^{-\alpha-1}\Phi' < 0$ для любого t. Умножим левую и правую части неравенства на $z' < 0$:

$$z'z'' \geqslant Az^{-\beta}z'.$$

Проинтегрируем неравенство от 0 до t. Будем при этом предполагать, что $\beta < 1$:

$$\frac{z'^2}{2} - \frac{z_0'^2}{2} \geqslant \frac{Az^{1-\beta}}{1-\beta} - \frac{Az_0^{1-\beta}}{1-\beta}.$$

Положим $B = (2A)^{-1}(1-\beta)z_0'^2 - z_0^{1-\beta}$ и потребуем выполнения условия $B > 0$. Таким образом, получим:

$$|z'| \geqslant \sqrt{\frac{2A}{1-\beta}} \cdot \sqrt{z^{1-\beta} + B}.$$

Так как $|z'| = -z'$, то неравенство равносильно следующему:

$$\frac{z'}{\sqrt{z^\gamma + B}} + \sqrt{\frac{2A}{\gamma}} \leqslant 0, \tag{12}$$

где $\gamma = 1 - \beta$. Из леммы 3 следует, что

$$\frac{1}{\sqrt{z^\gamma + B}} \geqslant \frac{1}{\sqrt{bz/(z+1) + B}}.$$

Учитывая знак z', получим следствие из (12):

$$\frac{z'}{\sqrt{bz/(z+1) + B}} + \sqrt{\frac{2A}{1-\beta}} \leqslant 0.$$

Рассмотрим это неравенство в общем виде:

$$\frac{dF}{dz} \cdot \frac{dz}{dt} + \rho \leqslant 0, \tag{13}$$

где $\rho = \sqrt{2A/\gamma}$, $F(z)$ — первообразная для функции, являющейся множителем при z', причем $dF/dz > 0$ для любого z, а значит, $F(z)$ — возрастающая функция. Пусть $\gamma > 0$.

Проинтегрируем (13) от 0 до t:

$$F(z(t)) - F(z(0)) + \rho t \leqslant 0. \tag{14}$$

Так как функция $F(z)$ возрастает на множестве $[0, \infty)$, то неравенство (14) можно равносильным переходом преобразовать с помощью функции, обратной к $F(\cdot)$:

$$z \leqslant F^{-1}(F(z_0) - \rho t) \quad \Leftrightarrow \quad \Phi \geqslant \left[F^{-1}(F(z_0) - \rho t)\right]^{-1/\alpha}.$$

Выражение в квадратных скобках положительно в некоторой окрестности нуля и равно нулю, если t удовлетворяет уравнению

$$F^{-1}(F(z_0) - \rho t) = 0 \quad \Leftrightarrow \quad F(z_0) - \rho t = F(0),$$

откуда

$$T_3 = \frac{1}{\rho}(F(z_0) - F(0)). \tag{15}$$

Значит, Φ оценивается снизу функцией, конечной при $t < T_3$ и бесконечной при $t = T_3$. Следовательно, T_3 может служить верхней оценкой для T.

Таким образом, задача построения верхней оценки для T сводится к отысканию функции $F(z)$. Найдем ее с точностью до постоянной интегрирования:

$$F(z) = \int \frac{dz}{\sqrt{bz/(z+1)+B}} = \frac{1}{\sqrt{B+b}} \int \sqrt{\frac{z+1}{z+q}}\, dz,$$

где $q = B/(B+b) < 1$. Воспользуемся заменой переменной:

$$z = \frac{1-q}{2} \cdot \operatorname{ch}\varphi - \frac{1+q}{2},$$

откуда $dz = \frac{1-q}{2} \cdot \operatorname{sh}\varphi\, d\varphi$. Заметим, что множеству $\{z\} = (0,\infty)$ соответствует множество $\{\varphi\} = \left(\operatorname{arch}\frac{1+q}{1-q}, \infty\right) \subset (0,\infty)$. Значит,

$$\begin{aligned} F(z) &= \frac{1}{\sqrt{B+b}} \int \sqrt{\frac{z+1}{z+q}}\, dz = \frac{1-q}{2\sqrt{B+b}} \int \sqrt{\frac{\operatorname{ch}\varphi+1}{\operatorname{ch}\varphi-1}} \operatorname{sh}\varphi\, d\varphi = \\ &= \frac{1-q}{2\sqrt{B+b}} \int \operatorname{cth}\frac{\varphi}{2} \cdot 2\operatorname{sh}\frac{\varphi}{2} \operatorname{ch}\frac{\varphi}{2}\, d\varphi = \frac{1-q}{2\sqrt{B+b}} \int 2\operatorname{ch}^2\frac{\varphi}{2}\, d\varphi = \\ &= \frac{1-q}{2\sqrt{B+b}} \int (\operatorname{ch}\varphi + 1)\, d\varphi = \frac{1-q}{2\sqrt{B+b}} (\operatorname{sh}\varphi + \varphi). \end{aligned}$$

Так как

$$\begin{aligned} \operatorname{sh}\varphi &= \sqrt{(\operatorname{ch}\varphi - 1)(\operatorname{ch}\varphi + 1)} = \\ &= \sqrt{\left(\frac{2z+1+q}{1-q} - 1\right)\left(\frac{2z+1+q}{1-q} + 1\right)} = \frac{2\sqrt{(z+q)(z+1)}}{1-q}, \end{aligned}$$

то

$$F(z) = \frac{1}{\sqrt{B+b}} \left(\sqrt{(z+q)(z+1)} + \operatorname{arch}\frac{2z+1+q}{1-q}\right).$$

В формулу (15) неявно входит параметр ε, который может принимать произвольные значения из некоторого множества: при выведении данной формулы на ε и параметры, зависящие от него, были наложены следующие ограничения:

$$\begin{cases} \varepsilon > 0, \\ 1 - \Lambda\varepsilon > 0, \\ \alpha > 0, \\ \beta > 0, \\ B > 0, \\ \gamma > 0, \end{cases}$$

то есть

$$\begin{cases} \varepsilon > 0, \\ \varepsilon < \Lambda^{-1}, \\ \varepsilon < \Lambda^{-1} \cdot \dfrac{\sigma}{\sigma+2}, \\ \alpha \equiv \dfrac{\sigma}{2} - \Lambda\varepsilon\left(\dfrac{\sigma}{2}+1\right) < 1, \\ M(\varepsilon) \equiv \dfrac{\alpha^2(1-\beta)}{2A} > \dfrac{\Phi_0^3}{\Phi_0'^2}, \\ \varepsilon < \Lambda^{-1} \cdot \dfrac{\sigma-1}{\sigma+2}. \end{cases} \tag{16}$$

Четвертое неравенство следует из того, что $\varepsilon > 0$ и $1 < \sigma \leqslant 2$. Первое, второе, третье и шестое — дают условие

$$\varepsilon \in E \equiv \left(0, \Lambda^{-1} \cdot \frac{\sigma - 1}{\sigma + 2}\right).$$

В пятом неравенстве правая часть зависит от начальных данных, но не зависит от ε, и может быть, вообще говоря, сколь угодно большой. Значит, нужно выбрать такое значение ε из промежутка E, при котором величина $M(\varepsilon)$ достаточно велика, чтобы пятое неравенство было непротиворечиво (если это возможно).

Выражая M через ε, получим:

$$M(\varepsilon) = \frac{1}{12C_4^4}\left(\frac{\sigma}{\Lambda(\sigma+2)} \cdot \varepsilon - \varepsilon^2\right).$$

Легко убедиться, что на промежутке E функция $M(\varepsilon)$ возрастает, причем

$$\sup_{\varepsilon} M(\varepsilon) = M|_{\varepsilon=(\sigma-1)/(\Lambda(\sigma+2))} = \frac{\sigma - 1}{12C_4^4\Lambda^2(\sigma+2)^2}.$$

Обозначим $M_0 = \sup\limits_{\varepsilon} M(\varepsilon)$, $D_0 = \Phi_0^3 {\Phi'_0}^{-2}$. Значит, если $M_0 \leqslant D_0$, система (16) противоречива для любого ε. Если же $M_0 > D_0$, то решениями системы будут такие ε, что $D_0 < M(\varepsilon) < M_0$. Пусть для определенности $M(\varepsilon) = (D_0 + M_0)/2$. Так как промежутку E соответствует меньший корень этого квадратного относительно ε уравнения, то

$$\varepsilon = \frac{\sigma}{2(\Lambda(\sigma+2))} - \sqrt{\frac{\sigma^2 - 2\sigma + 2}{4\Lambda^2(\sigma+2)^2} - \frac{6C_4^4\Phi_0^3}{{\Phi'_0}^2}}.$$

Несложно убедиться, что из условия (11) следует неотрицательность подкоренного выражения. Таким образом, формула (15) однозначно определяет верхнюю оценку для T. □

4 Заключение

В работе исследована начально-краевая задача для одного нелинейного уравнения соболевского типа. Результаты сформулированы в четырех теоремах. Первая утверждает, что при любых начальных данных из пространства H_0^1 задача однозначно разрешима, по крайней мере, локально по времени, а именно, решение находится в пространстве $C^1\left[0; T; H_0^1\right)$, где T — некоторое положительное число или бесконечность. При этом если величина T конечна, то норма решения в H_0^1 стремится к бесконечности при стремлении времени к T (решение «опрокидывается»). Основная цель работы состоит в том, чтобы найти верхние и нижние оценки для T.

Требуемые оценки дают теоремы 2, 3 и 4.

Теорема 2 дает достаточные условия для того, чтобы параметр T был бесконечным, а также достаточные условия для выполнения оценки вида $T \geqslant T_1 > 0$. При этом во втором случае не исключается случай $T = \infty$.

Теоремы 3 и 4 дают верхние оценки для величины T вида $T \leqslant T_2$ и $T \leqslant T_3$ при разных условиях, налагаемых на параметры задачи. Таким образом, если выполняются условия теоремы 3 или 4, то величина T заведомо конечна.

Выражения для T_1 и T_2 найдены в виде квадратурных формул; указаны частные случаи, когда T_1 и T_2 можно выразить явно. Для T_3 найдена явная формула.

Список литературы

[1] *Соболев С.Л.* Об одной новой задаче математической физики // Изв. АН СССР. Сер. мат. — 1954. — № 18. — С. 3–50.

[2] *Свешников А.Г., Альшин А.Б., Корпусов М.О.* Нелинейный функциональный анализ и его приложения к уравнениям в частных производных. — М.: Научный мир, 2008.

[3] *Свешников А.Г., Альшин А.Б., Корпусов М.О., Плетнер Ю.Д.* Линейные и нелинейные уравнения соболевского типа. — М.: Физматлит, 2007.

[4] *Аристов А.И.* Исследование качественных свойств решений одного нелинейного соболевского уравнения // Сборник статей молодых ученых факультета ВМК МГУ. — М.: Макс-Пресс. — С. 11–22.

[5] *Аристов А.И.* Оценки времени существования решений начально-краевой задачи для одного нелинейного соболевского уравнения // Научная конференция «Тихоновские чтения» (сборник тезисов). — М.: Макс-Пресс, 2010. — С. 27–28.

[6] *Янпольский А.Р.* Гиперболические функции. — М.: Физматгиз, 1960.

[7] *Зайцев В.Ф., Полянин А.Д.* Справочник по нелинейным дифференциальным уравнениям. — М.: Физико-математическая литература, 1993.

[8] *Беккенбах Э., Беллман Р.* Неравенства. — М.: УРСС, 2007.

[9] *Фихтенгольц Г. М.* Курс дифференциального и интегрального исчисления (том 2). — М.: Физматлит, 2003.

УДК 519.6

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ТРАНСПОРТНЫХ ПОТОКОВ НА КОЛЬЦЕВОЙ АВТОСТРАДЕ

© 2011 г. Е. Г. Дорогуш

dorogush@gmail.com

Кафедра системного анализа

1 Введение

С увеличением числа автомобилей на дорогах и невозможностью столь же быстро строить новые дороги задачи управления транспортными потоками становятся все более важными.

Прежде чем заниматься задачами управления и оптимизации, необходимо выбрать модель. Принято выделять два подхода к моделированию транспортных потоков: микроскопический, учитывающий каждый автомобиль, и макроскопический, оперирующий усредненными характеристиками, такими как поток и концентрация.

В работе изучается макроскопическая модель кольцевой автострады, являющаяся дискретизацией (фактически, схемой Годунова) гидродинамической модели, состоящей из закона сохранения, выраженного уравнением в частных производных, и предположения о существовании функциональной зависимости между потоком (числом автомобилей, пересекающих заданную воображаемую линию поперек дороги в единицу времени) и плотностью (числом автомобилей на участке дороги единичной длины). В гидродинамике считается, что зависимость эта описывается выпуклой функцией, в моделировании транспортных потоков — вогнутой, поэтому возмущение (например, локальное увеличение плотности — или затор) в жидкости распространяется со скоростью, большей скорости потока, а в транспортном потоке, напротив, с меньшей скоростью, то есть в направлении, противоположном движению.

2 Модель автомагистрали

В работах [1, 2] предложена гидродинамическая модель автомагистрали, согласно которой поток q и концентрация k связаны, во-первых, законом сохранения

$$\frac{\partial k(t,x)}{\partial t} + \frac{\partial q(t,x)}{\partial x} = 0,$$

и, во-вторых, некоторым определяемым эмпирически соотношением

$$q = q(k,t,x).$$

График зависимости потока от концентрации при фиксированных t и x называется *фундаментальной диаграммой*. Примерный вид фундаментальной диаграммы для автомагистрали показан на рисунке 1.

С увеличением концентрации поток увеличивается при небольших значениях k (свободный участок дороги) и уменьшается при больших значениях k (загруженный участок) вплоть до значения $k^{\max}$, при котором участок настолько загружен, что скорость движения автомобилей практически нулевая.

Мы будем изучать дискретизацию этой модели, CTM (the Cell Transmission Model), предложенную в статье [3].

Дорога разделена на N участков, на каждом из которых есть въезд и съезд. Через $n_i(t)$ обозначаем число автомобилей на i-м участке в момент времени $t \in \mathbb{Z}$, через $f_i(t)$ обозначаем

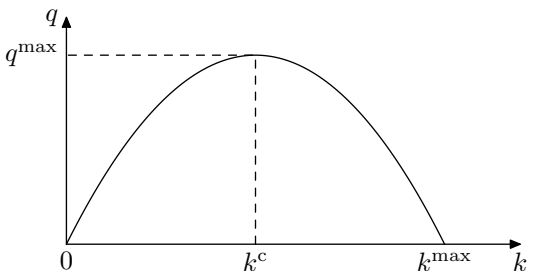


Рис. 1. Фундаментальная диаграмма в гидродинамической модели.

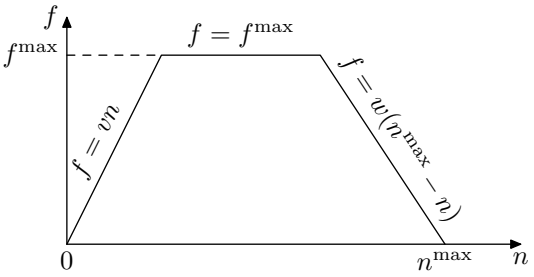


Рис. 2. Фундаментальная диаграмма в модели СТМ.

число автомобилей, переместившихся с i-го на $(i+1)$-й участок, $r_i(t)$, $s_i(t)$ — число автомобилей, въехавших на участок автомагистрали и съехавших с него соответственно. Изменение величины $n_i(t)$ подчиняется закону

$$n_i(t+1) = n_i(t) - f_i(t) + f_{i-1}(t) + r_i(t) - s_i(t). \tag{1}$$

Каждый участок характеризуется следующими параметрами.

$n_i^{\max}$	максимально возможное число автомобилей,
$f_i^{\max}$	максимальный поток,
$v_i \in (0,1)$	скорость свободного движения автомобиля на участке,
$w_i \in (0,1)$	скорость волны разрежения.

Предполагаем, что число автомобилей, съезжающих с участка дороги, пропорционально числу автомобилей, перемещающихся на следующий участок:

$$\frac{s_i(t)}{f_i(t)} = \frac{\beta_i^s}{\beta_i^f} = \text{const}, \qquad \beta_i^s + \beta_i^f = 1. \tag{2}$$

Значение $\beta_i^s = 0$ соответствует участку без съезда, $r_i(t) \equiv 0$ может означать участок без въезда.

Фундаментальная диаграмма имеет форму трапеции (рисунок 2), что в дискретной модели соответствует следующему соотношению:

$$f_i(t) = \min\left\{\beta_i^f v_i n_i(t),\ f_i^{\max},\ w_{i+1}\left(n_{i+1}^{\max} - n_{i+1}(t)\right)\right\}. \tag{3}$$

Будем изучать модель кольцевой дороги, поэтому равенства (1), (3) должны выполняться для всех участков ($i = 1, 2, \ldots, N$), при этом участок $N+1$ отождествляется с первым, а нулевой — с последним, N-м. Предполагается, что есть по крайней мере один съезд с дороги, то есть существует i, такое что $\beta_i^f < 1$ и $\beta_i^s > 0$.

Также будем учитывать очередь. Пусть задан запрос $d(t) \in \mathbb{R}^N$ — число автомобилей, подъезжающих ко въездам на интервале времени от $t-1$ до t. Длина очереди $q(t) \in \mathbb{R}^N$ изменяется по закону $q(t+1) = q(t) + d(t) - r(t)$. Начальную длину очереди считаем заданной. Входящий поток $r_i(t) = \min\{q_i(t) + d_i(t),\ n_i^{\max} - (n_i(t) + f_{i-1}(t) - f_i(t) - s_i(t))\}$. Пусть длина очереди не ограничена.

Далее будем придерживаться следующих обозначений. Для $x, y \in \mathbb{R}^N$

$$\begin{array}{lcl} x \leqslant y \text{ или } y \geqslant x & \Leftrightarrow & x_i \leqslant y_i \text{ для всех } i = 1, \ldots, N, \\ x < y \text{ или } y > x & \Leftrightarrow & x \leqslant y,\ x \neq y, \\ x \ll y \text{ или } y \gg x & \Leftrightarrow & x_i < y_i \text{ для всех } i = 1, \ldots, N. \end{array}$$

3 Положения равновесия системы

Позицией системы является тройка $\{t, n, q\}$.

Пусть запрос постоянный: $d(t) = d$. Тогда система стационарна и имеет смысл говорить о ее положениях равновесия.

В состоянии равновесия постоянны концентрации $n_i(t) = n_i$ и потоки $f_i(t) = f_i$, длина очереди не меняется ($q_i(t) = q_i$), значит, входящий поток равен запросу ($r_i(t) = r_i = d_i$). Из уравнения (1) следует, что числа f_i являются решением системы уравнений

$$-f_i + f_{i-1} + r_i - s_i = 0. \tag{4}$$

Поскольку

$$s_i = \frac{\beta_i^s}{\beta_i^f} f_i, \qquad \beta_i^s + \beta_i^f = 1,$$

то вектор f является решением системы линейных уравнений

$$Kf = r, \tag{5}$$

где

$$K = \begin{pmatrix} 1/\beta_1^f & 0 & 0 & \cdots & 0 & -1 \\ -1 & 1/\beta_2^f & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1/\beta_3^f & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1/\beta_{N-1}^f & 0 \\ 0 & 0 & 0 & \cdots & -1 & 1/\beta_N^f \end{pmatrix}.$$

Определитель матрицы K положителен в силу предположения о наличии съезда:

$$\det K = \prod_{i=1}^{N} \frac{1}{\beta_i^f} - 1 > 0,$$

следовательно, решение системы (5) существует и единственно.

Матрица $P = \{p_{ij}\}_{i,j=1}^N$, обратная к K, выглядит следующим образом:

$$p_{ii} = \frac{1}{\det K} \prod_{j \neq i} \frac{1}{\beta_j^f} > 0,$$

$$p_{i-s,i} = \frac{1}{\det K} \prod_{t=1}^{s-1} \frac{1}{\beta_{i-t}^f} > 0, \qquad s = 1, \ldots N-1.$$

Значит, все компоненты решения системы (5) неотрицательны ($K^{-1}r \geqslant 0$), если $r \geqslant 0$, и положительны ($K^{-1}r \gg 0$), если $r > 0$.

Будем называть входящий поток r *допустимым*, если для порожденного им вектора потока $f = f(r) = K^{-1}r$ выполнено неравенство $f \leqslant f^{\max}$.

Состояние автомагистрали n является *состоянием равновесия*, соответствующим входящему потоку r и порожденному им потоку $f(r) = K^{-1}r$, если вектор n является решением системы уравнений

$$f_i = \min\left\{\beta_i^f v_i n_i,\ f_i^{\max},\ w_{i+1}\left(n_{i+1}^{\max} - n_{i+1}\right)\right\}, \quad i = 1, \ldots, N. \tag{6}$$

Ясно, что если r не является допустимым, то у системы (6) решений нет.

Для любого i выполнены неравенства

$$\beta_i^f v_i n_i \geqslant f_i, \qquad w_i \left(n_i^{\max} - n_i\right) \geqslant f_{i-1},$$

следовательно, $\underline{n_i}(f) \leqslant n_i \leqslant \overline{n_i}(f)$, где

$$\underline{n_i}(f) = \frac{f_i}{\beta_i^f v_i}, \qquad \overline{n_i}(f) = n_i^{\max} - \frac{f_{i-1}}{w_i}.$$

Участок i в момент t является *незагруженным* (*свободным*), если $n_i(t) \leqslant \underline{n_i}(f^{\max})$, то есть

$$\beta_i^f v_i n_i(t) \leqslant f_i^{\max}. \tag{7}$$

Дорога называется незагруженной в момент t, если все ее участки в момент t не загружены.

В силу трапециевидной формы фундаментальной диаграммы естественным будет следующее предположение: если i-й участок в момент t не загружен, то выполнено неравенство

$$w_i \left(n_i^{\max} - n_i(t)\right) \geqslant f_{i-1}^{\max}, \tag{8}$$

или, что равносильно,

$$\frac{f_i^{\max}}{\beta_i^f v_i} \leqslant n_i^{\max} - \frac{f_{i-1}^{\max}}{w_i}. \tag{9}$$

Тогда для $f \leqslant f^{\max}$ справедливы неравенства

$$\underline{n_i}(f) \leqslant \underline{n_i}(f^{\max}) \overset{(9)}{\leqslant} \overline{n_i}(f^{\max}) \leqslant \overline{n_i}(f).$$

Утверждение 1. Допустимому входящему потоку r соответствует единственное положение равновесия $n^u(r)$, при котором дорога является незагруженной.

Доказательство. Поскольку вся дорога незагруженная, то выполнены неравенства

$$\beta_i^f v_i n_i \overset{(7)}{\leqslant} f_i^{\max} \overset{(8)}{\leqslant} w_{i+1} \left(n_{i+1}^{\max} - n_{i+1}\right).$$

Значит,

$$f_i = \min \left\{ \beta_i^f v_i n_i,\, f_i^{\max},\, w_{i+1} \left(n_{i+1}^{\max} - n_{i+1}\right) \right\} = \beta_i^f v_i n_i,$$

откуда

$$n_i^u = \frac{f_i}{\beta_i^f v_i} = \underline{n_i}(f).$$

Неравенство $n^u \leqslant \underline{n}(f^{\max})$ справедливо в силу допустимости входящего потока r ($f \leqslant f^{\max}$), значит, положение равновесия n^u соответствует незагруженной магистрали. □

3.1 Строго допустимый входящий поток

Назовем входящий поток r *строго допустимым*, если $f(r) = K^{-1} r \ll f^{\max}$.

Предположим, в некотором состоянии равновесия n участок i загружен, участок $i+1$ не загружен. Тогда

$$f_i^{\max} \overset{(8)}{\leqslant} w_{i+1} \left(n_{i+1}^{\max} - n_{i+1}\right).$$

Кроме того, $\beta_i^f v_i n_i > f_i^{\max}$ в силу определения загруженного участка. Значит, $f_i = f_i^{\max}$. Справедливо следующее утверждение.

Утверждение 2. Если входящий поток r строго допустим, то в состоянии равновесия n либо все участки незагружены, либо все загружены.

Доказательство. Если в положении равновесия есть как загруженные, так и незагруженные участки, то найдется номер i такой, что i-й участок загружен, $(i+1)$-й не загружен. Только что было показано, что в этом случае $f_i = f_i^{\max}$, чего быть не может, поскольку входящий поток строго допустим, то есть для всех i выполнено неравенство $f_i < f_i^{\max}$. □

Пусть $f_i < f_i^{\max}$ и i-й участок загружен. Тогда наименьшей из трех величин, определяющих поток f_i

$$f_i = \min\left\{\beta_i^f v_i n_i,\ f_i^{\max},\ w_{i+1}\left(n_{i+1}^{\max} - n_{i+1}\right)\right\},$$

является не первая в силу загруженности i-го участка, и не вторая в силу строгого неравенства $f_i < f_i^{\max}$. Следовательно,

$$f_i = w_{i+1}\left(n_{i+1}^{\max} - n_{i+1}\right) < f_i^{\max}. \tag{10}$$

Если бы $(i+1)$-й участок не был загружен, выполнялось бы, по предположению (8), обратное неравенство. Значит, участок $i+1$ загружен. По индукции можно доказать следующее утверждение.

Утверждение 3. Пусть $f_j < f_j^{\max}$, $j = i, \ldots, i+s$ и i-й участок загружен. Тогда участки $i+1$, $\ldots$, $i+s+1$ также загружены.

Выражение (10) дает возможность вычислять положение равновесия, соответствующее загруженной дороге.

Утверждение 4. Строго допустимому входящему потоку r соответствует единственное положение равновесия $n^c(r)$, при котором дорога загружена.

Доказательство. Из равенства в (10) следует, что

$$n_i^c = n_i^{\max} - \frac{f_{i-1}}{w_i} = \overline{n_i}(f).$$

Единственность доказана.

Так определенное положение равновесия соответствует загруженной магистрали, поскольку $f \ll f^{\max}$ в силу строгой допустимости входящего потока r и

$$\overline{n}(f) \gg \overline{n}(f^{\max}) \overset{(9)}{\geqslant} \underline{n}(f^{\max}).$$

Существование доказано. □

Итак, если входящий поток r строго допустим, то есть если $f = K^{-1}r \ll f^{\max}$, существует два состояния равновесия: $n^u = \underline{n}(f)$, в котором все участки незагружены, и $n^c = \overline{n}(f)$, в котором все участки загружены.

3.2 Общий случай

Пусть входящий поток r является допустимым, но не строго допустимым. Обозначим $I = \{i\colon f_i(r) = f_i^{\max}\} = \{i_1, \ldots, i_M\}$. Если r не строго допустимый, то $I \neq \varnothing$.

Рассмотрим группу участков $i-s$, $\ldots$, i, где $i-s$, $\ldots$, $i-1 \notin I$, $i \in I$. В соответствии с утверждением 3, если участок $i-\sigma$, $\sigma \in \{0, \ldots, s\}$ загружен, то следующие за ним участки $i-\sigma+1, \ldots, i$ загружены также. Значит, либо все участки рассматриваемой группы свободны, либо, начиная с некоторого номера, загружены.

Разберем все возможные случаи.

1. $i \notin I$, $f_i < f_i^{\max}$.

   (a) Участки i и $i+1$ свободны ($n_i \leqslant \underline{n_i}(f^{\max})$, $n_{i+1} \leqslant \underline{n_{i+1}}(f^{\max})$).

   В этом случае $f_i = \beta_i^f v_i n_i$, и потому

$$n_i = \frac{f_i}{\beta_i^f v_i} = \underline{n_i}(f).$$

(b) Участок i загружен ($n_i > \underline{n_i}(f^{\max})$).
$f_i = w_{i+1}(n_{i+1}^{\max} - n_{i+1})$, значит, $n_{i+1} = \overline{n_{i+1}}(f) > \underline{n_{i+1}}(f^{\max})$, то есть участок $i+1$ также загружен.

(c) Участок i свободен, $i+1$ загружен.
$f_i = \min\left\{\beta_i^f v_i n_i,\ w_{i+1}(n_{i+1}^{\max} - n_{i+1})\right\}$.

- $n_i = \underline{n_i}(f)$, $\underline{n_{i+1}}(f^{\max}) < n_{i+1} \leqslant \overline{n_{i+1}}(f)$, либо
- $\underline{n_i}(f) \leqslant n_i \leqslant \underline{n_i}(f^{\max})$, $n_{i+1} = \overline{n_{i+1}}(f)$.

2. $i \in I$, $f_i = f_i^{\max}$.
$n_i \geqslant \underline{n_i}(f) = \underline{n_i}(f)$, $n_{i+1} \leqslant \overline{n_{i+1}}(f) = \overline{n_{i+1}}(f^{\max})$.

Отметим, что участки с индексами в множестве I разбивают дорогу на M частей, описание множества состояний равновесия в каждой из которых может быть проведено независимо. Каждая часть состоит из участка с индексом в I и всех предшествующих ему участков с индексами не в I, если таковые есть. Множество состояний равновесия в каждой такой части представляет собою набор отрезков, параллельных координатным осям.

Ясно, что «естественные» ограничения на значения n, $\underline{n_i}(f) \leqslant n_i \leqslant \overline{n_i}(f)$, ограничивают множество всех состояний равновесия и, кроме того, задают наибольшее и наименьшее значение равновесного n: $n^u = \underline{n}(f)$, при котором вся дорога свободна и $n^c = \overline{n}(f)$, при котором вся дорога загружена.

Суммируем сказанное в следующем утверждении.

Утверждение 5. Допустимый входящий поток r порождает единственный вектор потока $f = K^{-1}r$. Все положения равновесия n заключены между векторами $n^u = \underline{n}(f)$ и $n^c = \overline{n}(f)$. Векторы n^u и n^c являются положениями равновесия, в первом все ячейки свободны, во втором все ячейки загружены.

1. Если входящий поток r строго допустим, других положений равновесия, кроме n^u и n^c, нет.

2. Если входящий поток r не является строго допустимым, множество положений равновесия представимо в виде декартова произведения множеств положений равновесия участков дороги, определенных следующим образом. Положим
$$I = \{i_1, \ldots, i_M\} = \{i\colon f_i = f_i^{\max}\}.$$
Пусть индексы i_m отсортированы по возрастанию. Разобьем множество индексов на M подмножеств
$$S_m = \{i_{m-1}+1, i_{m-1}+2, \ldots, i_m\}.$$
Эти подмножества и есть части дороги, положения равновесия на которых описываются независимо. Далее следует описание множества положений равновесия на S_m.

(a) Если $|S_m| = 1$, это означает, что $i_{m-1} = i_m - 1$. Множество положений равновесия есть отрезок
$$\underline{n_{i_m}}(f^{\max}) = \underline{n_{i_m}}(f) \leqslant n_{i_m} \leqslant \overline{n_{i_m}}(f) = \overline{n_{i_m}}(f^{\max}).$$

(b) Положение равновесия, в котором участки $i_{m-1}+1, \ldots, i$ свободны, участки $i+1, \ldots, i_m$ загружены (в том числе $i = i_m$ — все участки свободны, $i = i_{m-1}$ — все участки загружены).
$$\begin{gathered} n_q = \underline{n_i}(f), \quad i_{m-1}+1 \leqslant q \leqslant i-1, \\ n_q = \overline{n_i}(f), \quad i+2 \leqslant q \leqslant i_m, \\ \left[\begin{array}{ll} n_i = \underline{n_i}(f), & \underline{n_{i+1}}(f^{\max}) < n_{i+1} \leqslant \overline{n_{i+1}}(f), \\ \underline{n_i}(f) \leqslant n_i \leqslant \underline{n_i}(f^{\max}), & n_{i+1} = \overline{n_{i+1}}(f). \end{array}\right. \end{gathered}$$
Множество это представляет собою ломаную, сегменты которой параллельны координатным осям, соединяющую точки $(n_{i_{m-1}+1}^u, \ldots, n_{i_m}^u)$ и $(n_{i_{m-1}+1}^c, \ldots, n_{i_m}^c)$.

3.3 Полностью загруженная автомагистраль

Будем считать положением равновесия те состояния системы, в которых только значение вектора концентраций не меняется: $n(t) = n$. Тогда значение вектора потоков и вектора входящих потоков тоже не меняются: $f(t) = f$, $r(t) = r$.

Поскольку $r_i = \min\{q_i(t) + d_i,\, n_i^{\max} - (n_i + f_{i-1} - f_i - s_i)\}$, и случай, когда все $r_i = q_i(t) + d_i$ мы уже рассмотрели, осталось рассмотреть случай, когда по крайней мере для одного i выполнено равенство $r_i = n_i^{\max} - (n_i + f_{i-1} - f_i - s_i)$. При этом

$$n_i = n_i(t+1) = n_i + r_i + f_{i-1} - f_i - s_i = n_i^{\max}.$$

Значит, $n_i = n_i^{\max}$, $f_{i-1} = 0$, $s_{i-1} = 0$. Но тогда

$$0 = f_{i-2} + r_{i-1} - f_{i-1} - s_{i-1} = f_{i-2} + r_{i-1} \geqslant 0.$$

Значит, $f_{i-2} = 0$, $r_{i-1} = 0$ и $s_{i-2} = 0$. Из того, что $f_{i-2} = s_{i-2} = 0$ найдем, что $f_{i-3} = 0$, $s_{i-3} = 0$ и $r_{i-2} = 0$ и так далее. Получим, что $r = 0$, $f = 0$. Далее, поскольку $n_i = n_i^{\max} > 0$, но $f_i = 0$, то $n_{i+1} = n_{i+1}^{\max}$. Так рассуждая, придем к тому, что $n = n^{\max}$, то есть дорога *полностью загружена.* Кроме того, в состоянии равновесия, соответствующем не полностью загруженной дороге, $r_i = q_i + d_i$, значит, $q_i = q_i + d_i - r_i = 0$, то есть очередь не образуется.

Таким образом, состояниям дороги с постоянным вектором концентраций соответствуют все описанные ранее положения равновесия и состояние полной загруженности ($n = n^{\max}$). Наличие положения равновесия, соответствующего полностью загруженной дороге, отличает кольцевую автостраду от незамкнутой автомагистрали.

Далее под положением равновесия понимаем такое состояние автомагистрали, в котором сохраняется число автомобилей в каждой из ячеек (n_i), и не обязательно сохраняется длина очереди (q_i).

4 Траектории системы и устойчивость положений равновесия

Пусть запрос d постоянен. Введем отображение $g(\cdot) : (n(t), q(t)) \mapsto (n(t+1), q(t+1))$.

Утверждение 6. Отображение g непрерывно и монотонно: из $n^1 \leqslant n^2$ и $q^1 \leqslant q^2$ следует $g(n^1, q^1) \leqslant g(n^2, q^2)$.

Доказательство. Выпишем явный вид отображения $g(n, q) = (\tilde{n}, \tilde{q})$.

$$\tilde{n}_i = n_i + f_{i-1} - \frac{1}{\beta_i^f} f_i + r_i,$$
$$\tilde{q}_i = q_i + d_i - r_i,$$

где

$$f_i = \min\left\{\beta_i^f v_i n_i,\, f_i^{\max},\, w_{i+1}\left(n_{i+1}^{\max} - n_{i+1}\right)\right\},$$
$$r_i = \min\left\{q_i + d_i,\, n^{\max} - (n_i + f_{i-1} - f_i/\beta_i^f)\right\}.$$

Из непрерывности f_i и r_i как функций от n сразу же следует непрерывность отображения g.

Обозначим $\hat{n}_i = n_i + f_{i-1} - f_i/\beta_i^f$.

Если $n_i \leqslant \underline{n_i}(f^{\max})$,

$$\hat{n}_i = n_i + \min\left\{\beta_{i-1}^f v_{i-1} n_{i-1},\, f_{i-1}^{\max}\right\} - \min\left\{v_i n_i,\, f_i^{\max}/\beta_i^f,\, w_{i+1}/\beta_i^f (n_{i+1}^{\max} - n_{i+1})\right\},$$

если же $n_i > \underline{n_i}(f^{\max})$,

$$\hat{n}_i = n_i + \min\left\{\beta_{i-1}^f v_{i-1} n_{i-1},\, f_{i-1}^{\max},\, w_i(n_i^{\max} - n_i)\right\} - \frac{1}{\beta_i^f}\min\left\{f_i^{\max},\, w_{i+1}(n_{i+1}^{\max} - n_{i+1})\right\}.$$

В любом случае $\hat{n}_i$ монотонно возрастает по n_i (поскольку $v_i, w_i < 1$), не убывает по $n_{i\pm1}$ и не зависит от остальных компонент вектора n.

Заметим, что, поскольку $r_i = \min\{q_i + d_i,\, n_i^{\max} - \hat{n}_i\}$, то

$$\tilde{n}_i = \min\{\hat{n}_i + q_i + d_i,\, n_i^{\max}\},$$
$$\tilde{q}_i = \max\{0,\, \hat{n}_i + q_i + d_i - n_i^{\max}\}.$$

Из монотонности $\hat{n}$ по n следует, что если $n^1 \leqslant n^2$ и $q^1 \leqslant q^2$, то $\tilde{n}^1 \leqslant \tilde{n}^2$, $\tilde{q}^1 \leqslant \tilde{q}^2$. Монотонность отображения g доказана. □

Пусть запрос d таков, что $r = d$ — допустимый входящий поток.

Утверждение 7. Пусть n^e — положение равновесия, $n^e \neq n^{\max}$, в начальный момент очереди нет ($q(\tau) = 0$), и выполнено неравенство $n(\tau) \leqslant n^e$ (или $n(\tau) \geqslant n^e$). Тогда такое же неравенство справедливо для всех точек траектории $n(t; n(\tau))$ в моменты $t \geqslant \tau$: $n(t; n(\tau)) \leqslant n^e$ ($n(t; n(\tau)) \geqslant n^e$). Кроме того, если $n(\tau) \leqslant n^e$, то $q(t) = 0$ для всех t.

Доказательство. Доказательство можно провести по индукции с учетом монотонности отображения g и того факта, что $g(n^e, 0) = (n^e, 0)$. □

Из утверждения 7 следует, что траектория, оказавшаяся в момент τ в множестве $\mathcal{N} = \{n\colon n^u \leqslant n \leqslant n^c\}$, остается там и в последующие моменты времени: $n(t; n(\tau)) \in \mathcal{N}$, $t \geqslant \tau$, то есть множество $\mathcal{N}$ инвариантно относительно рассматриваемой системы. Вообще, для любых двух положений равновесия $n^{e_1} \leqslant n^{e_2}$ множество $\{n\colon n^{e_1} \leqslant n \leqslant n^{e_2}\}$ инвариантно относительно системы.

Утверждение 8. Траектория $n(t; n(0) = n^0)$, выходящая из точки $n^0 = (0, \ldots, 0)$ с нулевой длиной очереди ($q(0) = 0$), не убывает и сходится к положению равновесия n^u. Очередь при этом не образуется.

Доказательство. То, что очередь не образуется, следует из утверждения 7.

Доказательство монотонности $n(t; n^0)$ проведем по индукции. Ясно, что

$$n(1; n^0) \geqslant 0 = n(0; n^0).$$

Пусть $n(k; n^0) \geqslant n(k-1; n^0)$. Тогда

$$n(k+1; n^0) = g(n(k; n^0)) \geqslant g(n(k-1; n^0)) = n(k; n^0).$$

Таким образом, выполнена бесконечная цепочка неравенств

$$n^0 = n(0; n^0) \leqslant n(1; n^0) \leqslant n(2; n^0) \leqslant \ldots.$$

Кроме того, траектория $n(t; n^0)$ ограничена сверху значением n^u в силу утверждения 7. Следовательно, существует предел

$$\lim_{t\to\infty} n(t; n^0) = n^{\lim} \leqslant n^u,$$

который является положением равновесия в силу непрерывности отображения g:

$$n^{\lim} = \lim_{t\to\infty} n(t; n^0) = \lim_{t\to\infty} g(n(t-1; n^0)) = g\left(\lim_{t\to\infty} n(t-1; n^0)\right) = g(n^{\lim}).$$

Но n^u является нижней границей всех равновесий, $n^u \leqslant n^{\lim}$. Значит, $n^{\lim} = n^u$. □

4.1 Устойчивость положений равновесия

Положение равновесия $n^e \neq n^{\max}$ назовем устойчивым, если для любых $\varepsilon_{1,2} > 0$ найдутся $\delta_{1,2} > 0$ такие, что любая траектория, начинающаяся в δ_1-окрестности n^e с $\|q(0)\| < \delta_2$, остается всегда в ε_1-окрестности n^e, при этом норма вектора $q(t)$ не превосходит ε_2.

Положение равновесия $n^{\max}$ назовем устойчивым, если для любого $\varepsilon > 0$ найдется $\delta > 0$ такое, что любая траектория, начинающаяся в δ-окрестности $n^{\max}$, остается в ε-окрестности $n^{\max}$ независимо от начальной очереди.

Покажем, что определение устойчивости положения равновесия $n^e \neq n^{\max}$ эквивалентно следующему. Для любого $\varepsilon > 0$ найдется $\delta > 0$ такое, что любая траектория, начинающаяся в δ-окрестности n^e с нулевой очередью не выйдет из ε-окрестности n^e, и очередь останется нулевой.

Поскольку $n^e \neq n^{\max}$, то в точке n^e

$$r_i < n_i^{\max} - (n_i + f_{i-1} - f_i - s_i).$$

Значит, это неравенство верно и в некоторой окрестности точки n^e. Следовательно, при малых $q(0)$ и при $n(0)$ из этой малой окрестности n^e уже на первом шаге получим $q(1) = 0$. При этом

$$|n_i(1) - n_i^e| \leqslant |\hat{n}_i(0) - \hat{n}_i^e| + q_i(0),$$

где $\hat{n}_i = n_i + f_{i-1} - f_i/\beta_i^f$. Ясно, что функция f_i липшицева по n. Поэтому

$$\|n(1) - n^e\| \leqslant \lambda\|n(0) - n^e\| + \|q(0)\| \leqslant (\lambda + 1)\delta.$$

Следовательно, если положение равновесия n^e устойчиво в смысле второго определения, то оно устойчиво и в смысле первого определения. Поскольку, как уже было показано, $q(t) = 0$, $t = 1, 2, \ldots$ если $q(0) = 0$, а $n(0)$ принадлежит достаточно малой окрестности n^e, то обратное тоже верно.

Утверждение 9. Если входящий поток r строго допустимый, то положение равновесия n^u является устойчивым, а положение равновесия n^c устойчивым не является.

Доказательство. В окрестности положения равновесия n^u (n^c) выполнено неравенство $n \ll \ll \underline{n}(f^{\max})$ ($n \gg \overline{n}(f^{\max})$), поэтому в окрестности точки n^u

$$n_i(t+1) = n_i(t) + r_i + \beta_{i-1}v_{i-1}n_{i-1}(t) - v_i n_i(t) = (1 - v_i)n_i(t) + \beta_{i-1}v_{i-1}n_{i-1}(t) + r_i,$$

а в окрестности точки n^c

$$\begin{aligned} n_i(t+1) &= n_i(t) + r_i + w_i(n_i^{\max} - n_i(t)) - w_{i+1}/\beta_i^f(n_{i+1}^{\max} - n_{i+1}(t)) = \\ &= (1 - w_i)n_i(t) + w_{i+1}/\beta_i^f n_{i+1}(t) + r_i + (w_i n_i^{\max} - w_{i+1}n_{i+1}^{\max}/\beta_i^f). \end{aligned}$$

то есть $n(t+1) = A^u n(t) + r$ в окрестности n^u, и $n(t+1) = A^c n(t) + r + C^c$ в окрестности n^c, где

$$A^u = \begin{pmatrix} 1 - v_1 & 0 & 0 & \cdots & \beta_N v_N \\ \beta_1 v_1 & 1 - v_2 & 0 & \cdots & 0 \\ 0 & \beta_2 v_2 & 1 - v_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 - v_N \end{pmatrix}, \quad A^c = \begin{pmatrix} 1 - w_i & w_2/\beta_1^f & 0 & \cdots & 0 \\ 0 & 1 - w_2 & w_3/\beta_2^f & \cdots & 0 \\ 0 & 0 & 1 - w_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ w_1/\beta_N^f & 0 & 0 & \cdots & 1 - w_N \end{pmatrix}.$$

Поскольку n^u, n^c — положения равновесия, то $n^u = A^u n^u + r$, $n^c = A^c n^c + r + C^c$, значит, $n(t+1) - n^u = A^u(n(t) - n^u)$ в окрестности n^u, $n(t+1) - n^c = A^c(n(t) - n^c)$ в окрестности n^c.

Покажем, что матрица A^u не увеличивает 1-норму любого вектора, а матрица A^c увеличивает норму вектора с положительными компонентами. Для любого x

$$\|A^u x\|_1 = \sum_{i=1}^{N} |(A^u x)_i| \leqslant \sum_{i=1}^{N} ((1-v_i)|x_i| + \beta_{i-1} v_{i-1} |x_{i-1}|) = \sum_{i=1}^{N} (1-(1-\beta_i)v_i)|x_i| \leqslant \|x\|_1.$$

Для $x \gg 0$ выполнено неравенство $A^c x \gg 0$.

$$\|A^c x\|_1 = \sum_{i-1}^{N} ((1-w_i)x_i + w_{i+1}/\beta_i^f x_{i+1}) = \sum_{i=1}^{N} (1 + w_i(1/\beta_{i-1}^f - 1))x_i > \|x_i\|.$$

Следовательно, положение равновесия n^u устойчиво, а n^c не устойчиво. □

Лемма 1. Положение равновесия $n^e \neq n^{\max}$ устойчиво тогда и только тогда, когда для любого $\varepsilon > 0$ найдется $\delta > 0$ такое, что для любого $n(0)$, из δ-окрестности n^e, сравнимого с n^e (то есть $n(0) \geqslant n^e$ или $n(0) \leqslant n^e$), траектория, начинающаяся в этой точке с нулевой очередью, остается в ε-окрестности точки n^e.

Доказательство. Необходимость условия очевидна. Докажем достаточность.

Положим $\|x\| = \max\{|x_i|,\ i = 1, \ldots, N\}$.

Фиксируем $\varepsilon > 0$ и соответствующее ему $\delta > 0$. Для любого $n(0)$ из δ-окрестности точки n^e положим $n^+(0) = (n_i^+(0) = \max\{n_i^e, n_i(0)\})_{i=1}^N$, $n^-(0) = (n_i^-(0) = \min\{n_i^e, n_i(0)\})_{i=1}^N$. Ясно, что выполнены неравенства $n^-(0) \leqslant n^e \leqslant n^+(0)$, $n^-(0) \leqslant n(0) \leqslant n^+(0)$ и

$$\|n^{\pm}(0) - n^e\| = \max_{i=1,\ldots,N} \{|n_i^{\pm}(0) - n_i^e|\} \leqslant \max_{i=1,\ldots,N} \{|n_i(0) - n_i^e|\} \leqslant \delta.$$

Следовательно, для всех точек траектории $n(t)$, начинающейся с нулевой очередью, выполнено неравенство $n^-(t) \leqslant n(t) \leqslant n^+(t)$, и $\|n(t) - n^e\| \leqslant \max\{\|n^-(t) - n^e\|, \|n^+(t) - n^e\|\} \leqslant \varepsilon$. □

Лемма 2. Для любой точки n^*, $0 \leqslant n^* \leqslant n^c$, найдется ее окрестность такая, что на пересечении этой окрестности со множеством $n \leqslant n^*$ ($n \geqslant n^*$) $n(t+1)$ зависит от $n(t)$ линейно при $q(t) = 0$.

Доказательство. Если $n^* \leqslant n^c$, то в некоторой ее окрестности если $q(t) = 0$, то $r(t) = d(t)$ и не зависит от $n(t)$. Вспомним, что $n_i(t+1) = n_i(t) + r_i + f_{i-1}(t) - f_i(t)/\beta_i^f$.

Докажем, что найдется окрестность точки n^*, на пересечении которой с множеством $n \leqslant n^*$ f зависит от n линейно. $f_i = \min\left\{\beta_i^f v_i n_i,\ f_i^{\max},\ w_{i+1}(n_{i+1}^{\max} - n_{i+1})\right\}$.

Если $\beta_i^f v_i n_i^* \leqslant f_i^{\max}$, то при $n \leqslant n^*$ это неравенство сохранится, если же $\beta_i^f v_i n_i^* > f_i^{\max}$, то это неравенство сохранится в достаточно малой окрестности n^*. То же самое можно сказать о неравенствах $f_i^{\max} \leqslant w_{i+1}(n_{i+1}^{\max} - n_{i+1})$ и $\beta_i^f v_i n_i \leqslant w_{i+1}(n_{i+1}^{\max} - n_{i+1})$. Следовательно, при $n \leqslant n^*$ в достаточно малой окрестности точки n^* минимум достигается всегда на одной и той же функции ($\beta_i^f v_i n_i$, $f_i^{\max}$, или $w_{i+1}(n_{i+1}^{\max} - n_{i+1})$, каждая из который линейна по n, значит, f также зависит линейно от n по крайней мере на пересечении малой окрестности точки n^* со множеством $n \leqslant n^*$.

Для $n \geqslant n^*$ доказательство такое же. □

Утверждение 10 (Критерий устойчивости положения равновесия, соответствующего не полностью загруженной дороге)**.** Пусть входящий поток r допустим. Положение равновесия $n^e < n^{\max}$ не является устойчивым, если и только если

1. Для всех i или $n_i^e \geqslant \underline{n_i}(f^{\max})$, или $\beta_i^f v_i n_i^e \geqslant w_{i+1}(n_{i+1}^{\max} - n_{i+1}^e)$.
2. По крайней мере для одного i выполнены неравенства $n_i^e \geqslant \overline{n_i}(f_i^{\max})$ и $\beta_i^s > 0$.

Доказательство. Везде считаем, что начальная длина очереди равна нулю.

Часть 1. Пусть не выполнено первое условие: по крайней мере для одного i выполнены неравенства $n_i^e < \underline{n_i}(f^{\max})$, $\beta_i^f v_i n_i^e < w_{i+1}(n_{i+1}^{\max} - n_{i+1}^e)$. Тогда в некоторой окрестности точки n^e $f_i = \beta_i^f v_i n_i^e$.

Для всех n из достаточно малой окрестности n^e, сравнимых с n^e (либо $n \leqslant n^e$, либо $n \geqslant n^e$) $f(n)$ — линейная функция. Обозначим через $\mathcal{I}$ множество индексов i, для которых $f_i = \beta_i^f v_i n_i^e$. Ясно, что $\mathcal{I} \neq \varnothing$. Тогда для $i \notin I$ либо $f_i = f_i^{\max}$, либо $f_i = w_{i+1}(n_{i+1}^{\max} - n_{i+1})$. Если вектор $n(t)$ принадлежит достаточно малой окрестности n^e и сравним с n^e, $n(t+1)$ зависит от $n(t)$ линейно: $n(t+1) = An(t) + r + C$. Обозначим $\bar{\mathcal{I}} = \{1, \ldots, N\} \setminus \mathcal{I}$.

Случай $\bar{\mathcal{I}} = \varnothing$ уже рассмотрен при доказательстве устойчивости положения равновесия n^u для случая строго допустимого входящего потока. В этом случае матрица A устойчива. Рассмотрим случай $\bar{\mathcal{I}} \neq \varnothing$.

Докажем, что собственные числа матрицы A есть ее диагональные элементы. Вспомним, что $n_i(t+1) = n_i(t) + r_i + f_{i-1}(n(t)) - f_i(n(t))/\beta_i^f$. Рассмотрим подряд идущие столбцы и строки матрицы A с индексами из $\bar{\mathcal{I}}$ и следующие за ними строки и столбцы с индексами из $\mathcal{I}$. На рисунке 3 показана структура такого блока матрицы A. Пустые клетки означают нули, звездочки — возможные ненулевые элементы.

		1	2	3	4	5	6	
	$\mathcal{I}$	$\bar{\mathcal{I}}$	$\bar{\mathcal{I}}$	$\bar{\mathcal{I}}$	$\mathcal{I}$	$\mathcal{I}$	$\mathcal{I}$	$\bar{\mathcal{I}}$
	*							
1	*	*	*					
2			*	*				
3				*				
4					*			
5					*	*		
6						*	*	
							*	*

Рис. 3. Структура матрицы A (первая часть доказательства).

Если $i \in \mathcal{I}$, то $n_i(t+1)$ не зависит от $n_{i+1}(t)$, $n_{i-1}(t+1)$ не зависит от $n_i(t)$, а если $i \in \bar{\mathcal{I}}$, то $n_{i+1}(t+1)$ не зависит от $n_i(t)$. Поэтому определитель матрицы $A - \lambda I$ есть произведение ее диагональных элементов, значит, собственные числа матрицы A есть ее диагональные элементы.

Если $i \in \mathcal{I}$, то f_{i-1} от n_i не зависит, $f_i = \beta_i^f v_i n_i$, значит, $a_{ii} = 1 - v_i \in (0,1)$. Если же $i \in \bar{\mathcal{I}}$, то f_i не зависит от n_i. Если $i - 1 \in \bar{\mathcal{I}}$, то $a_{ii} = 1 - w_i \in (0,1)$, в противном случае $a_{ii} = 1$, но $a_{i\pm1,i}$ и все остальные элементы столбца равны нулю, то есть собственные значения, равные единице, всегда простые: им соответствует собственный вектор $(0, \ldots, 0, 1, 0, \ldots, 0)'$ (единица в i-й позиции). Следовательно, матрица A устойчивая и положение равновесия n^e устойчивое.

Часть 2. Пусть первое условие выполнено.

Рассмотрим пересечение малой окрестности точки n^e с множеством $n \geqslant n^e$. На этом множестве

$$f_i = \begin{cases} w_{i+1}(n_{i+1}^{\max} - n_{i+1}), & \text{если } n_{i+1}^e \geqslant \overline{n_{i+1}}(f^{\max}), \\ f_i^{\max}, & \text{иначе.} \end{cases}$$

Случай, когда все $f_i = w_{i+1}(n_{i+1}^{\max} - n_{i+1})$ был рассмотрен при доказательстве неустойчивости положения равновесия n^c для строго допустимого входящего потока. Было показано, что в этом случае матрица A неустойчивая. При этом $\beta^s \neq 0$ согласно модели.

Пусть по крайней мере для одного i $f_i = f_i^{\max}$. Обозначим $\mathcal{I} = \{i\colon n_i^e \geqslant \overline{n_{i+1}}(f^{\max})\}$. Тогда

$$a_{ii} = \begin{cases} 1 - w_i, & i-1 \in \mathcal{I}, \\ 1, & \text{иначе}, \end{cases}$$

$$a_{i,i+1} = \begin{cases} w_{i+1}/\beta_i^f, & i \in \mathcal{I}, \\ 0, & \text{иначе}. \end{cases}$$

Обозначим $\Delta n = n - n^e \geqslant 0$.

$$\|A\Delta n\|_1 = \sum_{i-1\in\mathcal{I}} (1-w_i)\Delta n_i + \sum_{i-1\notin\mathcal{I}} \Delta n_i + \sum_{i\in\mathcal{I}} \frac{w_{i+1}}{\beta_i^f}\Delta n_{i+1} = \|\Delta n_i\|_1 + \sum_{i\in\mathcal{I}} w_{i+1}\frac{\beta_i^s}{\beta_i^f}\Delta n_{i+1}.$$

Следовательно, если по крайней мере для одного $i \in \mathcal{I}$ $\beta_i^s > 0$, оператор A увеличивает норму вектора с положительными компонентами и является потому неустойчивым, в противном случае оператор A сохраняет норму вектора с неотрицательными компонентами и является устойчивым на множестве $\Delta n \geqslant 0$ (ибо в этом случае $A\Delta n \geqslant 0$).

Часть 3. Осталось доказать устойчивость n^e в случае, когда первое условие выполнено, а второе не выполнено. Случай $n \geqslant n^e$ уже рассмотрели, на пересечении этого множества с малой окрестностью точки n^e определение устойчивости выполнено.

Для $n \leqslant n^e$ в малой окрестности точки n^e либо $f_i = \beta_i^f v_i n_i$ для некоторых i, и, как показано в первой части доказательства, положение равновесия n^e устойчиво, либо для всех i

$$f_i = \begin{cases} w_{i+1}(n_{i+1}^{\max} - n_{i+1}), & n_{i+1}^e > \overline{n_{i+1}}(f^{\max}), \\ f_i^{\max}, & \text{иначе}. \end{cases}$$

Как и в предыдущей части, для $\Delta n < 0$

$$\|A\Delta n\|_1 = \|\Delta n\|_1 + \sum_{n_i^e > \overline{n_i}(f^{\max})} w_{i+1}\frac{\beta_i^s}{\beta_i^f}|\Delta n_{i+1}|.$$

Поскольку условие 2 не выполнено, то второе слагаемое равно нулю, оператор A не увеличивает норму и положение равновесия n^e устойчивое. □

Утверждение 11. Если у дороги есть по крайней мере один въезд и соответствующий ему запрос d_i ненулевой, то положение равновесия $n^{\max}$ устойчиво.

Доказательство. Обозначим через $\mathcal{I}$ множество номеров участков i, на которых есть въезд и для которых $d_i > 0$.

В окрестности точки $f^{\max}$ справедливо равенство $f_i = w_{i+1}(n_{i+1}^{\max} - n_{i+1})$.

Возьмем $n(0)$ из малой окрестности $n^{\max}$. Можем считать, что для $i \in \mathcal{I}$ выполнено равенство $n_i(0) = n_i^{\max}$ (ибо оно будет выполнено на первом же шаге). Если не выходить из достаточно малой окрестности точки $n^{\max}$, то всегда будет выполнено равенство $n_i(t) = n_i^{\max}$. Поэтому $f_{i-1}(t) \equiv 0$. Обозначим $\Delta n(t) = n^{\max} - n(t)$. Если $i - 1 \notin \mathcal{I}$, то

$$\Delta n_{i-1}(t+1) = \Delta n_{i-1}(t) - f_{i-2}(t) = (1 - w_{i-1})\Delta n_{i-1}(t).$$

Таким образом, $\Delta n_{i-1}(t)$ уменьшается в геометрической прогрессии: $\Delta n_{i-1}(t) = \alpha_{i-1}^t \Delta n_{i-1}(0)$, где $\alpha_{i-1} = 1 - w_{i-1}$.

Далее, если $i - 2 \notin \mathcal{I}$, то

$$\Delta n_{i-2}(t+1) = \Delta n_{i-2}(t) - f_{i-3}(t) + \frac{1}{\beta_i^f} f_{i-2}(t) = \alpha_{i-2}\Delta n_{i-2}(t) + \frac{1}{\beta_i^f} f_{i-2}(t),$$

где $\alpha_{i-2} = 1 - w_{i-2}$.

Докажем следующую лемму.

Лемма 3. Пусть последовательность неотрицательных чисел $\{x_k\}_{k=0}^{\infty}$ сходится к нулю при $k \to \infty$. Последовательность $\{y_k\}_{k=0}^{\infty}$ задается рекуррентным соотношением

$$y_{k+1} = \alpha y_k + x_k, \quad k = 1, 2, \ldots,$$

$0 < \alpha < 1$, $y_0 \geqslant 0$. Тогда $y_k \geqslant 0$ и $y_k \to 0$ при $k \to \infty$. Кроме того, если $x_k \leqslant X$ для всех k, то $y_k \leqslant Y = y_0 + X/(1-\alpha)$ для всех k.

Доказательство. Неотрицательность y_k очевидна. Покажем, что

$$y_k = \alpha^k y_0 + \sum_{i=0}^{k-1} x_i \alpha^{k-1-i}.$$

Для $k = 1$ равенство справедливо. Пусть оно справедливо для k. Тогда

$$y_{k+1} = \alpha y_k + x_k = \alpha^{k+1} y_0 + \sum_{i=0}^{k} x_i \alpha^{k-i}.$$

Из доказанного равенства следует, что если $x_k \leqslant X$ для всех X, то $y_k \leqslant y_0 + X/(1-\alpha)$.

Ясно, что $\alpha^k y_0 \to 0$ при $k \to \infty$. Обозначим $X_k = \max\{x_i \colon i \geqslant K\}$. Поскольку $x_k \to 0$, то X_k существует и конечно и стремится к нулю при $k \to \infty$. Представим сумму в следующем виде.

$$\sum_{i=0}^{k-1} x_i \alpha^{k-1-i} = \alpha^{k-1-N} \sum_{i=0}^{N} x_i \alpha_{N-i} + \sum_{i=N+1}^{k-1} x_i \alpha^{k-1-i} \leqslant$$

$$\leqslant \alpha^{k-1-N} X_0 + X_{N+1} \sum_{i=N+1}^{k-1} \alpha^{k-1-i} \leqslant \alpha^{k-1-N} X_0 + \frac{X_{N+1}}{1-\alpha}.$$

Для любого $\varepsilon > 0$ можно подобрать $K_x(\varepsilon)$ такое, что $X_{K_x} < \varepsilon(1-\alpha)/2$ и $K_y(\varepsilon)$ такое, что $\alpha^{k-1-K_x(\varepsilon)} X_0 < \varepsilon/2$ при $k \geqslant K_y(\varepsilon)$. Тогда вся сумма будет меньше ε, что и требовалось для доказательства сходимости последовательности $\{y_k\}_{k=0}^{\infty}$ к нулю. □

В качестве x_k возьмем $f_{i-2}(k)$, в качестве α — α_{i-2}, в качестве y_k — $\Delta n_{i-2}(k)$, и получим, что $\Delta n_{i-2}(t)$ тоже сходится к нулю, при этом не слишком сильно отдаляясь от нуля.

Если $i - 3 \notin \mathcal{I}$, рассуждая так же придем к тому, что $\Delta n_{i-3}(t) \to 0$ при $t \to \infty$ и так далее.

В итоге, если $\mathcal{I} \neq \varnothing$, то $\Delta n(t)$ сойдется к нулю при $t \to \infty$, при этом значение $n(t)$ не выйдет из достаточно малой окрестности точки $n^{\max}$. Устойчивость положения равновесия $n^{\max}$ доказана. □

4.2 Примеры

На рисунке 4 изображены траектории и положения равновесия системы для строго, не строго допустимого и для недопустимого входящего потока.

Если входящий поток строго допустимый (рисунок 4, *а*), то есть если $f \ll f^{\max}$, у системы три положения равновесия: n^u и $n^{\max}$ — устойчивые, n^c — неустойчивое.

В случае не строго допустимого потока, если $f_1 = f_1^{\max}$, $f_2 < f_2^{\max}$ (рисунок 4, *б*), положениями равновесия являются точки

$$n \in \{n_1^u \leqslant n_1 \leqslant n_1^c,\ n_2 = n_2^u\} \cup \{n_1 = n_1^u,\ n_2^u \leqslant n_2 \leqslant n_2^c\} \cup \{n^{\max}\}.$$

Если $f = f^{\max}$ (рисунок 4, *в*), положениями равновесия являются все точки прямоугольника $n^u \leqslant n \leqslant n^c$ и точка $n^{\max}$.

Если же входящий поток не является допустимым (рисунок 4, *г*), есть лишь одно, устойчивое, положение равновесия — точка $n^{\max}$.

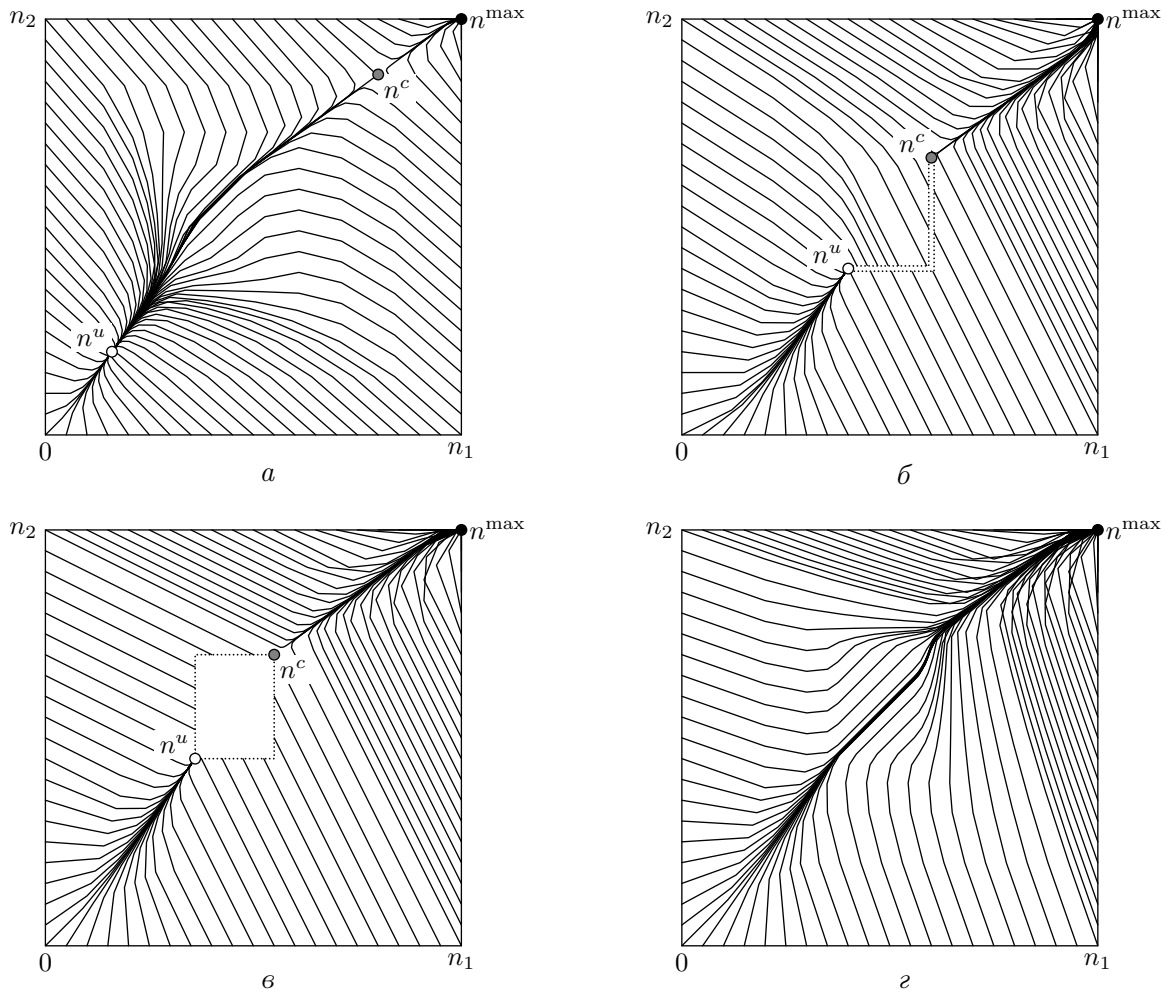


Рис. 4. Траектории и положения равновесия системы: (*а*) строго допустимый поток, (*б*) не строго допустимый поток, $f_1 = f_1^{\max}$, $f_2 < f_2^{\max}$, (*в*) не строго допустимый поток, $f = f^{\max}$, (*г*) недопустимый поток.

5 Заключение

В статье найдены положения равновесия дискретной динамической системы, описывающей кольцевую автомагистраль, при постоянном входящем потоке. Полностью исследована устойчивость положений равновесия. У системы, описывающей кольцевую автостраду, в отличие от аналогичной системы для незамкнутой автомагистрали, есть положение равновесия, соответствующее полностью загруженной дороге — нулевая скорость движения, максимальная плотность потока, то есть, фактически, затор на всем протяжении автострады. Такое положение равновесия устойчиво, но устойчивость эта нежелательна. Следовательно, необходимо ограничивать входящий поток, чтобы не допустить образования затора.

Список литературы

[1] *Lighthill M. J., Whitham G. B.* On kinematic waves. I. Flood movement in long rivers // Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences. — 1955. — Vol. 229, no. 1178. — Pp. 281–316.

[2] *Lighthill M. J., Whitham G. B.* On kinematic waves. II. A theory of traffic flow on long crowded

roads // Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences. — 1955. — Vol. 229, no. 1178. — Pp. 317–345.

[3] *Daganzo Carlos F.* The cell transmission model: A dynamic representation of highway traffic consistent with the hydrodynamic theory // Transportation Research Part B: Methodological. — 1994. — Vol. 28, no. 4. — Pp. 269–287.

[4] *Daganzo Carlos F.* The cell transmission model, part II: Network traffic // Transportation Research Part B: Methodological. — 1995. — Vol. 29, no. 2. — Pp. 79–93.

[5] *Kurzhanskiy Alex A.* Modeling and Software Tools for Freeway Operational Planning: Ph.D. thesis / EECS Department, University of California, Berkeley. — 2007. `http://www.eecs.berkeley.edu/Pubs/TechRpts/2007/EECS-2007-148.html`.

[6] *Gomes Gabriel, Horowitz Roberto, Kurzhanskiy Alex A., Varaiya Pravin, Kwon Jaimyoung.* Behavior of the cell transmission model and effectiveness of ramp metering // Transportation Research Part C: Emerging Technologies. — 2008. — Vol. 16, no. 4. — Pp. 485–513.

[7] *Gomes Gabriel, Horowitz Roberto.* Optimal freeway ramp metering using the asymmetric cell transmission model // Transportation Research Part C: Emerging Technologies. — 2006. — Vol. 14, no. 4. — Pp. 244–262.

УДК 530.145

РАСШИРЕНИЕ ОБЛАСТИ СЕКРЕТНОСТИ ПРОТОКОЛА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ФАЗОВО-ВРЕМЕННЫМ КОДИРОВАНИЕМ

© 2011 г. Д. А. Кронберг

kronberg@cmc.msu.ru

Кафедра квантовой информатики

Введение

Квантовая криптография, или квантовое распределение ключей, появилась в 1984 году, после публикации описания первого протокола, названного BB84 [3]. В отличие от классической криптографии, она не основывается на предположениях о технологических и вычислительных возможностях перехватчика, а использует известные на сегодняшний день законы квантовой механики для обеспечения секретности передаваемых ключей в самом общем случае. В протоколах квантовой криптографии действия перехватчика детектируются по ошибкам на приемной стороне, которые он неизбежно вносит при попытках получения секретной информации. Ошибка, превышающая критическую величину (зависящую от протокола), означает, что информация перехватчика о передаваемом ключе может не уступать информации о нем легитимных пользователей, что означает невозможность секретного распространения ключей. В этом случае выполнение протокола прекращается. Чем больше критическая ошибка протокола, тем более он устойчив к помехам в канале связи и тем большую скорость распределения ключей он способен обеспечить.

Протокол с фазово-временным кодированием, изначально предложенный в [8], ставит своей целью увеличение критической ошибки в квантовой криптографии, и, как показал анализ его стойкости [7, 9], он способен при определенных условиях обеспечивать секретность при ошибке на приемной стороне, меньшей 50 %, что является теоретическим пределом. Подобное увеличение критической ошибки вызвано тем, что детектирование перехватчика на приемной стороне ведется по двум параметрам: битовой ошибке и контрольным временным отсчетам. В этом главное отличие этого протокола от других известных схем квантовой криптографии, в которых детектирование перехватчика производится по одному параметру. Ниже будет описана конфигурация сигнальных состояний этого протокола.

В качестве одной из техник увеличения критической величины ошибки авторы [4] предложили использовать классический препроцессинг. Суть его сводится к тому, что после согласования базисов и раскрытия части передаваемой последовательности, когда легитимные пользователи (их принято называть Алисой и Бобом) имеют оценку вероятности ошибки на приемной стороне, они могут добавить классический шум к своим данным. Это усложнит задачу перехватчика (Евы) по получению информации из передаваемых состояний, благодаря чему критическая величина ошибки может быть увеличена. Так, для протокола BB84 она возрастает примерно с 11 % до 12,4 % [4].

Другая техника увеличения критической ошибки была предложена Маурером [5] и названа CAD — classical advantage distillation. Она заключается в том, что Алиса может на своей стороне объединить биты своей строки с одинаковыми значениями в блоки длины N и назвать Бобу лишь позиции соответствующих блоков, но не значения битов в них. Если на стороне Боба значения в блоке также совпадут, то это значение будет использоваться как один бит в новом ключе, а при несовпадении значений все позиции отбрасываются. Оказывается, такая техника также способна увеличить критическую ошибку. Для протокола BB84 критическая ошибка подобным способом увеличилась примерно до 20%.

В дальнейшем первый способ увеличения критической длины ключа будем называть «внесением дополнительного шума», а второй — «блочным исправлением ошибок».

Работа организована следующим образом. В первом разделе будут рассматриваются оба способа увеличения критической величины ключа для протокола BB84, а также возможность комбинирования этих методов. Затем во втором разделе аналогичные результаты будут применены к протоколу с фазово-временным кодированием.

1 Протокол BB84

В [10] была проанализирована стойкость протокола BB84 и построена наиболее общая атака на него, при которой достигается теоретический предел критической ошибки, равный примерно 11 %. Наиболее эффективной стратегией оказывается коллективная атака, которая сводится к тому, что к каждому передаваемому состоянию $|\psi\rangle$ Ева присоединяет свое состояние (анциллу) $|e\rangle$, а затем подвергает эти состояния совместной эволюции U_E, в результате чего система оказывается в сцепленном состоянии

$$|\Psi\rangle = U_E|\psi \otimes e\rangle.$$

Действие этого преобразования на состояния базиса «+» можно расписать как [10]

$$\begin{aligned} |x\rangle \to |X\rangle = U_E|\psi \otimes e\rangle = (1-q)|x\rangle|\psi_x\rangle + q|y\rangle|\theta_x\rangle, \\ |y\rangle \to |Y\rangle = U_E|\psi \otimes e\rangle = (1-q)|y\rangle|\psi_y\rangle + q|x\rangle|\theta_y\rangle, \end{aligned}$$

где $|\psi_i\rangle$ и $|\theta_i\rangle$ лежат в пространстве Евы $\mathcal{H}_E$. Из соображений симметрии и унитарности U_E должны выполняться соотношения

$$\begin{gathered} \langle\psi_x|\psi_y\rangle = \langle\theta_x|\theta_y\rangle = \varepsilon, \\ \langle\psi_i|\psi_i\rangle = 1, \quad \langle\theta_i|\theta_i\rangle = 1, \quad \langle\psi_i|\theta_j\rangle = 0, \\ \varepsilon = 1 - 2q. \end{gathered} \tag{1}$$

После передачи состояния по квантовому каналу Боб имеет дело с его частичным следом по пространству окружения $\mathcal{H}_E$:

$$\begin{aligned} \rho_x^B = \mathrm{Tr}_E|X\rangle\langle X| = (1-q)|x\rangle\langle x| + q|y\rangle\langle y|, \\ \rho_y^B = \mathrm{Tr}_E|Y\rangle\langle Y| = (1-q)|y\rangle\langle y| + q|x\rangle\langle x|. \end{aligned}$$

В нашем случае пространство окружения совпадает с пространством Евы — это соответствует наилучшему для нее случаю. Очевидно, что при измерении этих состояний ошибка на стороне Боба оказывается равной q. Ева же имеет дело с состояниями, задаваемыми частичным следом по пространству Алисы и Боба $\mathcal{H}_{AB}$ и стоит перед задачей различения следующих операторов плотности:

$$\begin{aligned} \rho_x^E = \mathrm{Tr}_E|X\rangle\langle X| = (1-q)|\psi_x\rangle\langle\psi_x| + q|\theta_x\rangle\langle\theta_x|, \\ \rho_y^E = \mathrm{Tr}_E|Y\rangle\langle Y| = (1-q)|\psi_y\rangle\langle\psi_y| + q|\theta_y\rangle\langle\theta_y|. \end{aligned} \tag{2}$$

Операторы $|\psi_i\rangle\langle\psi_i|$ соответствуют правильному исходу у Боба, а операторы $|\theta_i\rangle\langle\theta_i|$ — ошибочному. Коллективная атака подразумевает, что Ева производит измерение над всей последовательностью передаваемых состояний, и при этом доступная ей информация задается квантовой теоремой кодирования для канала с состояниями (2). Пропускная способность канала между Алисой и Евой дается величиной Холево и равна [11]

$$\chi\left(\{\rho_x^E, \rho_y^E\}\right) = H\left(\frac{1}{2}(\rho_x^E + \rho_y^E)\right) - \frac{1}{2}H(\rho_x^E) - \frac{1}{2}H(\rho_y^E). \tag{3}$$

Вычисляя величину (3) как функцию параметра q, можно получить, что информация Евы начинает превосходить взаимную информацию Алисы и Боба, когда q превышает 11 %, что является теоретическим пределом. Таким образом, построенная атака является наиболее эффективной.

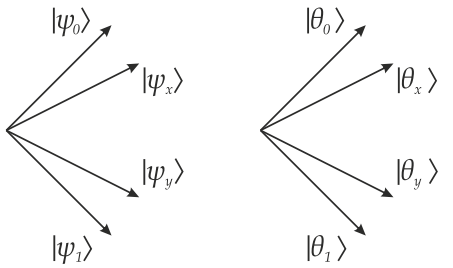


Рис. 1. Расположение векторов базиса, в котором выписываются матрицы операторов (2), относительно векторов $\{|\psi_i\rangle, |\theta_i\rangle\}$ в пространстве Евы.

1.1 Внесение дополнительного шума

Рассмотрим теперь, что происходит при внесении Алисой дополнительного шума, задаваемого вероятностью ошибки p. Исходная ошибка q на стороне Боба становится равной

$$Q = (1-p)(1-q) + pq, \tag{4}$$

а Ева, как нетрудно видеть, стоит перед необходимостью различения состояний

$$\begin{aligned} \rho_x^E &= \mathrm{Tr}_E|X\rangle\langle X| = (1-p)\left[(1-q)|\psi_x\rangle\langle\psi_x| + q|\theta_x\rangle\langle\theta_x|\right] + p\left[(1-q)|\psi_y\rangle\langle\psi_y| + q|\theta_y\rangle\langle\theta_y|\right], \\ \rho_y^E &= \mathrm{Tr}_E|Y\rangle\langle Y| = (1-p)\left[(1-q)|\psi_y\rangle\langle\psi_y| + q|\theta_y\rangle\langle\theta_y|\right] + p\left[(1-q)|\psi_x\rangle\langle\psi_x| + q|\theta_x\rangle\langle\theta_x|\right]. \end{aligned} \tag{5}$$

В этом случае можно посчитать величину Холево для этих состояний при заданной величине исходной ошибки q и оптимальном (для Алисы и Боба) выборе параметра шума p. Выпишем матрицы операторов (5) в базисе $\{|\psi_0\rangle, |\psi_1\rangle, |\theta_0\rangle, |\theta_1\rangle\}$, элементы которого расположены симметрично относительно векторов $|\psi_i\rangle$ и $|\theta_i\rangle$ (рисунок 1):

$$\rho_x^E = \frac{1}{2}\begin{pmatrix} (1-q)\left(1+(1-2p)\sqrt{1-\varepsilon^2}\right) & (1-q)\varepsilon & 0 & 0 \\ (1-q)\varepsilon & (1-q)\left(1-(1-2p)\sqrt{1-\varepsilon^2}\right) & 0 & 0 \\ 0 & 0 & q\left(1+(1-2p)\sqrt{1-\varepsilon^2}\right) & q\varepsilon \\ 0 & 0 & q\varepsilon & q\left(1-(1-2p)\sqrt{1-\varepsilon^2}\right) \end{pmatrix},$$

$$\rho_y^E = \frac{1}{2}\begin{pmatrix} (1-q)\left(1-(1-2p)\sqrt{1-\varepsilon^2}\right) & (1-q)\varepsilon & 0 & 0 \\ (1-q)\varepsilon & (1-q)\left(1+(1-2p)\sqrt{1-\varepsilon^2}\right) & 0 & 0 \\ 0 & 0 & q\left(1-(1-2p)\sqrt{1-\varepsilon^2}\right) & q\varepsilon \\ 0 & 0 & q\varepsilon & q\left(1+(1-2p)\sqrt{1-\varepsilon^2}\right) \end{pmatrix}.$$

Собственные значения этих матриц совпадают и равны

$$\begin{aligned} \lambda_{1,2} &= \frac{1-q}{2}\left(1 \pm \sqrt{1-4p(1-p)(1-\varepsilon^2)}\right), \\ \lambda_{3,4} &= \frac{q}{2}\left(1 \pm \sqrt{1-4p(1-p)(1-\varepsilon^2)}\right), \end{aligned}$$

а с учетом (1) их можно переписать в виде

$$\begin{aligned} \lambda_{1,2} &= \frac{1-q}{2}\left(1 \pm \sqrt{1-16pq(1-p)(1-q)}\right), \\ \lambda_{3,4} &= \frac{q}{2}\left(1 \pm \sqrt{1-16pq(1-p)(1-q)}\right). \end{aligned}$$

Для подсчета величины Холево для состояний Евы требуются также собственные значения оператора $\frac{1}{2}(\rho_x^E + \rho_y^E)$. Они не отличаются от аналогичных значений при отсутствии дополнительного шума и равны $\{(1-q)^2, q(1-q), q(1-q), q^2\}$. С учетом этого информация Евы вычисляется по формуле

$$I_{AE} = 2h(q) + \sum_{i=1}^{4} \lambda_i \log \lambda_i$$

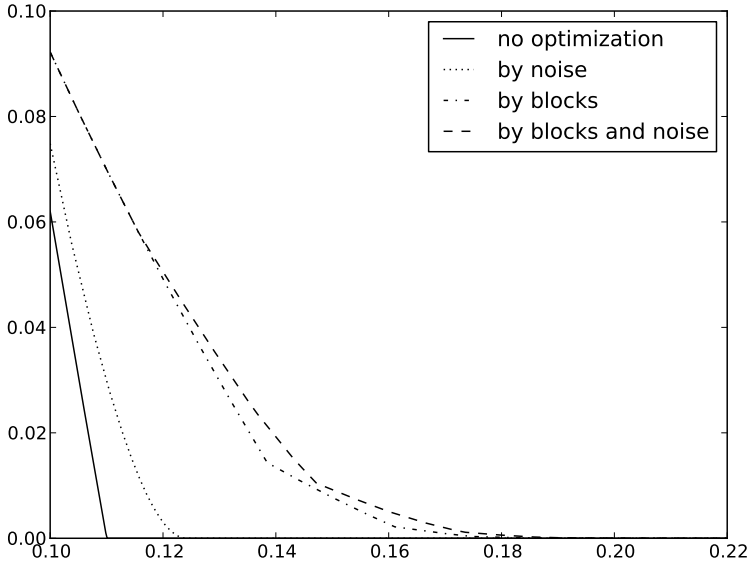


Рис. 2. Зависимость длины секретного ключа протокола BB84 от наблюдаемой на приемной стороне ошибки q при разных действиях перехватчика. Сплошная линия соответствует отсутствию предварительной обработки данных, пунктирная линия — проведению оптимизации по вносимому шуму, штрихпунктирная линия — оптимизации по блочному исправлению ошибок, штрихованная линия — комбинированию методов предварительной обработки данных. Показана только область, на которой применение методов предварительной обработки данных существенно меняет исходную длину ключа. При малых значениях ошибки все графики практически совпадают.

и зависит от двух параметров — p и q. Информация на приемной стороне с учетом (4) равна

$$I_{AB}(p,q) = 1 - h\big((1-p)q + (1-q)p\big) = 1 + Q\log Q + (1-Q)\log(1-Q).$$

Вычисления показывают, что при использовании дополнительного шума критическая величина ошибки, до которой возможно секретное распространение ключей, увеличивается примерно до 12,4 %, что соответствует результатам, изложенным в [4]. Отношение длины секретного ключа к общей длине передаваемой последовательности с учетом потерь, вызванных дополнительным шумом, равна

$$\frac{r}{n}(q) = \max_p \left(1 - h\big((1-p)q + (1-q)p\big) - 2h(q) - \sum_{i=1}^{4} \lambda_i \log \lambda_i\right).$$

На рисунке 2 пунктирной линией показан график зависимости длины секретного ключа от ошибки на приемной стороне без предварительной обработки данных и с внесением дополнительного шума. Увеличение длины секретного ключа достигается только там, где исходная ошибка близка к критической, в случае же небольшой исходной ошибки внесение дополнительного шума оказывается нецелесообразным.

1.2 Блочное исправление ошибок

При блочном исправлении ошибок с длиной блока, равной N, ошибка на стороне Боба будет равна

$$Q = \frac{q^N}{(1-q)^N + q^N}. \tag{6}$$

При этом, поскольку все блоки с разными исходами измерений на стороне Боба отбрасываются, Ева будет стоять перед необходимостью различать состояния, соответствующие получению только правильных или только ошибочных исходов. Это состояния

$$\begin{aligned}\rho_x^E &= (1-Q)|\psi_x\rangle^{\otimes N}\langle\psi_x|^{\otimes N} + Q|\theta_x\rangle^{\otimes N}\langle\theta_x|^{\otimes N},\\ \rho_y^E &= (1-Q)|\psi_y\rangle^{\otimes N}\langle\psi_y|^{\otimes N} + Q|\theta_y\rangle^{\otimes N}\langle\theta_y|^{\otimes N}.\end{aligned} \tag{7}$$

Так как состояния $|\psi_i\rangle$ и $|\theta_j\rangle$ взаимно ортогональны, собственные значения каждого из операторов плотности (7) будут равны

$$\lambda_1 = \frac{(1-q)^N}{(1-q)^N + q^N}, \quad \lambda_2 = \frac{q^N}{(1-q)^N + q^N}.$$

Далее, так как $\langle\psi_x^{\otimes N}|\psi_y\rangle^{\otimes N} = (\langle\psi_x|\psi_y\rangle)^N = \varepsilon^N$, нетрудно видеть, что собственные значения оператора-«полусуммы» $\rho^E = \frac{1}{2}(\rho_x^E + \rho_y^E)$, необходимые для подсчета величины Холево, равны

$$\begin{aligned}\lambda_{1,2} &= \frac{(1-q)^N}{(1-q)^N + q^N} \cdot \frac{1 \pm \varepsilon^N}{2},\\ \lambda_{3,4} &= \frac{q^N}{(1-q)^N + q^N} \cdot \frac{1 \pm \varepsilon^N}{2},\end{aligned} \tag{8}$$

а с учетом (1) их можно выразить только через q и параметр процедуры N. Взаимная информация Алисы и Боба равна

$$I_{AB} = 1 - h(Q) = 1 - h\left(\frac{q^N}{(1-q)^N + q^N}\right),$$

а значит, разность взаимных информаций между Алисой и Бобом и между Алисой и Евой

$$I_{AB} - I_{AE} = 1 - h(Q) - H(\rho^E) + h(Q) = 1 - H(\rho^E) = 1 + \sum_{i=1}^{4} \lambda_i \log \lambda_i$$

зависит только от собственных значений оператора ρ^E.

Длина финального ключа при использовании блочного исправления ошибок падает как из-за объединения битов исходной последовательности в блоки, так и из-за отбрасывания части блоков, значения битов в которых оказались разными. Окончательное отношение длины секретного ключа к длине последовательности при использовании блоков длины N равно

$$\frac{r}{n}(q, N) = \frac{(1-q)^N + q^N}{N}(1 - H(\rho^E)).$$

После максимизации по всем возможным длинам блоков (на практике нет существенной пользы от использования блоков длиной свыше 5) получаем

$$\frac{r}{n}(q) = \max_N \frac{(1-q)^N + q^N}{N}(1 - H(\rho^E)). \tag{9}$$

На рисунке 2 штрихпунктирная линия соответствует зависимости длины секретного ключа при использовании метода блочного исправления ошибок. Как можно видеть из графика, этот метод способен увеличить критическую ошибку сильнее, чем метод внесения дополнительного шума. Критическая ошибка при использовании блочного исправления ошибок возрастает примерно до 20 %, однако следует принимать во внимание, что для подобного увеличения критической ошибки нужно использовать блоки большой длины, что сильно уменьшает длину финального ключа.

1.3 Комбинирование методов

Технологии внесения дополнительного шума и блочного исправления ошибок можно объединить двумя способами. Эти способы отличаются порядком действий: можно сначала внести дополнительный шум в канал, а затем провести блочное исправление ошибок, либо наоборот: сначала объединить позиции исходной последовательности в блоки и согласовать значения битов в каждом из них, а затем внести в канал дополнительный шум. Как показывают вычисления, первый способ не дает никакой пользы, в то время как второй способен сделать величину критической ошибки протокола BB84 еще выше. В этом разделе будет рассмотрен только второй способ.

Состояния Евы, получающиеся после измерения Боба с исправлением ошибок блоками по N бит и внесения дополнительного шума, задаются комбинацией состояний (5) и (7):

$$\begin{aligned}
\rho_0^E &= (1-p)\left[\frac{(1-q)^N}{(1-q)^N+q^N}|\psi_x\rangle^{\otimes N}\langle\psi_x|^{\otimes N} + \frac{q^N}{(1-q)^N+q^N}|\theta_x\rangle^{\otimes N}\langle\theta_x|^{\otimes N}\right] + \\
&\quad + p\left[\frac{(1-q)^N}{(1-q)^N+q^N}|\psi_y\rangle^{\otimes N}\langle\psi_y|^{\otimes N} + \frac{q^N}{(1-q)^N+q^N}|\theta_y\rangle^{\otimes N}\langle\theta_y|^{\otimes N}\right], \\
\rho_1^E &= (1-p)\left[\frac{(1-q)^N}{(1-q)^N+q^N}|\psi_y\rangle^{\otimes N}\langle\psi_y|^{\otimes N} + \frac{q^N}{(1-q)^N+q^N}|\theta_y\rangle^{\otimes N}\langle\theta_y|^{\otimes N}\right] + \\
&\quad + p\left[\frac{(1-q)^N}{(1-q)^N+q^N}|\psi_x\rangle^{\otimes N}\langle\psi_x|^{\otimes N} + \frac{q^N}{(1-q)^N+q^N}|\theta_x\rangle^{\otimes N}\langle\theta_x|^{\otimes N}\right].
\end{aligned} \tag{10}$$

Собственные значения этих операторов (их матрицы проще всего выглядят в базисе $\{|\psi_0^N\rangle, |\psi_1^N\rangle, |\theta_0^N\rangle, |\theta_1^N\rangle\}$, симметричном относительно векторов $|\psi_i\rangle^{\otimes N}$ и $|\theta_i\rangle^{\otimes N}$, подобно базису на рисунке 1, построенному для векторов $|\psi_i\rangle$ и $|\theta_i\rangle$) равны

$$\begin{aligned}
\mu_{1,2} &= \frac{1}{2}\frac{(1-q)^N}{(1-q)^N+q^N}\left(1 \pm \sqrt{1-4p(1-p)(1-\varepsilon^{2N})}\right), \\
\mu_{3,4} &= \frac{1}{2}\frac{q^N}{(1-q)^N+q^N}\left(1 \pm \sqrt{1-4p(1-p)(1-\varepsilon^{2N})}\right).
\end{aligned}$$

Собственные значения оператора $\rho^E = \frac{1}{2}(\rho_x^E + \rho_y^E)$ так же, как и в случае отсутствия шума, равны (8). В итоге для длины секретного ключа получаем

$$\frac{r}{n}(q) = \max_N \frac{(1-q)^N+q^N}{N}\left[1 - h\left(\frac{q^N}{(1-q)^N+q^N}\right) + \sum_{i=1}^{4}(\lambda_i \log \lambda_i - \mu_i \log \mu_i)\right]. \tag{11}$$

На рисунке 2 штриховой линией показан график зависимости длины ключа от ошибки на приемной стороне при комбинировании методов предварительной обработки данных. Как может быть видно из этого графика, это позволяет добиться дополнительного увеличения длины секретного ключа. Критическая ошибка, до которой возможна генерация секретного ключа, при комбинировании методов оказывается равной приблизительно 23%, но, как и в случае блочного исправления ошибок, достигается лишь для больших длин блоков, не дающих большой практической пользы из-за малой длины конечного секретного ключа.

2 Протокол с фазово-временным кодированием

Протокол с фазово-временным кодированием, предложенный в [8], использует 4 базиса, которые разделены на 2 группы: «левые» и «правые». Для передачи состояний используется три временных окна, которые обозначаются как $|1\rangle$, $|2\rangle$, $|3\rangle$. Состояния из левого базиса являются комбинациями первых двух временных окон, состояния из правого базиса — комбинацией второго и третьего окна (рисунок 3).

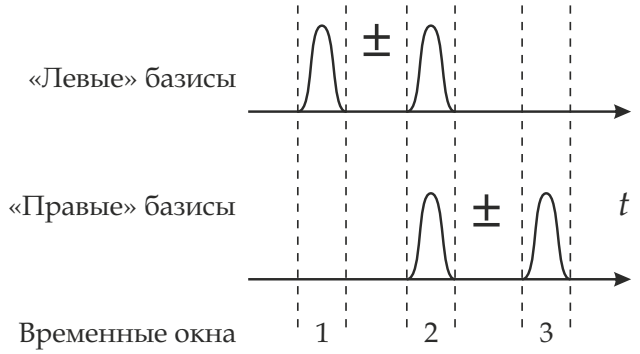


Рис. 3. Конфигурация базисных состояний в протоколе с фазово-временным кодированием.

Существует две версии протокола с фазово-временным кодированием. Первая из них использует ортогональные состояния внутри каждого базиса. Эти состояния равны

$$|0^{+L}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \qquad |0^{+R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + |3\rangle),$$
$$|1^{+L}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \qquad |1^{+R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - |3\rangle),$$
$$|0^{\times L}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle), \qquad |0^{\times R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + i|3\rangle),$$
$$|1^{\times L}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i|2\rangle), \qquad |1^{\times R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - i|3\rangle).$$

Как видно из приведенных формул, конфигурация состояний только в левых или только в правых базисах аналогична их расположению в протоколе BB84. На приемной стороне Боб случайным образом выбирает один из четырех базисов измерения: $\{+L, \times L, +R, \times R\}$. Наряду с информационным исходом он может получить отсчет в контрольном временном окне: результат 3 для состояния из левого базиса и результат 1 для правого. Для примера, оператор измерения в базисе «$+L$» выглядит так:

$$I = M_0^{+L} + M_1^{+L} + M_c = (|1\rangle + |2\rangle)(\langle 1| + \langle 2|) + (|1\rangle - |2\rangle)(\langle 1| - \langle 2|) + |3\rangle\langle 3|.$$

Неортогональная версия протокола с фазово-временным кодированием использует конфигурацию векторов в каждой паре базисов, похожую на их расположение в протоколе SARG04 [6], а именно

$$|0^{L_a}\rangle = \cos\frac{\eta}{2}|1\rangle + \sin\frac{\eta}{2}|2\rangle, \qquad |0^{R_a}\rangle = \cos\frac{\eta}{2}|2\rangle + \sin\frac{\eta}{2}|3\rangle,$$
$$|1^{L_a}\rangle = \cos\frac{\eta}{2}|1\rangle - \sin\frac{\eta}{2}|2\rangle, \qquad |1^{R_a}\rangle = \cos\frac{\eta}{2}|2\rangle - \sin\frac{\eta}{2}|3\rangle,$$
$$|0^{L_b}\rangle = \sin\frac{\eta}{2}|1\rangle - \cos\frac{\eta}{2}|2\rangle, \qquad |0^{R_b}\rangle = \sin\frac{\eta}{2}|2\rangle - \cos\frac{\eta}{2}|3\rangle,$$
$$|1^{L_b}\rangle = \sin\frac{\eta}{2}|1\rangle + \cos\frac{\eta}{2}|2\rangle, \qquad |1^{R_b}\rangle = \sin\frac{\eta}{2}|2\rangle + \cos\frac{\eta}{2}|3\rangle.$$

В этой версии угол между состояниями в каждом базисе равен η. Цель такой конфигурации — противодействие PNS-атаке [1], возможной при не строго однофотонных источниках и потерях в канале связи.

На приемной стороне Боб предпринимает «измерение с тремя исходами», которое при отсутствии ошибки в канале с некоторой вероятностью дает безошибочный результат, либо дает несовместный исход, когда конкретный результат получить не удалось. Также может быть

получен отсчет в контрольном временном окне. Так, для базиса «L_a», с учетом того, что состояния $|0^{L_a}\rangle$ и $|0^{L_b}\rangle$ ортогональны, получаем следующее разложение единицы:

$$I = M_0^{L_a} + M_1^{L_a} + M_?^{L_a} + M_c^{L_a},$$

где

$$M_0^{L_a} = \frac{|1^{L_a\perp}\rangle\langle 1^{L_a\perp}|}{1+\cos\eta} = \frac{|0^{L_b}\rangle\langle 0^{L_b}|}{1+\cos\eta},$$
$$M_1^{L_a} = \frac{|0^{L_a\perp}\rangle\langle 0^{L_a\perp}|}{1+\cos\eta} = \frac{|1^{L_b}\rangle\langle 1^{L_b}|}{1+\cos\eta},$$
$$M_?^{L_a} = |1\rangle\langle 1| + |2\rangle\langle 2| - M_0^{L_a} - M_1^{L_a},$$
$$M_c^{L_a} = |3\rangle\langle 3|.$$

Как показал анализ стойкости ортогональной [9] и неортогональной [7] версий протокола, при отсутствии отсчетов в контрольных временных окнах секретное распространение ключей возможно, когда ошибка на приемной стороне не превышает 50 %, что соответствует теоретическому пределу. При увеличении числа контрольных отсчетов критическая величина ошибки снижается.

Отметим, что для оценки стойкости и нахождения области секретности достаточно рассматривать только версию протокола с произвольным углом η между сигнальными состояниями: при значении этого угла, равном $\pi/2$, все результаты будут соответствовать результатам для ортогональной версии.

В этом разделе уже рассмотренные выше на примере BB84 методы предварительной обработки данных будут применены к протоколу с фазово-временным кодированием.

2.1 Схема оптимальной атаки

Коллективная атака на протокол с фазово-временным кодированием со всеми подробностями была рассмотрена в [7]. Напомним здесь основные выкладки этого построения.

Унитарное преобразование подслушивателя может быть расписано по временным окнам следующим образом:

$$U_E|1\rangle = |\widetilde{1}\rangle = |1\rangle|\psi_1^1\rangle + |2\rangle|\psi_2^1\rangle + |3\rangle|\psi_3^1\rangle,$$
$$U_E|2\rangle = |\widetilde{2}\rangle = |1\rangle|\psi_1^2\rangle + |2\rangle|\psi_2^2\rangle + |3\rangle|\psi_3^2\rangle,$$
$$U_E|3\rangle = |\widetilde{3}\rangle = |1\rangle|\psi_1^3\rangle + |2\rangle|\psi_2^3\rangle + |3\rangle|\psi_3^3\rangle.$$

При отправлении базисных состояний $|0_{La}\rangle$ и $|1_{La}\rangle$ они преобразуются в состояния

$$U_E|0_{La}\rangle = U_E(\cos\frac{\eta}{2}|1\rangle + \sin\frac{\eta}{2}|2\rangle) = |\widetilde{0_{La}}\rangle =$$
$$= |1\rangle(\cos\frac{\eta}{2}|\psi_1^1\rangle + \sin\frac{\eta}{2}|\psi_1^2\rangle) + |2\rangle(\cos\frac{\eta}{2}|\psi_2^1\rangle + \sin\frac{\eta}{2}|\psi_2^2\rangle) + |3\rangle(\cos\frac{\eta}{2}|\psi_3^1\rangle + \sin\frac{\eta}{2}|\psi_3^2\rangle),$$

$$U_E|1_{La}\rangle = U_E(\cos\frac{\eta}{2}|1\rangle - \sin\frac{\eta}{2}|2\rangle) = |\widetilde{1_{La}}\rangle =$$
$$= |1\rangle(\cos\frac{\eta}{2}|\psi_1^1\rangle - \sin\frac{\eta}{2}|\psi_1^2\rangle) + |2\rangle(\cos\frac{\eta}{2}|\psi_2^1\rangle - \sin\frac{\eta}{2}|\psi_2^2\rangle) + |3\rangle(\cos\frac{\eta}{2}|\psi_3^1\rangle - \sin\frac{\eta}{2}|\psi_3^2\rangle).$$

Операторы измерения Боба, отвечающие совместным исходам, записываются в этом базисе как

$$M_0^{La} = \frac{1}{1+\cos\eta}\left[\sin^2\frac{\eta}{2}|1\rangle\langle 1| + \cos^2\frac{\eta}{2}|2\rangle\langle 2| + \sin\frac{\eta}{2}\cos\frac{\eta}{2}(|1\rangle\langle 2| + |2\rangle\langle 1|)\right],$$
$$M_1^{La} = \frac{1}{1+\cos\eta}\left[\sin^2\frac{\eta}{2}|1\rangle\langle 1| + \cos^2\frac{\eta}{2}|2\rangle\langle 2| - \sin\frac{\eta}{2}\cos\frac{\eta}{2}(|1\rangle\langle 2| + |2\rangle\langle 1|)\right].$$

Состояния Евы после применения этих операторов равны

$$\rho^{OK}_{0_{La}} = \mathrm{Tr}_E\left[\frac{\sqrt{M^0_{La}}|\widetilde{0_{La}}\rangle\langle\widetilde{0_{La}}|\sqrt{M^0_{La}}^{\dagger}}{\langle\widetilde{0_{La}}|M^0_{La}|\widetilde{0_{La}}\rangle}\right] = \frac{1}{(1-2q)\sin^2\eta + q\cos^2\eta}\times$$
$$\times\Big[\cos^2\frac{\eta}{2}\sin^2\frac{\eta}{2}\left(|\psi^1_1\rangle\langle\psi^1_1| + |\psi^2_2\rangle\langle\psi^2_2| + |\psi^1_1\rangle\langle\psi^2_2| + |\psi^2_2\rangle\langle\psi^1_1| + |\psi^1_2\rangle\langle\psi^2_1| + |\psi^2_1\rangle\langle\psi^1_2|\right) +$$
$$+\cos^4\frac{\eta}{2}|\psi^1_2\rangle\langle\psi^1_2| + \sin^4\frac{\eta}{2}|\psi^2_1\rangle\langle\psi^2_1| +$$
$$+\cos\frac{\eta}{2}\sin^3\frac{\eta}{2}\left(|\psi^1_1\rangle\langle\psi^2_1| + |\psi^2_1\rangle\langle\psi^1_1| + |\psi^2_1\rangle\langle\psi^2_2| + |\psi^2_2\rangle\langle\psi^2_1|\right) +$$
$$+\cos^3\frac{\eta}{2}\sin\frac{\eta}{2}\left(|\psi^1_1\rangle\langle\psi^1_2| + |\psi^1_2\rangle\langle\psi^1_1| + |\psi^1_2\rangle\langle\psi^2_2| + |\psi^2_2\rangle\langle\psi^1_2|\right)\Big],$$

$$\rho^{Err}_{0_{La}} = \mathrm{Tr}_E\left[\frac{\sqrt{M^1_{La}}|\widetilde{0_{La}}\rangle\langle\widetilde{0_{La}}|\sqrt{M^1_{La}}^{\dagger}}{\langle\widetilde{0_{La}}|M^1_{La}|\widetilde{0_{La}}\rangle}\right] = \frac{1}{q}\times$$
$$\times\Big[\cos^2\frac{\eta}{2}\sin^2\frac{\eta}{2}\left(|\psi^1_1\rangle\langle\psi^1_1| + |\psi^2_2\rangle\langle\psi^2_2| - |\psi^1_1\rangle\langle\psi^2_2| - |\psi^2_2\rangle\langle\psi^1_1| - |\psi^1_2\rangle\langle\psi^2_1| - |\psi^2_1\rangle\langle\psi^1_2|\right) +$$
$$+\cos^4\frac{\eta}{2}|\psi^1_2\rangle\langle\psi^1_2| + \sin^4\frac{\eta}{2}|\psi^2_1\rangle\langle\psi^2_1| -$$
$$-\cos\frac{\eta}{2}\sin^3\frac{\eta}{2}\left(|\psi^1_1\rangle\langle\psi^2_1| + |\psi^2_1\rangle\langle\psi^1_1| + |\psi^2_1\rangle\langle\psi^2_2| + |\psi^2_2\rangle\langle\psi^2_1|\right) -$$
$$-\cos^3\frac{\eta}{2}\sin\frac{\eta}{2}\left(|\psi^1_1\rangle\langle\psi^1_2| + |\psi^1_2\rangle\langle\psi^1_1| + |\psi^1_2\rangle\langle\psi^2_2| + |\psi^2_2\rangle\langle\psi^1_2|\right)\Big],$$

$$\rho^{OK}_{1_{La}} = \mathrm{Tr}_E\left[\frac{\sqrt{M^1_{La}}|\widetilde{1_{La}}\rangle\langle\widetilde{1_{La}}|\sqrt{M^1_{La}}^{\dagger}}{\langle\widetilde{1_{La}}|M^1_{La}|\widetilde{1_{La}}\rangle}\right] = \frac{1}{(1-2q)\sin^2\eta + q\cos^2\eta}\times$$
$$\times\Big[\cos^2\frac{\eta}{2}\sin^2\frac{\eta}{2}\left(|\psi^1_1\rangle\langle\psi^1_1| + |\psi^2_2\rangle\langle\psi^2_2| + |\psi^1_1\rangle\langle\psi^2_2| + |\psi^2_2\rangle\langle\psi^1_1| + |\psi^1_2\rangle\langle\psi^2_1| + |\psi^2_1\rangle\langle\psi^1_2|\right) +$$
$$+\cos^4\frac{\eta}{2}|\psi^1_2\rangle\langle\psi^1_2| + \sin^4\frac{\eta}{2}|\psi^2_1\rangle\langle\psi^2_1| -$$
$$-\cos\frac{\eta}{2}\sin^3\frac{\eta}{2}\left(|\psi^1_1\rangle\langle\psi^2_1| + |\psi^2_1\rangle\langle\psi^1_1| + |\psi^2_1\rangle\langle\psi^2_2| + |\psi^2_2\rangle\langle\psi^2_1|\right) -$$
$$-\cos^3\frac{\eta}{2}\sin\frac{\eta}{2}\left(|\psi^1_1\rangle\langle\psi^1_2| + |\psi^1_2\rangle\langle\psi^1_1| + |\psi^1_2\rangle\langle\psi^2_2| + |\psi^2_2\rangle\langle\psi^1_2|\right)\Big],$$

$$\rho^{Err}_{1_{La}} = \mathrm{Tr}_E\left[\frac{\sqrt{M^0_{La}}|\widetilde{1_{La}}\rangle\langle\widetilde{1_{La}}|\sqrt{M^0_{La}}^{\dagger}}{\langle\widetilde{1_{La}}|M^0_{La}|\widetilde{1_{La}}\rangle}\right] = \frac{1}{q}\times$$
$$\times\Big[\cos^2\frac{\eta}{2}\sin^2\frac{\eta}{2}\left(|\psi^1_1\rangle\langle\psi^1_1| + |\psi^2_2\rangle\langle\psi^2_2| - |\psi^1_1\rangle\langle\psi^2_2| - |\psi^2_2\rangle\langle\psi^1_1| - |\psi^1_2\rangle\langle\psi^2_1| - |\psi^2_1\rangle\langle\psi^1_2|\right) +$$
$$+\cos^4\frac{\eta}{2}|\psi^1_2\rangle\langle\psi^1_2| + \sin^4\frac{\eta}{2}|\psi^2_1\rangle\langle\psi^2_1| +$$
$$+\cos\frac{\eta}{2}\sin^3\frac{\eta}{2}\left(|\psi^1_1\rangle\langle\psi^2_1| + |\psi^2_1\rangle\langle\psi^1_1| + |\psi^2_1\rangle\langle\psi^2_2| + |\psi^2_2\rangle\langle\psi^2_1|\right) +$$
$$+\cos^3\frac{\eta}{2}\sin\frac{\eta}{2}\left(|\psi^1_1\rangle\langle\psi^1_2| + |\psi^1_2\rangle\langle\psi^1_1| + |\psi^1_2\rangle\langle\psi^2_2| + |\psi^2_2\rangle\langle\psi^1_2|\right)\Big]$$

Будем использовать следующий ортонормированный базис для выписывания элементов приведенных матриц: $\{|\mu_1\rangle, |\mu_2\rangle, |\nu_1\rangle, |\nu_2\rangle\}$, где векторы удовлетворяют соотношениям

$$\langle\mu_1|\psi^1_1\rangle = \sqrt{1-2q}\cos a = \langle\mu_2|\psi^2_2\rangle,$$
$$\langle\mu_1|\psi^2_2\rangle = \sqrt{1-2q}\sin a = \langle\mu_2|\psi^1_1\rangle,$$

$$\langle\nu_1|\psi_2^1\rangle = \sqrt{1-2q}\cos b = \langle\nu_2|\psi_1^2\rangle,$$
$$\langle\nu_1|\psi_1^2\rangle = \sqrt{1-2q}\sin b = \langle\nu_2|\psi_2^1\rangle,$$

и параметры a и b выражаются через параметры перехватчика $\cos\alpha = \langle\psi_1^1|\psi_2^2\rangle$ и $\cos\beta = \langle\nu_1|\psi_2^1\rangle$ как

$$a = \frac{\pi}{4} - \frac{\alpha}{2}, \qquad b = \frac{\pi}{4} - \frac{\beta}{2}.$$

В свою очередь параметры q, α и β связаны соотношением

$$1 - 3q = (1-2q)\cos\alpha + q\cos\beta.$$

Для краткости введем следующие обозначения:

$$\begin{aligned}
m_1 &= \sqrt{1-2q}\cos\frac{\eta}{2}\sin\frac{\eta}{2}(\cos a + \sin a) = \frac{1}{2}\sqrt{1-2q}\sin\eta\sqrt{1+\cos\alpha},\\
m_2 &= \sqrt{1-2q}\cos\frac{\eta}{2}\sin\frac{\eta}{2}(\cos a - \sin a) = \frac{1}{2}\sqrt{1-2q}\sin\eta\sqrt{1-\cos\alpha},\\
n_1 &= \sqrt{q}(\sin^2\frac{\eta}{2}\sin b + \cos^2\frac{\eta}{2}\cos b) = \frac{1}{2}\sqrt{q}\left(\sqrt{1+\cos\beta} + \cos\eta\sqrt{1-\cos\beta}\right),\\
n_2 &= \sqrt{q}(\sin^2\frac{\eta}{2}\cos b + \cos^2\frac{\eta}{2}\sin b) = \frac{1}{2}\sqrt{q}\left(\sqrt{1+\cos\beta} - \cos\eta\sqrt{1-\cos\beta}\right),\\
k_1 &= \sqrt{q}(\sin^2\frac{\eta}{2}\sin b - \cos^2\frac{\eta}{2}\cos b) = \frac{1}{2}\sqrt{q}\left(-\sqrt{1-\cos\beta} - \cos\eta\sqrt{1+\cos\beta}\right),\\
k_2 &= \sqrt{q}(\sin^2\frac{\eta}{2}\cos b - \cos^2\frac{\eta}{2}\sin b) = \frac{1}{2}\sqrt{q}\left(\sqrt{1-\cos\beta} - \cos\eta\sqrt{1+\cos\beta}\right).
\end{aligned}$$

Матрицы плотности, соответствующие каждому из исходов Боба при посылке сигналов 0 и 1 теперь можно записать как

$$\begin{aligned}
\rho_{0_{La}}^{OK} &= \frac{1}{(1-2q)\sin^2\eta + q\cos^2\eta}\begin{pmatrix} m_1^2 & m_1^2 & m_1n_1 & m_1n_2\\ m_1^2 & m_1^2 & m_1n_1 & m_1n_2\\ m_1n_1 & m_1n_1 & n_1^2 & n_1n_2\\ m_1n_2 & m_1n_2 & n_1n_2 & n_2^2\end{pmatrix},\\
\rho_{0_{La}}^{Err} &= \frac{1}{q}\begin{pmatrix} m_2^2 & -m_2^2 & m_2k_1 & m_2k_2\\ -m_2^2 & m_2^2 & -m_2k_1 & -m_2k_2\\ m_2k_1 & -m_2k_1 & k_1^2 & k_1k_2\\ m_2k_2 & -m_2k_2 & k_1k_2 & k_2^2\end{pmatrix},\\
\rho_{1_{La}}^{OK} &= \frac{1}{(1-2q)\sin^2\eta + q\cos^2\eta}\begin{pmatrix} m_1^2 & m_1^2 & -m_1n_1 & -m_1n_2\\ m_1^2 & m_1^2 & -m_1n_1 & -m_1n_2\\ -m_1n_1 & -m_1n_1 & n_1^2 & n_1n_2\\ -m_1n_2 & -m_1n_2 & n_1n_2 & n_2^2\end{pmatrix},\\
\rho_{1_{La}}^{Err} &= \frac{1}{q}\begin{pmatrix} m_2^2 & -m_2^2 & -m_2k_1 & -m_2k_2\\ -m_2^2 & m_2^2 & m_2k_1 & m_2k_2\\ -m_2k_1 & m_2k_1 & k_1^2 & k_1k_2\\ -m_2k_2 & m_2k_2 & k_1k_2 & k_2^2\end{pmatrix}.
\end{aligned} \tag{12}$$

Для подсчета информации Холево требуется знать собственные значения трех матриц:

$$\begin{aligned}
\rho_{0_{La}} &= Pr(0|0)\rho_{0_{La}}^{OK} + Pr(1|0)\rho_{0_{La}}^{Err} = \\
&= \begin{pmatrix} m_1^2+m_2^2 & m_1^2-m_2^2 & m_1n_1+m_2k_1 & m_1n_2+m_2k_2 \\ m_1^2-m_2^2 & m_1^2+m_2^2 & m_1n_1-m_2k_1 & m_1n_2-m_2k_2 \\ m_1n_1+m_2k_1 & m_1n_1-m_2k_1 & n_1^2+k_1^2 & n_1n_2+k_1k_2 \\ m_1n_2+m_2k_2 & m_1n_2-m_2k_2 & n_1n_2+k_1k_2 & n_2^2+k_2^2 \end{pmatrix}, \\
\rho_{1_{La}} &= Pr(1|1)\rho_{1_{La}}^{OK} + Pr(0|1)\rho_{1_{La}}^{Err} = \\
&= \begin{pmatrix} m_1^2+m_2^2 & m_1^2-m_2^2 & -m_1n_1-m_2k_1 & -m_1n_2-m_2k_2 \\ m_1^2-m_2^2 & m_1^2+m_2^2 & -m_1n_1+m_2k_1 & -m_1n_2+m_2k_2 \\ -m_1n_1-m_2k_1 & -m_1n_1+m_2k_1 & n_1^2+k_1^2 & n_1n_2+k_1k_2 \\ -m_1n_2-m_2k_2 & -m_1n_2+m_2k_2 & n_1n_2+k_1k_2 & n_2^2+k_2^2 \end{pmatrix}, \\
\rho_{La} &= \frac{1}{2}(\rho_{0_{La}}+\rho_{1_{La}}) = \begin{pmatrix} m_1^2+m_2^2 & m_1^2-m_2^2 & 0 & 0 \\ m_1^2-m_2^2 & m_1^2+m_2^2 & 0 & 0 \\ 0 & 0 & n_1^2+k_1^2 & n_1n_2+k_1k_2 \\ 0 & 0 & n_1n_2+k_1k_2 & n_2^2+k_2^2 \end{pmatrix}.
\end{aligned} \tag{13}$$

Собственные значения матриц $\rho_{0_{La}}$ и $\rho_{1_{La}}$ совпадают и равны

$$\mu_{1,2} = \frac{1}{2}\left(1 \pm \sqrt{1+4c^2-4\gamma\delta}\right),$$

где для краткости введены обозначения

$$\begin{aligned}
\gamma &= \frac{(1-2q)\sin^2\eta}{(1-2q)\sin^2\eta + q\cos^2\eta + q}, \\
\delta &= \frac{q(\cos^2\eta+1)}{(1-2q)\sin^2\eta + q\cos^2\eta + q}, \\
c &= \frac{\sqrt{q(1-2q)}\sin\eta\cos\eta}{(1-2q)\sin^2\eta + q\cos^2\eta + q},
\end{aligned}$$

а собственные значения оператора ρ_{La} равны

$$\begin{aligned}
\lambda_{1,2} &= \frac{\gamma}{2}(1 \pm \cos\alpha), \\
\lambda_{3,4} &= \frac{\delta}{2}\left(1 \pm \frac{\sqrt{4\cos^2\eta + \cos^2\beta\sin^4\eta}}{1+\cos^2\eta}\right).
\end{aligned}$$

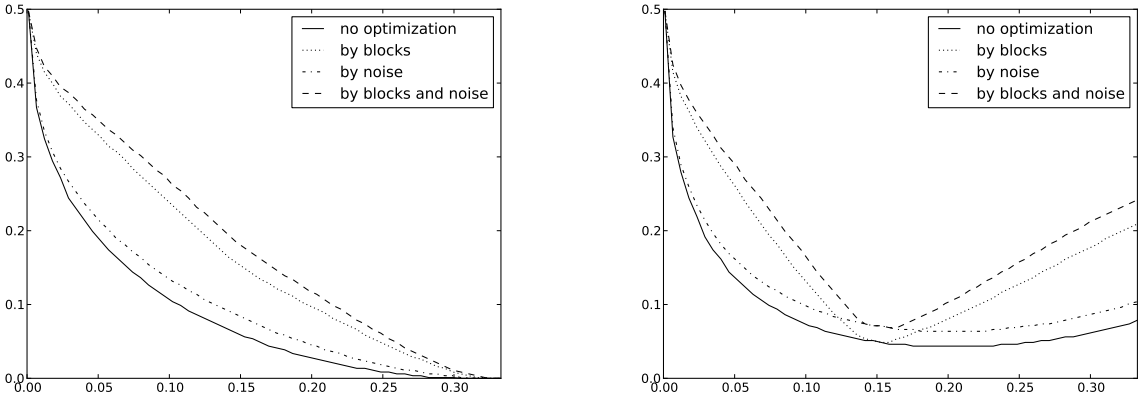
Из приведенных выражений легко получить формулу для величины Холево

$$\chi(\{\rho_{0_{La}}, \rho_{1_{La}}\}) = -\sum_{i=1}^{4}\lambda_i\log\lambda_i + \mu_1\log\mu_1 + \mu_2\log\mu_2. \tag{14}$$

На рисунке 4 сплошными линиями приведены границы области секретности для протокола с фазово-временным кодированием на плоскости (Q, q) для значений угла между информационными состояниями внутри базиса $\eta = \pi/2$ и $\eta = \pi/4$.

2.2 Внесение дополнительного шума

Посмотрим, как на состояния в пространстве Евы будет действовать дополнительный шум, внесенный Алисой и Бобом. Если без шума Ева стоит перед задачей различения состояний (13),



а *б*

Рис. 4. Границы области секретности протокола квантового распределения ключей с фазово-временным кодированием: *(а)* ортогональный случай, *(б)* значение угла $\eta = \pi/4$. Сплошными линиями показаны зависимости критической ошибки от контрольных отсчетов без использования предварительной обработки данных, штрихпунктирными линиями — при внесении дополнительного шума, пунктирными линиями — после блочного исправления ошибок, штриховыми линиями — после сочетания методов предварительной обработки данных.

то после внесения шума, подобно тому, как это происходит в протоколе BB84, состояния Евы будут равны

$$\begin{aligned}\rho_{0_{La}} &= (1-p)\left[Pr(0|0)\rho_{0_{La}}^{OK} + Pr(1|0)\rho_{0_{La}}^{Err}\right] + p\left[Pr(1|1)\rho_{1_{La}}^{OK} + Pr(0|1)\rho_{1_{La}}^{Err}\right] \\ \rho_{1_{La}} &= (1-p)\left[Pr(1|1)\rho_{1_{La}}^{OK} + Pr(0|1)\rho_{1_{La}}^{Err}\right] + p\left[Pr(0|0)\rho_{0_{La}}^{OK} + Pr(1|0)\rho_{0_{La}}^{Err}\right]\end{aligned} \tag{15}$$

Как видно, оператор плотности $\rho_{La} = \frac{1}{2}(\rho_{0_{La}} + \rho_{1_{La}})$ будет иметь тот же вид, что и без внесения шума, а собственные значения частичных состояний (15) изменятся. Для нахождения этих собственных значений необходимо решить алгебраические уравнения четвертой степени. Методы решения подобных уравнений хорошо известны.

На рисунке 4 штрихпунктирной линией показана область секретности протокола с фазово-временным кодированием при использовании дополнительного шума.

2.3 Блочное исправление ошибок

Как было показано на примере протокола BB84, при использовании блочного исправления ошибок можно добиться большего увеличения критической ошибки протокола, чем при использовании дополнительного шума. В случае протокола с фазово-временным кодированием это означает большее увеличение площади области секретности протокола по сравнению с отсутствием предварительной обработки данных.

Ошибка Боба при исправлении ошибки блоками длины N дается аналогичным (6) выражением

$$\widetilde{Q} = \frac{Q^N}{(1-Q)^N + Q^N}. \tag{16}$$

В то же время из-за неортогональности состояний (12) операторы плотности Евы после измерения Боба уже не будут представляться в виде суммы ортогональных состояний, как это было в случае протокола BB84. Выражение, аналогичное (7), принимает вид

$$\begin{aligned}\rho_0^E &= (1-\widetilde{Q})(\rho_0^{OK})^{\otimes N} + \widetilde{Q}(\rho_0^{Err})^{\otimes N}, \\ \rho_1^E &= (1-\widetilde{Q})(\rho_1^{OK})^{\otimes N} + \widetilde{Q}(\rho_1^{Err})^{\otimes N},\end{aligned}$$

где ρ_i^{OK} и ρ_0^{Err} даются выражениями (12).

Собственные значения этих операторов и оператора плотности $\rho_{La} = \frac{1}{2}(\rho_{0_{La}} + \rho_{1_{La}})$ вычисляются численно. На рисунке 4 пунктирной линией показана граница области секретности для протокола с фазово-временным кодированием после оптимизации по блокам, длина которых N принимает значения от 1 до 4.

2.4 Комбинирование методов

Так же, как и в случае протокола BB84, будем рассматривать случай блочного исправления ошибок, после которого следует внесение дополнительного шума. При сочетании этих методов предварительной обработки данных состояния перехватчика будут даваться выражением, подобным (10):

$$\rho_0^E = (1-p)\left[(1-\widetilde{Q})(\rho_0^{OK})^{\otimes N} + \widetilde{Q}(\rho_0^{Err})^{\otimes N}\right] + p\left[(1-\widetilde{Q})(\rho_1^{OK})^{\otimes N} + \widetilde{Q}(\rho_1^{Err})^{\otimes N}\right],$$
$$\rho_1^E = (1-p)\left[(1-\widetilde{Q})(\rho_1^{OK})^{\otimes N} + \widetilde{Q}(\rho_1^{Err})^{\otimes N}\right] + p\left[(1-\widetilde{Q})(\rho_0^{OK})^{\otimes N} + \widetilde{Q}(\rho_0^{Err})^{\otimes N}\right].$$

Как и при блочном исправлении ошибок, явным образом вычислить собственные значения этих операторов затруднительно, и приходится прибегать к численным методам. Отметим, что практическая значимость длины блока более 5 невелика, так как это не ведет к существенному изменению области секретности. На рисунке 4 штриховой линией показана граница области секретности при использовании шума и блоков длиной от 1 до 4. Как видно из рисунка, комбинирование методов позволяет расширить область секретности протокола с фазово-временным кодированием.

Заключение

В статье были получены области секретности на плоскости наблюдаемых параметров для ортогональной и неортогональной версий протокола квантового распределения ключей с фазово-временным кодированием с учетом возможности предварительной классической обработки данных. Было показано, что этот протокол позволяет существенно расширить свою область секретности благодаря технически элементарным действиям легитимных пользователей.

Автор выражает благодарность профессору С. Н. Молоткову за постановку задачи и помощь в подготовке этой работы.

Список литературы

[1] *Acin A., Gisin N., and Scarani V.* Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks // Phys. Rev. A. — 2004. — Vol. 69, 012309.

[2] *Bae J., Acin A.* Key distribution from quantum channel using two-way communication protocols // Phys. Rev. A. — 2007. — Vol. 75, 012334.

[3] *Bennett C.H., Brassard G.* Quantum Cryptography: Public Key Distribution and Coin Tossing // Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces. — Bangalore, India: 1984. — Pp. 175–179.

[4] *Kraus B., Gisin N., Renner R.* Lower and Upper Bounds on secret-Key Rate for Quantum Key Distribution Protocols Using One-Way classical communication // Phys. Rev. Lett. — 2005. — Vol. 95, 080501.

[5] *Maurer U.* Secret key agreement by public discussion from common information // IEEE Trans. Inf. Theory. — 1993. — Vol. 39, Pp. 733–742.

[6] *Scarani V., Acin A., Ribordy G., Gisin N.* Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations // Phys. Rev. Lett. — 2004. — Vol. 92, 057901.

[7] *Кронберг Д.А., Молотков С.Н.* Двухпараметрическая квантовая криптография на временных сдвигах, устойчивая к атаке с расщеплением по числу фотонов // ЖЭТФ. — 2009. — Т. 136. — С. 650–683.

[8] *Кулик С.П., Молотков С.Н., Маккавеев А.П.* Комбинированный метод фазово-временного кодирования // Письма в ЖЭТФ. — 2007. — Т. 85. — С. 354–359.

[9] *Молотков С.Н.* О криптографической стойкости системы квантовой криптографии с фазово-временным кодированием // ЖЭТФ. — 2008. — Т. 134. — С. 39–64.

[10] *Молотков С.Н., Тимофеев А.В.* Явная атака на ключ в квантовой криптографии (протокол BB84), достигающая теоретического предела ошибки $Q_c \approx 11\,\%$ // Письма в ЖЭТФ. — 2007. — Т. 85. — С. 632–637.

[11] *Холево А.С.* Введение в квантовую теорию информации. — М.: МЦНМО, 2002.

УДК 514.752

ОЦЕНКА РАДИУСА ПОКРЫТИЯ МНОГОМЕРНОЙ ЕДИНИЧНОЙ СФЕРЫ МЕТРИЧЕСКОЙ СЕТЬЮ, ПОРОЖДЕННОЙ СФЕРИЧЕСКОЙ СИСТЕМОЙ КООРДИНАТ

© 2011 г. Т. С. Майская

tmayskaya@nes.ru

Кафедра системного анализа

1 Введение

В данной статье изучается радиус покрытия многомерной единичной сферы (сферы направлений) метрической сетью, порождаемой сферическими координатами. Анализ радиуса покрытия этой сети представляет большой практический интерес в связи с тем, что использование сферических координат до последнего времени являлось единственным реализуемым способом построения более-менее равномерного покрытия сферы (здесь мы отвлекаемся от мало изученных эффективных сетей, генерируемых адаптивными методами аппроксимации выпуклых компактных тел [2, 3]). Направления, порождаемые сферическими координатами на сфере, используются, в частности, в неадаптивных алгоритмах полиэдральной аппроксимации выпуклых компактных тел (например, множеств достижимости динамических систем [7]) и т.д.

В статье даются верхняя и нижняя оценки радиуса покрытия сферы метрической сетью, порожденной сферической системой координат. Показывается, что в асимптотике при стремлении угла к нулю эти оценки совпадают. Проводится сравнение радиуса покрытия изучаемой сети с радиусом покрытия оптимальной метрической сети на единичной сфере.

Пусть E^m — m-мерное евклидово пространство с обычными скалярным произведением, нормой и метрикой.

Рассмотрим сферическую систему координат в E^m [1].

$$\begin{cases} x_1 = r \prod\limits_{i=1}^{m-1} \sin\alpha_i, \\ x_k = r\cos\alpha_{k-1} \prod\limits_{i=k}^{m-1} \sin\alpha_i \quad \text{при} \quad k = 2, 3, \ldots, m-1, \\ x_m = r\cos\alpha_{m-1}, \end{cases} \tag{1}$$

в которой $r \geqslant 0$, а сферические углы $\alpha_1, \alpha_2, \ldots, \alpha_{m-2}$ изменяются в пределах $0 \leqslant \alpha_i < \pi$ и $0 \leqslant \alpha_{m-1} < 2\pi$.

Тогда единичная сфера (сфера направлений) $S^{m-1} \subset E^m$ задается соотношением (1) при $r = 1$. Пусть

$$\Psi = \left(\prod_{i=1}^{m-1} \sin\alpha_i, \ldots, \cos\alpha_{k-1} \prod_{i=k}^{m-1} \sin\alpha_i, \ldots, \cos\alpha_{m-1} \right).$$

Под сетью, порождаемой сферическими координатами на единичной сфере S^{m-1}, будем понимать конечное подмножество S^{m-1}:

$$M_{\text{Sph}} = \{\Psi\colon \alpha_i = s_i\gamma_i,\ s_i = 0, 1, \ldots, S_i,\ i = 1, 2, \ldots, m-2,\ \alpha_{m-1} = l\alpha,\ l = 0, 1, \ldots, L\}, \tag{2}$$

Работа была частично поддержана ФЦП «Научные и научно-педагогические кадры инновационной России» (государственный контракт 2010-1.2.1-000-029-072)

где $S_i = \left[\frac{\pi}{\gamma_i}\right]$, $i = 1, \ldots, m-2$, $L = \left[\frac{2\pi}{\alpha}\right]$ — натуральные числа, причем углы γ_i, $i = 1, \ldots, m-2$, и α удовлетворяют следующим условиям:

$$0 < \gamma_i < \frac{\pi}{4},\ i = 1, \ldots, m-2, \quad 0 < \alpha < \frac{\pi}{4}.$$

Под *радиусом покрытия* сферы S^{m-1} произвольным конечным множеством $M \subseteq S^{m-1}$ будем понимать величину

$$\varepsilon\left(M, S^{m-1}\right) := \min\left\{\varepsilon\colon S^{m-1} \subseteq (M)_\varepsilon\right\},$$

где $(M)_\varepsilon = \{\Psi_1 + \Psi_2\colon \Psi_1 \in M, \|\Psi_2\| \leqslant \varepsilon\}$.

Заметим, что для любого $\Psi \in S^{m-1}$ найдется $\Psi' \in M$, что

$$\left\|\Psi - \Psi'\right\| \leqslant \varepsilon,$$

то есть M образует ε-сеть на S^{m-1} с $\varepsilon = \varepsilon\left(M, S^{m-1}\right)$.

Статья имеет следующую структуру. В разделе 2 формулируются основные результаты, связанные с построением верхней и нижней оценок радиуса покрытия сферы сетями рассматриваемого типа (2). При этом показывается, что в асимптотике при стремлении угла к нулю эти оценки совпадают. В разделе 3 полученные оценки сравниваются с оценками для оптимальных сетей на единичной сфере. Полученные результаты конкретизируются для отдельных размерностей, в том числе и при $m \to \infty$. В разделе 4 приводятся доказательства основных результатов, сформулированных в разделе 2.

2 Основные результаты: оценки радиуса покрытия

В данном разделе формулируются результаты о верхней (теорема 1) и нижней (теорема 2) оценках радиуса покрытия единичной сферы сетью (2) в общем случае. Затем доказываются следствия этих утверждений для случая большого числа точек сети.

Теорема 1. *Для радиуса покрытия сети M_{Sph}, определенной в (2), справедлива следующая верхняя оценка:*

$$\left[\varepsilon\left(M_{\mathrm{Sph}}, S^{m-1}\right)\right]^2 \leqslant 2\left(m - 1 - \sum_{i=1}^{m-2} \cos\frac{\gamma_i}{2} - \cos\frac{\alpha}{2}\right). \tag{3}$$

Теорема 2. *При выполнении условия*

$$0 < \gamma_s \leqslant \frac{2}{\sqrt{m-2}},\ s = 1, \ldots, m-2,$$

для радиуса покрытия сети M_{Sph}, определенной в (2), справедлива следующая нижняя оценка:

$$\begin{aligned}\left[\varepsilon\left(M_{\mathrm{Sph}}, S^{m-1}\right)\right]^2 \geqslant 2\Bigg[\Bigg(\Bigg(\ldots\Bigg(\Bigg(\Big(1-\cos\frac{\gamma_1}{2}\Big)\frac{1}{2}\Big(\cos\frac{\gamma_2}{2}+\cos\frac{3\gamma_2}{2}\Big)+\Big(1-\cos\frac{\gamma_2}{2}\Big)\Bigg)\cdot\\ \cdot\frac{1}{2}\Big(\cos\frac{\gamma_3}{2}+\cos\frac{3\gamma_3}{2}\Big)+\Big(1-\cos\frac{\gamma_3}{2}\Big)\Bigg)\ldots\Bigg)\cdot\\ \cdot\frac{1}{2}\Big(\cos\frac{\gamma_{m-2}}{2}+\cos\frac{3\gamma_{m-2}}{2}\Big)+\Big(1-\cos\frac{\gamma_{m-2}}{2}\Big)\Bigg)\cdot\\ \cdot\frac{1}{2}\Big(\cos\frac{\alpha}{2}+\cos\frac{3\alpha}{2}\Big)+\Big(1-\cos\frac{\alpha}{2}\Big)\Bigg].\end{aligned} \tag{4}$$

Доказательства этих теорем трудоемки, поэтому они отнесены в конец статьи.

Из теорем 1 и 2 можно легко получить следствия, которые выполняются при достаточно большом числе точек в сети.

Следствие 1. *Пусть* $\gamma_1 = \gamma_2 = \ldots = \gamma_{m-2} = \gamma$. *Тогда*

$$\left[\varepsilon\left(M_{\text{Sph}}, S^{m-1}\right)\right]^2 = \frac{\gamma^2}{4}(m-2) + \frac{\alpha^2}{4} + O\left((\gamma^2+\alpha^2)^2\right). \tag{5}$$

Доказательство. Из формулы (3), используя разложение в ряд Тейлора, сразу получаем приближенную оценку

$$\left[\varepsilon\left(M_{\text{Sph}}, S^{m-1}\right)\right]^2 \leqslant 2\left(m-1-\sum_{i=1}^{m-2}\cos\frac{\gamma_i}{2} - \cos\frac{\alpha}{2}\right) =$$
$$= 2\left(m-1-(m-2)\left(1-\frac{\gamma^2}{8}+O\left(\gamma^4\right)\right)-1+\frac{\alpha^2}{8}+O\left(\alpha^4\right)\right) =$$
$$= \frac{\gamma^2}{4}(m-2) + \frac{\alpha^2}{4} + O\left(\gamma^4\right) + O\left(\alpha^4\right).$$

Для получения нижней оценки воспользуемся формулой (4). Заметим, что ее можно написать в следующем рекурсивном виде:

$$B_1 = 1 - \cos\frac{\gamma_1}{2};$$
$$B_i = B_{i-1}\cdot\frac{1}{2}\left(\cos\frac{\gamma_i}{2} + \cos\frac{3\gamma_i}{2}\right) + \left(1-\cos\frac{\gamma_i}{2}\right), \quad i = 2,3,\ldots,m-2;$$
$$\left[\varepsilon\left(M, S^{m-1}\right)\right]^2 \geqslant 2\left(B_{m-2}\cdot\frac{1}{2}\left(\cos\frac{\alpha}{2}+\cos\frac{3\alpha}{2}\right)+\left(1-\cos\frac{\alpha}{2}\right)\right).$$

Используя разложение Тейлора, отсюда получаем:

$$B_1 = \frac{\gamma^2}{8} + O\left(\gamma^4\right);$$
$$B_i = B_{i-1}\cdot\left(1-\frac{5\gamma^2}{8}+O\left(\gamma^4\right)\right)+\left(\frac{\gamma^2}{8}+O\left(\gamma^4\right)\right) = B_{i-1}+\frac{\gamma^2}{8}+O\left(\gamma^4\right), \quad i = 2,3,\ldots,m-2.$$

Отсюда сразу следует нижняя оценка радиуса покрытия:

$$\left[\varepsilon\left(M_{\text{Sph}}, S^{m-1}\right)\right]^2 \geqslant 2\left(B_{m-2}\cdot\left(1-\frac{5\alpha^2}{8}+O\left(\alpha^4\right)\right)+\left(\frac{\alpha^2}{8}+O\left(\alpha^4\right)\right)\right) =$$
$$= 2\left(\left(\frac{\gamma^2}{8}\cdot(m-2)+O\left(\gamma^4\right)\right)\left(1-\frac{5\alpha^2}{8}+O\left(\alpha^4\right)\right)+\frac{\alpha^2}{8}+O\left(\alpha^4\right)\right) =$$
$$= \frac{\gamma^2}{4}(m-2)+\frac{\alpha^2}{4}+O\left(\gamma^4\right)+O\left(\alpha^4\right)+O\left(\alpha^2\gamma^2\right).$$

□

В следующем утверждении полученная оценка уточняется для случая $\gamma = \alpha$.

Обозначим через $M^{k,m}_{\text{Sph}} \subseteq S^{m-1}$ сеть (2) мощности k, для которой $\gamma_1 = \gamma_2 = \ldots = \gamma_{m-2} = \gamma = \alpha$.

Следствие 2. *Имеет место оценка*

$$\lim_{k\to\infty}\left[k^{\frac{1}{m-1}}\cdot\varepsilon\left(M^{k,m}_{\text{Sph}}, S^{m-1}\right)\right] = \frac{\pi\sqrt[m-1]{2}\sqrt{m-1}}{2}. \tag{6}$$

Доказательство. Так как при малом угле α из (2) следует

$$k = L\prod_{i=1}^{m-1} S_i \approx \left(\frac{\pi}{\gamma}\right)^{m-2}\cdot\frac{2\pi}{\alpha} = \frac{2\pi^{m-1}}{\alpha^{m-1}},$$

то, используя утверждение Следствия 1, получаем:

$$\left[\varepsilon\left(M_{\text{Sph}}^{k,m}, S^{m-1}\right)\right]^2 = \frac{\gamma^2}{4}(m-2) + \frac{\alpha^2}{4} + O\left((\gamma^2+\alpha^2)^2\right) =$$
$$= \frac{\alpha^2}{4}(m-1) + O\left(\alpha^4\right) \approx \left(\frac{\pi\ \sqrt[m-1]{2}}{\sqrt[m-1]{k}}\right)^2\cdot\frac{m-1}{4}.$$

□

3 Сравнение с оценками для оптимальных сетей

Оценки, полученные в предыдущем разделе, позволяют сравнить сеть на S^{m-1}, порожденную сферической системой координат, с оптимальной сетью, которая определяется следующим образом. Пусть M — произвольная конечная сеть на S^{m-1}, ее мощность обозначим через $|M|$. Сеть на S^{m-1} мощностью k называется *оптимальной* [4] и обозначается $M_{\text{opt}}^{k,m}$, если она имеет наименьший радиус покрытия среди сетей на сфере, имеющих ту же мощность, то есть

$$\varepsilon\left(M_{\text{opt}}^{k,m}, S^{m-1}\right) = \min\left\{\varepsilon\left(M, S^{m-1}\right) : M\subseteq S^{m-1}, |M| = k\right\}.$$

Рассмотрим также минимальное число точек в сети при фиксированном радиусе покрытия:

$$k_{\text{opt}}^m(\varepsilon) := \min\left\{k\colon \varepsilon\left(M_{\text{opt}}^{k,m}, S^{m-1}\right)\leqslant\varepsilon\right\}. \tag{7}$$

Из [3] следуют асимптотические оценки для оптимальных сетей:

$$\lim_{k\to\infty}\left[k^{\frac{1}{m-1}}\cdot\varepsilon\left(M_{\text{opt}}^{k,m}, S^{m-1}\right)\right] = \left(\frac{\sigma_m}{\pi_{m-1}}\cdot\vartheta_{m-1}\right)^{\frac{1}{m-1}}, \tag{8}$$

$$\lim_{\varepsilon\to 0}\left[\varepsilon^{m-1}\cdot k_{\text{opt}}^m(\varepsilon)\right] = \frac{\sigma_m}{\pi_{m-1}}\cdot\vartheta_{m-1}, \tag{9}$$

где $\pi_m = \frac{\pi^{\frac{m}{2}}}{\Gamma\left(1+\frac{m}{2}\right)}$ — объем единичного шара в пространстве E^m, $\sigma_m = (\pi_m r^m)'_r\big|_{r=1} = m\pi_m$ — площадь поверхности единичного шара в пространстве E^m, ϑ_m — плотность редчайшего покрытия E^m единичными шарами [5].

Пусть

$$k_{\text{Sph}}^m(\varepsilon) := \min\{k\colon \varepsilon\left(M_{\text{Sph}}^{k,m}, S^{m-1}\right)\leqslant\varepsilon\}. \tag{10}$$

Теорема 3. *Имеют место оценки*

$$\lim_{k\to\infty}\left[\frac{\varepsilon\left(M_{\text{opt}}^{k,m}, S^{m-1}\right)}{\varepsilon\left(M_{\text{Sph}}^{k,m}, S^{m-1}\right)}\right] = \left(\frac{m\pi_m\vartheta_{m-1}}{2\pi_{m-1}}\right)^{\frac{1}{m-1}}\cdot\frac{2}{\pi\sqrt{m-1}} \tag{11}$$

и

$$\lim_{\varepsilon\to 0}\left[\frac{k_{\text{opt}}^m(\varepsilon)}{k_{\text{Sph}}^m(\varepsilon)}\right] = \frac{m\pi_m\vartheta_{m-1}2^{m-2}}{\pi_{m-1}\pi^{m-1}(m-1)^{\frac{m-1}{2}}}. \tag{12}$$

Доказательство. Из следствия 2 сразу получаем:

$$\lim_{k\to\infty}\left[k^{\frac{1}{m-1}}\cdot\varepsilon\left(M^{k,m}_{\text{Sph}},S^{m-1}\right)\right]=2^{\frac{1}{m-1}}\cdot\frac{\pi\sqrt{m-1}}{2},\tag{13}$$

$$\lim_{\varepsilon\to0}\left[\varepsilon^{m-1}\cdot k^m_{\text{Sph}}\,(\varepsilon)\right]=\frac{\pi^{m-1}(m-1)^{\frac{m-1}{2}}}{2^{m-2}}.\tag{14}$$

Первая оценка теоремы следует из (13) и (8). Вторая оценка теоремы следует из (14) и (9). □

Проанализируем выражения (11) и (12).

Для малых размерностей пространства оценки (11) и (12) принимают вид*:

m	2	3	4	5
$\lim\limits_{k\to\infty}\frac{\varepsilon\left(M^{k,m}_{\text{opt}},S^{m-1}\right)}{\varepsilon\left(M^{k,m}_{\text{Sph}},S^{m-1}\right)}$	1	$\frac{4}{\sqrt[4]{3}\sqrt{6\pi}}\approx0{,}70$	$\left[\frac{2\vartheta_3}{\pi^2\sqrt{3}}\right]^{\frac13}\leqslant\frac{\sqrt{5}}{(4\pi)^{\frac13}\sqrt{3}}\approx0{,}56$	$\frac{2\sqrt[4]{\vartheta_4}}{\pi\sqrt[4]{6}}\leqslant\left[\frac{16}{15\pi^2\sqrt{5}}\right]^{\frac14}\approx0{,}47$
$\lim\limits_{\varepsilon\to0}\frac{k^m_{\text{opt}}(\varepsilon)}{k^m_{\text{Sph}}(\varepsilon)}$	1	$\frac{8}{3\pi\sqrt{3}}\approx0{,}49$	$\frac{2\vartheta_3}{\pi^2\sqrt{3}}\leqslant\frac{5\sqrt{5}}{12\pi\sqrt{3}}\approx0{,}17$	$\frac{8\vartheta_4}{3\pi^4}\leqslant\frac{16}{15\pi^2\sqrt{5}}\approx0{,}05$

Из таблицы видно, что сеть, порожденная сферической системой координат, при $m>3$ сильно уступает оптимальной сети. Хотя в трехмерном пространстве для покрытия единичной сферы требуется только в два раза большее число узлов, чем при использовании оптимальной сети, для пятимерного пространства узлов потребуется уже в 20 раз больше.

Покажем, что при увеличении размерности пространства сеть, порожденная сферической системой координат, становится неприемлемой для более-менее равномерного покрытия единичной сферы. Для этого рассмотрим асимптотическое поведение выражений (11) и (12) при $m\to\infty$.

Теорема 4. *Имеют место оценки*

$$\limsup_{m\to\infty}\left[\sqrt{m}\cdot\lim_{k\to\infty}\left[\frac{\varepsilon\left(M^{k,m}_{\text{opt}},S^{m-1}\right)}{\varepsilon\left(M^{k,m}_{\text{Sph}},S^{m-1}\right)}\right]\right]\leqslant\frac{2e}{\pi}\tag{15}$$

и

$$\limsup_{m\to\infty}\left[\left(\frac{\pi}{2}\right)^m m^{\frac{m-5}{2}}\cdot\frac{1}{\ln m}\cdot\lim_{\varepsilon\to0}\left[\frac{k^m_{\text{opt}}\,(\varepsilon)}{k^m_{\text{Sph}}\,(\varepsilon)}\right]\right]\leqslant\frac74\cdot\pi\sqrt{\pi}\cdot e^{\frac12}.\tag{16}$$

Доказательство. Сначала найдем оценку для $\frac{\pi_m}{\pi_{m-1}}$. Учитывая, что

$$\pi_m=\frac{\pi^{\frac{m}{2}}}{\Gamma\left(1+\frac{m}{2}\right)},$$

получаем:

$$\pi_{2p}=\frac{\pi^p}{p!},\quad\frac{\pi^p\sqrt{\pi}}{(p+1)!}\leqslant\pi_{2p+1}\leqslant\frac{\pi^p\sqrt{\pi}}{p!},\quad p\geqslant1;\quad\pi_1=2;$$

$m=2p$:

$$\frac{\pi_2}{\pi_1}=\frac{\pi}{2}<\sqrt{\pi},\quad\frac{\pi_m}{\pi_{m-1}}=\frac{\pi_{2p}}{\pi_{2p-1}}\leqslant\frac{\pi^p p!}{p!\pi^{p-1}\sqrt{\pi}}=\sqrt{\pi};$$

*Здесь используются формулы $\pi_1=2$, $\pi_2=\pi$, $\pi_3=\frac{4\pi}{3}$, $\pi_4=\frac{\pi^2}{2}$, $\pi_5=\frac{8\pi^2}{15}$, а также оценки для ϑ_m, взятые из [6]: $\vartheta_1=1$, $\vartheta_2=\frac{2\pi}{\sqrt{27}}$, $\vartheta_3\leqslant\frac{5\pi\sqrt{5}}{24}$, $\vartheta_4\leqslant\frac{2\pi^2}{5\sqrt{5}}$.

$m = 2p + 1$:

$$\frac{\pi_m}{\pi_{m-1}} = \frac{\pi_{2p+1}}{\pi_{2p}} \leqslant \frac{p!\pi^p\sqrt{\pi}}{p!\pi^p} = \sqrt{\pi}.$$

Таким образом,

$$\frac{\pi_m}{\pi_{m-1}} \leqslant \sqrt{\pi}, \quad \forall m \geqslant 2.$$

В [6] показано, что

$$\vartheta_m \leqslant m\ln m + m\ln\ln m + 5m, \quad m \geqslant 24.$$

Откуда получаем:

$$\vartheta_m \leqslant 7m\ln m, \quad \forall m \geqslant 24.$$

Учитывая это, а также следующий известный факт:

$$\lim_{n\to\infty} \sqrt[n]{n} = 1,$$

получаем:

$$\limsup_{m\to\infty}\left[\sqrt{m}\cdot\lim_{k\to\infty}\left[\frac{\varepsilon\left(M_{\text{opt}}^{k,m}, S^{m-1}\right)}{\varepsilon\left(M_{\text{Sph}}^{k,m}, S^{m-1}\right)}\right]\right] =$$

$$= \limsup_{m\to\infty}\left[\sqrt{m}\cdot\left(\frac{m\pi_m\vartheta_{m-1}}{2\pi_{m-1}}\right)^{\frac{1}{m-1}}\cdot\frac{2}{\pi\sqrt{m-1}}\right] \leqslant$$

$$\leqslant \limsup_{m\to\infty}\left[\left(\frac{7(m-1)m\sqrt{\pi}\ln(m-1)}{2}\right)^{\frac{1}{m-1}}\cdot\frac{2\sqrt{m}}{\pi\sqrt{m-1}}\right] = \frac{2e}{\pi}$$

и

$$\limsup_{m\to\infty}\left[\left(\frac{\pi}{2}\right)^m m^{\frac{m-5}{2}}\cdot\frac{1}{\ln m}\cdot\lim_{\varepsilon\to 0}\left[\frac{k_{\text{opt}}^m(\varepsilon)}{k_{\text{Sph}}^m(\varepsilon)}\right]\right] =$$

$$= \limsup_{m\to\infty}\left[\left(\frac{\pi}{2}\right)^m m^{\frac{m-5}{2}}\cdot\frac{1}{\ln m}\cdot\frac{m\pi_m\vartheta_{m-1}2^{m-2}}{\pi_{m-1}\pi^{m-1}(m-1)^{\frac{m-1}{2}}}\right] \leqslant$$

$$\leqslant \limsup_{m\to\infty}\left[\left(\frac{\pi}{2}\right)^m m^{\frac{m-5}{2}}\cdot\frac{1}{\ln m}\cdot\frac{7\sqrt{\pi}m\cdot 2^{m-2}\ln(m-1)}{\pi^{m-1}(m-1)^{\frac{m-1}{2}-1}}\right] =$$

$$= \limsup_{m\to\infty}\left[\frac{7\pi^2\cdot\ln(m-1)\cdot m^{\frac{m-3}{2}}}{4\sqrt{\pi}\ln m\cdot(m-1)^{\frac{m-3}{2}}}\right] = \frac{7}{4}\cdot\pi\sqrt{\pi}\cdot e^{\frac{1}{2}}. \qquad \square$$

Из теоремы 4 видно, что при больших размерностях пространства выражение $\lim\limits_{\varepsilon\to 0}\left[\frac{k_{\text{opt}}^m(\varepsilon)}{k_{\text{Sph}}^m(\varepsilon)}\right]$ стремится к нулю со скоростью примерно m^m, что говорит о крайней неэффективности использования сферических координат для покрытия сферы при больших m.

4 Доказательства теорем 1 и 2

Лемма 1. *Для произвольных векторов*

$$\Psi_1 = \left(\prod_{i=1}^{m-1}\sin\alpha_i, \ldots, \cos\alpha_{k-1}\prod_{i=k}^{m-1}\sin\alpha_i, \ldots, \cos\alpha_{m-1}\right) \in M_{\text{Sph}},$$

$$\Psi_2 = \left(\prod_{i=1}^{m-1} \sin\beta_i, \ldots, \cos\beta_{k-1} \prod_{i=k}^{m-1} \sin\beta_i, \ldots, \cos\beta_{m-1} \right) \in S^{m-1}$$

справедливо

$$\langle \Psi_1, \Psi_2 \rangle = \Bigg(\Bigg(\ldots \Bigg(\Bigg((\cos(\alpha_1 - \beta_1) - 1) \frac{1}{2} (\cos(\alpha_2 - \beta_2) - \cos(\alpha_2 + \beta_2)) + (\cos(\alpha_2 - \beta_2) - 1) \Bigg) \times$$

$$\times \frac{1}{2} (\cos(\alpha_3 - \beta_3) - \cos(\alpha_3 + \beta_3)) + (\cos(\alpha_3 - \beta_3) - 1) \Bigg) \ldots \Bigg) \times$$

$$\times \frac{1}{2} (\cos(\alpha_{m-2} - \beta_{m-2}) - \cos(\alpha_{m-2} + \beta_{m-2})) + (\cos(\alpha_{m-2} - \beta_{m-2}) - 1) \Bigg) \times$$

$$\times \frac{1}{2} (\cos(\alpha_{m-1} - \beta_{m-1}) - \cos(\alpha_{m-1} + \beta_{m-1})) + \cos(\alpha_{m-1} - \beta_{m-1}). \quad (17)$$

Доказательство.

$$\langle \Psi_1, \Psi_2 \rangle = \prod_{i=1}^{m-1} \sin\alpha_i \sin\beta_i + \ldots + \cos\alpha_{k-1} \cos\beta_{k-1} \prod_{i=k}^{m-1} \sin\alpha_i \sin\beta_i + \ldots + \cos\alpha_{m-1} \cos\beta_{m-1}.$$

Применяя формулу косинуса разности углов для первых двух слагаемых, имеем:

$$\langle \Psi_1, \Psi_2 \rangle = \cos(\alpha_1 - \beta_1) \prod_{i=2}^{m-1} \sin\alpha_i \sin\beta_i + \cos\alpha_2 \cos\beta_2 \prod_{i=3}^{m-1} \sin\alpha_i \sin\beta_i + \ldots +$$

$$+ \cos\alpha_{k-1} \cos\beta_{k-1} \prod_{i=k}^{m-1} \sin\alpha_i \sin\beta_i + \ldots + \cos\alpha_{m-1} \cos\beta_{m-1}.$$

Далее воспользуемся формулой

$$\sin\alpha \sin\beta = \frac{1}{2} (\cos(\alpha - \beta) - \cos(\alpha + \beta)),$$

для первого слагаемого:

$$\cos(\alpha_1 - \beta_1) \prod_{i=2}^{m-1} \sin\alpha_i \sin\beta_i = (\cos(\alpha_1 - \beta_1) - 1) \prod_{i=2}^{m-1} \sin\alpha_i \sin\beta_i + \prod_{i=2}^{m-1} \sin\alpha_i \sin\beta_i =$$

$$= (\cos(\alpha_1 - \beta_1) - 1) \frac{1}{2} (\cos(\alpha_2 - \beta_2) - \cos(\alpha_2 + \beta_2)) \prod_{i=3}^{m-1} \sin\alpha_i \sin\beta_i + \prod_{i=2}^{m-1} \sin\alpha_i \sin\beta_i.$$

В результате получим:

$$\langle \Psi_1, \Psi_2 \rangle = (\cos(\alpha_1 - \beta_1) - 1) \frac{1}{2} (\cos(\alpha_2 - \beta_2) - \cos(\alpha_2 + \beta_2)) \prod_{i=3}^{m-1} \sin\alpha_i \sin\beta_i +$$

$$+ \prod_{i=2}^{m-1} \sin\alpha_i \sin\beta_i + \cos\alpha_2 \cos\beta_2 \prod_{i=3}^{m-1} \sin\alpha_i \sin\beta_i + \ldots +$$

$$+ \cos\alpha_{k-1} \cos\beta_{k-1} \prod_{i=k}^{m-1} \sin\alpha_i \sin\beta_i + \ldots + \cos\alpha_{m-1} \cos\beta_{m-1}.$$

Опять применим формулу косинуса разности для второго и третьего слагаемых:

$$\langle \Psi_1, \Psi_2 \rangle = (\cos(\alpha_1 - \beta_1) - 1)\,\frac{1}{2}\,(\cos(\alpha_2 - \beta_2) - \cos(\alpha_2 + \beta_2)) \prod_{i=3}^{m-1} \sin\alpha_i \sin\beta_i +$$
$$+ \cos(\alpha_2 - \beta_2) \prod_{i=3}^{m-1} \sin\alpha_i \sin\beta_i + \ldots + \cos\alpha_{k-1}\cos\beta_{k-1} \prod_{i=k}^{m-1} \sin\alpha_i \sin\beta_i + \ldots + \cos\alpha_{m-1}\cos\beta_{m-1}.$$

Далее объединяем первое и второе слагаемые, вынося за скобку общий множитель

$$\prod_{i=3}^{m-1} \sin\alpha_i \sin\beta_i,$$

получая:

$$\left((\cos(\alpha_1 - \beta_1) - 1)\,\frac{1}{2}\,(\cos(\alpha_2 - \beta_2) - \cos(\alpha_2 + \beta_2)) + \cos(\alpha_2 - \beta_2)\right) \prod_{i=3}^{m-1} \sin\alpha_i \sin\beta_i =$$
$$= \left((\cos(\alpha_1 - \beta_1) - 1)\,\frac{1}{2}\,(\cos(\alpha_2 - \beta_2) - \cos(\alpha_2 + \beta_2)) + \cos(\alpha_2 - \beta_2) - 1\right) \prod_{i=3}^{m-1} \sin\alpha_i \sin\beta_i +$$
$$+ \prod_{i=3}^{m-1} \sin\alpha_i \sin\beta_i =$$
$$= \left((\cos(\alpha_1 - \beta_1) - 1)\,\frac{1}{2}\,(\cos(\alpha_2 - \beta_2) - \cos(\alpha_2 + \beta_2)) + \cos(\alpha_2 - \beta_2) - 1\right) \times$$
$$\times\,\frac{1}{2}\,(\cos(\alpha_3 - \beta_3) - \cos(\alpha_3 + \beta_3)) \cdot \prod_{i=4}^{m-1} \sin\alpha_i \sin\beta_i + \prod_{i=3}^{m-1} \sin\alpha_i \sin\beta_i.$$

Выражение для скалярного произведения примет вид:

$$\langle \Psi_1, \Psi_2 \rangle = \left((\cos(\alpha_1 - \beta_1) - 1)\,\frac{1}{2}\,(\cos(\alpha_2 - \beta_2) - \cos(\alpha_2 + \beta_2)) + \cos(\alpha_2 - \beta_2) - 1\right) \times$$
$$\times\,\frac{1}{2}\,(\cos(\alpha_3 - \beta_3) - \cos(\alpha_3 + \beta_3)) \cdot \prod_{i=4}^{m-1} \sin\alpha_i \sin\beta_i +$$
$$+ \prod_{i=3}^{m-1} \sin\alpha_i \sin\beta_i + \cos\alpha_3\cos\beta_3 \prod_{i=4}^{m-1} \sin\alpha_i \sin\beta_i + \ldots +$$
$$+ \cos\alpha_{k-1}\cos\beta_{k-1} \prod_{i=k}^{m-1} \sin\alpha_i \sin\beta_i + \ldots + \cos\alpha_{m-1}\cos\beta_{m-1}.$$

Действуя аналогично, то есть применяя поочередно формулы косинуса разности и произведе-

ния синусов, получаем в результате следующее выражение для скалярного произведения:

$$\begin{aligned}\langle\Psi_1,\Psi_2\rangle = \Bigg(\Bigg(\Bigg(\dots\Bigg(\Bigg((\cos(\alpha_1-\beta_1)-1)\,\frac{1}{2}\,(\cos(\alpha_2-\beta_2)-\cos(\alpha_2+\beta_2))+(\cos(\alpha_2-\beta_2)-1)\Bigg)\times\\ \times\frac{1}{2}\,(\cos(\alpha_3-\beta_3)-\cos(\alpha_3+\beta_3))+(\cos(\alpha_3-\beta_3)-1)\Bigg)\dots\Bigg)\times\\ \times\frac{1}{2}\,(\cos(\alpha_{m-3}-\beta_{m-3})-\cos(\alpha_{m-3}+\beta_{m-3}))+(\cos(\alpha_{m-3}-\beta_{m-3})-1)\Bigg)\times\\ \times\frac{1}{2}\,(\cos(\alpha_{m-2}-\beta_{m-2})-\cos(\alpha_{m-2}+\beta_{m-2}))+(\cos(\alpha_{m-2}-\beta_{m-2})-1)\Bigg)\cdot\sin\alpha_{m-1}\sin\beta_{m-1}+\\ +\sin\alpha_{m-1}\sin\beta_{m-1}+\cos\alpha_{m-1}\cos\beta_{m-1}.\end{aligned}$$

Откуда получаем равенство (17). □

Доказательство теоремы 1. Зафиксируем произвольные векторы $\Psi_1\in M_{\mathrm{Sph}}$, $\Psi_2\in S^{m-1}$:

$$\Psi_1=\left(\prod_{i=1}^{m-1}\sin\alpha_i,\dots,\cos\alpha_{k-1}\prod_{i=k}^{m-1}\sin\alpha_i,\dots,\cos\alpha_{m-1}\right),$$
$$\Psi_2=\left(\prod_{i=1}^{m-1}\sin\beta_i,\dots,\cos\beta_{k-1}\prod_{i=k}^{m-1}\sin\beta_i,\dots,\cos\beta_{m-1}\right).$$

Для доказательства теоремы достаточно найти верхнюю оценку для квадрата нормы разности векторов Ψ_1 и Ψ_2.

Согласно равенству (17),

$$\begin{aligned}&\|\Psi_1-\Psi_2\|^2=2-2\,\langle\Psi_1,\Psi_2\rangle=\\ &=2-2\Bigg(\Bigg(\Bigg(\dots\Bigg(\Bigg((\cos(\alpha_1-\beta_1)-1)\,\frac{1}{2}\,(\cos(\alpha_2-\beta_2)-\cos(\alpha_2+\beta_2))+(\cos(\alpha_2-\beta_2)-1)\Bigg)\times\\ &\qquad\times\frac{1}{2}\,(\cos(\alpha_3-\beta_3)-\cos(\alpha_3+\beta_3))+(\cos(\alpha_3-\beta_3)-1)\Bigg)\dots\Bigg)\times\\ &\qquad\times\frac{1}{2}\,(\cos(\alpha_{m-2}-\beta_{m-2})-\cos(\alpha_{m-2}+\beta_{m-2}))+(\cos(\alpha_{m-2}-\beta_{m-2})-1)\Bigg)\times\\ &\qquad\times\frac{1}{2}\,(\cos(\alpha_{m-1}-\beta_{m-1})-\cos(\alpha_{m-1}+\beta_{m-1}))+\cos(\alpha_{m-1}-\beta_{m-1})\Bigg).\end{aligned}\tag{18}$$

Для начала заметим, что так как $0\leqslant\alpha_i<\pi$, $0\leqslant\beta_i<\pi$ при $i=1,2,\dots,m-2$, то

$$\frac{1}{2}\,(\cos(\alpha_i-\beta_i)-\cos(\alpha_i+\beta_i))=\sin\alpha_i\sin\beta_i\geqslant 0,\quad i=1,2,\dots,m-2.$$

Поэтому оценка для скалярного произведения выглядят следующим образом:

$$\begin{aligned}\langle\Psi_1,\Psi_2\rangle\geqslant\Bigg(\Bigg(\dots\Bigg(\Bigg((\cos(\alpha_1-\beta_1)-1)\,\frac{1}{2}\,(\cos(\alpha_2-\beta_2)+1)+(\cos(\alpha_2-\beta_2)-1)\Bigg)\times\\ \times\frac{1}{2}\,(\cos(\alpha_3-\beta_3)+1)+(\cos(\alpha_3-\beta_3)-1)\Bigg)\dots\Bigg)\times\\ \times\frac{1}{2}\,(\cos(\alpha_{m-2}-\beta_{m-2})+1)+(\cos(\alpha_{m-2}-\beta_{m-2})-1)\Bigg)\times\\ \times\frac{1}{2}\,(\cos(\alpha_{m-1}-\beta_{m-1})+1)+\cos(\alpha_{m-1}-\beta_{m-1}),\end{aligned}$$

а для квадрата нормы разности векторов

$$\|\Psi_1-\Psi_2\|^2 \leqslant 2\left[\left(\left(\dots\left(\left((1-\cos(\alpha_1-\beta_1))\,\frac{1}{2}\,(\cos(\alpha_2-\beta_2)+1)+(1-\cos(\alpha_2-\beta_2))\right)\times\right.\right.\right.$$
$$\left.\left.\left.\times\,\frac{1}{2}\,(\cos(\alpha_3-\beta_3)+1)+(1-\cos(\alpha_3-\beta_3))\right)\dots\right)\times$$
$$\left.\times\,\frac{1}{2}\,(\cos(\alpha_{m-2}-\beta_{m-2})+1)+(1-\cos(\alpha_{m-2}-\beta_{m-2}))\right)\times$$
$$\times\,\frac{1}{2}\,(\cos(\alpha_{m-1}-\beta_{m-1})+1)+(1-\cos(\alpha_{m-1}-\beta_{m-1}))\Bigg].$$

Теперь наложим ограничение на разность углов:

$$-\frac{\gamma_i}{2}\leqslant\alpha_i-\beta_i\leqslant\frac{\gamma_i}{2},\quad i=1,\dots,m-2;\quad -\frac{\alpha}{2}\leqslant\alpha_{m-1}-\beta_{m-1}\leqslant\frac{\alpha}{2}. \tag{19}$$

Тогда

$$\|\Psi_1-\Psi_2\|^2 \leqslant 2\left[\left(\left(\dots\left(\left(\left(1-\cos\frac{\gamma_1}{2}\right)\frac{1}{2}\,(1+1)+\left(1-\cos\frac{\gamma_2}{2}\right)\right)\times\right.\right.\right.$$
$$\left.\left.\left.\times\,\frac{1}{2}\,(1+1)+\left(1-\cos\frac{\gamma_3}{2}\right)\right)\dots\right)\cdot\frac{1}{2}\,(1+1)+\left(1-\cos\frac{\gamma_{m-2}}{2}\right)\right)\cdot\frac{1}{2}\,(1+1)+\left(1-\cos\frac{\alpha}{2}\right)\Bigg].$$

Упрощая полученное выражение, в итоге имеем:

$$\|\Psi_1-\Psi_2\|^2 \leqslant 2\left(m-1-\sum_{i=1}^{m-2}\cos\frac{\gamma_i}{2}-\cos\frac{\alpha}{2}\right). \tag{20}$$

Итак, мы получили, что для произвольных векторов $\Psi_1\in M_{\text{Sph}}$, $\Psi_2\in S^{m-1}$, введенных в начале доказательства, для которых выполнено ограничение на разность углов (19) справедлива оценка (20). Из этого следует, что для произвольного вектора $\Psi_2\in S^{m-1}$ всегда найдется такой вектор $\Psi_1\in M_{\text{Sph}}$, что выполнена оценка (20). Таким образом, верхняя оценка (3) для радиуса покрытия доказана. □

Доказательство теоремы 2. Зафиксируем произвольные векторы $\Psi_1\in M_{\text{Sph}}$, $\Psi_2\in S^{m-1}$ таким же образом, как это было сделано в доказательстве теоремы 1. Пусть

$$\begin{cases}|\alpha_i-\beta_i|=\dfrac{\gamma_i}{2},\quad i=1,\dots,m-2;\quad |\alpha_{m-1}-\beta_{m-1}|=\dfrac{\alpha}{2};\\ \dfrac{\pi}{2}-\dfrac{\gamma_i}{2}\leqslant\beta_i\leqslant\dfrac{\pi}{2}+\dfrac{\gamma_i}{2},\quad i=1,\dots,m-2;\quad \dfrac{\pi}{2}-\dfrac{\alpha}{2}\leqslant\beta_{m-1}\leqslant\dfrac{\pi}{2}+\dfrac{\alpha}{2}.\end{cases} \tag{21}$$

Тогда из формулы (17) получаем:

$$\langle\Psi_1,\Psi_2\rangle=\left(\left(\dots\left(\left(\left(\cos\frac{\gamma_1}{2}-1\right)\frac{1}{2}\left(\cos\frac{\gamma_2}{2}-\cos(\alpha_2+\beta_2)\right)+\left(\cos\frac{\gamma_2}{2}-1\right)\right)\times\right.\right.\right.$$
$$\left.\left.\left.\times\,\frac{1}{2}\left(\cos\frac{\gamma_3}{2}-\cos(\alpha_3+\beta_3)\right)+\left(\cos\frac{\gamma_3}{2}-1\right)\right)\dots\right)\times$$
$$\left.\times\,\frac{1}{2}\left(\cos\frac{\gamma_{m-2}}{2}-\cos(\alpha_{m-2}+\beta_{m-2})\right)+\left(\cos\frac{\gamma_{m-2}}{2}-1\right)\right)\times$$
$$\times\,\frac{1}{2}\left(\cos\frac{\alpha}{2}-\cos(\alpha_{m-1}+\beta_{m-1})\right)+\cos\frac{\alpha}{2}.$$

Заметим также, что

$$\alpha_i + \beta_i = 2\beta_i \pm \frac{\gamma_i}{2}, \quad i = 1, \ldots, m-2; \quad \alpha_{m-1} + \beta_{m-1} = 2\beta_{m-1} \pm \frac{\alpha}{2};$$
$$\pi - \frac{3\gamma_i}{2} \leqslant 2\beta_i \pm \frac{\gamma_i}{2} \leqslant \pi + \frac{3\gamma_i}{2}, \quad i = 1, \ldots, m-2; \quad \pi - \frac{3\alpha}{2} \leqslant 2\beta_{m-1} \pm \frac{\alpha}{2} \leqslant \pi + \frac{3\alpha}{2}.$$

Следовательно,

$$\cos(\alpha_i + \beta_i) \leqslant \cos\left(\pi - \frac{3\gamma_i}{2}\right) = -\cos\frac{3\gamma_i}{2}, \quad i = 1, \ldots, m-2;$$
$$\cos(\alpha_{m-1} + \beta_{m-1}) \leqslant \cos\left(\pi - \frac{3\alpha}{2}\right) = -\cos\frac{3\alpha}{2}.$$

Откуда получаем следующую оценку на скалярное произведение:

$$\begin{aligned}\langle \Psi_1, \Psi_2 \rangle \leqslant \Bigg(\Bigg(\ldots\Bigg(\Bigg(\Big(\cos\frac{\gamma_1}{2} - 1\Big)\frac{1}{2}\Big(\cos\frac{\gamma_2}{2} + \cos\frac{3\gamma_2}{2}\Big) + \Big(\cos\frac{\gamma_2}{2} - 1\Big)\Bigg) \times \\ \times \frac{1}{2}\Big(\cos\frac{\gamma_3}{2} + \cos\frac{3\gamma_3}{2}\Big) + \Big(\cos\frac{\gamma_3}{2} - 1\Big)\Bigg)\ldots\Bigg) \times \\ \times \frac{1}{2}\Big(\cos\frac{\gamma_{m-2}}{2} + \cos\frac{3\gamma_{m-2}}{2}\Big) + \Big(\cos\frac{\gamma_{m-2}}{2} - 1\Big)\Bigg) \times \\ \times \frac{1}{2}\Big(\cos\frac{\alpha}{2} + \cos\frac{3\alpha}{2}\Big) + \cos\frac{\alpha}{2}.\end{aligned}$$

Тогда соответствующая оценка для квадрата нормы разности векторов выглядит следующим образом:

$$\begin{aligned}\|\Psi_1 - \Psi_2\|^2 \geqslant 2\Bigg[\Bigg(\Bigg(\ldots\Bigg(\Bigg(\Big(1 - \cos\frac{\gamma_1}{2}\Big)\frac{1}{2}\Big(\cos\frac{\gamma_2}{2} + \cos\frac{3\gamma_2}{2}\Big) + \Big(1 - \cos\frac{\gamma_2}{2}\Big)\Bigg) \times \\ \times \frac{1}{2}\Big(\cos\frac{\gamma_3}{2} + \cos\frac{3\gamma_3}{2}\Big) + \Big(1 - \cos\frac{\gamma_3}{2}\Big)\Bigg)\ldots\Bigg) \times \\ \times \frac{1}{2}\Big(\cos\frac{\gamma_{m-2}}{2} + \cos\frac{3\gamma_{m-2}}{2}\Big) + \Big(1 - \cos\frac{\gamma_{m-2}}{2}\Big)\Bigg) \times \\ \times \frac{1}{2}\Big(\cos\frac{\alpha}{2} + \cos\frac{3\alpha}{2}\Big) + \Big(1 - \cos\frac{\alpha}{2}\Big)\Bigg]. \quad (22)\end{aligned}$$

Итак, мы получили, что для произвольных векторов $\Psi_1 \in M_{\text{Sph}}$, $\Psi_2 \in S^{m-1}$, введенных в начале доказательства, для которых выполнено ограничение (21), справедлива оценка (22).

Заметим, что вектор $\Psi_2 \in S^{m-1}$, для которого существует такой вектор $\Psi_1 \in M_{\text{Sph}}$, что выполняются ограничения (21), всегда существует. Зафиксируем такой вектор $\Psi_2 \in S^{m-1}$. Покажем, что оценка (22) справедлива для любого вектора $\Psi_1 \in M_{\text{Sph}}$.

С этого момента будем считать, что выполнено следующее ограничение на углы γ_i:

$$0 < \gamma_i \leqslant \frac{2}{\sqrt{m-2}}, \; i = 1, \ldots, m-2,$$

Скалярное произведение векторов рассмотрим как функцию от $(\alpha_1, \ldots, \alpha_{m-1})$:

$$\begin{aligned}&\langle \Psi_1, \Psi_2 \rangle = \\ &= \prod_{i=1}^{m-1} \sin\alpha_i \sin\beta_i + \ldots + \cos\alpha_{k-1}\cos\beta_{k-1}\prod_{i=k}^{m-1}\sin\alpha_i\sin\beta_i + \ldots + \cos\alpha_{m-1}\cos\beta_{m-1} = \\ &= f(\alpha_1, \ldots, \alpha_{m-1}).\end{aligned}$$

Покажем, что максимум этой функции на множестве

$$\{\alpha_i = s_i\gamma_i,\ s_i = 0,1,\dots,S_i,\ i = 1,2,\dots,m-2,\ \alpha_{m-1} = l\alpha,\ l = 0,1,\dots,L\} \tag{23}$$

достигается на векторе $(\alpha_1^*,\dots,\alpha_{m-1}^*)$ таком, что

$$|\alpha_i^* - \beta_i| = \frac{\gamma_i}{2}, \quad i = 1,\dots,m-2; \quad \left|\alpha_{m-1}^* - \beta_{m-1}\right| = \frac{\alpha}{2}.$$

Запишем необходимое условие экстремума по переменной α_1:

$$f_{\alpha_1}(\alpha_1,\alpha_2^*,\dots,\alpha_{m-1}^*) = (\cos\alpha_1\sin\beta_1 - \sin\alpha_1\cos\beta_1)\prod_{i=2}^{m-1}\sin\alpha_i^*\sin\beta_i = 0.$$

Если $\prod_{i=2}^{m-1}\sin\alpha_i^*\sin\beta_i = 0$, то функция f не зависит от значения угла α_1. Поэтому в этом случае можно брать любое значение α_1^*, в частности такое, что

$$|\alpha_1^* - \beta_1| = \frac{\gamma_1}{2}.$$

Пусть $\prod_{i=2}^{m-1}\sin\alpha_i^*\sin\beta_i \neq 0$. Тогда

$$\sin(\beta_1 - \alpha_1) = 0 \quad \Longrightarrow \quad \alpha_1 = \beta_1.$$

С учетом (21) и (23) имеем:

$$|\alpha_1^* - \beta_1| = \frac{\gamma_1}{2}.$$

Запишем необходимое условие экстремума по переменной α_2:

$$\begin{aligned} f_{\alpha_2}(\alpha_1^*,\alpha_2,\alpha_2^*\dots,\alpha_{m-1}^*) &= \\ &= (\sin\alpha_1^*\sin\beta_1\cos\alpha_2\sin\beta_2 + \cos\alpha_1^*\cos\beta_1\cos\alpha_2\sin\beta_2 - \sin\alpha_2\cos\beta_2)\times \\ &\qquad \times\prod_{i=3}^{m-1}\sin\alpha_i^*\sin\beta_i = 0. \end{aligned}$$

Если $\prod_{i=3}^{m-1}\sin\alpha_i^*\sin\beta_i = 0$, то функция f не зависит от значения угла α_2. Поэтому в этом случае можно брать любое значение α_2^*, в частности такое, что

$$|\alpha_2^* - \beta_2| = \frac{\gamma_2}{2}.$$

Пусть $\prod_{i=3}^{m-1}\sin\alpha_i^*\sin\beta_i \neq 0$. Тогда

$$\cos(\beta_1 - \alpha_1^*)\cos\alpha_2\sin\beta_2 - \sin\alpha_2\cos\beta_2 = 0 \quad \Longrightarrow \quad \cos\frac{\gamma_1}{2}\cos\alpha_2\sin\beta_2 = \sin\alpha_2\cos\beta_2.$$

Покажем, что

$$\cos\frac{\gamma_1}{2}\cos\alpha_2\sin\beta_2 = \sin\alpha_2\cos\beta_2 \quad \Longrightarrow \quad \beta_2 - \frac{\gamma_2}{2} \leqslant \alpha_2 \leqslant \beta_2 + \frac{\gamma_2}{2}.$$

Действительно, пусть

$$g(\alpha_2) = \cos\frac{\gamma_1}{2}\cos\alpha_2\sin\beta_2 - \sin\alpha_2\cos\beta_2.$$

Тогда если $\frac{\pi}{2} - \frac{\gamma_2}{2} \leqslant \beta_2 \leqslant \frac{\pi}{2}$, то

$$\begin{aligned} g\left(\beta_2 + \frac{\gamma_2}{2}\right) &= \cos\frac{\gamma_1}{2}\cos\left(\beta_2 + \frac{\gamma_2}{2}\right)\sin\beta_2 - \sin\left(\beta_2 + \frac{\gamma_2}{2}\right)\cos\beta_2 \leqslant \\ &\leqslant \left\{\frac{\pi}{2} \leqslant \beta_2 + \frac{\gamma_2}{2} \leqslant \frac{\pi}{2} + \frac{\gamma_2}{2}\right\} \leqslant \cos\frac{\gamma_1}{2}\cos\frac{\pi}{2}\sin\beta_2 - \sin\left(\beta_2 + \frac{\gamma_2}{2}\right)\cos\frac{\pi}{2} = 0, \end{aligned}$$

$$g\left(\beta_2-\frac{\gamma_2}{2}\right)=\cos\frac{\gamma_1}{2}\cos\left(\beta_2-\frac{\gamma_2}{2}\right)\sin\beta_2-\sin\left(\beta_2-\frac{\gamma_2}{2}\right)\cos\beta_2=$$
$$=\cos\frac{\gamma_1}{2}\sin\frac{\gamma_2}{2}+\left(\cos\frac{\gamma_1}{2}-1\right)\sin\left(\beta_2-\frac{\gamma_2}{2}\right)\cos\beta_2\geqslant\left\{\frac{\pi}{2}-\gamma_2\leqslant\beta_2-\frac{\gamma_2}{2}\leqslant\frac{\pi}{2}-\frac{\gamma_2}{2}\right\}\geqslant$$
$$\geqslant\cos\frac{\gamma_1}{2}\sin\frac{\gamma_2}{2}+\left(\cos\frac{\gamma_1}{2}-1\right)\sin\left(\frac{\pi}{2}-\frac{\gamma_2}{2}\right)\cos\left(\frac{\pi}{2}-\frac{\gamma_2}{2}\right)=$$
$$=\cos\frac{\gamma_1}{2}\sin\frac{\gamma_2}{2}+\left(\cos\frac{\gamma_1}{2}-1\right)\cos\frac{\gamma_2}{2}\sin\frac{\gamma_2}{2}\geqslant$$
$$\geqslant\left\{0<\gamma_1\leqslant\frac{2}{\sqrt{m-2}}\leqslant 2\ \Rightarrow\ \cos\frac{\gamma_1}{2}\geqslant\cos 1>\cos\frac{\pi}{3}=\frac{1}{2}\right\}\geqslant\frac{1}{2}\sin\frac{\gamma_2}{2}\left(1-\cos\frac{\gamma_2}{2}\right)\geqslant 0,$$

Если $\frac{\pi}{2}\leqslant\beta_2\leqslant\frac{\pi}{2}+\frac{\gamma_2}{2}$, то

$$g\left(\beta_2+\frac{\gamma_2}{2}\right)=\cos\frac{\gamma_1}{2}\cos\left(\beta_2+\frac{\gamma_2}{2}\right)\sin\beta_2-\sin\left(\beta_2+\frac{\gamma_2}{2}\right)\cos\beta_2=$$
$$=-\cos\frac{\gamma_1}{2}\sin\frac{\gamma_2}{2}+\left(\cos\frac{\gamma_1}{2}-1\right)\sin\left(\beta_2+\frac{\gamma_2}{2}\right)\cos\beta_2\leqslant\left\{\frac{\pi}{2}+\frac{\gamma_2}{2}\leqslant\beta_2+\frac{\gamma_2}{2}\leqslant\frac{\pi}{2}+\gamma_2\right\}\leqslant$$
$$\leqslant-\cos\frac{\gamma_1}{2}\sin\frac{\gamma_2}{2}+\left(\cos\frac{\gamma_1}{2}-1\right)\sin\left(\frac{\pi}{2}+\frac{\gamma_2}{2}\right)\cos\left(\frac{\pi}{2}+\frac{\gamma_2}{2}\right)=$$
$$=-\cos\frac{\gamma_1}{2}\sin\frac{\gamma_2}{2}+\left(1-\cos\frac{\gamma_1}{2}\right)\cos\frac{\gamma_2}{2}\sin\frac{\gamma_2}{2}\leqslant\left\{\cos\frac{\gamma_1}{2}\geqslant\frac{1}{2}\right\}\leqslant$$
$$\leqslant-\frac{1}{2}\sin\frac{\gamma_2}{2}\left(1-\cos\frac{\gamma_2}{2}\right)\leqslant 0,$$

$$g\left(\beta_2-\frac{\gamma_2}{2}\right)=\cos\frac{\gamma_1}{2}\cos\left(\beta_2-\frac{\gamma_2}{2}\right)\sin\beta_2-\sin\left(\beta_2-\frac{\gamma_2}{2}\right)\cos\beta_2\geqslant$$
$$\geqslant\left\{\frac{\pi}{2}-\frac{\gamma_2}{2}\leqslant\beta_2-\frac{\gamma_2}{2}\leqslant\frac{\pi}{2}\right\}\geqslant\cos\frac{\gamma_1}{2}\cos\frac{\pi}{2}\sin\beta_2-\sin\left(\beta_2-\frac{\gamma_2}{2}\right)\cos\frac{\pi}{2}=0.$$

Мы получили, что $g\left(\beta_2+\frac{\gamma_2}{2}\right)\leqslant 0$ и $g\left(\beta_2-\frac{\gamma_2}{2}\right)\geqslant 0$. Откуда следует, что нуль функции $g(\alpha_2)$ принадлежит указанному отрезку:

$$\beta_2-\frac{\gamma_2}{2}\leqslant\alpha_2\leqslant\beta_2+\frac{\gamma_2}{2}.$$

Следовательно,

$$|\alpha_2^*-\beta_2|=\frac{\gamma_2}{2}.$$

Покажем, что аналогичный результат верен и в случае α_i^*, $i=3,\ldots,m-1$.
Пусть

$$|\alpha_j^*-\beta_j|=\frac{\gamma_j}{2},\quad j=1,\ldots,i-1.$$

Запишем необходимое условие экстремума по переменной α_i:

$$f_{\alpha_i}(\alpha_1^*,\ldots,\alpha_{i-1}^*,\alpha_i,\alpha_{i+1}^*,\ldots,\alpha_{m-1}^*)=$$
$$=\left(h(\alpha_1^*,\ldots,\alpha_{i-1}^*)\cos\alpha_i\sin\beta_i-\sin\alpha_i\cos\beta_i\right)\prod_{k=i+1}^{m-1}\sin\alpha_k^*\sin\beta_k=0,$$

где

$$h(\alpha_1^*,\ldots,\alpha_{i-1}^*)=\prod_{k=1}^{i-1}\sin\alpha_k^*\sin\beta_k+\cos\alpha_1^*\cos\beta_1\prod_{k=2}^{i-1}\sin\alpha_k^*\sin\beta_k+\ldots+$$
$$+\cos\alpha_{i-2}^*\cos\beta_{i-2}\sin\alpha_{i-1}^*\sin\beta_{i-1}+\cos\alpha_{i-1}^*\cos\beta_{i-1}.$$

С одной стороны,

$$h(\alpha_1^*,\dots,\alpha_{i-1}^*)=\cos(\alpha_1^*-\beta_1)\prod_{k=2}^{i-1}\sin\alpha_k^*\sin\beta_k+\cos\alpha_2^*\cos\beta_2\prod_{k=3}^{i-1}\sin\alpha_k^*\sin\beta_k+\ldots+$$
$$+\cos\alpha_{i-2}^*\cos\beta_{i-2}\sin\alpha_{i-1}^*\sin\beta_{i-1}+\cos\alpha_{i-1}^*\cos\beta_{i-1}\leqslant$$
$$\leqslant\prod_{k=2}^{i-1}\sin\alpha_k^*\sin\beta_k+\cos\alpha_2^*\cos\beta_2\prod_{k=3}^{i-1}\sin\alpha_k^*\sin\beta_k+\ldots+$$
$$+\cos\alpha_{i-2}^*\cos\beta_{i-2}\sin\alpha_{i-1}^*\sin\beta_{i-1}+\cos\alpha_{i-1}^*\cos\beta_{i-1}=$$

$$=\cos(\alpha_2^*-\beta_2)\prod_{k=3}^{i-1}\sin\alpha_k^*\sin\beta_k+\cos\alpha_3^*\cos\beta_3\prod_{k=4}^{i-1}\sin\alpha_k^*\sin\beta_k+\ldots+$$
$$+\cos\alpha_{i-2}^*\cos\beta_{i-2}\sin\alpha_{i-1}^*\sin\beta_{i-1}+\cos\alpha_{i-1}^*\cos\beta_{i-1}\leqslant\ldots\leqslant$$
$$\leqslant\sin\alpha_{i-1}^*\sin\beta_{i-1}+\cos\alpha_{i-1}^*\cos\beta_{i-1}=\cos\frac{\gamma_{i-1}}{2}.$$

С другой стороны, пользуясь тем, что

$$0<\gamma_i\leqslant\frac{2}{\sqrt{m-2}},\ i=1,\dots,m-2,$$

имеем

$$h(\alpha_1^*,\dots,\alpha_{i-1}^*)=\prod_{k=1}^{i-1}\sin\alpha_k^*\sin\beta_k+\cos\alpha_1^*\cos\beta_1\prod_{k=2}^{i-1}\sin\alpha_k^*\sin\beta_k+\ldots+$$
$$+\cos\alpha_{i-2}^*\cos\beta_{i-2}\sin\alpha_{i-1}^*\sin\beta_{i-1}+\cos\alpha_{i-1}^*\cos\beta_{i-1}=$$
$$=\Bigg(\Bigg(\ldots\Bigg(\Bigg((\cos(\alpha_1^*-\beta_1)-1)\,\frac12\,(\cos(\alpha_2^*-\beta_2)-\cos(\alpha_2^*+\beta_2))+(\cos(\alpha_2^*-\beta_2)-1)\Bigg)\times$$
$$\times\frac12\,(\cos(\alpha_3^*-\beta_3)-\cos(\alpha_3^*+\beta_3))+(\cos(\alpha_3^*-\beta_3)-1)\Bigg)\ldots\Bigg)\times$$
$$\times\frac12\,\big(\cos(\alpha_{i-2}^*-\beta_{i-2})-\cos(\alpha_{i-2}^*+\beta_{i-2})\big)+\big(\cos(\alpha_{i-2}^*-\beta_{i-2})-1\big)\Bigg)\times$$
$$\times\frac12\,\big(\cos(\alpha_{i-1}^*-\beta_{i-1})-\cos(\alpha_{i-1}^*+\beta_{i-1})\big)+\cos(\alpha_{i-1}^*-\beta_{i-1})\geqslant$$
$$\geqslant\sum_{j=1}^{i-1}\cos\frac{\gamma_j}{2}-i+2\geqslant\sum_{j=1}^{i-1}\left(1-\frac{\gamma_j^2}{8}\right)-i+2=1-\sum_{j=1}^{i-1}\frac{\gamma_j^2}{8}\geqslant1-\frac{i-1}{2(m-2)}\geqslant\frac12.$$

Таким образом,

$$\frac12\leqslant h(\alpha_1^*,\dots,\alpha_{i-1}^*)\leqslant\cos\frac{\gamma_{i-1}}{2}.$$

Далее действуем аналогично случаю $i=2$. Полагая $\prod_{k=i+1}^{m-1}\sin\alpha_k^*\sin\beta_k\neq0$, имеем:

$$h(\alpha_1^*,\dots,\alpha_{i-1}^*)\cos\alpha_i\sin\beta_i-\sin\alpha_i\cos\beta_i=0.$$

Покажем, что

$$h(\alpha_1^*,\dots,\alpha_{i-1}^*)\cos\alpha_i\sin\beta_i=\sin\alpha_i\cos\beta_i\quad\Longrightarrow\quad\beta_i-\frac{\gamma_i}{2}\leqslant\alpha_i\leqslant\beta_i+\frac{\gamma_i}{2},$$

где через γ_{m-1} обозначен угол α для того, чтобы не рассматривать отдельно случай $i = m-1$, который по сути ничем не отличается от остальных случаев.

Пусть

$$g(\alpha_i) = h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\cos\alpha_i \sin\beta_i - \sin\alpha_i \cos\beta_i.$$

Тогда если $\frac{\pi}{2} - \frac{\gamma_i}{2} \leqslant \beta_i \leqslant \frac{\pi}{2}$, то

$$\begin{aligned} g\left(\beta_i + \frac{\gamma_i}{2}\right) &= h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\cos\left(\beta_i + \frac{\gamma_i}{2}\right)\sin\beta_i - \sin\left(\beta_i + \frac{\gamma_i}{2}\right)\cos\beta_i \leqslant \\ &\leqslant \left\{\frac{\pi}{2} \leqslant \beta_i + \frac{\gamma_i}{2} \leqslant \frac{\pi}{2} + \frac{\gamma_i}{2},\ h(\alpha_1^*, \ldots, \alpha_{i-1}^*) \geqslant 0\right\} \leqslant \\ &\leqslant h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\cos\frac{\pi}{2}\sin\beta_i - \sin\left(\beta_i + \frac{\gamma_i}{2}\right)\cos\frac{\pi}{2} = 0, \end{aligned}$$

$$\begin{aligned} g\left(\beta_i - \frac{\gamma_i}{2}\right) &= h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\cos\left(\beta_i - \frac{\gamma_i}{2}\right)\sin\beta_i - \sin\left(\beta_i - \frac{\gamma_i}{2}\right)\cos\beta_i = \\ &= h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\sin\frac{\gamma_i}{2} + \left(h(\alpha_1^*, \ldots, \alpha_{i-1}^*) - 1\right)\sin\left(\beta_i - \frac{\gamma_i}{2}\right)\cos\beta_i \geqslant \\ &\geqslant \left\{\frac{\pi}{2} - \gamma_i \leqslant \beta_i - \frac{\gamma_i}{2} \leqslant \frac{\pi}{2} - \frac{\gamma_i}{2},\ \frac{1}{2} \leqslant h(\alpha_1^*, \ldots, \alpha_{i-1}^*) \leqslant \cos\frac{\gamma_{i-1}}{2}\right\} \geqslant \\ &\geqslant h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\sin\frac{\gamma_i}{2} + \left(h(\alpha_1^*, \ldots, \alpha_{i-1}^*) - 1\right)\sin\left(\frac{\pi}{2} - \frac{\gamma_i}{2}\right)\cos\left(\frac{\pi}{2} - \frac{\gamma_i}{2}\right) = \\ &= h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\sin\frac{\gamma_i}{2} + \left(h(\alpha_1^*, \ldots, \alpha_{i-1}^*) - 1\right)\cos\frac{\gamma_i}{2}\sin\frac{\gamma_i}{2} \geqslant \frac{1}{2}\sin\frac{\gamma_i}{2}\left(1 - \cos\frac{\gamma_i}{2}\right) \geqslant 0, \end{aligned}$$

Если $\frac{\pi}{2} \leqslant \beta_i \leqslant \frac{\pi}{2} + \frac{\gamma_i}{2}$, то

$$\begin{aligned} g\left(\beta_i + \frac{\gamma_i}{2}\right) &= h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\cos\left(\beta_i + \frac{\gamma_i}{2}\right)\sin\beta_i - \sin\left(\beta_i + \frac{\gamma_i}{2}\right)\cos\beta_i = \\ &= -h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\sin\frac{\gamma_i}{2} + \left(h(\alpha_1^*, \ldots, \alpha_{i-1}^*) - 1\right)\sin\left(\beta_i + \frac{\gamma_i}{2}\right)\cos\beta_i \leqslant \\ &\leqslant \left\{\frac{\pi}{2} + \frac{\gamma_i}{2} \leqslant \beta_i + \frac{\gamma_i}{2} \leqslant \frac{\pi}{2} + \gamma_i,\ \frac{1}{2} \leqslant h(\alpha_1^*, \ldots, \alpha_{i-1}^*) \leqslant \cos\frac{\gamma_{i-1}}{2}\right\} \leqslant \\ &\leqslant -h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\sin\frac{\gamma_i}{2} + \left(h(\alpha_1^*, \ldots, \alpha_{i-1}^*) - 1\right)\sin\left(\frac{\pi}{2} + \frac{\gamma_i}{2}\right)\cos\left(\frac{\pi}{2} + \frac{\gamma_i}{2}\right) = \\ &= -h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\sin\frac{\gamma_i}{2} + \left(1 - h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\right)\cos\frac{\gamma_i}{2}\sin\frac{\gamma_i}{2} \leqslant -\frac{1}{2}\sin\frac{\gamma_i}{2}\left(1 - \cos\frac{\gamma_i}{2}\right) \leqslant 0, \end{aligned}$$

$$\begin{aligned} g\left(\beta_i - \frac{\gamma_i}{2}\right) &= h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\cos\left(\beta_i - \frac{\gamma_i}{2}\right)\sin\beta_i - \sin\left(\beta_i - \frac{\gamma_i}{2}\right)\cos\beta_i \geqslant \\ &\geqslant \left\{\frac{\pi}{2} - \frac{\gamma_i}{2} \leqslant \beta_i - \frac{\gamma_i}{2} \leqslant \frac{\pi}{2},\ h(\alpha_1^*, \ldots, \alpha_{i-1}^*) \geqslant 0\right\} \geqslant \\ &\geqslant h(\alpha_1^*, \ldots, \alpha_{i-1}^*)\cos\frac{\pi}{2}\sin\beta_i - \sin\left(\beta_i - \frac{\gamma_i}{2}\right)\cos\frac{\pi}{2} = 0. \end{aligned}$$

Мы получили, что $g\left(\beta_i + \frac{\gamma_i}{2}\right) \leqslant 0$ и $g\left(\beta_i - \frac{\gamma_i}{2}\right) \geqslant 0$. Откуда следует, что нуль функции $g(\alpha_i)$ принадлежит указанному отрезку:

$$\beta_i - \frac{\gamma_i}{2} \leqslant \alpha_i \leqslant \beta_i + \frac{\gamma_i}{2}.$$

Следовательно,

$$|\alpha_i^* - \beta_i| = \frac{\gamma_i}{2}.$$

Таким образом, мы доказали, что для некоторого фиксированного вектора

$$\Psi_2 = \left(\prod_{i=1}^{m-1} \sin\beta_i, \ldots, \cos\beta_{k-1} \prod_{i=k}^{m-1} \sin\beta_i, \ldots, \cos\beta_{m-1} \right) \in S^{m-1}$$

и для любого вектора $\Psi \in M_{\text{Sph}}$ существует такой вектор

$$\Psi_1 = \left(\prod_{i=1}^{m-1} \sin\alpha_i, \ldots, \cos\alpha_{k-1} \prod_{i=k}^{m-1} \sin\alpha_i, \ldots, \cos\alpha_{m-1} \right) \in M_{\text{Sph}},$$

что выполняется

$$\|\Psi - \Psi_2\| \geqslant \|\Psi_1 - \Psi_2\|,$$

причем

$$|\alpha_i - \beta_i| = \frac{\gamma_i}{2}, \quad i = 1, \ldots, m-2; \quad |\alpha_{m-1} - \beta_{m-1}| = \frac{\alpha}{2}.$$

Получили, что оценка (22) справедлива для любого вектора $\Psi_1 \in M_{\text{Sph}}$, а значит нижняя оценка (4) для радиуса покрытия доказана. □

В заключение хотелось бы выразить глубокую благодарность д.ф.-м.н. Г. К. Каменеву за постановку задачи и полезные замечания, а также проф. А. В. Лотову за помощь в работе над статьей.

Список литературы

[1] *Торп Дж.* Начальные главы дифференциальной геометрии. — Изд. Платон: 1982.

[2] *Лотов А. В., Бушенков В. А., Каменев Г. К., Черных О. Л.* Компьютер и поиск компромисса. Метод достижимых целей. — М.: Наука, 1997.

[3] *Каменев Г. К.* Полиэдральная аппроксимация шара Методом Глубоких Ям с оптимальным порядком роста мощности гранной структуры. // В кн.: Тр. Межд конф. «Численная геометрия, построение расчетных сеток и высокопроизводительные вычисления». — М.: ВЦ РАН, 2010. — С. 47–52.

[4] *Каменев Г. К.* Оптимальные адаптивные методы полиэдральной аппроксимации выпуклых тел. — М.: ВЦ РАН, 2007.

[5] *Роджерс К.* Укладки и покрытия. — М.: Мир, 1968.

[6] *Конвей Дж., Слоэн Н.* Упаковки шаров, решетки и группы. Т. 1. — М.: Мир, 1990.

[7] *Самсонов С. П.* Восстановление выпуклого множества по его опорной функции с заданной точностью // Вестн. МГУ. Сер. 15. Вычисл. матем. и кибернетика. — 1983. — № 1. — С. 68–71.

УДК 512.624.3

О КРИПТОАНАЛИЗЕ LILI-128, ОСНОВАННОМ НА ЧАСТИЧНОМ ОПРОБОВАНИИ И МОНОМИАЛЬНОЙ СОВМЕСТНОСТИ СИСТЕМ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ

© 2011 г. А. С. Мелузов

asmeluzov@cs.msu.ru, asmelouzov@mail.ru

Кафедра математической кибернетики

1 Введение

Задача решения систем полиномиальных булевых уравнений является актуальной для многих разделов математики. В теории конечных автоматов, теории кодирования и криптологии возникают задачи изучения и решения систем булевых уравнений. Задача решения произвольной системы полиномиальных булевых уравнений является NP-трудной [1]. Но, поскольку в теории NP-полных задач сложность оценивается «в худшем случае», то теоретический и практический интерес представляет разработка эффективных алгоритмов для конкретных классов систем булевых уравнений.

Предлагаются различные методики, в том числе, построение с помощью алгоритма Бухбергера или алгоритмов F_4 и F_5, разработанных Ж.-К. Фажере [2,3], базиса Грёбнера идеала, описываемого системой уравнений [4]; линеаризация системы с использованием дополнительных приемов повышения эффективности [5–10]. Для некоторых частных классов систем разработаны алгоритмы решения, использующие быстрый обход дерева решений системы [11,12], а также ассоциативные принципы использования памяти [13].

Одним из важнейших применений задачи решения систем булевых уравнений является алгебраический криптоанализ. Моделируя работу криптографического алгоритма с помощью системы полиномиальных булевых уравнений мы можем свести задачу поиска криптографического ключа к задаче поиска решения системы полиномиальных булевых уравнений. В данном направлении проведены исследования множества криптографических алгоритмов.

В настоящей статье предлагается метод решения систем булевых уравнений, основанный на частичном опробовании и использовании мономиальной совместности редуцированных систем для определения ключа потокового шифра LILI-128 [15].

2 Описание шифратора LILI-128 и постановка задачи

2.1 Потоковый шифратор LILI-128

Потоковый шифратор LILI-128 состоит из двух фильтрующих генераторов (39-разрядный $\mathrm{LFSR}_c(f_c)$ и 89-разрядный $\mathrm{LFSR}_d(f_d)$), первый из которых управляет режимом работы второго. Ключом шифратора является начальное заполнение регистров сдвига фильтрующих генераторов, а в качестве гаммирующей последовательности используется выходная последовательность второго фильтрующего генератора.

Первый фильтрующий генератор состоит из линейного регистра сдвига LFSR_c и фильтрующей функции f_c. Выходная последовательность данного генераторов определяет число тактов (1, 2, 3 или 4), которое должен совершить второй фильтрующий генератор $\mathrm{LFSR}_d(f_d)$.

При этом, элементы LILI-128 имеют следующие параметры:

- LFSR_c — линейный регистр обратной связи с полиномом обратных связей $\lambda^{39} \oplus \lambda^{35} \oplus \oplus \lambda^{33} \oplus \lambda^{31} \oplus \lambda^{17} \oplus \lambda^{15} \oplus \lambda^{14} \oplus \lambda^2 \oplus 1$;

- фильтрующая функция управляющего генератора $f_c\colon \mathrm{GF}(2)^2 \to \mathrm{GF}(4)$, $f_c = 2u_{12} + u_{20} + 1$. Значение функции f_c на каждом такте работы шифратора определяет, сколько тактов работы совершит линейный регистр обратной связи второго фильтрующего генератора;

- LFSR_d — линейный регистр обратной связи с полиномом обратных связей $\lambda^{89} \oplus \lambda^{83} \oplus \lambda^{80} \oplus \lambda^{55} \oplus \lambda^{53} \oplus \lambda^{42} \oplus \lambda^{39} \oplus \lambda \oplus 1$;

- фильтрующая функция $f_d\colon \mathrm{GF}(2)^{10} \to \mathrm{GF}(2)$, которая в описании шифратора была задана таблицей, но по таблице можно построить соответствующий полином степени 6:

$$
\begin{aligned}
&f_d(x_0, x_1, x_3, x_7, x_{12}, x_{20}, x_{30}, x_{44}, x_{65}, x_{80}) = \\
&\quad = x_{12} + x_7 + x_3 + x_1 + x_{80}x_{20} + x_{80}x_7 + x_{65}x_3 + x_{65}x_0 + x_{44}x_1 + x_{44}x_0 + x_{30}x_{20} + \\
&\quad + x_{80}x_{65}x_{12} + x_{80}x_{65}x_7 + x_{80}x_{65}x_3 + x_{80}x_{65}x_1 + x_{80}x_{44}x_7 + x_{80}x_{44}x_3 + x_{80}x_{30}x_{20} + \\
&\quad + x_{80}x_{30}x_{12} + x_{80}x_{30}x_7 + x_{65}x_{44}x_{20} + x_{65}x_{44}x_3 + x_{65}x_{30}x_{20} + x_{65}x_{30}x_7 + x_{65}x_{30}x_3 + \\
&\quad + x_{80}x_{65}x_{44}x_{20} + x_{80}x_{65}x_{44}x_7 + x_{80}x_{65}x_{44}x_3 + x_{80}x_{65}x_{44}x_0 + x_{80}x_{65}x_{30}x_{20} + \\
&\quad + x_{80}x_{65}x_{30}x_7 + x_{80}x_{65}x_{30}x_1 + x_{80}x_{44}x_{30}x_{12} + x_{80}x_{44}x_{30}x_3 + x_{65}x_{44}x_{30}x_7 + \\
&\quad + x_{65}x_{44}x_{30}x_1 + x_{65}x_{30}x_{20}x_{12} + x_{65}x_{30}x_{20}x_7 + \\
&\quad + x_{80}x_{65}x_{44}x_{30}x_7 + x_{80}x_{65}x_{44}x_{30}x_3 + x_{80}x_{65}x_{30}x_{20}x_{12} + \\
&\quad + x_{80}x_{65}x_{30}x_{20}x_7 + x_{65}x_{44}x_{30}x_{20}x_{12} + x_{65}x_{44}x_{30}x_{20}x_7 + \\
&\quad + x_{80}x_{65}x_{44}x_{30}x_{20}x_{12} + x_{80}x_{65}x_{44}x_{30}x_{20}x_7.
\end{aligned}
$$

Схема работы шифратора приведена на рисунке 1.

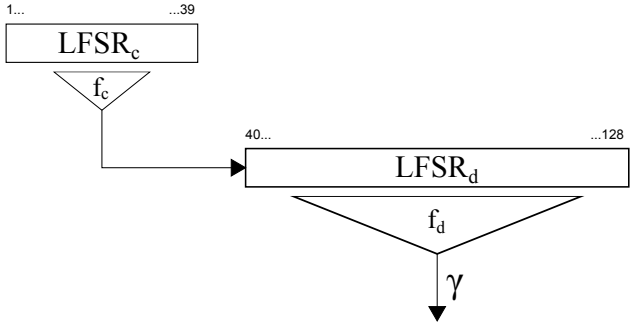


Рис. 1. Схема работы шифратора LILI-128.

Отметим здесь одну интересную особенность работы двух регистров LILI-128, доказанную в работе [14].

Лемма 1. После каждых $\delta_c = 2^{39} - 1$ тактов работы регистра LFSR_c, регистр LFSR_d совершит ровно $\delta_d = 5 \cdot 2^{38} - 1$ тактов.

2.2 Описание атаки

Пусть $c(t)$ — последовательность бит шифрованного текста, полученная в результате побитового сложения битов открытого текста $u(t)$ и бит шифрующей последовательности $\gamma(t)$, вырабатываемой шифратором. В таком случае, если нам известна последовательность $c(t)$, $1 \leqslant t \leqslant m$ (например, передаваемая по незащищенному каналу связи), и, кроме того, известна последовательность бит открытого текста $u(t)$, $1 \leqslant t \leqslant m$, то мы можем восстановить биты шифрующей последовательности $\gamma(t) = c(t) \oplus u(t)$, $1 \leqslant t \leqslant m$ (m — количество известных соответствий бит открытого и шифрованного текста).

Задача состоит в восстановлении по известной части шифрующей последовательности исходного значения ключа LILI-128 (то есть исходного заполнения линейных регистров сдвига).

Успешная реализация атаки, позволит восстановить шифрующую последовательность любой необходимой длины и, следовательно, по шифрованному тексту восстановить весь открытый текст.

Существуют различные подходы к криптоанализу потоковых шифров и, в частности, LILI-128. В следующем разделе рассмотрены некоторые из них.

3 Существующие подходы к криптоанализу LILI-128

По вопросам, связанным с криптоанализом LILI-128, за прошедшее с момента опубликования описания шифратора время было опубликовано значительное число работ. Сами авторы шифратора в работе [15] утверждают, что оценка трудоемкости восстановления ключа по известным шифрованному и соответствующему ему открытому тексту не ниже 2^{112} операций.

Необходимо отметить, что в работе [16] была отмечена крайне низкая стойкость LILI-128 к атакам со связанными ключами, однако, значительно интереснее рассматривать другую атаку, не требующую доступа к самому шифратору.

Среди работ, посвященных восстановлению значения исходного заполнения регистров по известной гаммирующей последовательности можно выделить два широко распространенных подхода. Это алгебраический и корелляционный подходы к задаче восстановления ключа потокового шифратора LILI-128 по известной последовательности открытого и шифрованного текста.

Суть алгебраического подхода состоит в составлении системы алгебраических уравнений, описывающей работу LILI-128, и последующего решения полученной системы одним из известных методов.

Корреляционный подход состоит в предварительном составлении таблицы возможных шифрующих последовательностей, генерируемых поточным шифратором при некоторых начальных заполнениях регистров, и последующего сопоставления известной последовательности со значениями в таблице [17].

Рассмотрим существующие подходы подробнее.

В работе [18] предложен алгебраический метод криптографического анализа LILI-128. Предлагается строить систему булевых алгебраических уравнений от переменных ключа. Основная идея статьи заключается в том, чтобы не использовать имеющие алгебраическую степень 6 уравнения вида

$$f_d(L^i(x_1, x_2, \ldots, x_{89})) = \gamma_i,$$

где $L(x_1, x_2, \ldots, x_{89})$ — линейный оператор, определяемый полиномом обратных связей LFSR_d, а γ_i — i-й бит гаммирующей последовательности (выходная последовательность фильтрующего генератора $\mathrm{LFSR}_d(f_d)$).

Вместо этого предлагается использовать уравнения одного из следующих трех видов:

$$f_d(L^i(x_1, x_2, \ldots, x_{89})) \cdot g(L^i(x_1, x_2, \ldots, x_{89})) = \gamma_i \cdot g(L^i(x_1, x_2, \ldots, x_{89})),$$
$$0 = g(L^i(x_1, x_2, \ldots, x_{89})), \quad f_d \cdot g \equiv 0, \quad \gamma_i = 1,$$
$$f_d(L^i(x_1, x_2, \ldots, x_{89})) \cdot g(L^i(x_1, x_2, \ldots, x_{89})) = 0, \quad \gamma_i = 0,$$

где g — аннигилятор функции f, подобранный таким образом, чтобы степень уравнения была не выше 4. В работе [18] обозначено, что для функции f_d для любого значения γ_i можно построить 14 линейно независимых уравнений степени не выше 4. При любом значении бита гаммирующей последовательности для составления системы мы сможем использовать 14 линейно независимых уравнений. Благодаря такому подходу мы получим в 14 раз больше уравнений в системе. Кроме того, поскольку их степень не будет превышать 4, то максимальное количество мономов в построенной таким образом системе равно $\sum_{i=1}^{4} \binom{89}{i} \approx 2^{21}$. Предполагается, что для успешного применения метода линеаризации необходимо чтобы число уравнений было также примерно равно 2^{21}, то есть необходимое число бит открытого и шифрованного текста, которые должны быть известны, должно быть равно $2^{21}/14$. В результате, проводя полное опробование начального заполнения LFSR_c (вариант A), и учитывая, что трудоемкость решения линейной системы уравнений методом Штрассена в соответствии с [19] составляет $7 \cdot T^{\log_2 7}$

битовых операций (или, по утверждению [18], на ЭВМ с 64-битной архитектурой регистров, $\frac{7}{64} \cdot T^{\log_2 7}$ тактов процессора), получим общую трудоемкость метода $2^{39} \cdot 7 \cdot T^{\log_2 7} \approx 2^{102}$ битовых операций.

В качестве альтернативы (вариант Б) предлагается взять гораздо более длинную последовательность открытого и шифрованного текста и воспользоваться Леммой 1. Так за $2^{39} - 1$ такт работы первого регистра, второй будет сдвигаться ровно на $5 \cdot 2^{38} - 1$ тактов. Тогда, выбирая в потоке известной гаммирующей последовательности биты, находящиеся на позициях с номерами $\alpha + \beta(2^{39} - 1)$ можно на их основе составить систему алгебраических уравнений без необходимости опробовать управляющий регистр. Трудоемкость такого подхода составит $7 \cdot T^{\log_2 7} \approx 2^{63}$ битовых операций и потребует знания примерно 2^{57} бит открытого/шифрованного текста, либо 2^{18} бит с заданных определенным образом позиций.

Другой подход — логический криптоанализ предложен в работе [20]. Авторы предлагают при фиксированном начальном заполнении первого (управляющего) фильтрующего генератора технику построения системы КНФ, решением которой является исходное заполнение LFSR_d в случае, если предположение о начальном заполнении LFSR_c и части LFSR_d оказалось верно. В работе предлагается использовать постоянно совершенствуемое программное обеспечения для решения SAT-проблемы (задачи выполнимости КНФ). Авторами отмечено, что при верном выборе заполнения управляющего регистра решение задачи выполнимости построенной КНФ занимает в среднем в 10 раз меньше времени, чем доказательство невыполнимости построенной КНФ при неверно предположенном начальном заполнении LFSR_c или части LFSR_d. Далее авторы предлагают выбрать пороговый временной параметр t_{th} с помощью которого будут отсекаться «затянувшиеся» вычисления, которые, скорее всего, не приведут к решению. Время, необходимое для поиска ключа потокового шифра LILI-128 авторы статьи оценивают в 10^{25} секунд. Кроме приведенных подходов к криптоанализу потоковых шифров, широко

Таблица 1. Зависимость между параметрами при использовании различных методов.

Метод	**Изв. шифр. послед.**	**Трудоемкость**	**Память**
[21]	2^{30}	$2^{77,5}$	2^{45}
[18], вариант А	2^{18}	2^{102}	2^{40}
[18], вариант Б	2^{57}	2^{63}	2^{40}
[14]	2^{46}	2^{61}	$2^{51,5}$
Опробование, вариант А	$2^{6,5}$	2^{128}	$2^{6,5}$
Опробование, вариант Б	$2^{45,5}$	2^{89}	$2^{6,5}$

известны корреляционные атаки на ключ по известной гаммирующей последовательности.

Наиболее успешной корреляционной атакой на LILI-128 является быстрая корреляционная атака, предложенная в работе [21]. Генерируемая вторым фильтрующим генератором последовательность распознается как линейный код с определенной вероятностью. Трудоемкость метода составляет 2^{71} операций со строками матрицы размером $2^{30} \times 89$ (то есть около $2^{77,5}$ битовых операций).

В работе [14] использована техника *time-memory tradeoff* применительно к рассматриваемой задаче криптоанализа. В данной работе предложен метод, который, по утверждению авторов, имеет трудоемкость около $2^{48} \cdot \omega$, где ω — трудоемкость работы алгоритма *DES*, требует 2^{46} бит известной гаммирующей последовательности и использует около $2^{51,48}$ бит памяти для хранения предварительно вычисленной таблицы возможных значений бит гаммирующей последовательности. Заявленная надежность метода при этом составляет около 0,9.

В таблице 1 приведены трудоемкости, размеры известных шифрующих последовательностей и память, необходимые для успешного проведения криптоанализа различными методами.

Для составления таблицы 1 использовалась оценка трудоемкости *DES* в 2^{13} битовых операций. Последние строки таблицы соответствуют тривиальному опробованию регистров с последующей проверкой на 89 битах гаммирующей последовательности (вариант А) и опробованию только регистра LFSR_d с использованием Леммы 1 (вариант Б).

На рисунке 2 приведено расположение параметров, заданных в таблице 1 в пространстве «трудоемкость (C)–размер известной шифрующей последовательности (m)» в логарифмиче-

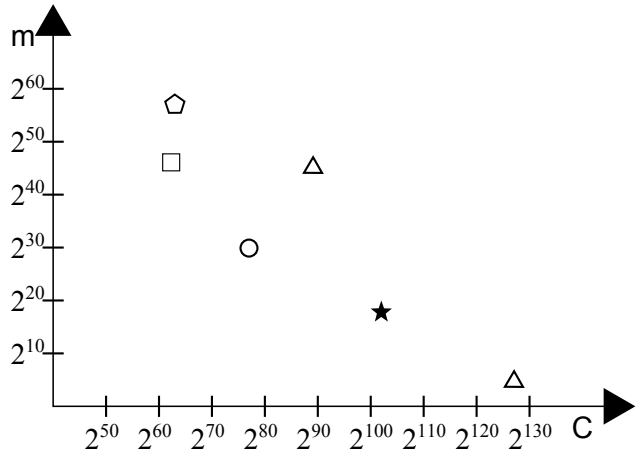


Рис. 2. Соотношение трудоемкости (C) и количества известных бит гаммирующей последовательности (m) в различных методах криптоанализа.

ском масштабе. Строкам таблице 1 в порядке очередности соответствуют следующие фигуры — круг, звезда, пятиугольник, квадрат, два треугольника.

4 Частичное опробование и мономиальная совместность

Введем сначала определение мономиальной совместности системы полиномиальных уравнений.

Определение. Система полиномиальных уравнений называется *мономиально совместной*, если система линейных уравнений, полученная из исходной системы путем переобозначения всех мономов степени не ниже 1 символами новых переменных (этот процесс называется линеаризацией системы), является совместной относительно новых переменных. И наоборот, если получаемая после переобозначения система линейных уравнений несовместна относительно новых переменных, то исходная система называется *мономиально несовместной*.

Для такого определения будет верным следующее утверждение.

Утверждение 1. Если система является мономиально несовместной, то она является несовместной и в обычном смысле.

Исходя из результатов исследования случайных систем булевых полиномиальных уравнений, будут верны следующие лемма и теорема [23].

Лемма 2. Для любых $z \geqslant 0, l \geqslant 1, T \geqslant 1$ верно, что вероятность совместности случайной системы линейных булевых уравнений, описываемой матрицей со сторонами $T + l + z$ и T в 2^{z-2} раз меньше вероятности совместности случайной системы линейных булевых уравнений, описываемой матрицей со сторонами $T + l$ и T.

Теорема 1. Пусть, задано множество элементарных исходов Ω — множество систем из T полиномиальных уравнений степени не выше d над полем GF(2) от s неизвестных. Пусть n — наибольшее среди целых положительных решений неравенства. Пусть ξ — случайная величина, равная трудоемкости решения системы уравнений при опробовании $k = s - n$ переменных (заданных множеством X, $|X| = k$) и последующей проверке на мономиальную совместность, в предположении независимости и равномерного распределения коэффициентов при мономах системы.

Тогда математическое ожидание $E(\xi)$ имеет верхнюю асимптотическую оценку $O(2^k \times T^\omega)$. Где ω — коэффициент, зависящий от применяемого метода решения линейных систем.

5 Метод определения ключа

Перейдем к описанию вариации алгебраического подхода к криптоанализу LILI-128. Будем опробовать все возможные начальные заполнения управляющего генератора LFSR_c, после чего будем строить системы полиномиальных уравнений в соответствии с методикой, предложенной Н. Куртуа в работе [18]. За счет использования анигилляторов, на каждый известный бит гаммирующей последовательности будем получать 14 линейно независимых уравнений степени не выше 4.

Будем определенным (описанным далее) образом выбирать параметр k — число опробуемых переменных, а также некоторым образом сами эти переменные. При опробовании всех возможных значений выбранных переменных получим 2^k редуцированных систем полиномиальных уравнений от $n = 89 - k$ переменных, степени не выше 4. Проверим каждую из полученных систем на мономиальную совместность, используя для приведения к треугольному виду метод Штрассена [19]. Системы, несовместные мономиально, в силу утверждения 1, не имеют решения в обычном смысле, а значит соответствующие им предположения о значениях выбранных k переменных не приводят к решению системы и их можно не рассматривать. Для редуцированных систем, совместных мономиально, уже фактически проведена линеаризация, остается только проверить решение.

Приведем формальное описание предлагаемого алгоритма восстановления исходного заполнения регистров LILI-128 по известной гаммирующей последовательности.

Алгоритм 1. Перед началом работы выбирается параметр k и, соответственно, конкретные k бит LFSR_d, которые будут опробоваться на третьем шаге.

1. Выбираем очередное значение начального заполнения LFSR_c для опробования.
2. Зная управляющую выходную последовательность фильтрующего генератора $\mathrm{LFSR}_c(f_c)$ и зная результат работы $\mathrm{LFSR}_d(f_d)$, строим систему полиномиальных уравнений степени не выше 4 от 89 неизвестных, описывающую работу $\mathrm{LFSR}_d(f_d)$.
3. Выбираем очередное значение опробуемых k переменных, подставляем выбранные значения в построенную на шаге 2 систему уравнений и получаем редуцированную систему уравнений. Если все варианты значений опробуемых переменных исследованы, переходим к шагу 1.
4. Проводим линеаризацию редуцированной системы уравнений, переобозначая все мономы степени 2 и выше новыми переменными. Выясняем, совместна ли полученная линеаризованная система, используя алгоритм Штрассена. Если несовместна переходим к шагу 3.
5. Решаем редуцированную систему любым методом.

6 Расчет трудоемкости метода

Рассмотрим теперь вопрос трудоемкости предложенного метода криптоанализа. Поскольку уравнения, получаемые при криптоанализе LILI-128, разнообразны и уже после нескольких тактов шифратора зависят от всех бит исходного заполнения регистра (ранее чем через 89 тактов работы регистра LFSR_d), то при достаточно больших k (скажем, $k \geqslant 5$) для оценки вероятности мономиальной совместности редуцированной системы случайную модель, приведенную в работе [23]. В таком случае, будет действовать лемма 2, а значит, можно оценить вероятность мономиальной совместности получаемых редуцированных систем в зависимости от величины параметра k, определяющего количество мономов в редуцированной системе, и числа уравнений в системе.

Пусть T — количество уравнений в редуцированной системе, $n = 89 - k$ — число переменных, от которых зависит редуцированная система, $S_{n,4} = \sum_{i=1}^{4} \binom{n}{i}$ — максимально возможное количество мономов в редуцированной системе (переменных в линеаризованной системе). Подставляя в неравенство $T - S_{n,d} > n + 2$ из теоремы 1 указанные параметры, будем получать следующее неравенство:

$$T - S_{(89-k),4} > (89 - k) + 2, \tag{1}$$

Тогда, если n и T удовлетворяют неравенству (1), то математическое ожидание трудоемкости решения (или доказательства отсутствия решений) каждой из редуцированных систем уравнений можно оценить сверху как $C(T)+\frac{1}{2^n}\cdot 2^n$, где $C(T)$ — трудоемкость определения мономиальной совместности системы с помощью алгоритма Штрассена. Действительно, в силу леммы 2, вероятность мономиальной совместности системы при заданных параметрах не превосходит $\frac{1}{2^n}$ и при этом, трудоемкость решения редуцированной системы в отношении которой выяснена ее мономиальная совместность, очевидно, не превосходит трудоемкости осуществления полного перебора 2^n. В действительности же трудоемкость решения мономиально совместной редуцированной системы гораздо ниже, поскольку в ходе проверки на мономиальную совместность уже получено решение линеаризованной системы и остается его лишь проверить.

Заметим, что поскольку на каждый известный бит гаммирующей последовательности приходится 14 линейно независимых уравнений, то m — число необходимых бит последовательности равно $\frac{T}{14}$. Таким образом, выбирая количество известных бит ключа и подставляя данное значение в неравенство (1), можно определять число переменных, которые следует опробовать на шаге 3 Алгоритма 1. И наоборот, подставляя число опробуемых переменных в (1), можно определять необходимое для восстановления ключа число известных бит гаммирующей последовательности. Перейдем теперь к оценке трудоемкости метода в целом. В качестве

Таблица 2. Зависимость между параметрами метода.

k	**Известная гамма**(m)	**Средняя трудоемкость**	**Требуемая память (бит)**
0	$2^{17,5}$	2^{100}	$2^{42,6}$
4	$2^{17,2}$	2^{103}	$2^{42,3}$
9	$2^{16,9}$	2^{105}	$2^{42,0}$
14	$2^{16,5}$	2^{110}	$2^{41,6}$
19	$2^{16,1}$	2^{115}	$2^{41,2}$
24	$2^{15,7}$	2^{117}	$2^{40,8}$
29	$2^{15,2}$	2^{122}	$2^{40,3}$
34	$2^{14,7}$	2^{124}	$2^{39,8}$
39	$2^{14,1}$	2^{130}	$2^{39,2}$

оценки трудоемкости решения редуцированной системы уравнений будем использовать приведенную выше оценку математического ожидания трудоемкости решения (или доказательства отсутствия решений) редуцированной системы уравнений $\approx C(T)$, где, в соответствии с [19] $C(T) = 7 \cdot T^{\log_2 7}$ битовых операций. Всего таких редуцированных систем, в соответствии с Алгоритмом 1, необходимо решить не более $2^{39} \cdot 2^k$. Таким образом, общая трудоемкость предлагаемого метода в среднем составит не более $2^{39} \cdot 2^k \cdot 7 \cdot T^{\log_2 7}$ битовых операций.

Заметим, что объем требуемой памяти для работы этого метода зависит от размера исходной системы уравнений, который можно оценить как $S_{89,4} \cdot T = \sum_{i=1}^{4} \binom{89}{i} \cdot 14 \cdot m \approx 2^{25,1} \cdot m$ бит.

Варьируя, количество известных бит гаммирующей последовательности, будем получать различные параметры метода (число опробуемых переменных и, следовательно, трудоемкость решения системы), приведенные таблице 2.

Данные по трудоемкости в таблице приведены в битовых операциях и могут быть уменьшены на несколько двоичных порядков за счет распараллеливания обработки [18].

7 Заключение

В настоящей работе предложено обобщение алгебраического метода криптоанализа шифратора LILI-128. Обобщенный метод позволяет рассчитывать средние трудоемкости метода для объемов шифрующих последовательностей меньших, чем известные ранее. Получены средние трудоемкости для различных объемов известных шифрующих последовательностей.

На рисунке 3 приведен график зависимости трудоемкости от размеров известной гаммирующей последовательности. Звездой и пятиугольником на графике отмечены результаты,

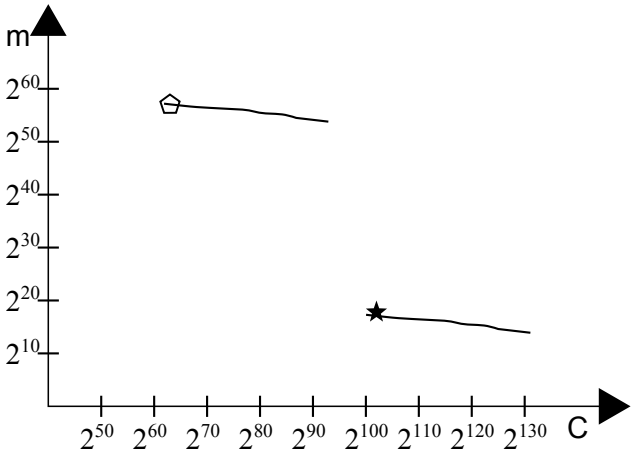


Рис. 3. Соотношение трудоемкости (C) и количества известных бит гаммирующей последовательности (m).

полученные в работе [18]. Кривые линии на графике — возможные значения трудоемкости и количества известной гаммы при различных параметрах метода, предлагаемого в настоящей статье. Из графика хорошо видно, что предлагаемый метод обобщает результат, полученный ранее и расширяет диапазон значений параметров, при которых возможен криптоанализ LILI-128.

Список литературы

[1] *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982. — 416 с.

[2] *Faugère J.-C.* A new efficient algorithm for computation Gröebner bases (F_4) // Journal of pure and applied algebra. — 1999. — Vol. 139, no. 1. — Pp. 61–88.

[3] *Faugère J.-C.* A new efficient algorithm for computation Gröebner bases without reduction to zero (F_5) // Proceedings of the 2002 international symposium on Symbolic and algebraic computation. — 2002. — Pp. 75–83.

[4] *О'Ши Д., Кокс Д., Литтл Д.* Идеалы, многообразия и алгоритмы. — М.: Мир. — 2000. — 687 с.

[5] *Courtois N., Meier W.* Algebraic attacks on stream ciphers with linear feedback // Eurocrypt. Springer, 2003. LNCS 2656. — Pp. 345–359.

[6] *Meier W., Pasalic E., Carlet C.* Algebraic attacks and decompozition of boolean functions // Eurocrypt. Springer, 2004. LNCS 3027. — Pp. 474–491.

[7] *Armknecht F.* On the existence of low-degree equations for algebraic attacks // Cryptology ePrint Archive: Report 2004/185. — `http://eprint.iacr.org/2004/185`.

[8] *Courtois N., Klimov A., Patarin J., Shamir A.* Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations // In B. Preneel, editor, Advances in Cryptology, EUROCRYPT 2000, volume 1807 of LNCS. — Springer-Verlag, Berlin, 2000. — Pp. 392–407.

[9] *Courtois N., Pieprzyk J.* Cryptanalysis of block chiphers with overdefined systems of equations // Cryptology ePrint Archive, Report 2002/044, 2002.

[10] *Courtois N., Pieprzyk J.* Cryptanalysis of block chiphers with overdefined systems of equations. In Y. Zheng, editor // Advances in cryptology. — Asiacrypt'2002. Proc. 8th Int. Conf. on the

Theory and Application of Cryptology and Information Security, volume 2501 of Lect. Notes Comput. Sci. — Springer, 2002. — Pp. 267–287.

[11] *Semaev I.* On solving sparse algebraic equations over finite fields I // Proceedings of WCC'07, 2007. INRIA. — Pp. 361–370.

[12] *Semaev I.* On solving sparse algebraic equations over finite fields II. — 2007. — `http://eprint.iacr.org/2007/280`.

[13] *Мелузов А. С.* Использование ассоциативных принципов обработки информации для построения алгоритмов решения систем булевых уравнений // Журнал вычислительной математики и математической физики. — 2010. — Т. 50, № 11. — С. 2028–2044.

[14] *Markku-Juani Olavi Saarinen.* A time-memory tradeoff attack against LILI-128 // FSE 2002, LNCS 2365, Springer. — Pp. 231-236.

[15] *Dawson E., Clark A., Golić J., Millan W., Penna L., Simpson L.* The LILI-128 keystream generator // Proc. of first NESSIE workshop.

[16] *Babbage S.* Cryptanalysis of LILI-128 // Nessie project internal report. — `https://www.cosic.esat.kuleuven.ac.be/nessie/reports/`.

[17] *Chepyzhov V., Johansson T., Smeets B.* A simple algorithm for fast correlation attacks on stream ciphers // Fast Software Encryption, FSE'2000, to appear in Lecture Notes in Computer Science, Springer-Verlag, 2000.

[18] *Courtois N.* Algebraic Attacks on Stream Ciphers with Linear Feedback // Advances in Cryptology. — EUROCRYPT 2003. — Springer, 2003.

[19] *Strassen V.* Gaussian elimination is not optimal // Numerische Mathematik. — 1969. — Vol. 13. — Pp. 354–356.

[20] *Логачев О. А., Смышляев С. В.* Логический криптоанализ потокового шифра LILI-128 // Материалы 8-й Общероссийской конференции МаБИТ-09.

[21] *Jonsson F., Johansson T.* A Fast Correlation Attack on LILI-128. — `http://www.it.lth.se/thomas/papers/paper140.ps`.

[22] *Колчин В. Ф.* Случайные графы. — М.: ФИЗМАТЛИТ, 2004. — 256 с.

[23] *Мелузов А. С.* Построение эффективных алгоритмов решения систем полиномиальных булевых уравнений методом опробования части переменных. — Принято для публикации в журнал «Дискретная математика», 2011.

УДК 517.977.5

МЕТОД БРОЙДЕНА ДЛЯ РЕШЕНИЯ ЗАДАЧ РАВНОВЕСНОГО ПРОГРАММИРОВАНИЯ

© 2011 г. А. В. Ничипорчук

anichiporchuk@gmail.com

Кафедра оптимального управления

Введение

Распространенная постановка задач оптимизации, использующая функцию от одного аргумента, нередко оказывается несостоятельной в проблемах с двумя и более конфликтующими сторонами — к примеру, в различных игровых и экономических моделях. В таких случаях целесообразно совершить переход к равновесной постановке задачи. Пусть имеется некоторая функция $\Phi(v, w)$, определенная на произведении $\mathbb{R}^n \times \mathbb{R}^n$. Необходимо найти точку $v_* \in \mathbb{R}^n$, удовлетворяющую неравенству:

$$\Phi(v_*, v_*) \leqslant \Phi(v_*, w) \quad \forall w \in \mathbb{R}^n. \tag{1}$$

Такую точку называют равновесной точкой задачи (1). Проблема существования точек равновесия изучена достаточно хорошо и равносильна проблеме существования неподвижных точек $v \in W(v)$ экстремального отображения $W(v)$ функции $\Phi(v, w)$ на $\mathbb{R}^n$, определяемого из условия

$$\Phi(v, W(v)) = \min_{w \in \mathbb{R}^n} \Phi(v, w), \quad v \in \mathbb{R}^n,\ W(v) \in \mathbb{R}^n.$$

Такая постановка является обобщением оптимизационной постановки: если функция $\Phi(v, w)$ не зависит от переменной v, то неравенство (1) фактически является определением точки минимума функции. Кроме того, к такой постановке сводится различные классы задач, например, седловые задачи и игры Нэша.

Основное затруднение при работе с равновесной постановкой заключается в отсутствии широкого спектра численных методов. Большинство из существующих методов разработано и исследовано при значительных ограничениях на функцию $\Phi(v, w)$, и только малая часть подходит для решения более общей задачи вида (1).

Метод Ньютона для задач равновесного программирования

Этот метод является аналогом метода Ньютона для задач оптимизации. Ключевым вопросом является построение удобного обобщения второй производной для функции $\Phi(v, w)$. В статье [1] был предложен следующий способ построения матрицы вторых производных. Пусть функция $\Phi(v, w)$ обладает следующими производными:

$$\frac{\partial \Phi(v, w)}{\partial w}, \quad \frac{\partial^2 \Phi(v, w)}{\partial w^2}, \quad \frac{\partial^2 \Phi(v, w)}{\partial v\, \partial w}, \quad v, w \in \mathbb{R}^n.$$

Тогда вектор

$$\nabla_w \Phi(v, v) = \frac{\partial \Phi(v, w)}{\partial w} \bigg|_{w=v},$$

являющийся сужением градиента функции $\Phi(v, w)$ по переменной w, будем считать аналогом градиента функции, а матрицу

$$\square \Phi(v, v) = \left(\frac{\partial^2 \Phi(v, w)}{\partial w^2} + \frac{\partial^2 \Phi(v, w)}{\partial v\, \partial w} \right) \bigg|_{w=v}, \quad v \in \mathbb{R}^n,$$

— аналогом матрицы вторых производных. В случае существования обратного оператора $\square\Phi(v_k, v_k)$ получаем выражение для $(k+1)$-го приближения метода Ньютона:

$$v_{k+1} = v_k - (\square\Phi(v_k, v_k))^{-1}\nabla_w\Phi(v_k, v_k). \tag{2}$$

Метод Ньютона имеет более высокую скорость сходимости по сравнению с методами первого порядка, однако обладает и недостатками — например, требует больших вычислительных затрат для обращения матрицы вторых производных, а также сходится локально — то есть необходимо выбирать стартовую точку в определенной степени близко к решению. Попытка устранить данные недостатки приводит к рассмотрению квазиньютоновских методов, связанных с заменой обращенной матрицы вторых производных на некоторую матрицу A_k. При выборе этой матрицы необходимо следить за сохранением симметричности при переходе от A_k к A_{k+1}, а также за «близостью» матрицы A_k к обращенной матрице вторых производных минимизируемой функции (то есть за соблюдением условия $\lim_{k\to\infty}\|A_k - (\square\Phi(v_k, v_k))^{-1}\| = 0$). Для перехода от матрицы A_k к матрице A_{k+1} предлагается использовать формулу вида:

$$A_{k+1} = \phi(A_k),$$

где матрица A_0 задается как параметр метода.

Примером метода, удовлетворяющего перечисленным условиям, может служить обобщение метода Бройдена для задач оптимизации [2]. Как показано ниже, условия сходимости этого метода не налагают строгих ограничений на функцию $\Phi(v, w)$, что дает возможность применять его для широкого класса задач. Кроме того, принадлежность этого метода к семейству квазиньютоновских позволяет снизить затратность вычислений без особого ущерба для скорости сходимости метода к решению.

Метод Бройдена для задач равновесного программирования

Для решения задачи (1) предлагается следующий метод:

$$\begin{cases} v_{k+1} = v_k - H_k\nabla_w\Phi(v_k, v_k), \\ H_{k+1} = H_k + \dfrac{(s_k - H_k y_k)y_k^T}{y_k^T y_k}, \\ y_k = \nabla_w\Phi(v_{k+1}, v_{k+1}) - \nabla_w\Phi(v_k, v_k), \\ s_k = v_{k+1} - v_k, \\ v_0 \in \mathbb{R}^n,\ H_0 \in \mathbb{R}^{n\times n}. \end{cases} \tag{3}$$

Перед тем, как сформулировать достаточные условия сходимости предложенного метода к решению рассматриваемой задачи равновесного программирования, обсудим некоторые встречающиеся далее обозначения и приведем три вспомогательные леммы.

Любой вектор размерности n будем трактовать как вектор-столбец; транспонированный вектор, соответственно, будет вектор-строкой. Под нормой вектора или транспонированного вектора понимается классическая норма, то есть квадратный корень из суммы квадратов всех его координат. Под $\|H\|$, где $H \in \mathbb{R}^{n\times n}$ будем понимать обычную операторную норму, то есть $\sup_{\|x\|=1}\|Hx\|$. Обозначение $\|H\|_F$ подразумевает норму Фробениуса, которая равна квадратному корню из суммы квадратов всех элементов матрицы. Также отметим, что справедливы два простых соотношения:

$$\|H\| \leqslant \|H\|_F \quad \forall H \in \mathbb{R}^{n\times n}; \quad \|Hxx^T\|_F = \|Hx\|\cdot\|x\| \quad \forall H \in \mathbb{R}^{n\times n}, x \in \mathbb{R}^n. \tag{4}$$

Лемма 1. *Пусть функция* $\Phi\colon \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ *имеет на* $\mathbb{R}^n \times \mathbb{R}^n$ *непрерывные частные производные* $\Phi_{wv}(v, w)$ *и* $\Phi_{ww}(v, w)$, *и пусть для некоторого* $v^* \in \mathbb{R}^n$ *выполнено неравенство*

$$\|\square\Phi(v, v) - \square\Phi(v^*, v^*)\| \leqslant L\|v - v^*\| \quad \forall v \in \mathbb{R}^n, \tag{5}$$

где $\square\Phi(v,v) = \Phi_{wv}(v,v) + \Phi_{ww}(v,v)$. *Тогда для всех* $u,\ v \in \mathbb{R}^n$

$$\|\nabla_w\Phi(v,v) - \nabla_w\Phi(u,u) - \square\Phi(v^*,v^*)(v-u)\| \leqslant L\max\{\|v-v^*\|,\ \|u-v^*\|\}\|v-u\|. \qquad (6)$$

Если, кроме того, $\Phi(v,w)$ *выпукла по* w *на* $\mathbb{R}^n$ *и обладает на* $\mathbb{R}^n \times \mathbb{R}^n$ *свойством сильной кососимметричности с константой* $\beta > 0$, *что означает выполнение неравенства*

$$\Phi(v,v) - \Phi(v,w) - \Phi(w,v) + \Phi(w,w) \geqslant \beta\|v-w\|^2 \quad \forall v,w \in \mathbb{R}^n, \qquad (7)$$

то справедливо неравенство:

$$\beta\|v-u\| \leqslant \|\nabla_w\Phi(v,v) - \nabla_w\Phi(u,u)\| \quad \forall u,v \in \mathbb{R}^n. \qquad (8)$$

Доказательство. Сначала покажем, что справедливо следующее неравенство:

$$\int_0^1 \|\alpha a + (1-\alpha)b\|d\alpha \leqslant \max\{\|a\|,\|b\|\} \quad \forall a,b \in \mathbb{R}^n. \qquad (9)$$

Для этого заметим, что для любого $\alpha \in [0,1]$

$$\|\alpha a + (1-\alpha b)\| \leqslant \alpha\|a\| + (1-\alpha)\|b\| \leqslant$$
$$\leqslant \alpha\max\{\|a\|,\|b\|\} + (1-\alpha)\max\{\|a\|,\|b\|\} = \max\{\|a\|,\|b\|\}.$$

Интегрируя обе части этого соотношения по α от 0 до 1, получаем (9). Далее, пользуясь формулой конечных приращений, имеем

$$\|\nabla_w\Phi(v,v) - \nabla_w\Phi(u,u) - \square\Phi(v^*,v^*)(v-u)\| = \Big\|\int_0^1 \Big(\frac{\partial}{\partial v}\nabla_w\Phi\big(u+t(v-u),u+t(v-u)\big)+$$
$$+\frac{\partial}{\partial w}\nabla_w\Phi\big(u+t(v-u),u+t(v-u)\big)\Big)\cdot(v-u)dt - \int_0^1 \square\Phi(v^*,v^*)(v-u)dt\Big\| =$$
$$= \Big\|\int_0^1 \Big(\square\Phi\big(u+t(v-u),u+t(v-u)\big) - \square\Phi\big(v^*,v^*\big)\Big)(v-u)dt\Big\| \leqslant$$
$$\leqslant \int_0^1 \Big\|\Big(\square\Phi(u+t(v-u),u+t(v-u) - \square\Phi(v^*,v^*)\Big)\Big\|\Big\|v-u\Big\|dt \leqslant$$
$$\leqslant L\int_0^1 \|u+t(v-u)-v^*\|dt\cdot\|v-u\| = L\|v-u\|\int_0^1 \|(1-t)(u-v^*)+t(v-v^*)\|dt.$$

Наконец, учитывая (9), получаем:

$$\|\nabla_w\Phi(v,v) - \nabla_w\Phi(u,u) - \square\Phi(v^*,v^*)(v-u)\| \leqslant L\max\{\|v-v^*\|,\ \|u-v^*\|\}\|v-u\|.$$

Первая часть леммы доказана. Для доказательства второй части заметим, что если функция $\Phi(v,w)$ обладает свойством сильной кососимметричности (7), является выпуклой и дифференцируемой по второму аргументу, то для нее [3] справедливо неравенство:

$$\beta\|v-u\|^2 \leqslant \langle\nabla_w\Phi(v,v) - \nabla_w\Phi(u,u), v-u\rangle \leqslant \|\nabla_w\Phi(v,v) - \nabla_w\Phi(u,u)\|\|v-u\| \ \forall u,v \in \mathbb{R}^n.$$

Если $v = u$, то неравенство (8) выполняется автоматически. При $v \neq u$ можно поделить обе части последнего соотношения на положительный множитель $\|v-u\|$, тогда мы имеем

$$\beta\|v-u\| \leqslant \|\nabla_w\Phi(v,v) - \nabla_w\Phi(u,u)\| \quad \forall u,v \in \mathbb{R}^n.$$

Лемма 1 доказана. □

Лемма 2. *Для любой ненулевой матрицы $B \in \mathbb{R}^{n\times n}$ и ненулевого вектора $s \in \mathbb{R}^n$ справедливо*

$$\left\| B\left[E - \frac{ss^T}{s^T s}\right]\right\|_F = \sqrt{1-\theta^2}\|B\|_F, \tag{10}$$

где $E \in \mathbb{R}^{n\times n}$ — единичная матрица, а $\theta = \dfrac{\|Bs\|}{\|B\|_F \cdot \|s\|} \in [0,1]$.

Доказательство. Известно, что для любой $B \in \mathbb{R}^{n\times n}$ $\|B\|_F^2 = \mathrm{tr}(B^T B)$, где под $\mathrm{tr}\, B^T B$ понимается след матрицы $B^T B$. С учетом этого для любых векторов u и v имеем

$$\|B[E-uv^T]\|_F^2 = \mathrm{tr}[(B-Buv^T)^T(B-Buv^T)] = \mathrm{tr}[B^TB] - \mathrm{tr}[B^T(Bu)v^T] - \\ - \mathrm{tr}[v(Bu)^TB] + \mathrm{tr}[v(Bu)^T(Bu)v^T] = \|B\|_F^2 - 2v^TB^TBu + \|Bu\|^2\|v\|^2.$$

Учитывая тот факт, что $s^Ts = \|s\|^2$, $s^TB^TBs = (Bs)^TBs = \|Bs\|^2$ и полагая $u = v = \frac{s}{\|s\|}$, получаем

$$\left\| B\left[E - \frac{ss^T}{s^Ts}\right]\right\|_F^2 = \|B\|_F^2 - 2\frac{\|Bs\|^2}{\|s\|^2} + \frac{\|Bs\|^2}{\|s\|^2} = \|B\|_F^2\left(1 - \frac{\|Bs\|^2}{\|B\|_F^2\cdot\|s\|^2}\right).$$

Лемма 2 доказана. □

Лемма 3 (лемма Банаха [4])**.** *Пусть $A \in \mathbb{R}^{n\times n}$ — невырожденная матрица. Тогда если $B \in \mathbb{R}^{n\times n}$ и $\|A^{-1}\|\|B\| < 1$, то $A+B$ — невырожденная и*

$$\|(A+B)^{-1}\| \leqslant \frac{\|A^{-1}\|}{1-\|A^{-1}\|\|B\|}.$$

Перейдем к формулировке и доказательству теоремы о сходимости метода (3).

Теорема 1. *Пусть выполнены следующие условия.*

1. *Функция $\Phi(v,w)\colon \mathbb{R}^n\times\mathbb{R}^n \to \mathbb{R}$ выпукла по w на $\mathbb{R}^n$, при каждом фиксированном w непрерывна по v на $\mathbb{R}^n$, имеет на $\mathbb{R}^n\times\mathbb{R}^n$ непрерывные частные производные $\Phi_{wv}(v,w)$ и $\Phi_{ww}(v,w)$ и обладает свойством сильной кососимметричности на $\mathbb{R}^n\times\mathbb{R}^n$ с коэффициентом β;*

2. *Для любых $v \in \mathbb{R}^n$ выполняется неравенство:*

$$\|\square\Phi(v,v) - \square\Phi(v^*,v^*)\| \leqslant L\|v-v^*\|,$$

где v^* — решение задачи (1), а $\square\Phi(v,v) = \Phi_{wv}(v,v) + \Phi_{ww}(v,v)$.

3. *Матрица $\square\Phi(v^*,v^*)$ невырождена.*

Тогда существуют положительные константы ε и δ такие, что если $\|v_0 - v^*\| < \varepsilon$ и $\|H_0 - (\square\Phi(v^*,v^*))^{-1}\|_F < \delta$, то последовательность $\{v_k\}_{k=1}^{+\infty}$, генерируемая методом (3), сходится к v^* со сверхлинейной скоростью, то есть

$$\lim_{k\to\infty}\frac{\|v_{k+1}-v^*\|}{\|v_k-v^*\|} = 0.$$

Доказательство. Известно, что если функция $\Phi(v,w)$ выпукла и дифференцируема по w, непрерывна по v при каждом фиксированном w, а также обладает свойством сильной кососимметричности, то, во-первых, решение v^* задачи (1) существует и единственно, и, во-вторых, $\nabla_w\Phi(v^*,v^*)=0$. Фиксируем произвольное $r\in(0,1)$. В качестве $\varepsilon(r),\ \delta(r)$ возьмем такие положительные числа ε и δ, что

$$L\|(\square\Phi(v^*,v^*))^{-1}\|\frac{\varepsilon}{1-r}\leqslant\delta, \tag{11}$$

$$2\|\square\Phi(v^*,v^*)\|\delta+(\|(\square\Phi(v^*,v^*))^{-1}\|+2\delta)L\varepsilon\leqslant r, \tag{12}$$

Ясно, что нетрудно подобрать достаточно малые положительные числа, удовлетворяющие этим условиям. Сначала покажем, что если начальное приближение v_0 и матрица H_0 удовлетворяют условиям $\|v_0-v^*\|<\varepsilon(r)=\varepsilon$, $\|H_0-(\square\Phi(v^*,v^*))^{-1}\|_F<\delta(r)=\delta$, то для любого натурального k справедливо $\|v_k-v^*\|\leqslant r^k\|v_0-v^*\|$, $\|H_k-(\square\Phi(v^*,v^*))^{-1}\|_F<2\delta$. Обоснование этого факта проведем по индукции.

Шаг 1 — базис индукции

Покажем, что если $\|v_0-v^*\|<\varepsilon(r)=\varepsilon$, $\|H_0-(\square\Phi(v^*,v^*))^{-1}\|_F<\delta(r)=\delta$, то из этого вытекает $\|v_1-v^*\|\leqslant r\|v_0-v^*\|$. Применим лемму Банаха, положив

$$A=(\square\Phi(v^*,v^*))^{-1},\ B=H_0-(\square\Phi(v^*,v^*))^{-1}.$$

Из (12) вытекает, что

$$\delta\|\square\Phi(v^*,v^*)\|\leqslant\frac{1}{2}\cdot\big(2\|\square\Phi(v^*,v^*)\|\delta+(L\varepsilon\|(\square\Phi(v^*,v^*))^{-1}\|+2L\varepsilon\delta)\big)\leqslant\frac{r}{2}<1/2,$$

поэтому если $\|H_0-(\square\Phi(v^*,v^*))^{-1}\|_F<\delta$, то $\|H_0-(\square\Phi(v^*,v^*))^{-1}\|<2\delta$, и выполнено условие

$$\|H_0-(\square\Phi(v^*,v^*))^{-1}\|\cdot\|\square\Phi(v^*,v^*)\|<1.$$

Значит, H_0 невырождена и

$$\|H_0^{-1}\|\leqslant\frac{\|\square\Phi(v^*,v^*)\|}{1-\|\square\Phi(v^*,v^*)\|\cdot\|H_0-(\square\Phi(v^*,v^*))^{-1}\|}\leqslant\frac{\|\square\Phi(v^*,v^*)\|}{1-\delta\|\square\Phi(v^*,v^*)\|}.$$

Помимо этого, учитывая (4), получаем такую оценку:

$$\|H_0\|\leqslant\|H_0-(\square\Phi(v^*,v^*))^{-1}\|+\|(\square\Phi(v^*,v^*))^{-1}\|\leqslant2\delta+\|(\square\Phi(v^*,v^*))^{-1}\|.$$

Далее, пользуясь уравнениями метода, леммой 1 и тем, что $\nabla_w\Phi(v^*,v^*)=0$, запишем такую цепочку соотношений:

$$\begin{gathered}\|v_1-v^*\|=\|-(v_1-v_0+v_0-v^*)\|=\|H_0\nabla_w\Phi(v_0,v_0)-(v_0-v^*)\|\leqslant\\ \leqslant\|H_0(\nabla_w\Phi(v_0,v_0)-\nabla_w\Phi(v^*,v^*)-\square\Phi(v^*,v^*)(v_0-v^*))+(H_0\square\Phi(v^*,v^*)-E)(v_0-v^*)\|\leqslant\\ \leqslant\|H_0\|\|\nabla_w\Phi(v_0,v_0)-\nabla_w\Phi(v^*,v^*)-\square\Phi(v^*,v^*)(v_0-v^*)\|+\\ +\|E-H_0\square\Phi(v^*,v^*)\|\|v_0-v^*\|\leqslant\|H_0\|\cdot L\|v_0-v^*\|^2+\\ +\|E-H_0\square\Phi(v^*,v^*)\|\cdot\|v_0-v^*\|=\|v_0-v^*\|\cdot(\|H_0\|\cdot L\|v_0-v^*\|+\|E-H_0\square\Phi(v^*,v^*)\|)=\\ =\|v_0-v^*\|\cdot(\|H_0\|\cdot L\|v_0-v^*\|+\|(\square\Phi(v^*,v^*))^{-1}\square\Phi(v^*,v^*)-H_0\square\Phi(v^*,v^*)\|)\leqslant\\ \leqslant\|v_0-v^*\|\cdot(\|H_0\|\cdot L\|v_0-v^*\|+\|\square\Phi(v^*,v^*)\|\cdot\|H_0-(\square\Phi(v^*,v^*))^{-1}\|).\end{gathered}$$

Тогда с учетом этой оценки, (11) и (12) окончательно имеем:

$$\|v_1-v^*\|\leqslant\|v_0-v^*\|\cdot(\|H_0\|\cdot L\|v_0-v^*\|+\|\square\Phi(v^*,v^*)\|\cdot\|H_0-(\square\Phi(v^*,v^*))^{-1}\|)\leqslant$$

$$\leqslant \|v_0 - v^*\|(\|H_0\|L\varepsilon + 2 \cdot \square\Phi(v^*, v^*)\delta) \leqslant$$
$$\leqslant \|v_0 - v^*\|((2\delta + \|(\square\Phi(v^*, v^*))^{-1}\|)L\varepsilon + 2 \cdot \square\Phi(v^*, v^*)\delta) \leqslant r\|v_0 - v^*\|.$$

Шаг 2 — индукционный переход

Сначала отметим, что если вдруг оказалось, что на каком-то шаге $y_k = 0$, то и $s_k = 0$, откуда в силу уравнений метода необходимо выполнено $\nabla_w\Phi(v_k, v_k) = 0$, поэтому точка v_k является решением исходной задачи и работу метода надо останавливать. В дальнейших рассуждениях мы будем считать, что $y_k \neq 0$ для любых натуральных k.

Пусть доказано, что матрицы H_k невырождены, $\|H_k - (\square\Phi(v^*, v^*))^{-1}\|_F \leqslant 2\delta$ и, кроме того, $\|v_{k+1} - v^*\| \leqslant r\|v_k - v^*\|$ для всех $k = 0, 1, \ldots, m$. Заметим, что тогда справедливо соотношение $\|v_k - v^*\| \leqslant r^k\|v_0 - v^*\|$ для всех $k = 0, 1, \ldots, m+1$, и, в силу уравнения метода (3), определяющего матрицу H_{k+1},

$$H_{k+1} - (\square\Phi(v^*, v^*))^{-1} = H_k\left(E - \frac{y_k y_k^T}{y_k^T y_k}\right) + \frac{s_k y_k^T}{y_k^T y_k} - (\square\Phi(v^*, v^*))^{-1} =$$
$$= (H_k - (\square\Phi(v^*, v^*))^{-1})\left(E - \frac{y_k y_k^T}{y_k^T y_k}\right) + \frac{s_k y_k^T}{y_k^T y_k} - (\square\Phi(v^*, v^*))^{-1}\frac{y_k y_k^T}{y_k^T y_k} =$$
$$= (H_k - (\square\Phi(v^*, v^*))^{-1})\left(E - \frac{y_k y_k^T}{y_k^T y_k}\right) + \frac{(s_k - (\square\Phi(v^*, v^*))^{-1}y_k)y_k^T}{y_k^T y_k}.$$

Из этого с учетом леммы 2, определения векторов s_k и y_k и предположения индукции вытекает

$$\|H_{k+1} - (\square\Phi(v^*, v^*))^{-1}\|_F \leqslant \left\|(H_k - (\square\Phi(v^*, v^*))^{-1})\left(E - \frac{y_k y_k^T}{y_k^T y_k}\right)\right\|_F +$$
$$+ \left\|\frac{(s_k - (\square\Phi(v^*, v^*))^{-1}y_k)y_k^T}{y_k^T y_k}\right\|_F \leqslant \sqrt{1-\theta^2}\|H_k - (\square\Phi(v^*, v^*))^{-1}\|_F +$$
$$+ \frac{\|v_{k+1} - v_k - (\square\Phi(v^*, v^*))^{-1}(\nabla_w\Phi(v_{k+1}, v_{k+1}) - \nabla_w\Phi(v_k, v_k))\|}{\|y_k\|} \leqslant$$
$$\leqslant \sqrt{1-\theta^2}\|H_k - (\square\Phi(v^*, v^*))^{-1}\|_F +$$
$$+ L\|(\square\Phi(v^*, v^*)^{-1}\|\frac{\max\{\|v_{k+1} - v^*\|, \|v_k - v^*\|\} \cdot \|\nabla_w\Phi(v_{k+1}, v_{k+1}) - \nabla_w\Phi(v_k, v_k)\|}{\|\nabla_w\Phi(v_{k+1}, v_{k+1}) - \nabla_w\Phi(v_k, v_k)\|} \leqslant$$
$$\leqslant \sqrt{1-\theta^2}\|H_k - (\square\Phi(v^*, v^*))^{-1}\|_F + Lr^k\|(\square\Phi(v^*, v^*)^{-1}\|\|v_0 - v^*\| \leqslant$$
$$\leqslant \|H_k - (\square\Phi(v^*, v^*))^{-1}\| + Lr^k\gamma\varepsilon,$$

где $\gamma \geqslant \|(\square\Phi(v^*, v^*)^{-1}\|$. Суммируя эти неравенства по k от 0 до m, имеем

$$\|H_{m+1} - (\square\Phi(v^*, v^*))^{-1}\|_F \leqslant \|H_0 - (\square\Phi(v^*, v^*))^{-1}\|_F + L\varepsilon\gamma(1 + \ldots + r^m) \leqslant$$
$$\leqslant \|H_0 - (\square\Phi(v^*, v^*))^{-1}\|_F + L\varepsilon\gamma\frac{1}{1-r} \leqslant \|H_0 - (\square\Phi(v^*, v^*))^{-1}\|_F + \delta \leqslant 2\delta.$$

Таким образом, если выполнено индукционное предположение, то выполнено неравенство $\|H_{m+1} - (\square\Phi(v^*, v^*))^{-1}\|_F \leqslant 2\delta$. А из этого факта рассуждениями, полностью аналогичными рассуждениям из шага 1, нетрудно получить, что и $\|v_{m+2} - v^*\| \leqslant r\|v_{m+1} - v^*\|$. Действительно, тогда верно, что $\|H_{m+1} - (\square\Phi(v^*, v^*))^{-1}\| \leqslant 2\delta$. Применим лемму Банаха, приняв

$$A = (\square\Phi(v^*, v^*))^{-1},\ B = H_{m+1} - (\square\Phi(v^*, v^*))^{-1}.$$

Из (12) вытекает, что

$$\delta\|\square\Phi(v^*, v^*)\| \leqslant \frac{1}{2} \cdot 2\|\square\Phi(v^*, v^*)\|\delta + (L\varepsilon\|(\square\Phi(v^*, v^*))^{-1}\| + 2L\varepsilon\delta) \leqslant \frac{r}{2} < 1/2,$$

поэтому если $\|H_{m+1} - (\Box\Phi(v^*, v^*))^{-1}\|_F < \delta$, то $\|H_{m+1} - (\Box\Phi(v^*, v^*))^{-1}\| < 2\delta$, и выполнено условие

$$\|H_{m+1} - (\Box\Phi(v^*, v^*))^{-1}\| \cdot \|\Box\Phi(v^*, v^*)\| < 1.$$

Поэтому H_{m+1} невырождена и

$$\|H_{m+1}^{-1}\| \leqslant \frac{\|\Box\Phi(v^*, v^*)\|}{1 - \|\Box\Phi(v^*, v^*)\| \cdot \|H_{m+1} - (\Box\Phi(v^*, v^*))^{-1}\|} \leqslant \frac{\|\Box\Phi(v^*, v^*)\|}{1 - \delta\|\Box\Phi(v^*, v^*)\|}.$$

После этого имеем

$$\begin{gathered}
\|v_{m+2} - v^*\| = \|-(v_{m+2} - v_{m+1} + v_{m+1} - v^*)\| = \|H_{m+1}\nabla_w\Phi(v_{m+1}, v_{m+1}) - (v_{m+1} - v^*)\| \leqslant \\
\leqslant \|H_{m+1}(\nabla_w\Phi(v_{m+1}, v_{m+1}) - \nabla_w\Phi(v^*, v^*) - \Box\Phi(v^*, v^*)(v_{m+1} - v^*))\| + \\
+ \|(H_{m+1}\Box\Phi(v^*, v^*) - E)(v_{m+1} - v^*)\| \leqslant \\
\leqslant \|H_{m+1}\|\|\nabla_w\Phi(v_{m+1}, v_{m+1}) - \nabla_w\Phi(v^*, v^*) - \Box\Phi(v^*, v^*)(v_{m+1} - v^*)\| + \\
+ \|E - H_{m+1}\Box\Phi(v^*, v^*)\|\|v_{m+1} - v^*\| \leqslant \|H_{m+1}\| \cdot L\|v_{m+1} - v^*\|^2 + \\
+ \|E - H_{m+1}\Box\Phi(v^*, v^*)\| \cdot \|v_{m+1} - v^*\| = \\
= \|v_{m+1} - v^*\| \cdot (\|H_{m+1}\| \cdot L\|v_{m+1} - v^*\| + \|E - H_{m+1}\Box\Phi(v^*, v^*)\|) = \\
= \|v_{m+1} - v^*\| \cdot (\|H_{m+1}\| \cdot L\|v_{m+1} - v^*\| + \|(\Box\Phi(v^*, v^*))^{-1}\Box\Phi(v^*, v^*) - H_{m+1}\Box\Phi(v^*, v^*)\|) \leqslant \\
\leqslant \|v_{m+1} - v^*\| \cdot (\|H_{m+1}\| \cdot L\|v_{m+1} - v^*\| + \|\Box\Phi(v^*, v^*)\| \cdot \|H_{m+1} - (\Box\Phi(v^*, v^*))^{-1}\|).
\end{gathered}$$

Тогда с учетом (11) и (12) окончательно имеем:

$$\begin{gathered}
\|v_{m+2} - v^*\| \leqslant \\
\leqslant \|v_{m+1} - v^*\| \cdot (\|H_{m+1}\| \cdot L\|v_{m+1} - v^*\| + \|\Box\Phi(v^*, v^*)\| \cdot \|H_{m+1} - (\Box\Phi(v^*, v^*))^{-1}\|) \leqslant \\
\leqslant \|v_{m+1} - v^*\|(\|H_{m+1}\|L\varepsilon + 2 \cdot \Box\Phi(v^*, v^*)\delta) \leqslant \\
\leqslant \|v_{m+1} - v^*\|((2\delta + \|(\Box\Phi(v^*, v^*))^{-1}\|)L\varepsilon + 2 \cdot \Box\Phi(v^*, v^*)\delta) \leqslant \\
\leqslant \|v_{m+1} - v^*\| \cdot \frac{\frac{r}{1+r}}{1 - \frac{r}{1+r}} = \|v_{m+1} - v^*\| \cdot \frac{\frac{r}{1+r}}{\frac{1}{1+r}} = r\|v_{m+1} - v^*\|.
\end{gathered}$$

Индукционный переход закончен.

Итак, в силу того, что $r \in (0, 1)$, ясно, что $\|v_k - v^*\| \leqslant r^k\|v_0 - v^*\|$ для всех $k = 0, 1, 2, \ldots$, и $\lim_{k\to+\infty}\|v_k - v^*\| = 0$.

Наконец, обоснуем сверхлинейную скорость сходимости. Используя уже полученную оценку, заметим, что

$$\begin{aligned}
\|H_{k+1} - (\Box\Phi(v^*, v^*))^{-1}\|_F \leqslant \sqrt{1 - \theta^2}\|H_k - (\Box\Phi(v^*, v^*))^{-1}\|_F + \\
+ L\gamma\max\{\|v_{k+1} - v^*\|, \|v_k - v^*\|\}, \quad (13)
\end{aligned}$$

где

$$\theta_k = \frac{\|(H_k - (\Box\Phi(v^*, v^*))^{-1})y_k\|}{\|H_k - (\Box\Phi(v^*, v^*))^{-1}\|_F\|y_k\|},\ H_k \neq (\Box\Phi(v^*, v^*))^{-1} \text{ и } \theta_k = 0, \text{ если } H_k = (\Box\Phi(v^*, v^*))^{-1}.$$

Если существует подпоследовательность $\{H_k\}$, сходящаяся к $(\Box\Phi(v^*, v^*))^{-1}$, то, сверхлинейная скорость обосновывается следующим образом. Пусть изначально нами было выбрано некое r_0 и отвечающие ему $\varepsilon(r_0)$ и $\delta(r_0)$. Тогда $\|v_{k+1} - v^*\| \leqslant r_0^k\|v_0 - v^*\|$ для всех k. Но тогда понятно, что если мы возьмем некое $r_1 < r_0$, то, для некоторого номера m будет справедливо $\|v_m - v^*\| \leqslant \varepsilon(r_1)$, $\|H_m - (\Box\Phi(v^*, v^*))^{-1}\|_F \leqslant \delta(r_1)$, и, по доказанному, для всех последующих номеров k будет справедливо $\|v_{k+1} - v^*\| \leqslant r_1\|v_k - v^*\|$. Продолжая эти рассуждения, мы приходим к выводу, что для любого $r > 0$ найдется такой номер $m(r)$, что, начиная с него, $\|v_{k+1} - v^*\| \leqslant r\|v_k - v^*\|$. А это по сути и есть сверхлинейная скорость сходимости.

Если такой подпоследовательности нет, то последовательность $\{\|H_k - (\square\Phi(v^*, v^*))^{-1}\|\}$ отделена от нуля. Неравенство (13) с учетом того, что $\sqrt{1-\alpha} \leqslant 1 - \alpha/2 \ \forall \alpha \in [0,1]$, приводится к виду

$$\frac{1}{2}\theta_k^2\|H_k - (\square\Phi(v^*, v^*))^{-1}\|_F \leqslant \|H_k - (\square\Phi(v^*, v^*))^{-1}\|_F - \|H_{k+1} - (\square\Phi(v^*, v^*))^{-1}\|_F + \\ + L\gamma \max\{\|v_{k+1} - v^*\|, \|v_k - v^*\|\} \quad \forall k \in \mathbb{N}.$$

Суммируя эти неравенства по k от 0 до n, и учитывая тот факт, что, по доказанному выше $\|v_{k+1} - v^*\| \leqslant \|v_k - v^*\|$, имеем

$$\sum_{k=0}^{n} \theta_k^2\|H_k - (\square\Phi(v^*, v^*)))^{-1}\|_F = \|H_0 - (\square\Phi(v^*, v^*))^{-1}\|_F - \|H_{n+1} - (\square\Phi(v^*, v^*))^{-1}\|_F + \\ + \sum_{k=1}^{n} L\gamma\|v_k - v^*\|.$$

Переходя к пределу при $n \to \infty$, получаем

$$\sum_{k=0}^{\infty} \theta_k^2\|H_k - (\square\Phi(v^*, v^*))^{-1}\|_F = \|H_0 - (\square\Phi(v^*, v^*))^{-1}\|_F - \overline{\lim_{k\to\infty}}\|H_{k+1} - (\square\Phi(v^*, v^*))^{-1}\|_F + \\ + L\gamma \sum_{k=1}^{\infty}\|v_k - v^*\|.$$

Ряд $\sum_{k=1}^{\infty}\|v_k - v^*\|$ сходится по признаку Даламбера. Значит,

$$\sum_{k=1}^{\infty} \theta_k^2\|H_k - (\square\Phi(v^*, v^*))^{-1}\|_F = \sum_{k=1}^{\infty} \frac{\|(H_{i_k} - (\square\Phi(v^*, v^*))^{-1})y_{i_k}\|^2}{\|H_{i_k} - (\square\Phi(v^*, v^*))^{-1}\|_F\|y_{i_k}\|^2} < \infty,$$

где i_k — те номера, для которых верно $H_{i_k} \neq (\square\Phi(v^*, v^*))^{-1}$. Вспомним, что последовательность $\{\|H_k - (\square\Phi(v^*, v^*))^{-1}\|_F\}$ ограничена сверху, поэтому, в силу необходимого условия сходимости числового ряда,

$$\lim_{k\to+\infty} \frac{\|(H_k - (\square\Phi(v^*, v^*))^{-1})y_k\|}{\|y_k\|} = 0. \tag{14}$$

В силу уравнений метода (3), $H_k y_k = H_k \nabla_w \Phi(v_{k+1}, v_{k+1}) + s_k$. Из этого вытекает

$$(H_k - (\square\Phi(v^*, v^*))^{-1})y_k = H_k\nabla_w\Phi(v_{k+1}, v_{k+1}) - (\square\Phi(v^*, v^*))^{-1}[y_k - \square\Phi(v^*, v^*)s_k] \Rightarrow \\ \Rightarrow \nabla_w\Phi(v_{k+1}, v_{k+1}) = H_k^{-1} \cdot ((H_k - (\square\Phi(v^*, v^*))^{-1})y_k + (\square\Phi(v^*, v^*))^{-1}[y_k - \square\Phi(v^*, v^*)s_k]),$$

стало быть, с учетом леммы 1,

$$\|\nabla_w\Phi(v_{k+1}, v_{k+1})\| \leqslant \\ \leqslant \|H_k^{-1}\|\|(H_k - (\square\Phi(v^*, v^*))^{-1})y_k\| + \|(\square\Phi(v^*, v^*))^{-1}\|\|y_k - \square\Phi(v^*, v^*)s_k\| \leqslant \\ \leqslant \|H_k^{-1}\|(\|[H_k - (\square\Phi(v^*, v^*))^{-1}]y_k\| + L\|(\square\Phi(v^*, v^*))^{-1}\|\max\{\|v_k - v^*\|, \|v_{k+1} - v^*\|\}\|s_k\|.$$

Поскольку $\|v_{k+1} - v^*\| \leqslant \|v_k - v^*\|$, окончательно имеем

$$\|\nabla_w\Phi(v_{k+1}, v_{k+1})\| \leqslant \|H_k^{-1}\|(\|[H_k - (\square\Phi(v^*, v^*))^{-1}]y_k\| + L\|(\square\Phi(v^*, v^*))^{-1}\|\|v_k - v^*\|\|s_k\|. \tag{15}$$

С учетом (5) справедлива следующая оценка:

$$\|y_k\| = \|\nabla_w\Phi(v_{k+1}, v_{k+1}) - \nabla_w\Phi(v_k, v_k)\| \leqslant$$

$$\leqslant \max_{t\in[0,1]}\|\square\Phi(v_k+t(v_{k+1}-v_k),v_k+t(v_{k+1}-v_k))\|\|v_{k+1}-v_k\|\leqslant$$
$$\leqslant (\max_{t\in[0,1]}\|\square\Phi(v_k+t(v_{k+1}-v_k),v_k+t(v_{k+1}-v_k))-\square\Phi(v^*,v^*)\|+\|\square\Phi(v^*,v^*)\|)\|v_{k+1}-v_k\|\leqslant$$
$$\leqslant (L\max_{t\in[0,1]}(\|tv_{k+1}-tv^*+(1-t)v_k-(1-t)v^*\|)+\|\square\Phi(v^*,v^*)\|)\|v_{k+1}-v_k\|\leqslant$$
$$\leqslant (L\max_{t\in[0,1]}(t\|v_{k+1}-v^*\|+(1-t)\|v_k-v^*\|)+\|\square\Phi(v^*,v^*)\|)\|v_{k+1}-v_k\|\leqslant$$
$$\leqslant (L\varepsilon+\|\square\Phi(v^*,v^*)\|)\|v_{k+1}-v_k\|=\rho\|v_{k+1}-v_k\|=\rho\|s_k\|.$$

Используя ее, и тот факт, что, по лемме 1, $\beta\|s_k\|\leqslant\|y_k\|$, из (15) получаем

$$\frac{\|\nabla_w\Phi(v_{k+1},v_{k+1})\|}{\rho\|s_k\|}\leqslant\frac{\|\nabla_w\Phi(v_{k+1},v_{k+1})\|}{\|y_k\|}\leqslant\frac{\|[H_k-(\square\Phi(v^*,v^*))^{-1}]y_k\|}{\|y_k\|}+$$
$$+L\|(\square\Phi(v^*,v^*))^{-1}\|\|v_k-v^*\|\frac{\|s_k\|}{\|y_k\|}\leqslant\frac{\|[H_k-(\square\Phi(v^*,v^*))^{-1}]y_k\|}{\|y_k\|}+$$
$$+L\|(\square\Phi(v^*,v^*))^{-1}\|\|v_k-v^*\|\frac{1}{\beta}.$$

Переходя к пределу в этом соотношении и учитывая, что $\|v_k-v^*\|\to 0$, из (14) имеем

$$\lim_{k\to+\infty}\frac{\|\nabla_w\Phi(v_{k+1},v_{k+1})\|}{\|s_k\|}=\lim_{k\to+\infty}\frac{\|[H_k-(\square\Phi(v^*,v^*))^{-1}]y_k\|}{\|y_k\|}=0.$$

Наконец, по лемме 1, $\|\nabla_w\Phi(v_{k+1},v_{k+1})\|=\|\nabla_w\Phi(v_{k+1},v_{k+1})-\nabla_w\Phi(v^*,v^*)\|\geqslant\beta\|v_{k+1}-v^*\|$, $\|s_k\|\leqslant\|v_{k+1}-v^*\|+\|v_k-v^*\|\leqslant 2\|v_k-v^*\|$. Значит,

$$0\leqslant\lim_{k\to+\infty}\frac{\|v_{k+1}-v^*\|}{\|v_k-v^*\|}\leqslant\frac{2}{\beta}\lim_{k\to+\infty}\frac{\|\nabla_w\Phi(v_{k+1},v_{k+1})\|}{\|s_k\|}=0,$$

что и является необходимым соотношением. Теорема доказана. □

Заключение

В данной работе рассмотрена постановка задачи равновесного программирования, для ее решения разработан аналог известного квазиньютоновского метода Бройдена. Сформулирована и доказана теорема о сверхлинейной скорости сходимости метода к решению.

Автор выражает благодарность своему научному руководителю кандидату физико-математических наук Б. А. Будаку за постановку задачи и помощь в подготовке этой работы.

Список литературы

[1] *Антипин А.С., Васильев Ф.П., Стукалов А.С., Ячимович М.* Метод Ньютона для решения задач равновесного программирования // Вычислительные методы и программирование. — 2006. — Т. 7. — С. 202–210.

[2] *Broyden C.G., Dennis Jr. J.E., More J.J.* On the Local and Superlinear Convergence of Quasi-Newton // Inst Maths Applies. — 1973. — Vol. 12. — Pp. 223–245.

[3] *Будак Б.А.* Непрерывные методы решения задач равновесного программирования: Дисс. на соиск. уч. степени к.ф.-м.н.; 01.01.09. — М., 2003. — 134 с.

[4] *Ortega J.M.* Numerical analysis: a second course. — SIAM, 1990.

УДК 517.977

ПРИМЕНЕНИЕ УСЛОВИЙ ВТОРОГО ПОРЯДКА В ИССЛЕДОВАНИИ ЛОКАЛЬНОЙ ОПТИМАЛЬНОСТИ НЕКОТОРЫХ ТРАЕКТОРИЙ В ЗАДАЧЕ РИДСА-ШЕППА

© 2011 г. И. А. Самыловский

barbudo.sam@cs.msu.ru

Кафедра оптимального управления

1 Введение

Рассмотрим следующую задачу оптимального управления:

$$\begin{cases} \dot{x} = u\sin\varphi, & x(t_0) = 0, & x(T) = x_T, \\ \dot{y} = u\cos\varphi, & y(t_0) = 0, & y(T) = y_T, \\ \dot{\varphi} = v, & \varphi(t_0) = 0, & \varphi(T) \text{ свободно}, \\ |u| \leqslant 1, & |v| \leqslant 1, & \mathrm{J} = T \to \min. \end{cases} \tag{1}$$

В статье Ридса и Шеппа [2] система (1) предлагалась для моделирования движения на плоскости (x, y) автомобиля, способного менять направление линейной скорости на противоположное. Здесь u есть линейная скорость, φ представляет собой угол между вектором скорости $(\dot{x}, \dot{y})$ и осью ординат. При фиксированном $u = 1$ задача (1) превращается в известную задачу Маркова–Дубинса, изучавшуюся в [1]. Так как в задаче (1) множество значений управления есть выпуклый компакт (квадрат на плоскости), и управляемая система линейна по обоим управлениям, то по теореме Филиппова решение здесь всегда существует. Анализ принципа максимума позволяет выделить все типы траекторий, подозрительных на оптимальность. В работе [5] показано, что некоторые из них не являются оптимальными в глобальном смысле. В данной работе, пользуясь условиями «второго» порядка, полученными в [3], мы изучаем вопрос об их локальной оптимальности.

2 Принцип максимума

Пусть в задаче (1) процесс $(x(t), y(t), \varphi(t), u(t), v(t))$, $t \in [0, T]$ удовлетворяет принципу максимума Понтрягина. Это означает, что найдется нетривиальный набор множителей Лагранжа, состоящий из $\alpha \geqslant 0$, липшицевых функций $\psi_x(t)$, $\psi_y(t)$, $\psi_\varphi(t)$, порождающий *функцию Понтрягина*

$$H = (\psi_x \sin\varphi + \psi_y \cos\varphi)u + \psi_\varphi v, \tag{2}$$

так что выполняются сопряженные уравнения

$$-\dot{\psi}_x = H_x = 0, \qquad -\dot{\psi}_y = H_y = 0, \qquad -\dot{\psi}_\varphi = H_\varphi = \psi_x \cos\varphi - \psi_y \sin\varphi, \tag{3}$$

условие трансверсальности:

$$\psi_\varphi(T) = 0,$$

«закон сохранения энергии»:

$$H(x, y, \varphi, u, v) \equiv \alpha \geqslant 0,$$

и условие максимума:

$$\max_{|u'|\leqslant 1,\ |v'|\leqslant 1} H(x, y, \varphi, u', v') = H(x, y, \varphi, u, v) \quad \text{для почти всех } t. \tag{4}$$

В силу «сепарабельности» H по u и v последнее условие разбивается на два отдельных:

$$\max_{|u'|\leqslant 1}(\psi_x \sin\varphi + \psi_y \cos\varphi)u' = (\psi_x \sin\varphi + \psi_y \cos\varphi)u, \quad \max_{|v'|\leqslant 1} \psi_\varphi v' = \psi_\varphi v \quad \text{для почти всех } t. \quad (5)$$

В свою очередь, эти условия означают, что

$$u \in \operatorname{Sign}(\psi_x \sin\varphi + \psi_y \cos\varphi), \quad v \in \operatorname{Sign}\psi_\varphi, \quad (6)$$

где $\operatorname{Sign} z = \partial|z|$ есть многозначная функция

$$\operatorname{Sign} z = \begin{cases} 1, & z > 0, \\ -1, & z < 0, \\ [-1,1], & z = 0. \end{cases} \quad (7)$$

Если $u(t) \in \operatorname{Sign} z(t)$, а функция $z(t)$ обращается в нуль лишь на множестве меры нуль, то можно писать «обычное» равенство $u(t) = \operatorname{sign} z(t)$. В работе [5] показано, что все стационарные траектории имеют кусочно-постоянные управления u и v.

3 Рассматриваемые типы траекторий

В данной работе рассматриваются стационарные траектории, на которых управление v не обращается в нуль. На них сопряженная переменная ψ_φ (соответствующая фазовой переменной φ) имеет вид, представленный на рисунке 1.

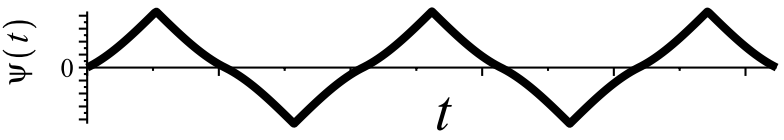


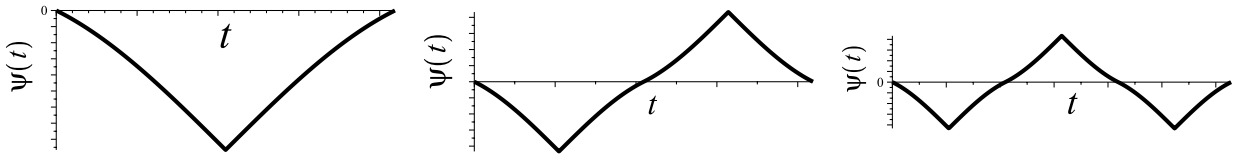
Рис. 1. Сопряженная переменная ψ_φ.

Здесь каждая «шапочка» имеет длину 2α, $\alpha \in (0, \pi/2)$, управление u меняет знак на противоположный в точках локального экстремума функции ψ_φ (в нашем случае это точки $n\alpha$, $n = 1, 3, 5, \ldots$) а управление v меняет знак на противоположный при переходе к следующей шапочке. Число шапочек не ограничено. Допускается также сдвиг графика относительно вертикальной оси. В конечный момент времени $\psi_\varphi = 0$. Для удобства введем следующее

Обозначение. $f = (c_1, c_2, \ldots, c_n)$ означает, что $f(t)$ — кусочно-постоянная (вектор-) функция, принимающая значения c_1, c_2, …, c_n на соответствующих интервалах (t_0, t_1), (t_1, t_2), …, (t_{n-1}, t_n), причем $t_n = T$.

Мы рассмотрим несколько типов таких траекторий: с одной (Тип 1), двумя (Тип 2) и тремя (Тип 3) шапочками. Им соответствуют следующие управления.

- **Тип 1:** $(u, v) = ((1, -1), (-1, -1))$ на интервалах $(0, \alpha)$, $(\alpha, 2\alpha)$.
- **Тип 2:** $(u, v) = ((1, -1), (-1, -1), (-1, 1), (1, 1))$ на интервалах $(0, \alpha)$, $(\alpha, 2\alpha)$, $(2\alpha, 3\alpha)$, $(3\alpha, 4\alpha)$.
- **Тип 3:** $(u, v) = ((1, -1), (-1, -1), (-1, 1), (1, 1), (1, -1), (-1, -1))$ на интервалах $(0, \alpha)$, $(\alpha, 2\alpha)$, $(2\alpha, 3\alpha)$, $(3\alpha, 4\alpha)$, $(4\alpha, 5\alpha)$, $(5\alpha, 6\alpha)$.

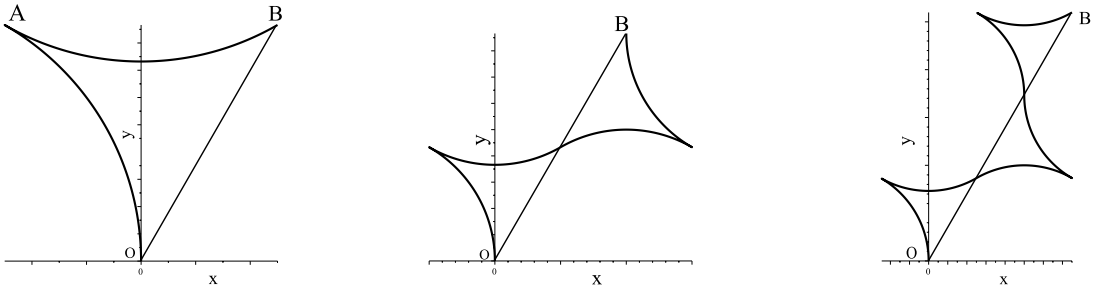


Тип 1 *Тип 2* *Тип 3*

Рис. 2. Сопряженные переменные.

4 Постановка конечномерных задач

Как показано в [3], для выяснения вопроса о локальной оптимальности траектории релейного типа в задаче (1) достаточно установить ее локальную оптимальность в суженной конечномерной задаче, состоящей в варьировании лишь моментов переключения. Составим эти задачи для перечисленных выше типов траекторий. При записи ограничений используем вид траекторий на плоскости (x, y), представленный на рисунке 3.



Тип 1 *Тип 2* *Тип 3*

Рис. 3. Фазовые траектории.

На рисунках 3 точка B есть конечная точка траектории соответствующего типа.

- Для типа 1: $B = (2(1 - \cos\alpha)\cos\alpha, 2(1 - \cos\alpha)\sin\alpha)$.
- Для типа 2: $B = (4(1 - \cos\alpha)\cos\alpha, 4(1 - \cos\alpha)\sin\alpha)$.
- Для типа 3: $B = (6(1 - \cos\alpha)\cos\alpha, 6(1 - \cos\alpha)\sin\alpha)$.

Угол между OB и осью абсцисс равен параметру α.

4.1 Тип 1. Траектории с одной «шапочкой»

Конечномерная задача с параметром $\alpha \in (0, \pi/2)$ имеет вид

$$\begin{cases} t_2 \to \min, \\ g_1 = 2\cos t_1 - \cos t_2 - 1 - 2(1 - \cos\alpha)\cos\alpha = 0, \\ g_2 = 2\sin t_1 - \sin t_2 - 2(1 - \cos\alpha)\sin\alpha = 0. \end{cases} \tag{8}$$

Подпространство критических вариаций для точки $\hat{t} = (\hat{t}_1, \hat{t}_2) = (\alpha, 2\alpha)$ имеет вид

$$\mathcal{K} = \{g_i'(\hat{t})\bar{t} = 0,\ i = 1, 2\}. \tag{9}$$

Это приводит нас к системе

$$\begin{cases} -2\sin\alpha \cdot \bar{t}_1 + \sin 2\alpha \cdot \bar{t}_2 = 0, \\ 2\cos\alpha \cdot \bar{t}_1 - \cos 2\alpha \cdot \bar{t}_2 = 0. \end{cases} \tag{10}$$

Нетрудно убедиться, что $\mathcal{K} = \{0\}$, что, как известно, означает справедливость следующего утверждения.

Утверждение 1. *Траектория типа 1 доставляет сильный локальный минимум первого порядка в задаче* (1) *при любом* $\alpha \in (0, \pi/2)$.

4.2 Тип 2. Траектории с двумя «шапочками»

Конечномерная задача с параметром $\alpha \in (0, \pi/2)$ имеет вид

$$\begin{cases} t_4 \to \min, \\ g_1 = 2\cos t_1 - 2\cos t_2 + 2\cos(t_3 - 2t_2) - \cos(t_4 - 2t_2) - 1 - 4(1-\cos\alpha)\cos\alpha = 0, \\ g_2 = 2\sin t_1 - 2\sin t_2 - 2\sin(t_3 - 2t_2) + \sin(t_4 - 2t_2) - 4(1-\cos\alpha)\sin\alpha = 0. \end{cases} \tag{11}$$

Для полученной задачи составим функцию Лагранжа

$$\begin{aligned} \mathcal{L}(t_1, t_2, t_3, t_4, \beta_1, \beta_2) = t_4 + \\ + \beta_1[2\cos t_1 - 2\cos t_2 + 2\cos t_3 - 2t_2 - \cos t_4 - 2t_2 - 4(1-\cos\alpha)\cos\alpha - 1] + \\ + \beta_2[2\sin t_1 - 2\sin t_2 - 2\sin t_3 - 2t_2 + \sin t_4 - 2t_2 - 4(1-\cos\alpha)\sin\alpha]. \end{aligned}$$

Выписав для точки $\hat{t} = (\hat{t}_1, \hat{t}_2, \hat{t}_3, \hat{t}_4) = (\alpha, 2\alpha, 3\alpha, 4\alpha)$ необходимые условия экстремума

$$\left(\frac{\mathrm{d}L}{\mathrm{d}t_i}\right)_{t=\hat{t}} = 0, \quad i = 1, 2, 3, 4,$$

мы получим систему множителей Лагранжа $(1, -\operatorname{ctg}\alpha, -1)$.
Матрица вторых производных функции Лагранжа:

$$\left(\frac{\mathrm{d}^2\mathcal{L}}{\mathrm{d}t^2}\right)_{t=\hat{t}} = \frac{2}{\sin\alpha}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4-3\cos\alpha & -2 & \cos\alpha \\ 0 & -2 & 1 & 0 \\ 0 & \cos\alpha & 0 & -1/2\cos\alpha \end{pmatrix}.$$

Действуя аналогично (9)–(10), находим подпространство критических вариаций

$$\mathcal{K} = \{\bar{t}_1 = (\cos\alpha - 1)\bar{t}_2 + \bar{t}_3,\ \bar{t}_4 = 0\}.$$

Таким образом, на подпространстве $\mathcal{K}$ квадратичная форма

$$\Omega(\bar{t}) = \left(\left(\frac{\mathrm{d}^2\mathcal{L}}{\mathrm{d}t^2}\right)_{t=\hat{t}} \bar{t}, \bar{t}\right)$$

имеет тот же знак, что и

$$\tilde{\Omega} = \bar{t}_2^2(\cos^2\alpha - 5\cos\alpha + 5) + 2(\cos\alpha - 3)\bar{t}_2\bar{t}_3 + 2\bar{t}_3^2,$$

знак которой определяется, в свою очередь, детерминантом

$$D(\tilde{\Omega}) = \begin{vmatrix} \cos^2\alpha - 5\cos\alpha + 5 & \cos\alpha - 3 \\ \cos\alpha - 3 & 2 \end{vmatrix} = \cos^2\alpha - 4\cos\alpha + 1.$$

Полученный квадратный трехчлен относительно $\cos\alpha$ имеет корни $2 \pm \sqrt{3}$. Приняв во внимание ограничения $\alpha \in (0, \pi/2)$, приходим к тому, что

$$\begin{aligned} D(\tilde{\Omega}) < 0 \quad &\text{при} \quad \alpha \in (0, \arccos(2-\sqrt{3})), \\ D(\tilde{\Omega}) > 0 \quad &\text{при} \quad \alpha \in (\arccos(2-\sqrt{3}), \pi/2). \end{aligned}$$

Это значит, что при $\alpha \in (\arccos(2-\sqrt{3}), \pi/2)$ квадратичная форма Ω положительно определена на $\mathcal{K}$, при $\alpha = \arccos(2-\sqrt{3})$ квадратичная форма Ω неотрицательно определена на $\mathcal{K}$, а при $\alpha \in (0, \arccos(2-\sqrt{3}))$ найдется $\bar{t} \in \mathcal{K}$, для которого $\Omega(\bar{t}) < 0$.

Это равносильно следующему утверждению.

Утверждение 2. *При* $\alpha \in (\arccos(2-\sqrt{3}), \pi/2)$ *траектория типа 2 доставляет строгий сильный минимум в задаче* (1). *При* $\alpha \in (0, \arccos(2-\sqrt{3}))$ *траектория типа 2 не доставляет сильный минимум. При* $\alpha = \arccos(2-\sqrt{3})$ *траектория типа 2 удовлетворяет лишь необходимому условию оптимальности второго порядка.*

4.3 Тип 3. Траектории с тремя «шапочками»

Конечномерная задача с параметром $\alpha \in (0, \pi/2)$ имеет вид

$$\begin{cases} t_6 \to \min, \\ g_1 = 2\cos t_1 - 2\cos t_2 + 2\cos(t_3 - 2t_2) - 2\cos(t_4 - 2t_2) + 2\cos(t_5 - 2t_4 + 2t_2) - \\ \quad - \cos(t_6 - 2t_4 + 2t_2) - 1 - 6(1 - \cos\alpha)\cos\alpha = 0, \\ g_2 = 2\sin t_1 - 2\sin t_2 - 2\sin(t_3 - 2t_2) + 2\sin(t_4 - 2t_2) + 2\sin(t_5 - 2t_4 + 2t_2) + \\ \quad + \sin(t_6 - 2t_4 + 2t_2) - 6(1 - \cos\alpha)\sin\alpha = 0. \end{cases} \tag{12}$$

Для полученной задачи составим функцию Лагранжа:

$$\begin{aligned} \mathcal{L}(t_1, t_2, t_3, t_4, \beta_1, \beta_2) = t_4 &+ \beta_1[2\cos t_1 - 2\cos t_2 + 2\cos(t_3 - 2t_2) - 2\cos(t_4 - 2t_2) + \\ &+ 2\cos(t_5 - 2t_4 + 2t_2) - \cos(t_6 - 2t_4 + 2t_2) - 1 - 6(1 - \cos\alpha)\cos\alpha)] + \\ &+ \beta_2[2\sin t_1 - 2\sin t_2 - 2\sin(t_3 - 2t_2) + 2\sin(t_4 - 2t_2) + \\ &+ 2\sin(t_5 - 2t_4 + 2t_2) + \sin(t_6 - 2t_4 + 2t_2) - 6(1 - \cos\alpha)\sin\alpha]. \end{aligned}$$

Выписав для точки $\hat{t} = (\hat{t}_1, \hat{t}_2, \hat{t}_3, \hat{t}_4, \hat{t}_5, \hat{t}_6) = (\alpha, 2\alpha, 3\alpha, 4\alpha, 5\alpha, 6\alpha)$ необходимые условия экстремума

$$\left(\frac{\mathrm{d}L}{\mathrm{d}t_i}\right)_{t=\hat{t}} = 0, \quad i = 1, 2, 3, 4, 5, 6,$$

мы получим систему множителей Лагранжа $(1, -\operatorname{ctg}\alpha, -1)$.

Матрица вторых производных функции Лагранжа:

$$\left(\frac{\mathrm{d}^2\mathcal{L}}{\mathrm{d}t^2}\right)_{t=\hat{t}} = \frac{2}{\sin\alpha} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 8 - 7\cos\alpha & -2 & 4(\cos\alpha - 1) & 2 & -\cos\alpha \\ 0 & -2 & 1 & 0 & 0 & 0 \\ 0 & 4(\cos\alpha - 1) & 0 & 4 - 3\cos\alpha & -2 & \cos\alpha \\ 0 & 2 & 0 & -2 & 1 & 0 \\ 0 & -\cos\alpha & 0 & \cos\alpha & 0 & -1/2\cos\alpha \end{pmatrix}.$$

Действуя аналогично (9)–(10), находим подпространство критических вариаций

$$\mathcal{K} = \{\bar{t_1} = 2(1 - \cos\alpha)(\bar{t}_4 - 2\bar{t}_2) + \bar{t}_3 - \bar{t}_5, \bar{t}_6 = 0\}.$$

На подпространстве $\mathcal{K}$ квадратичная форма

$$\Omega(\bar{t}) = \left(\left(\frac{\mathrm{d}^2\mathcal{L}}{\mathrm{d}t^2}\right)_{t=\hat{t}} \bar{t}, \bar{t}\right)$$

с точностью до множителя имеет вид

$$\begin{aligned} \tilde{\Omega}(\bar{t}) = {} & 16\bar{t}_2^2\cos^2\alpha - 39\bar{t}_2^2\cos\alpha + 4\bar{t}_4^2\cos^2\alpha - 11\bar{t}_4^2\cos\alpha + \\ & + 24\bar{t}_2^2 - 12\bar{t}_2\bar{t}_3 + 12\bar{t}_2\bar{t}_5 - 24\bar{t}_2\bar{t}_4 + 2\bar{t}_3^2 - 2\bar{t}_3\bar{t}_5 + \bar{4}t_3\bar{t}_4 + 2\bar{t}_5^2 - 8\bar{t}_5t_4 + 8\bar{t}_4^2 + \\ & + 40\bar{t}_2\cos\alpha\bar{t}_4 - 4\bar{t}_4\cos\alpha\bar{t}_3 + 4\bar{t}_4\cos\alpha\bar{t}_5 - 16\bar{t}_2\cos^2\alpha\bar{t}_4 + 8\bar{t}_2\cos\alpha\bar{t}_3 - 8\bar{t}_2\cos\alpha\bar{t}_5. \end{aligned}$$

Приведя подобные члены, получим, что

$$\begin{aligned} \tilde{\Omega}(\bar{t}) = {} & (16\cos^2\alpha - 39\cos\alpha + 24)\bar{t}_2^2 + 2\bar{t}_2\bar{t}_3(-6 + 4\cos\alpha) + 2\bar{t}_2\bar{t}_4(-12 + 20\cos\alpha - 8\cos^2\alpha) + \\ & + 2\bar{t}_2\bar{t}_5(6 - 4\cos\alpha) + 2\bar{t}_3^2 + 2\bar{t}_3\bar{t}_4(2 - 2\cos\alpha) - 2\bar{t}_2\bar{t}_5 + 2\bar{t}_3^2 + 2\bar{t}_3\bar{t}_4(2 - 2\cos\alpha) - 2\bar{t}_3\bar{t}_5 + \\ & + (4\cos^2\alpha + 8 - 11\cos\alpha)\bar{t}_4^2 + 2\bar{t}_4\bar{t}_5(2\cos\alpha - 4) + 2\bar{t}_5^2 \end{aligned}$$

с матрицей

$$\begin{pmatrix} 16\cos^2\alpha - 39\cos\alpha + 2 & -6 + 4\cos\alpha & -12 + 20\cos\alpha - 8\cos^2\alpha & 6 - 4\cos\alpha \\ -6 + 4\cos\alpha & 2 & 2 - 2\cos\alpha & -1 \\ -12 + 20\cos\alpha - 8\cos^2\alpha & 2 - 2\cos\alpha & 4\cos^2\alpha + 8 - 11\cos\alpha & 2\cos\alpha - 4 \\ 6 - 4\cos\alpha & -1 & 2\cos\alpha - 4 & 2 \end{pmatrix}.$$

Замечаем, что угловой минор третьего порядка для любого $\alpha \in (0, \pi/2)$ имеет вид

$$34\cos^2\alpha - 12\cos^3\alpha - 24\cos\alpha = 2\cos\alpha(-6\cos^2\alpha + 17\cos\alpha - 12) < 0.$$

Это означает, что при $\alpha \in (0, \pi/2)$ найдется $\bar{t} \in \mathcal{K}$ такое, что квадратичная форма $\Omega(\bar{t}) < 0$. Отсюда вытекает

Утверждение 3. *При любом $\alpha \in (0, \pi/2)$ траектория типа 3 не доставляет сильный минимум в задаче (1).*

5 Основные результаты

Применены на практике условия «второго» порядка, полученных в [3]. С их помощью изучен вопрос о локальной оптимальности траекторий типов 1, 2 и 3 в задаче Ридса-Шеппа со свободным правым концом (1) при различных значениях параметра $\alpha \in (0, \pi/2)$.

Список литературы

[1] *Dubins L.E.* On curves of minimal length with a constraint on average curvatue and with prescribed initial and terminal positions and tangents // American J. of Mathematics. — 1957. — Vol. 79. — Pp. 497–516.

[2] *Reeds J.A., Shepp L.A.* Optimal path for a car that goes both forwards and backwards // Pacific J. of Mathematics. — 1990. — Vol. 145, no. 2. — Pp. 367–393.

[3] *Maurer H., Osmolovskii N.P.* Second order sufficient conditions for time-optimal bang-bang control // SIAM J. on Control and Optimization. — 2003. — Vol. 42, no. 6. — Pp. 2239–2263.

[4] *Филиппов А.Ф.* О некоторых вопросах теории оптимального регулирования // Вестник МГУ, сер. матем., мех., астрон., физ., хим. — 1959. — № 2. — С. 25–32.

[5] *Dmitruк A.V., Samylovskiy I.A.* Optimal Synthesis in the Reeds and Shepp problem with free final direction // J. of Mathematical Scienses. — (In press).

УДК 511.178

МАКСИМАЛЬНАЯ МОЩНОСТЬ (k,l)-МНОЖЕСТВА, СВОБОДНОГО ОТ СУММ В ЦИКЛИЧЕСКОЙ ГРУППЕ

© 2011 г. В. Г. Саргсян

vahe_sargsyan@yahoo.com

Кафедра математической кибернетики

1 Введение

Пусть G — абелева группа порядка $n > 1$. Подмножество $A \subseteq G$ называется (k,l)-*множеством, свободным от сумм (MCC),* если уравнение $x_1+x_2+\ldots+x_k = y_1+y_2+\ldots+y_l$ не имеет решения в A. Через $\lambda_{k,l}(G)$ обозначим максимальную мощность (k,l)-множества, свободного от сумм в абелевой группе G.

Перечислительные задачи, связанные с понятием множества, свободного от сумм, привлекали большое внимание математиков с момента появления в 1988 году статьи Камерона и Эрдёша. В этой статье найдены оценки число множеств, свободных от сумм в отрезке $[1,\ldots,n]$ натуральных чисел, и высказана гипотеза о том, что указанное число не превосходит $O(2^{n/2})$. Гипотеза Камерона-Эрдёша о числе множеств, свободных от сумм доказана в 2003 году независимо А. А. Сапоженко [1] и Б. Грином [5]. Вместе с тем интенсивно рассматривались обобщения проблемы Камерона-Эрдёша, в частности, речь шла о числе (k,l)-множеств, свободных от сумм. Актуальной является задача получения асимптотики числа (k,l)-множеств, свободных от сумм.

Типичными являются следующие задачи.

Задача 1. Определить максимальную мощность (k,l)-множества, свободного от сумм в абелевой группе.

Задача 2. Определить количество (k,l)-множеств, свободных от сумм в абелевой группе.

Цель этой работы — определить максимальную мощность $\lambda_{k,l}(Z_n)$ для (k,l)-множества, свободного от сумм в циклической группе Z_n. Мы докажем, что

$$\lambda_{k,l}(Z_n) = \max_{d|n}\left\{\left(\left\lfloor\frac{d-1-\delta(d)}{k+l}\right\rfloor+1\right)\cdot\frac{n}{d}\right\},$$

где $\delta(d) = \text{НОД}(d,k-l)$.

Задача 1 при различных k и l решалась такими авторами как Х. П. Яп и П. Х. Диананда [10], Б. Грин и И. Ружа [6], Т. Виер и А. Я. М. Чин [9], Я. о. Хамидун и А. Плейдж[3], В. Ф. Лев [8] и Б. Байнок [2]. В [4] доказана следующая

Теорема 1. Пусть G — абелева группа порядка n, тогда

$$\max_{d|\exp(G)}\left\{\left\lfloor\frac{d+1}{3}\right\rfloor\cdot\frac{n}{d}\right\} \leqslant \lambda_{2,1}(G) \leqslant \max_{d|n}\left\{\left\lfloor\frac{d+1}{3}\right\rfloor\cdot\frac{n}{d}\right\}.$$

В 1969 году такой же результат для множества, свободного от сумм в циклической группе был получен Х. П. Япом и П. Х. Дианандой [10].

Теорема 2. Для любого n справедливо равенство

$$\lambda_{2,1}(Z_n) = \max_{d|n}\left\{\left\lfloor\frac{d+1}{3}\right\rfloor\cdot\frac{n}{d}\right\} = \begin{cases}\frac{p+1}{p}\cdot\frac{n}{3}, & \text{если } p \text{ наименьшее число такое, что } p|n \text{ и } p\equiv 2 \pmod 3,\\ \lfloor\frac{n}{3}\rfloor, & \text{иначе.}\end{cases}$$

В 2005 году Б. Грин и И. Ружа [6] доказали, что $\lambda_{2,1}(G)$ совпадает с нижней оценкой в теореме 1.

Теорема 3. Пусть G — абелева группа порядка n, тогда

$$\lambda_{2,1}(G) = \lambda_{2,1}(Z_{\exp(G)}) \cdot \frac{n}{\exp(G)} = \max_{d|\exp(G)} \left\{ \left\lfloor \frac{d+1}{3} \right\rfloor \cdot \frac{n}{d} \right\}.$$

Как следствие отсюда вытекает, что

$$\frac{2}{7}n \leqslant \lambda_{2,1}(G) \leqslant \frac{1}{2}.$$

Нижняя оценка достигается при $\exp(G) = 7$, а верхняя оценка — при четном $\exp(G)$.

Т. Виер и А. Я. М. Чин [9] решали задачу 1 для циклической группы простого порядка и доказали следующее утверждение.

Теорема 4. Если p простое число, то

$$\lambda_{k,l}(Z_p) = \left\lceil \frac{p-1}{k+l} \right\rceil.$$

Я. о. Хамидун и А. Плейдж [3] решали задачу 1 для произвольной абелевой группы с ограничением вида $\text{НОД}(n, k-l) = 1$. Ими доказаны следующие три утверждения.

Теорема 5. Пусть G — абелева группа порядка n и $\text{НОД}(n, k-l) = 1$. Если $\exp(G)$ имеет делитель, не совпадающий с $1 \pmod{(k+l)}$, то

$$\lambda_{k,l}(G) = \max_{d|\exp(G)} \left\{ \left(\left\lfloor \frac{d-2}{k+l} \right\rfloor + 1 \right) \cdot \frac{n}{d} \right\}.$$

Теорема 6. Пусть $\text{НОД}(n, k-l) = 1$, тогда

$$\lambda_{k,l}(Z_n) = \max_{d|n} \left\{ \left(\left\lfloor \frac{d-2}{k+l} \right\rfloor + 1 \right) \cdot \frac{n}{d} \right\}.$$

Теорема 7. Пусть G — абелева группа порядка n, тогда

$$\max_{d|\exp(G)} \left\{ \frac{\alpha_{k,l}(Z_d) \cdot n}{d} \right\} \leqslant \lambda_{k,l}(G) \leqslant \max \left(\frac{n - \varepsilon(G)}{k+l}, \max_{d|\exp(G)} \left\{ \frac{\alpha_{k,l}(Z_d) \cdot n}{d} \right\} \right),$$

где

$$\varepsilon(G) = \begin{cases} 0, & \text{если } |G| \equiv 0 \pmod 2, \\ 1, & \text{если } |G| \equiv 1 \pmod 2. \end{cases}$$

В 2007 году Б. Байнок [2] исследовал задачу 1 для абелевой группы без ограничения на НОД вида $(n, k-l) = 1$. Он доказал следующие три утверждения.

Теорема 8. Пусть G — абелева группа порядка n, тогда

$$\max_{d|\exp(G)} \left\{ \left(\left\lfloor \frac{d-1-\delta(d)}{k+l} \right\rfloor + 1 \right) \cdot \frac{n}{d} \right\} \leqslant \lambda_{k,l}(G) \leqslant \max_{d|n} \left\{ \left(\left\lfloor \frac{d-2}{k+l} \right\rfloor + 1 \right) \cdot \frac{n}{d} \right\},$$

где $\delta(d) = \text{НОД}(d, k-l)$.

Теорема 9. Пусть G — абелева группа порядка n. Если $\exp(G)$ имеет делитель d, не принадлежащий к $\{1,\dots,\delta(d)\} \pmod{(k+l)}$, то

$$\lambda_{k,l}(G) = \lambda_{k,l}(Z_{\exp(G)}) \cdot \frac{n}{\exp(G)},$$

где $\delta(d) = \text{НОД}(d, k-l)$.

Теорема 10. Для любого n справедливо равенство

$$\lambda_{k,l}(Z_n) = \max_{d|n} \left\{ \frac{\alpha_{k,l}(Z_d) \cdot n}{d} \right\},$$

где $\alpha_{k,l}(Z_d)$ определяется следующим образом:

i) если $d|(k-l)$, то $\alpha_{k,l}(Z_d) = 0$;

ii) если $\text{НОД}(d, k-l) = 1$, то

$$\alpha_{k,l}(Z_d) = \max \left\{ \frac{d}{p}, \left\lfloor \frac{d-2}{k+l} \right\rfloor + 1 \right\},$$

где p — наименьший простой делитель d;

iii) если $1 < \text{НОД}(d, k-l) < d$, то

$$\max \left\{ \frac{d}{\rho_1}, \left\lfloor \frac{d-1-\delta(d)}{k+l} \right\rfloor + 1 \right\} \leqslant \alpha_{k,l}(Z_d) \leqslant \max \left\{ \frac{d}{\rho_1}, \frac{d}{2\rho_2}, \left\lfloor \frac{d-2}{k+l} \right\rfloor + 1 \right\},$$

где $\delta(d) = \text{НОД}(d, k-l)$, ρ_1 — наименьший делитель d такой, что $(k-l)$ не делится на ρ_1, а ρ_2 — наименьший делитель d такой, что $(k-l)$ делится на ρ_2.

В данной статье доказывается, что

$$\alpha_{k,l}(Z_n) = \left\lfloor \frac{n-1-\delta}{k+l} \right\rfloor + 1,$$

где $\delta = \text{НОД}(n, k-l)$.

2 Определения и вспомогательные утверждения

Положим $kA = \{x_1 + x_2 + ... + x_k \mid x_1, ..., x_k \in A\}$, а $c \star A = \{c \cdot a \mid a \in A\}$, для любого $c \in Z_n$. Определение (k,l)-множества, свободного от сумм эквивалентно тому, что $kA \cap lA = \emptyset$, что, в свою очередь, эквивалентно тому, что $0 \notin kA - lA = \{x_1 + x_2 + \dots + x_k - y_1 - y_2 - \dots - y_l \mid x_1, \dots, x_k,\ y_1, \dots, y_l \in A\}$. Через $\alpha_{k,l}(Z_n)$ обозначим максимальную мощность (k,l)-арифметической прогрессии, свободной от сумм в циклической группе Z_n. Предположим, что $k \neq l \pmod{n}$ и $k > l$.

Лемма 1 ([4], лемма 6.18)**.** Пусть Z_n — циклическая группа порядка n, A и B непустые подмножества группы Z_n такие, что $(A+B)$-арифметическая прогрессия с разностью d и $|A+B| < \frac{n}{d}$, тогда

$$|A+B| \geq |A| + |B| - 1.$$

Положим $\delta = \text{НОД}(n, k-l)$, $n = \delta \cdot n_1$, $k-l = \delta \cdot m_1$, а $R = \{0, n_1, 2 \cdot n_1, \dots, (\delta-1) \cdot n_1\}$, $|R| = \delta$.

Лемма 2. Пусть A — (k,l)-множество, свободное от сумм в Z_n. Тогда

i) $A \cap R = \emptyset$,

ii) Для любого $c \in Z_n$ множество $c \star A$ является (k,l)-множеством, свободным от сумм, тогда и только тогда, когда $0 \notin c \star A$,

iii) $(kA - lA) \cap R = \emptyset$.

Доказательство. i) Предположим противное, и пусть $i \cdot n_1 \in A (i \in \{0, \dots, \delta - 1\})$, тогда $(k-l) \cdot i \cdot n_1 \in kA - lA$, а с другой стороны $(k-l) \cdot i \cdot n_1 = \delta \cdot m_1 \cdot i \cdot n_1 = n \cdot m_1 \cdot i = 0$, то есть $0 \in kA - lA$, что противоречит тому, что A-(k,l) свободно от сумм.

ii) Если $0 \in c \star A$, то, очевидно $c \star A$ не является (k,l)-множеством, свободным от сумм. Теперь предположим, что $0 \notin c \star A$, но $c \star A$ не является (k,l)-множеством, свободным от сумм, то есть существуют $x_1, x_2, \dots, x_k, y_1, y_2, \dots, y_l \in A$ такие, что $c \cdot x_1 + c \cdot x_2 + \dots + c \cdot x_k = c \cdot y_1 + c \cdot y_2 + \dots + c \cdot y_l$, то есть $x_1 + x_2 + \dots + x_k = y_1 + y_2 + \dots + y_l$, что противоречит тому, что A-(k,l) свободно от сумм.

Как следствие получим, что это множество $\delta \star A$ является (k,l)-свободным от сумм.

iii) Предположим противное, и пусть $i \cdot n_1 \in (kA - lA)$ $(i \in \{0, \dots, \delta - 1\})$, тогда $\delta \cdot i \cdot n_1 \in \delta \star (kA - lA) = k(\delta \star A) - l(\delta \star A)$, а с другой стороны $\delta \cdot i \cdot n_1 = 0$, то есть $0 \in k(\delta \star A) - l(\delta \star A)$, что противоречит тому, что $\delta \star A$ является (k,l)-свободным от сумм. □

Лемма 3 ([2], лемма 9)**.** Для любого n справедливо неравенство

$$\alpha_{k,l}(Z_n) \geqslant \left\lfloor \frac{n-1-\delta}{k+l} \right\rfloor + 1,$$

где $\delta = \text{НОД}(n, k-l)$.

3 Полученный результат

Теорема 11. Для любого n справедливо равенство

$$\alpha_{k,l}(Z_n) = \left\lfloor \frac{n-1-\delta}{k+l} \right\rfloor + 1,$$

где $\delta = \text{НОД}(n, k-l)$.

Доказательство. Пусть $A = \{a, a+d, a+2d, \dots, a+(|A|-1)d\} \subseteq Z_n$ арифметическая прогрессия с разностью d и (k,l)-свободная от сумм. Ясно, что подгруппа

$$Z^{(d)} := \{0, d, 2d, \dots, \left(\frac{n}{d} - 1\right) \cdot d\},$$

порожденная элементом d, является максимальной по длине арифметической прогрессией с разностью d в Z_n. Так как

$$kA - lA = \{(k-l)a + id \mid i \in \left[-l(|A|+1), k(|A|+1)\right]\}$$

является арифметической прогрессией с разностью d и $0 \notin (kA - lA)$, то

$$(kA - lA) \subseteq \left\{\{(k-l)a\} + \{0, d, 2d, \dots, \left(\frac{n}{d} - 1\right) \cdot d\}\right\} \setminus \{0\}.$$

Отсюда следует, что

$$|kA - lA| < \frac{n}{d}.$$

Поскольку удовлетворяются условия леммы 1, получаем

$$|kA| + |lA| - 1 \leqslant |kA - lA|,$$

а из леммы 2(iii) следует, что

$$|kA| + |lA| - 1 \leqslant |kA - lA| \leqslant n - \delta.$$

В дальнейшем, последовательно применяя лемму 1 $(k-1)$ раз, получим

$$k|A| - (k-1) + l|A| - (l-1) - 1 \leqslant |kA| + |lA| - 1 \leqslant |kA - lA| \leqslant n - \delta,$$

то есть

$$|A| \leqslant \left\lfloor \frac{n-1-\delta}{k+l} \right\rfloor + 1.$$

Отсюда, с учетом леммы 3, следует, что

$$\alpha_{k,l}(Z_n) = \left\lfloor \frac{n-1-\delta}{k+l} \right\rfloor + 1. \qquad \square$$

Следствие. Для любого n справедливо равенство

$$\lambda_{k,l}(Z_n) = \max_{d|n} \left\{ \left(\left\lfloor \frac{d-1-\delta(d)}{k+l} \right\rfloor + 1 \right) \cdot \frac{n}{d} \right\},$$

где $\delta(d) = \text{НОД}(d, k-l)$.

Доказательство. По теореме 10

$$\lambda_{k,l}(Z_n) = \max_{d|n} \left\{ \frac{\alpha_{k,l}(Z_d) \cdot n}{d} \right\}.$$

Подставив вместо $\alpha_{k,l}(Z_d)$ его значение из теоремы 11, получим

$$\lambda_{k,l}(Z_n) = \max_{d|n} \left\{ \frac{\alpha_{k,l}(Z_d) \cdot n}{d} \right\} = \max_{d|n} \left\{ \left(\left\lfloor \frac{d-1-\delta(d)}{k+l} \right\rfloor + 1 \right) \cdot \frac{n}{d} \right\},$$

где $\delta(d) = \text{НОД}(d, k-l)$, что и требовалось доказать. $\square$

Список литературы

[1] *Сапоженко А.А.* Гипотеза Камерона-Эрдёша // ДАН. — 2003. — Т. 393, № 6. — С. 749–752.

[2] *Bajnok B.* On the maximum size of a (k,l)-sum-free subset of an abelian group // International Journal of Number Theory. — 2009. — Vol. 5, no. 6. — Pp. 953–971.

[3] *ould Hamidoune Y., Plagne A.* A new critical pair theorem applied to sum-free sets in Abelian groups // Commentarii Mathematici Helvetici. — 2004. — Vol. 79. — Pp. 183–207.

[4] *Wallis W.D., Street A.P., Wallis J.S.* Combinatorics: Room squares, sum-free sets, Hadamard matrices, Lecture Note in Mathematics // Berlin, Heidelberg, New York: Springer-Verlag, 1972. — Vol. 292. — P. 494.

[5] *Green B.* The Cameron–Erdos conjecture // Bull. London Math. Soc. — 2004. — Vol. 36, no. 6. — Pp. 769–778.

[6] *Green B., Ruzsa I.* Sum-free sets in abelian groups // Israel Journal of Mathematics. — 2005. — Vol. 147. — Pp. 157–188.

[7] *Nathanson M.B.* Additive number theory: Inverse problems and the geometry of sumsets, Graduate Texts in Mathematics // Berlin, Heidelberg, New York: Springer-Verlag, 1996. — P. 312.

[8] *Lev V.F.* Large sum-free sets in Z/pZ // Israel Journal of Mathematics. — 2006. — Vol. 154. — Pp. 221–233.

[9] *Bier T., Chin A.Y.M.* On (k, l)-sets in cyclic groups of odd prime order // Bull. Austral. Math. Soc. — 2001. — Vol. 63, no. 1. — Pp. 115–121.

[10] *Diananda P.H., Yap H.P.* Maximal sum-free sets of elements of finite groups // Proc. Japan Acad. — 1969. — Vol. 45. — Pp. 1–5.

УДК 57.087.1

СОЗДАНИЕ ПРОГРАММНОЙ СРЕДЫ ДЛЯ СТАТИСТИЧЕСКОЙ ОБРАБОТКИ ДАННЫХ БИОИМПЕДАНСНЫХ ИЗМЕРЕНИЙ

© 2011 г. О. А. Старунова

starunova@cmc.msu.ru

Кафедра вычислительных технологий и моделирования

1 Введение

Одним из современных направлений фундаментальных и прикладных исследований является изучение состава тела человека [1]. Анализаторы состава тела применяются в биологии и медицине для исследования закономерностей роста и развития организма, характеристики пищевого статуса и состояния гидратации, диагностики заболеваний и других целей. Возможность их использования в эпидемиологии связана со скринингом населения для формирования групп риска развития сердечно-сосудистых заболеваний с целью снижения уровня преждевременной заболеваемости и смертности.

Методом оценки состава тела, пригодным для проведения скрининговых обследований, является биоимпедансный анализ. Данный метод основан на измерении комплексной величины импеданса тела человека как характеристики его пассивных электрических свойств [2, 3]. Благодаря началу на рубеже 1980-х–1990-х годов серийного выпуска биоимпедансного оборудования в ряде стран мира собраны и проанализированы большие массивы данных биоимпедансных измерений [4]. Этап массового накопления таких данных в России начался в 2008 году в результате создания национальной сети Центров здоровья [5]. Необходимость корректной автоматизированной обработки данных и формирования популяционных норм компонентного состава тела с учетом половозрастных и антропометрических различий индивидов привела к идее создания для этих целей специализированного программного обеспечения.

Целью работы является описание интерфейса и функционала вновь создаваемого программного продукта BIAStatistica для обработки данных биоимпедансных измерений.

2 Постановка задачи

Разрабатываемый пакет программ BIAStatistica (от англ. *BioImpedance Analyzer Statistical Application*) должен включать в себя набор вычислителей и графический пользовательский интерфейс, которые позволят пользователю:

- загружать в программу файл формата `xls`, в котором находится база данных, содержащая результаты биоимпедансного обследования пациентов;
- задавать критерии, по которым пациенты исключаются из рассматриваемой базы или, напротив, включаются в выборку для дальнейших расчетов;
- вычислять основные статистические характеристики обследованных групп и результатов измерений (такие как размер выборки, выборочные средние, дисперсии, максимальные и минимальные значения и т. п.), получать гистограммы распределений;
- определять тип распределений показателей состава тела, включая проверку на нормальность или логнормальность, оценивать параметры распределений;
- проводить корреляционный и регрессионный анализ данных;
- получать регрессионные модели и сопоставлять их при помощи различных информационных критериев;
- моделировать границы нормальных значений признаков и оценивать согласованность модели и данных;
- настраивать форматы выходных данных — графических и текстовых файлов, содержащих результаты обработки данных.

3 Особенности реализации пакета BIAStatistica

Для создания пакетов статистической обработки и анализа данных наиболее удобным представляется язык программирования R [6], который фактически стал стандартом для использования в таких целях. Язык R поддерживает широкий набор статистических и численных методов и обладает хорошей расширяемостью с помощью пакетов. Однако среда R, несмотря на удобство, универсальность (может работать во всех популярных операционных системах) и доступность (свободно распространяемое программное обеспечение), имеет ряд существенных недостатков. Во-первых, R является не компилятором, а строковым интерпретатором, поэтому скрипт, написанный на R, невозможно превратить в исполняемый файл. Это означает, что всякий желающий пользоваться программой на языке R вынужден иметь на своем компьютере программную среду R и все необходимые дополнительные пакеты. На данный момент обойти это ограничение не удалось, поэтому вместе с пакетом BIAStatistica поставляется среда R. К счастью, среда R не требует отдельной установки, и для ее нормальной работы достаточно скопировать на жесткий диск директорию, содержащую все необходимые файлы. Второй недостаток более существенный. Он состоит в том, что, по-видимому, R не обладает удобными инструментами для создания графического интерфейса пользователя, и необходимо привлекать дополнительные программные средства.

Предполагается, что основными потребителями пакета программ BIAStatistica станут врачи и биологи. Как правило, большинство из них являются пользователями ОС Windows. С учетом этого программное обеспечение для биоимпедансных анализаторов чаще всего разрабатывается также под Windows. Поэтому мы не ставили задачей обеспечить переносимость приложения на другие платформы и ограничили выбор программных средств продуктами, исполняемыми под ОС Windows.

Удобным и естественным инструментом для создания графического интерфейса приложений, работы с данными в формате `xls`, запуска процессов и обработки потоков ввода-вывода является среда Borland C++ Builder (далее BCB), в которой и разрабатывается графический интерфейс программы BIAStatistica. Затем на основе данных, введенных или выбранных пользователем, формируется входной текстовый файл, содержащий команды языка R. Далее из программы в BCB запускается R, на исполнение которому передается сгенерированный текстовый файл. Результат вычислений перенаправляется в выходные текстовые или графические файлы, отображаемые в соответствующих элементах интерфейса.

Входные файлы получаются, как правило, небольшого размера, так как язык R обладает значительным набором уже реализованных статистических функций и процедур работы с графикой [7, 8]. На компьютере средней вычислительной мощности обмен между BCB и R происходит практически мгновенно. Однако в зависимости от размера массива исходных данных процесс настройки параметров моделей может занимать сравнительно долгое время.

4 Иллюстрация интерфейса и возможностей программы

В настоящее время программа находится в относительно ранней стадии разработки, поэтому реализованные возможности носят демонстрационный характер и не претендуют на полноту статистического анализа. Главное окно программы содержит несколько вкладок.

- **Начало работы: «Загрузить данные».** На этой вкладке пользователю предлагается выбрать файл в формате `xls`, содержащий базу данных биоимпедансных измерений, а также указать пути к директориям, в которые необходимо сохранять результаты работы.

- **«Фильтр данных».** Функционал этой вкладки позволяет пользователю перегруппировать исходные данные и удалить записи, содержащие артефакты измерений. Эта возможность обеспечивается благодаря заданию условий (критерии включения и исключения), в соответствии с которыми данные будут выбраны для последующего анализа либо временно проигнорированы. На вкладке перечислен ряд параметров, для которых можно задать интервалы допустимых значений. Если значения параметров пациента не удовле-

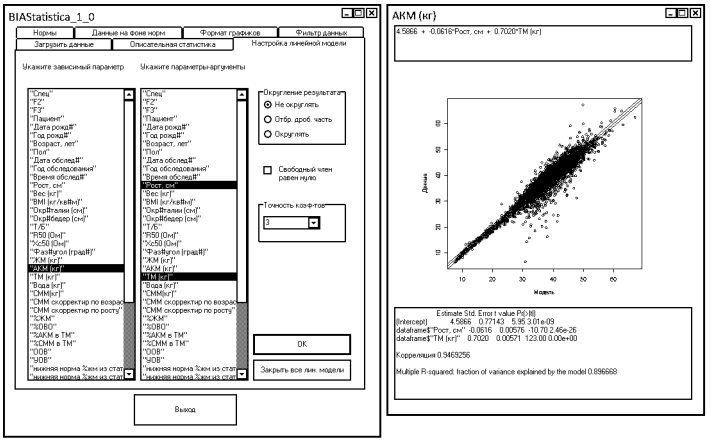


Рис. 1. Построение линейной модели для параметра «Активная клеточная масса».

творяют хотя бы одному из перечисленных условий, то такой пациент исключается из дальнейшего анализа.

- **«Описательная статистика».** На этой вкладке доступны функции наглядного представления данных в форме графиков, а также основные статистические показатели выборки.

- **«Настройка линейной модели».** Нередко при анализе результатов обследования состава тела необходимо получать линейные регрессионные модели, характеризующие зависимость переменной отклика от объясняющих (независимых) переменных. Для этого в программе предусмотрена возможность выбора соответствующей линейной комбинации и настройки ее коэффициентов методом наименьших квадратов.

На рисунке 1 показан пример построения линейной модели для параметра «Активная клеточная масса» (АКМ) в предположении о линейной зависимости АКМ от возраста пациента и от значения параметра «Тощая масса» (ТМ). Исходные данные в нашем примере представляют собой результаты биоимпедансной оценки состава тела с использованием анализатора АВС-01 «Медасс» (АО НТЦ «Медасс», Москва) у 3874 здоровых мужчин в возрасте от 5 до 80 лет [9]. Левое окно демонстрирует интерфейс вкладки «Линейная модель», на которой размещаются опции построения такой модели. Правое окно, заголовок которого соответствует имени настраиваемого параметра и номеру попытки построить модель для данного параметра, является результатом построения линейной модели с выбранными опциями.

Верхнее текстовое поле содержит итоговую формулу для оценки величины АКМ. На графике можно видеть, как соотносятся оценки АКМ, полученные на основе встроенной формулы биоимпедансного анализатора (по оси ординат), и с помощью линейной модели (по оси абсцисс). Сплошная линия на графике соответствует прямой $y = x$. Нижнее текстовое поле содержит более подробную информацию о коэффициентах модели.

- **«Нормы».** Границы нормальных значений компонентного состава тела строятся как персентильные кривые, зависящие от пола и возраста. Формальная классификация значений признаков (ниже нормы/норма/выше нормы) проводится на основе того, каким персентилям соответствуют данные для конкретного пациента.

Для построения границ нормальной изменчивости параметров состава тела используется набор пакетов семейства GAMLSS (Generalized Additive Models for Location, Scale and Shape), написанных на языке R [10, 11], применяемый для аналогичных вычислений при характеристике процессов роста и развития детей в отчетах Всемирной организации здравоохранения за последние несколько лет [12].

Идея метода состоит в следующем [10, 13, 14]. Предположим, что интересующий параметр y имеет медиану μ, а величина y^λ (или, для $\lambda = 0$, $\log_e y$) распределена нормально со средним

значением 0. Пусть σ — коэффициент вариации параметра y. Тогда величина

$$z = \frac{y/\mu^{\lambda} - 1}{\lambda \times \sigma}, \qquad \lambda \neq 0, \tag{1}$$

$$z = \frac{\log(y/\mu)}{\sigma}, \qquad \lambda = 0 \tag{2}$$

имеет распределение, близкое к $N(0,1)$. Распределение z называется распределением Бокса-Кокса-Кола-Грина (Box-Cox-Cole-Green, BCCG). Величину z называют значением Альтмана (иногда просто z-значением, или z-скором (калька с англ. z-scores)). Для каждого конкретного измерения y_i численное значение соответствующего z_i выражает меру отклонения данного наблюдения от медианы. Зная z_i, можно однозначно установить, какая часть измерений из генеральной совокупности по предсказанию модели лежит левее измерения y_i. Например, значение $z = 0$ соответствует 50-му персентилю, а $z = -1$ — персентилю 15,87, то есть 15,87 % значений в генеральной совокупности лежит левее соответствующего y_i.

Написанное выше верно для случая, когда все параметры распределения y (то есть величины λ, μ, σ) зависят от объясняющей переменной t. Тогда λ, μ, σ можно приблизить кубическими сплайнами $L(t)$, $M(t)$, $S(t)$.

Из формул (1)–(2) получаем, что $C_{100\alpha}(t)$ — персентильная кривая параметра y, соответствующая 100α-му персентилю (то есть кривая, под которой по предположению лежит 100α процентов значений параметра y из генеральной совокупности), задается выражением

$$C_{100\alpha}(t) = M(t)(1 + L(t)S(t)Z_{\alpha})^{1/L(t)}, \qquad \text{при } L(t) \neq 0, \tag{3}$$

$$C_{100\alpha}(t) = M(t)\exp[S(t)Z_{\alpha}], \qquad \text{при } L(t) = 0. \tag{4}$$

Таким образом, персентильные кривые параметра y можно однозначно получить, зная степени свободы сплайнов, приближающих $L(t)$, $M(t)$, $S(t)$. Степень свободы сплайна представляет собой компромисс между точностью описания данных и гладкостью получаемых кривых.

Оценка качества полученной модели строится на основе информационного критерия

$$D + df \times \log n, \tag{5}$$

где D — отклонение модельного прогноза от данных, df — сумма степеней свободы кубических сплайнов, n — размер выборки. Таким образом, увеличение точности путем повышения числа степеней свободы (то есть уменьшение первого слагаемого) штрафуется увеличением второго слагаемого.

GAMLSS — это обобщение метода LMS для моделирования поведения случайных величин из широкого класса распределений [10, 14]: распределение не обязано быть нормальным или логнормальным, оно может иметь значительную асимметрию и коэффициент эксцесса. Кроме того, его параметры могут нелинейно зависеть от нескольких объясняющих величин (например, от возраста и длины тела).

На рисунке 2 показан пример построения зависящих от возраста границ нормальных значений параметра «Рост». Исходные данные те же, что и в примере построения линейной модели. Левое окно демонстрирует интерфейс вкладки «Нормы». Правое окно является результатом построения границ нормальной возрастной изменчивости с выбранными опциями.

Границы норм представляют собой параметрическое семейство кривых, соответствующих указанным в левом окне персентилям. Персентильные кривые зависят от четырех параметров, которые, в свою очередь, являются функциями возраста. Это медиана (Mu), разброс (Sigma), скос (Nu) — характеристика симметричности распределения, и эксцесс (Tau) — характеризует, насколько остра вершина у графика плотности распределения. Каждый из указанных параметров моделируется кубическим сплайном с заданной степенью свободы. Сплайны можно визуализировать, нажав на кнопку «Построить LMS-кривые». Так как скорость изменения большинства интересующих параметров высока в начальном периоде жизни и затем снижается, то приходится компенсировать эту неоднородность степенным преобразованием возрастной шкалы (за это в GAMLSS-модели отвечает параметр Lambda).

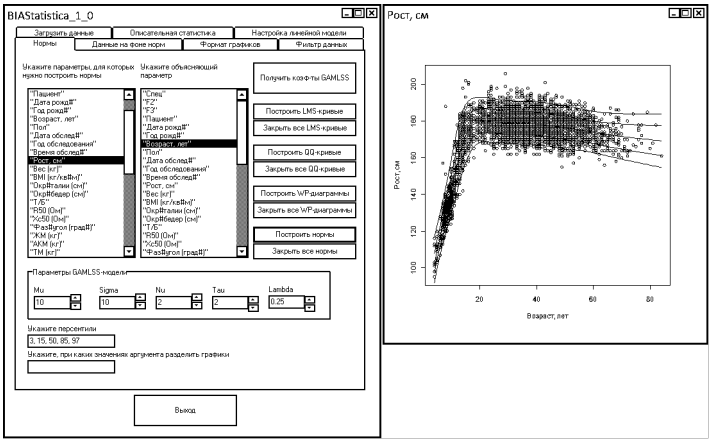


Рис. 2. Построение границ нормальной возрастной изменчивости для параметра «Рост».

Для оценки качества полученной модели используется информация о частных отклонениях данных от медианы. Если модель адекватно описывает данные, то распределение отклонений должно быть близко к стандартному нормальному распределению. Графики плотности распределения отклонений и другую информацию о соответствии модели и данных можно проанализировать, нажав на кнопки «Построить QQ-кривые» и «Построить WP-диаграммы».

- **«Данные на фоне норм»** Для характеристики отдельных групп пациентов удобно иметь возможность представить данные на фоне границ нормальных значений признаков для соответствующего пола и возраста. Описанный элемент интерфейса предоставляет такую возможность.

5 Заключение

Таким образом, в работе впервые предложена технология автоматизированной обработки данных биоимпедансных измерений, реализованная в виде программы-оболочки BIAStatistica. Программа позволяет строить кривые нормальной изменчивости параметров биоимпеданса и состава тела, получать основные статистические характеристики соответствующих распределений и информацию о взаимосвязи признаков. В дальнейшем планируется расширить функционал программы за счет реализации альтернативных алгоритмов формирования границ норм, повышения возможностей визуализации и сравнительного анализа данных.

Список литературы

[1] *Heymsfield S.B., Lohman T.G., Wang Z., Going S.B.* Human body composition (2nd ed.). — Champaign, IL: Human Kinetics, 2005. — 523 p.

[2] *Grimnes S., Martinsen O.G.* Bioimpedance and bioelectricity basics (2nd ed.). — L.: Academic Press, 2008. — 471 p.

[3] *Николаев Д.В., Смирнов А.В., Бобринская И.Г., Руднев С.Г.* Биоимпедансный анализ состава тела человека. — М.: Наука, 2009. — 392 с.

[4] *Bosy-Westphal A., Danielzik S., Dörhöfer R.-P. et al.* Phase angle from bioelectrical impedance analysis: population reference values by age, sex, and body mass index // J. Parent. Enteral Nutr. — 2006. — V. 30. — P. 309–316.

[5] *Гайдашев А.Э., Сахно Ю.Ф., Решетников И.С.* Возможности, значение и роль скрининговых исследований в Центрах здоровья для снижения уровня преждевременной заболеваемости и смертности от кардиоваскулярных заболеваний // Функциональная диагностика. — 2009. — № 3. — С. 2–7.

[6] The Comprehensive R Archive Network. — http://cran.r-project.org/.

[7] *Maindonald J.H.* Using R for Data Analysis and Graphics. Introduction, Code and Commentary. — Centre for Mathematics and Its Applications, Australian National University, 2008. — http://cran.r-project.org/doc/contrib/usingR.pdf.

[8] *Venables W.N., Smith D.M. and the R Development Core Team.* An introduction to R. — R Development Core Team, 2010. — 103 p. — http://cran.r-project.org/doc/manuals/R-intro.pdf.

[9] *Смирнов А.В., Колесников В.А., Николаев Д.В., Ерюкова Т.А.* АВС-01 «Медасс»: анализатор оценки баланса водных секторов организма с программным обеспечением (руководство пользователя). — М.: АО НТЦ «Медасс», 2009. — 38 с.

[10] *Stasinopoulos D.M., Rigby R.A.* Generalized additive models for location, scale and shape (GAMLSS) in R // J. Stat. Software. — 2007. — Vol. 23. — http://www.jstatsoft.org/v23/i07.

[11] Generalized Additive Models for Location, Scale and Shape (GAMLSS). — http://gamlss.org.

[12] *de Onis M., Onyango A.W., Borghi E. et al.* Development of a WHO growth reference for school-aged children and adolescents // Bull. World Health Org. — 2007. — Vol. 85. — P. 660–667.

[13] *Cole T.J., Green P.J.* Smoothing reference centile curves: the LMS method and penalized likelihood // Stat. Med. — 1992. — Vol. 11. — P. 1305–1319.

[14] *Cole T.J., Stanojevic S., Stocks J. et al.* Age- and size-related reference ranges: A case study of spirometry through childhood and adulthood // Stat. Med. — 2009. — Vol. 28. — P. 880–898.

УДК 519.718.7

БЕСПОВТОРНЫЕ ФУНКЦИИ НАИМЕНЬШЕЙ ТЕСТОВОЙ СЛОЖНОСТИ

© 2011 г. Д. В. Чистиков

dch@cs.msu.ru

Кафедра математической кибернетики

1 Введение

Рассмотрим функциональный *базис* $\mathfrak{B}$ (множество функций алгебры логики), обладающий свойством *наследственности*, то есть содержащий вместе с каждой функцией f все ее *подфункции* f^x_σ, получаемые подстановкой констант на места переменных. Функцию называем *бесповторной* в базисе $\mathfrak{B}$, если она представима формулой над этим базисом, в которой символы переменных не повторяются.

Для существенно зависящей от всех своих переменных и бесповторной в наследственном базисе $\mathfrak{B}$ функции $f(x_1, \ldots, x_n)$ рассмотрим задачу *тестирования относительно бесповторной альтернативы*, заключающуюся в построении *теста* — множества наборов аргументов, отличающего f от всех остальных бесповторных в том же базисе функций, зависящих от x_1, $x_2, \ldots, x_n$. Минимальную длину теста (количество наборов в нем) функции f в базисе $\mathfrak{B}$ будем обозначать символом $T_\mathfrak{B}(f)$. Рассмотрим величину

$$T(f) = \min_\mathfrak{B} T_\mathfrak{B}(f),$$

где минимум берется по всем наследственным базисам $\mathfrak{B}$, в которых функция f является бесповторной. Нетрудно понять, что $T(f)$ есть $T_{\mathfrak{B}(f)}(f)$, где символом $\mathfrak{B}(f)$ обозначен наследственный базис, состоящий из всех подфункций функции f, включая f.

Настоящая работа посвящена определению экстремального значения $\min T(f)$, где минимум берется по множеству всех булевых функций, существенно зависящих от n переменных, и нахождению всех функций — элементов $\operatorname{Argmin} T(f)$. В работе доказывается, что при любом фиксированном $n \geqslant 5$ наименьшее значение величины $T(f)$ равно 5, и описываются все функции, на которых это значение достигается. В терминах $T_\mathfrak{B}(f)$ результат настоящей работы заключается в нахождении всех функций f, удовлетворяющих неравенству $T_\mathfrak{B}(f) \leqslant 5$ для какого-либо параметра $\mathfrak{B}$ и любого $n \geqslant 5$.

Задача тестирования относительно бесповторной альтернативы была поставлена А. А. Вороненко в работе [1] и изучалась для различных булевых базисов. Оценкам величины $T_\mathfrak{B}(f)$ для индивидуальных бесповторных функций в базисе всех функций двух переменных посвящена работа [2], в базисе из конъюнкции и дизъюнкции — работы [3, 6]. Зависимость длины теста дизъюнкции n переменных от базиса исследована в статье [4], а в работе [5] установлено, что в случае суперлинейной скорости роста $T_\mathfrak{B}(x_1 \vee \ldots \vee x_n)$ (для этого достаточно наличия в $\mathfrak{B}$ хотя бы одной функции с изолированным набором, например $x \oplus y$) существует бесповторная функция f, обладающая подфункцией f^x_σ большей тестовой сложности, чем она сама: $T_\mathfrak{B}(f) < T_\mathfrak{B}(f^x_\sigma)$.

Последний результат не позволяет в общем случае получать нижние оценки значений $T_\mathfrak{B}(f)$ из оценок для $T_\mathfrak{B}(f^x_\sigma)$ и свидетельствует о том, что функции сравнительно невысокой тестовой сложности могут иметь достаточно замысловатое строение. Результаты настоящей работы, однако, показывают, что на функции, наиболее простые в смысле характеристики $T(f)$, этот вывод распространить нельзя. Везде в дальнейшем под *тестовой сложностью* функции f будем понимать именно значение $T(f)$.

Функции f и f' одного числа переменных называются *обобщенно однотипными*, если одна получается из другой какой-либо перестановкой переменных и навешиванием отрицаний на некоторые переменные, а также, возможно, на саму функцию. Немонотонные обобщенно однотипные функции имеют одинаковую тестовую сложность.

Теорема 1. *При любом $n \geqslant 3$ функция*

$$\mathrm{XOR}_n(x_1, \ldots, x_n) = (x_1 \vee \ldots \vee x_n)(\overline{x}_1 \vee \ldots \overline{x}_n)$$

имеет тестовую сложность 5.

Теорема 2. *Если $n \geqslant 5$ и функция f существенно зависит от n переменных, то*

$$T(f) \geqslant 5.$$

Теорема 3. *Если $n \geqslant 5$ и для функции f, существенно зависящей от n переменных, справедливо равенство*

$$T(f) = 5,$$

то f обобщенно однотипна с XOR_n.

Доказательству этих трех фактов и посвящена основная часть настоящей статьи.

2 Экстремальное значение

Докажем вначале верхнюю оценку теоремы 1. Нам понадобится следующее известное определение: функция $f(x_1, \ldots, x_n)$ называется *поляризуемой*, если для некоторого вектора $\delta = (\delta_1, \ldots, \delta_n) \in E_2^n$ функция $f(x_1^{\delta_1}, \ldots, x_n^{\delta_n})$ монотонна. Подходящий вектор δ называют *вектором поляризации* функции f. Отметим, что поляризуемая функция f имеет единственный вектор поляризации тогда и только тогда, когда она зависит существенно от всех своих переменных, причем $\delta_i = 1$ означает монотонную зависимость f от x_i, а $\delta_i = 0$ — антимонотонную.

Лемма 1. *При любом $n \geqslant 3$ справедливо неравенство $T(\mathrm{XOR}_n) \leqslant 5$.*

Доказательство. Заметим, что все функции базиса $\mathfrak{B}(\mathrm{XOR}_n)$, кроме самой функции XOR_n, поляризуемы. Возьмем в тест для XOR_n оба нулевых набора этой функции, наборы, соседние с ними по какой-нибудь одной переменной x_i, и еще один произвольный набор. Покажем, что всякое выбранное таким образом множество является тестом. В самом деле, произвольная функция, совпадающая с XOR_n на первых четырех наборах, не является ни монотонной, ни антимонотонной по переменной x_i и, следовательно, неполяризуема. Все неполяризуемые функции, бесповторные в базисе $\mathfrak{B}(\mathrm{XOR}_n)$ и существенно зависящие от n переменных, обобщенно однотипны с XOR_n. Наличие трех единичных наборов означает, что нулевых наборов у функции ровно два (оба вошли в тест). Лемма доказана. □

Нижнюю оценку теоремы 1 мы получим как следствие одного из вспомогательных утверждений, доказывающих теорему 2.

Лемма 2. *Если функция f отлична от постоянной и хотя бы одна из функций $x \,\&\, y$, $x \vee y$ не является бесповторной в базисе $\mathfrak{B}(f)$, то $T(f) = n + 1$, где n — число существенных переменных f.*

Доказательство. Случай $n = 1$ проверяется непосредственно. Пусть $n \geqslant 2$. Если f не монотонна, то базис $\mathfrak{B}(f)$ содержит отрицание, поэтому из условий леммы следует, что он не содержит ни конъюнкции, ни дизъюнкции двух переменных, то есть состоит только из линейных функций. Следовательно, функция f линейна и существенно зависит от всех своих переменных x_1, x_2, …, x_n, а ее альтернативами являются все остальные $2^{n+1} - 1$ линейные функции этих переменных. Каждый входящий в тест набор накладывает линейное ограничение на вектор из $n + 1$ коэффициента в полиноме Жегалкина f. Из определения теста следует однозначная разрешимость соответствующей системы линейных уравнений, необходимым условием которой является неравенство $m \geqslant n + 1$, где m — число уравнений, так что $T(f) \geqslant n + 1$. Точное равенство следует из того, что значения f на множестве из нулевого набора и всех наборов, соседних с нулевым, доказывают существенность всех переменных и однозначно определяют свободный член. Если же f монотонна и зависит существенно хотя бы от двух переменных, то она обязательно является их конъюнкцией либо дизъюнкцией. Нетрудно проверить, что и в этом случае $T(f) = n + 1$. Лемма доказана. □

Лемма 3. *Любая частичная булева функция, определенная на множестве из не более чем* 5 *наборов и доопределимая до монотонной (поляризуемой), доопределима также до бесповторной в базисе* $\{\&, \vee\}$ *(соответственно* $\{\&, \vee, \neg\}$*).*

Доказательство. Не ограничивая общности рассуждений, будем считать, что f монотонна и определена на 5 наборах, причем число q ее нулей меньше числа единиц. Если $q = 0$, то f доопределима до константы 1; если $q = 1$ и $f(\alpha_1, \ldots, \alpha_n) = 0$, то f доопределима до конъюнкции всех переменных x_i таких, что $\alpha_i = 0$. Если же $q = 2$, то f доопределима до дизъюнкции двух таких конъюнкций, которая бесповторна в силу закона дистрибутивности. Лемма доказана. □

Замечание. Примером частичной булевой функции, которая определена на множестве из 6 наборов, доопределима до монотонной, но не до бесповторной в базисе $\{\&, \vee\}$, может служить функция f, полученная из медианы $xy \vee yz \vee zx$ заменой значений $f(0,0,0)$ и $f(1,1,1)$ на неопределенное.

Заметим, что из результатов работ [3] и [6] следует, что для всех бесповторных функций f в базисе $\{\&, \vee, \neg\}$, существенно зависящих от $n \geqslant 5$ переменных, $T(f) \geqslant 6$. Это позволяет сформулировать следующий результат.

Следствие 1. *Пусть все переменные поляризуемой булевой функции* $f(x_1, \ldots, x_n)$ *являются существенными. Тогда при* $n \geqslant 5$ *справедливо неравенство*

$$T(f) \geqslant 6.$$

Доказательство для функций f, не являющихся бесповторными в базисе $\{\&, \vee, \neg\}$, следует из леммы 2 и леммы 3.

Лемма 4. *Для всякой существенно зависящей от* $n \geqslant 3$ *переменных неполяризуемой и нелинейной функции* $f(x_1, \ldots, x_n)$ *справедливо неравенство* $T(f) \geqslant 5$.

Доказательство. Всякий тест для f должен содержать не менее двух нулевых и двух единичных наборов, в противном случае частичная булева функция, задаваемая значениями f на наборах теста, доопределима до поляризуемой и, следовательно, до заведомо отличной от f бесповторной в базисе $\{\&, \vee, \neg\}$. Не ограничивая общности рассуждений, будем считать, что нулевыми являются набор $\mathbf{0}$ со всеми нулевыми компонентами и набор α, имеющий в своей записи единицы в компонентах с номерами 1, 2, …, k (общий случай сводится к данному рассмотрением подходящей обобщенно однотипной функции). Пусть d — количество единичных наборов β в тесте, удовлетворяющих условию $\beta \leqslant \alpha$. Рассмотрим в зависимости от d несколько случаев.

Отметим, что если $d \leqslant 1$, то упомянутая частичная функция доопределима до поляризуемой. Действительно, если $d = 0$, то f неотличима от $x_{k+1} \vee \ldots \vee x_n$. Если $d = 1$, то f неотличима от $x_1^{\beta_1} \,\&\, \ldots \,\&\, x_k^{\beta_k} \vee x_{k+1} \vee \ldots \vee x_n$, где $\beta = (\beta_1, \ldots, \beta_k, 0, \ldots, 0)$. Пусть теперь $d = 2$. Отметим, что в этом случае обязательно $k = n$, иначе f неотличима от $f_\sigma^{x_n}$ при любом σ ($f_\sigma^{x_n} \not\equiv f$ в силу того, что f существенно зависит от x_n). Пусть указанному условию удовлетворяют наборы β' и β''. Если эти наборы сравнимы ($\beta' \leqslant \beta''$), то f неотличима от $x_1^{\beta_1} \,\&\, \ldots \,\&\, x_r^{\beta_r}$, где 1, 2, …, r — номера общих компонент β' и β'', а β_1, β_2, …, β_r — их значения. Если β' и β'' несравнимы, но имеют общую первую компоненту со значением 0, то f неотличима от $\overline{x}_1 \cdot (K' \vee K'')$, где K' — конъюнкция переменных с номерами i такими, что $\beta'_i = 1$ и $\beta''_i = 0$, а K'' — конъюнкция переменных с номерами j такими, что $\beta'_j = 0$ и $\beta''_j = 1$. Случай наличия общей компоненты со значением 1 рассматривается аналогичным образом.

Осталось рассмотреть случай, когда β' и β'' не имеют общих компонент. Поскольку $k = n$, то $\beta'_i = \overline{\beta}''_i = \beta_i$ для $1 \leqslant i \leqslant n$. Положим для определенности $\beta_i = 1$ при $1 \leqslant i \leqslant m$ и $\beta_i = 0$ при $m + 1 \leqslant i \leqslant n$ ($1 \leqslant m < n$). Заметим, что на четырех наборах теста $f(x_1, \ldots, x_n)$ неотличима от функций

$$\overline{f}(x_1, \ldots, x_m, \overline{x}_{m+1}, \ldots, \overline{x}_n),$$
$$\overline{f}(\overline{x}_1, \ldots, \overline{x}_m, x_{m+1}, \ldots, x_n),$$
$$f(x_{i_1}, \ldots, x_{i_m}, x_{j_{m+1}}, \ldots, x_{j_n}),$$

где $(i_1, \ldots, i_m)$ и $(j_{m+1}, \ldots, j_n)$ — произвольные перестановки на множествах $\{1, \ldots, m\}$ и $\{m+1, \ldots, n\}$ соответственно. Поскольку f очевидно бесповторна в базисе $\mathfrak{B}(f)$, то и перечисленные функции являются бесповторными в этом базисе. Это означает, что если выбранное нами множество из четырех наборов является тестом для f, то все перечисленные альтернативы должны с f совпадать. Покажем, что в этом случае у f имеется линейная остаточная подфункция двух переменных, существенно зависящая от обеих, и, следовательно, в силу наследственности рассматриваемого базиса, f неотличима от бесповторной в нем альтернативы $x_1 \oplus x_n$.

Обратим внимание, что из приведенных выше соотношений следует, что числа m и $n-m$ нечетны: рассмотрение, скажем, четного $m = 2t$ приводит к противоречивой цепочке равенств

$$\begin{aligned} &f(0, \ldots, 0, 1, \ldots, 1, x_{m+1}, \ldots, x_n) = \\ &= \overline{f}(1, \ldots, 1, 0, \ldots, 0, x_{m+1}, \ldots, x_n) = \\ &= \overline{f}(0, \ldots, 0, 1, \ldots, 1, x_{m+1}, \ldots, x_n) \end{aligned}$$

(в каждой строке среди $2t$ первых аргументов в точности по t нулей и единиц; равенства следуют из совпадения f со второй и третьей из перечисленных ранее функций). Положим $m = 2t+1$ и $n - m = 2s+1$ и условимся обозначать $f = f(x_1, \mathbf{y}, \mathbf{z}, x_{m+1}, \mathbf{u}, \mathbf{v})$, где $\mathbf{y}$, $\mathbf{z}$ ($\mathbf{u}$, $\mathbf{v}$) — векторные аргументы размерности t (s). Отметим, что если, к примеру, $t = 0$ ($m = 1$), то наша цель достигнута, ибо соотношение

$$f(0, x_2, \mathbf{u}, \mathbf{v}) = \overline{f}(1, x_2, \mathbf{u}, \mathbf{v})$$

означает, что $f = x_1 \oplus f_0^{x_1}(x_2, \mathbf{u}, \mathbf{v})$ и подстановка констант обнаруживает у f искомую линейную подфункцию.

Осталось рассмотреть последний случай. Пользуясь теми же правилами, что и выше, приходим к соотношениям

$$\begin{aligned} &f(0, \mathbf{0}, \mathbf{1}, 0, \mathbf{0}, \mathbf{1}) = \overline{f}(1, \mathbf{1}, \mathbf{0}, 0, \mathbf{0}, \mathbf{1}) = \overline{f}(1, \mathbf{0}, \mathbf{1}, 0, \mathbf{0}, \mathbf{1}), \\ &f(0, \mathbf{0}, \mathbf{1}, 0, \mathbf{0}, \mathbf{1}) = \overline{f}(0, \mathbf{0}, \mathbf{1}, 1, \mathbf{1}, \mathbf{0}) = \overline{f}(0, \mathbf{0}, \mathbf{1}, 1, \mathbf{0}, \mathbf{1}), \\ &\overline{f}(0, \mathbf{0}, \mathbf{1}, 1, \mathbf{0}, \mathbf{1}) = f(1, \mathbf{1}, \mathbf{0}, 1, \mathbf{0}, \mathbf{1}) = f(1, \mathbf{0}, \mathbf{1}, 1, \mathbf{0}, \mathbf{1}). \end{aligned}$$

Функция $f(x_1, \mathbf{0}, \mathbf{1}, x_{m+1}, \mathbf{0}, \mathbf{1})$, таким образом, линейна и существенно зависит от двух переменных. Лемма доказана. □

Теорема 2 следует из леммы 2, следствия 1 и леммы 4. Нижняя оценка теоремы 1 вытекает непосредственно из леммы 4.

3 Вид тестов для функций наименьшей сложности

Следующие два раздела посвящены доказательству теоремы 3. В настоящем разделе определяется вид тестов для функций f, удовлетворяющих соотношению $T(f) \leqslant 5$. Основной результат формулируется для случая $n \geqslant 5$. При доказательстве используется следующий критерий доопределимости частичных булевых функций до поляризуемых.

Лемма 5. *Частичная булева функция $f(x_1, \ldots, x_n)$ не является доопределимой до поляризуемой тогда и только тогда, когда для каждого набора $\delta \in E_2^n$ найдется такая пара наборов α, $\beta \in E_2^n$, что $f(\alpha) = 1$, $f(\beta) = 0$ и $\alpha_i = \delta_i$ при всех i со свойством $\alpha_i \neq \beta_i$.*

Доказательство. Функция f не является доопределимой до поляризуемой в том и только том случае, когда никакой набор $\delta \in E_2^n$ не может быть вектором ее поляризации. Нетрудно убедиться, что f нельзя доопределить до монотонной тогда и только тогда, когда найдется такая пара наборов α, $\beta \in E_2^n$, что $f(\alpha) = 1$, $f(\beta) = 0$ и $\alpha \leqslant \beta$. Следовательно, f нельзя доопределить до поляризуемой тогда и только тогда, когда для каждого $\delta \in E_2^n$ найдется такая пара наборов α, $\beta \in E_2^n$, что $f(\alpha^\delta) = 1$, $f(\beta^\delta) = 0$ и $\alpha \leqslant \beta$. Обозначим теперь $\alpha'_i = \alpha_i^{\delta_i}$,

$\beta'_i = \beta_i^{\delta_i}$ и $\delta'_i = \overline{\delta}_i$, тогда условия переписываются в виде $f(\alpha') = 1$, $f(\beta') = 0$ и $\alpha' \oplus \delta' \leqslant \beta' \oplus \delta'$. Последнее условие выполняется тогда и только тогда, когда при $\alpha'_i \neq \beta'_i$ всегда $\delta'_i = \alpha'_i$. Снятие штрихов приводит к формулировке леммы. □

Лемма 6. *Всякая неполяризуемая булева функция $h(x_1, \ldots, x_n)$, зависящая существенно от всех своих $n \geqslant 5$ переменных и удовлетворяющая неравенству $T(h) \leqslant 5$, обобщенно однотипна с функцией f, допускающей тест вида $\{\mathbf{0}, \mathbf{1}, \alpha^{(1)}, \alpha^{(2)}, \alpha^{(3)}\}$, где $f(\mathbf{0}) = f(\mathbf{1}) = 0$, $f(\alpha^{(s)}) = 1$ для $s = 1, 2, 3$ и*

$$\text{(I)} \quad \begin{cases} \alpha^{(1)} = (0, 1, \mathbf{0}), \\ \alpha^{(2)} = (1, 0, \mathbf{0}), \\ \alpha^{(3)} = (0, 0, \mathbf{1}) \end{cases} \qquad \textit{либо} \qquad \text{(II)} \quad \begin{cases} \alpha^{(1)} = (0, \mathbf{1}, \mathbf{1}), \\ \alpha^{(2)} = (1, \mathbf{0}, \mathbf{0}), \\ \alpha^{(3)} = (0, \mathbf{0}, \mathbf{1}). \end{cases}$$

Доказательство. Значения h на наборах теста задают некоторую частичную булеву функцию g. Если эта функция доопределима до поляризуемой, то по лемме 3 она доопределима и до бесповторной в базисе $\{\&, \vee, \neg\}$, которая заведомо отлична от h в силу неполяризуемости h. Следовательно, функцию g нельзя доопределить до поляризуемой.

Не ограничивая общности рассуждений, предположим, что в тест вошло ровно два нулевых набора h (если этих наборов меньше, то g заведомо доопределима до поляризуемой). Пусть Γ — подкуб наименьшей размерности, содержащий оба этих набора, а d — число единичных наборов теста, принадлежащих Γ. Если $\Gamma \neq E_2^n$, то в случае $d = 3$ функцию h нельзя отличить от ее проекции h' на Γ, а в случае $d \leqslant 2$ — от дизъюнкции h' с некоторыми литералами фиксированных переменных Γ. В последнем случае h обязана с такой альтернативой совпадать, но тогда наборы теста, принадлежащие Γ, должны составлять тест для функции h'. Случай $d \leqslant 1$ соответствует функции g, доопределимой до поляризуемой, и поэтому исключается, а случай $d = 2$ соответствует тесту из четырех наборов для неполяризуемой функции h'. Согласно леммам 2 и 4, функция h' обязательно зависит от не более чем трех переменных. Поскольку вне Γ лежит лишь один набор теста, количество дизъюнктируемых с h литералов равно 1. Следовательно, $n \leqslant 4$, что противоречит условию леммы.

Таким образом, возможен только случай $\Gamma = E_2^n$. Перейдем к обобщенно однотипной функции f, обеспечив наличие в тесте наборов $\mathbf{0}$ и $\mathbf{1}$ со значениями $f = 0$. Воспользуемся критерием из леммы 5 для функции g', задаваемой значениями f на наборах теста, и учтем, что существуют ровно два набора β со свойством $g'(\beta) = 0$. Согласно лемме 5, для каждого $\delta \in E_2^n$ найдется такой набор α, что $g'(\alpha) = 1$ и либо при каждом i с $\alpha_i \neq 0$ справедливо $\alpha_i = \delta_i$, либо при каждом i с $\alpha_i \neq 1$ справедливо $\alpha_i = \delta_i$. Иными словами, либо при каждом i из равенства $\alpha_i = 1$ следует равенство $\delta_i = 1$, либо при каждом i из равенства $\alpha_i = 0$ следует равенство $\delta_i = 0$. Данное условие является условием сравнимости наборов α и δ в булевом кубе E_2^n. Итак, единичные наборы теста $\alpha^{(1)}$, $\alpha^{(2)}$, $\alpha^{(3)}$ должны удовлетворять следующему требованию: для каждого набора $\delta \in E_2^n$ хотя бы один набор $\alpha^{(s)}$ сравним с δ.

Пусть k_s — число единичных компонент в наборе $\alpha^{(s)}$, $0 < k_s < n$. Число наборов куба E_2^n, сравнимых с $\alpha^{(s)}$, равно $2^{k_s} + 2^{n-k_s} - 1$, причем в число этих наборов входят $\mathbf{0}$ и $\mathbf{1}$. Следовательно, числа k_s для $s = 1, 2, 3$ должны удовлетворять соотношению

$$\sum_{s=1}^{3} \left(2^{n-k_s} + 2^{k_s} - 3\right) + 2 \geqslant 2^n.$$

Не ограничивая общности рассуждений, будем полагать, что $k_s \leqslant n - k_s$ для всех s. Заметим, что из неравенства $k_s \geqslant 2$ следует неравенство $2^{n-k_s} + 2^{k_s} \leqslant 4 + 2^{n-2}$, поэтому если все k_s больше либо равны 2, то из приведенного выше соотношения вытекает неравенство $5 \geqslant 2^{n-2}$, противоречащее условию леммы. Следовательно, среди наборов $\alpha^{(s)}$ есть набор, содержащий ровно одну единицу.

Пусть этот набор имеет вид $(1, \mathbf{0})$. С этим набором сравнимы те и только те ненулевые наборы булева куба, первая компонента которых равна 1, поэтому множество наборов, сравнимых хотя бы с одним из двух других единичных наборов теста, должно содержать все наборы с первой компонентой 0. Это возможно в двух следующих случаях: если в тесте содержится набор

$(0, \mathbf{1})$ и еще один произвольный набор, а также если в тесте есть второй набор, содержащий только одну единицу, и противоположный ему набор в подкубе $(1, -)$. Лемма доказана. □

Утверждение леммы 6 является ключевым в доказательстве теоремы 3. Дальнейшие рассуждения исследуют два выделенных случая и определяют множества подходящих функций f, при этом используется найденный вид возможных тестов, которые считаются фиксированными. В случае (I) полагается

$$f = f(x_1, x_2, \mathbf{y}), \tag{1}$$

а в случае (II) соответственно

$$f = f(x, \mathbf{y}, \mathbf{z}), \tag{2}$$

где $\mathbf{y} = (y_1, \ldots, y_m)$ и $\mathbf{z} = (z_1, \ldots, z_k)$, причем $m \geqslant 1$ и $k \geqslant 1$. Всюду в дальнейшем, когда говорится о функциях вида (1) и (2), считаются выполненными соотношения леммы 6. Некоторые из результатов оказываются справедливыми и в случае $n < 5$.

4 Описание всех функций наименьшей сложности

Настоящий раздел посвящен второй части доказательства теоремы 3. Вначале разбирается случай функции f вида (1), затем — случай f вида (2).

Будем говорить, что функция $g(\mathbf{u}, \mathbf{v})$ зависит *симметрическим образом* от переменных $\mathbf{v}$, если для любой перестановки $\mathbf{v}'$ набора переменных $\mathbf{v}$ справедливо тождество $g(\mathbf{u}, \mathbf{v}) \equiv \equiv g(\mathbf{u}, \mathbf{v}')$.

Лемма 7. *В представлениях* (1) *и* (2) *зависимость* f *от переменных* $\mathbf{y}$ *и* $\mathbf{z}$ *симметрическая.*

Доказательство. Всякая перестановка переменных внутри наборов $\mathbf{y}$ и $\mathbf{z}$ не изменяет наборов теста, поэтому все получаемые таким образом альтернативы должны совпадать с f. □

Лемма 8. *Если* $T(f) \leqslant 5$ *для* $f(x_1, \ldots, x_n)$ *вида* (1) *с* $n \geqslant 4$, *то все собственные подфункции функции* f *поляризуемы.*

Доказательство. Предположим, что $g(u_1, \ldots, u_s)$ — неполяризуемая собственная подфункция функции f наименьшей размерности s. Ясно, что $2 \leqslant s \leqslant m + 1$. Не ограничивая общности рассуждений, будем полагать, что для g справедливы равенства $g(u_1, \mathbf{0}) = u_1$ и $g(u_1, \mathbf{1}) = = \overline{u}_1$. Нетрудно видеть, что в этом случае функция f совпадает на наборах теста с функцией $g(x_1 \vee x_2, \mathbf{y}')$, где $\mathbf{y}'$ — произвольный поднабор набора $\mathbf{y}$, имеющий длину $s-1$. Если $s-1 < m$, то существуют как минимум два различных поднабора $\mathbf{y}'$ этой длины и, следовательно, имеются две отличные друг от друга возможные альтернативы для f, поскольку в силу нашего выбора g эта функция существенно зависит от всех своих переменных. Обе эти альтернативы не могут одновременно совпадать с f, поэтому мы приходим к противоречию с определением теста.

Рассмотрим теперь случай $s = m + 1$, $\mathbf{y}' = \mathbf{y}$. Наличие неотличимой альтернативы для f означает, что эта альтернатива и есть f. Рассмотрим функцию $h = \overline{g}(\overline{u}_1, \mathbf{u}')$, где $\mathbf{u}' = (u_2, \ldots, u_s)$. Нетрудно видеть, что g совпадает с h на четырех наборах $(0, \mathbf{0})$, $(0, \mathbf{1})$, $(1, \mathbf{0})$, $(1, \mathbf{1})$, так что функцию f на наборах теста нельзя отличить от функции $h(x_1 \vee x_2, \mathbf{y})$. Следовательно, h тождественно равна g, откуда следует, что $g(u_1, u_2, \mathbf{0}) = u_1 \oplus u_2 \oplus g(0, 0, \mathbf{0})$. Эта подфункция не является поляризуемой, так что $s = 2$, $m = 1$ и $n = 3$, что противоречит условию леммы. □

Лемма 9. *Если* $T(f) \leqslant 5$ *для* $f(x_1, \ldots, x_n)$ *вида* (1) *и все собственные подфункции* f *поляризуемы, то* f *обобщенно однотипна с* XOR_n.

Доказательство. Из условия леммы следует, что $f(1,1,\mathbf{0}) = 1$ и $f(0,1,\mathbf{1}) = f(1,0,\mathbf{1}) = 1$, иначе функция $f(x_1,x_2,\mathbf{0}) = x_1 \oplus x_2$ или соответственно $f(0,x_2,\mathbf{y})$ неполяризуема. Симметрическая зависимость f от переменных $\mathbf{y}$ обеспечивает одинаковый характер монотонности этих переменных для каждой отдельно взятой подфункции $f_{\sigma_i}^{x_i}$. Так как $f(0,0,\mathbf{0}) = 0$ и $f(0,0,\mathbf{1}) = 1$, то подфункция $f_0^{x_1}$ монотонна по всем $\mathbf{y}$, откуда $f(0,1,\mathbf{y}) \equiv 1$ в силу равенства $f(0,1,\mathbf{0}) = 1$. Точно так же заключаем, что $f(1,0,\mathbf{y}) \equiv 1$.

Заметим теперь, что из всех подфункций вида $f(x_1,\alpha_2,\beta)$ только $f(x_1,0,\mathbf{0})$ и $f(x_1,1,\mathbf{1})$ зависят существенно от переменной x_1, поскольку в противном случае неполяризуемой является некоторая собственная подфункция функции f. Это означает, что при $\mathbf{y} \neq \mathbf{0},\mathbf{1}$ всегда $f(\overline{x}_1,x_2,\mathbf{y}) = f(x_1,x_2,\mathbf{y})$. Одно из значений f в последнем равенстве равно 1 в силу рассуждений предыдущего абзаца, поэтому равно 1 и другое, а значит, f принимает значение 0 только на наборах $\mathbf{0}$ и $\mathbf{1}$. □

Следствие 2. *Если $T(f) \leqslant 5$ для $f(x_1,\ldots,x_n)$ вида (1), то либо $n = 3$, либо $f = \mathrm{XOR}_n$.*

Доказательство следует из лемм 8 и 9.

Далее исследуется случай функции f вида (2).

Лемма 10. *Если $T(f) \leqslant 5$ для $f(x_1,\ldots,x_n)$ вида (2) с $n \geqslant 4$, то все собственные подфункции функции f поляризуемы, причем зависимость f от переменных $\mathbf{z}$ не является антимонотонной.*

Доказательство. Второе утверждение следует из равенств $f(0,\mathbf{0},\mathbf{0}) = 0$ и $f(0,\mathbf{0},\mathbf{1}) = 1$. Докажем первое утверждение. Пусть $g(u_1,\ldots,u_s)$ — неполяризуемая подфункция функции f наименьшей размерности s. Не ограничивая общности рассуждений, будем полагать справедливыми равенства $g(u_1,\mathbf{0}) = u_1$ и $g(u_1,\mathbf{1}) = \overline{u}_1$. Выберем какие-нибудь переменные y и z из наборов $\mathbf{y}$ и $\mathbf{z}$ соответственно. Предположим вначале, что $s \leqslant n-2$. Составим множество $\mathbf{x}'$ из произвольных $s-1 \leqslant n-3$ переменных f, отличных от x,y,z. Составим функцию $h = g(x,\mathbf{x}') \vee \overline{y}z$. Нетрудно видеть, что h совпадает с f на всех пяти наборах теста. Если при этом $k+m \geqslant 3$, то, выбирая другие переменные y,z, можно составить альтернативу h', отличную от h и обладающую таким же свойством, что противоречит определению теста. Следовательно, $k = m = 1$ и $n = 3$, но тогда $s = 1$, что противоречит неполяризуемости g. Таким образом, возможен только случай $s = n-1$.

Из условий леммы имеем $s \geqslant 3$. Рассмотрим в этом случае функцию $h = g(x,y,\mathbf{x}'',z)$, где $\mathbf{x}''$ — произвольный набор из $s-3 = n-4$ переменных f, отличных от x,y,z. Ясно, что h совпадает с f на наборах $\mathbf{0}$, $\mathbf{1}$, $(0,\mathbf{1},\mathbf{1})$, $(1,\mathbf{0},\mathbf{0})$. Если $h = 1$ на наборе $(x,\mathbf{y},\mathbf{z}) = (0,\mathbf{0},\mathbf{1})$, то h неотличима от f на всех наборах теста и имеет на одну существенную переменную меньше, что невозможно. Следовательно, h на этом наборе равна 0. С другой стороны, функция $h'(\mathbf{x}) = h'(x,\mathbf{y},\mathbf{z}) = \overline{h}(\overline{x},\mathbf{y},\mathbf{z})$ тоже совпадает с f на наборах $\mathbf{0}$, $\mathbf{1}$, $(0,\mathbf{1},\mathbf{1})$, $(1,\mathbf{0},\mathbf{0})$ и имеет $n-1$ существенную переменную, поэтому на наборе $(0,\mathbf{0},\mathbf{1})$ обязательно также $h' = 0$. Но тогда функция $h(x,\mathbf{y},\mathbf{z})$ при $(\mathbf{y},\mathbf{z}) = (\mathbf{0},\mathbf{1})$ переходит в подфункцию $h(x,\mathbf{0},\mathbf{1}) = x$. Следовательно, функция $g_1^{\tilde{z}}$ также является неполяризуемой, что противоречит выбору g. □

Переменные $\mathbf{u}$ функции $g(\mathbf{u},\mathbf{v})$ будем называть *неполяризуемыми*, если каждая переменная из $\mathbf{u}$ не является ни монотонной, ни антимонотонной для g. Утверждения леммы 7 и леммы 10 означают, что всякая функция f вида (2) с $T(f) \leqslant 5$ и $n \geqslant 4$ зависит от групп переменных $\mathbf{y}$ и $\mathbf{z}$ симметрическим образом, причем зависимость от переменных $\mathbf{y}$ может быть монотонной, антимонотонной или неполяризуемой, а зависимость от переменных $\mathbf{z}$ — монотонной либо неполяризуемой. Дальнейшие рассуждения показывают, что во всех шести возможных комбинациях функция f либо совпадает с XOR_n, либо имеет малую размерность $n = 3$. Нам понадобится следующее вспомогательное утверждение.

Лемма 11. *Пусть все собственные подфункции неполяризуемой функции $g(\mathbf{u},\mathbf{v})$ поляризуемы и g зависит от неполяризуемых переменных $\mathbf{v}$ симметрическим образом. Тогда найдется такой набор α, что обе функции $g(\alpha,\mathbf{v})$ и $g(\overline{\alpha},\mathbf{v})$ являются конъюнкциями (дизъюнкциями) литералов всех переменных $\mathbf{v}$ с противоположными наборами степеней $\mathbf{0}$ и $\mathbf{1}$, а для всякого набора $\gamma \neq \alpha,\overline{\alpha}$ подфункция $g(\gamma,\mathbf{v})$ тождественно равна некоторой постоянной.*

Доказательство. Поскольку все собственные подфункции функции g поляризуемы, то для каждой переменной v из $\mathbf{v}$ найдется единственный набор значений остальных переменных, переводящий g в подфункцию v, причем противоположный набор переводит g в $\overline{v}$. Все остальные одномерные подфункции f переменной v тождественно равны постоянным. Симметрическая зависимость g от $\mathbf{v}$ означает, что для всех подфункций вида $g(\gamma, \mathbf{v})$, кроме двух, изменение значения одной переменной v не влияет на значение g, поэтому все такие подфункции являются константами.

Рассмотрим теперь подфункцию $g(\alpha, \mathbf{v})$ и заметим, что предыдущие рассуждения сохраняют справедливость для всех наборов значений остальных переменных $\mathbf{v}$, кроме одного. Значение рассматриваемой подфункции зависит только от числа единиц в наборе $\mathbf{v}$, поэтому возможны лишь случаи конъюнкции и дизъюнкции всех переменных $\mathbf{v}$ или их отрицаний. Подфункция $g(\overline{\alpha}, \mathbf{v})$ при этом получается из $g(\alpha, \mathbf{v})$ навешиванием отрицаний на все переменные $\mathbf{v}$. □

Начнем перебор со случая отсутствия у f монотонных и антимонотонных переменных.

Лемма 12. *Пусть $T(f) \leqslant 5$ для $f(x_1, \ldots, x_n)$ вида (2), причем все собственные подфункции f поляризуемы, а f не является ни монотонной, ни антимонотонной по переменным $\mathbf{y}, \mathbf{z}$. Тогда $f = \mathrm{XOR}_n$.*

Доказательство. Воспользуемся результатом леммы 11 для $\mathbf{v} = (x)$, $\mathbf{v} = \mathbf{y}$ и $\mathbf{v} = \mathbf{z}$. Пусть отличны от постоянных функции $f(a, \beta, \mathbf{z})$ и $f(\overline{a}, \overline{\beta}, \mathbf{z})$, а также $f(x, \gamma, \delta)$ и $f(x, \overline{\gamma}, \overline{\delta})$. Если при этом γ не совпадает ни с β, ни с $\overline{\beta}$, то $f(x, \gamma, \delta) = f(x, \gamma, \delta')$ для любого δ' и все функции $f(x, \gamma, \delta')$ также отличны от постоянных. Это противоречит лемме 11, поэтому множества констант, подставляемых на места $x, \mathbf{y}, \mathbf{z}$ для получения неконстантных подфункций, должны быть одни и те же (на место каждого из трех поднаборов подставляются два противоположных набора констант). Поэтому навешиванием отрицаний на некоторые переменные функция f переводится в функцию g, у которой неконстантными являются подфункции $g(0, \mathbf{0}, \mathbf{z})$, $g(1, \mathbf{1}, \mathbf{z})$, $g(0, \mathbf{y}, \mathbf{0})$, $g(1, \mathbf{y}, \mathbf{1})$.

Рассмотрим вначале случай, когда неконстантными являются также функции $g(x, \mathbf{0}, \mathbf{1})$ и $g(x, \mathbf{1}, \mathbf{0})$. Если $m = k = 1$, то значение $g(0, 1, 1)$ должно совпадать со значениями $g(1, 1, 1)$, $g(0, 0, 1)$, $g(0, 1, 0)$, а значение $g(1, 0, 0)$ — со значениями $g(0, 0, 0)$, $g(1, 1, 0)$, $g(1, 0, 1)$, поэтому функция g обобщенно однотипна с функцией $xy \vee yz \vee zx$, которая, как нетрудно убедиться, требует не менее 6 наборов для тестирования. Следовательно, хотя бы одно из чисел m, k больше единицы.

Не ограничивая общности рассуждений, рассмотрим случай $m > 1$. Пусть β — произвольный набор значений переменных $\mathbf{y}$, отличный от $\mathbf{0}$ и $\mathbf{1}$. Обозначим

$$c_1 = g(0, \mathbf{0}, \mathbf{1}) = g(0, \beta, \mathbf{1}) = g(0, \mathbf{1}, \mathbf{1}),$$
$$c_2 = g(1, \mathbf{0}, \mathbf{0}) = g(1, \beta, \mathbf{0}) = g(1, \mathbf{1}, \mathbf{0}).$$

Так как

$$g(0, \beta, \mathbf{1}) = g(1, \beta, \mathbf{1}) = g(1, \beta, \mathbf{0}),$$

то $c_1 = c_2$. В то же время

$$g(1, \mathbf{0}, \mathbf{1}) = g(1, \mathbf{0}, \mathbf{0}) = c_2,$$
$$g(1, \mathbf{1}, \mathbf{1}) = g(0, \mathbf{1}, \mathbf{1}) = c_1$$

и, поскольку $g(1, \beta, \mathbf{1}) = g(0, \beta, \mathbf{1})$, то подфункция $g(1, \mathbf{y}, \mathbf{1})$ тождественно равна постоянной, что противоречит нашим предположениям.

Осталось рассмотреть случай неконстантных функций $g(x, \mathbf{0}, \mathbf{0})$ и $g(x, \mathbf{1}, \mathbf{1})$. Нетрудно убедиться, что для любой пары отличных от $\mathbf{0}$ и $\mathbf{1}$ наборов значения g на них совпадают, поэтому функция g обобщенно однотипна с XOR_n, а функция f с ней совпадает. Лемма доказана. □

Следующая лемма доказывает невозможность «смешанных» вариантов, когда зависимость по одной из групп переменных $\mathbf{y}, \mathbf{z}$ монотонная или антимонотонная, а по другой — неполяризуемая.

Лемма 13. *Пусть $T(f) \leqslant 5$ для $f(x_1, \ldots, x_n)$ вида (2), все собственные подфункции f поляризуемы и f не является ни монотонной, ни антимонотонной по одной из групп переменных $\mathbf{y}, \mathbf{z}$. Тогда f не является ни монотонной, ни антимонотонной и по другой из этих групп переменных.*

Доказательство. Рассмотрим три случая и приведем каждый из них к противоречию с леммой 11. Предположим вначале, что f монотонно зависит от $\mathbf{y}$. Так как $f(1, \mathbf{1}, \mathbf{1}) = 0$, то $f(1, \mathbf{0}, \mathbf{1}) = 0 \neq 1 = f(1, \mathbf{0}, \mathbf{0})$. С другой стороны, $f(0, \mathbf{0}, \mathbf{0}) = 0 \neq 1 = f(0, \mathbf{0}, \mathbf{1})$ и мы пришли к противоречию.

Допустим теперь, что f антимонотонна по переменным $\mathbf{y}$. Тогда для любого набора этих переменных справедливы соотношения $f(0, \mathbf{y}, \mathbf{0}) = 0 \neq 1 = f(0, \mathbf{y}, \mathbf{1})$. Первое равенство следует из условия $f(0, \mathbf{0}, \mathbf{0}) = 0$, а второе — из условия $f(0, \mathbf{1}, \mathbf{1}) = 1$. Произвольность выбора $\mathbf{y}$ приводит к противоречию.

Рассмотрим теперь случай монотонной зависимости f от переменных $\mathbf{z}$. Из равенств $f(1, \mathbf{0}, \mathbf{0}) = 1$ и $f(1, \mathbf{1}, \mathbf{1}) = 0$ следует, что $f(1, \mathbf{0}, \mathbf{z}) = 1 \neq 0 = f(1, \mathbf{1}, \mathbf{z})$ для любого $\mathbf{z}$, что приводит к противоречию и доказывает утверждение леммы. □

Из оставшихся двух случаев рассмотрим вначале тот, в котором f монотонна по переменным $\mathbf{y}$ и $\mathbf{z}$.

Лемма 14. *Не существует функции $f(x_1, \ldots, x_n)$ вида (2), удовлетворяющей условию $T(f) \leqslant 5$, не имеющей неполяризуемых собственных подфункций и монотонно зависящей от переменных $\mathbf{y}$ и $\mathbf{z}$.*

Доказательство. Так как $f(1, \mathbf{0}, \mathbf{0}) = 1$, то из монотонности f по переменным $\mathbf{y}, \mathbf{z}$ следует $f(1, \mathbf{1}, \mathbf{1}) = 1$, что неверно. □

Следующая лемма посвящена рассмотрению последнего оставшегося случая.

Лемма 15. *Пусть $T(f) \leqslant 5$ для $f(x_1, \ldots, x_n)$ вида (2), причем все подфункции f поляризуемы, а f антимонотонна по переменным $\mathbf{y}$ и монотонна по переменным $\mathbf{z}$. Тогда $n = 3$ и $f = x\,\overline{y} \vee \overline{x}\,z$.*

Доказательство. Рассмотрим набор $\mathbf{x}' = (0, 1, \mathbf{0}, 0, \mathbf{1})$, полученный из $(x, \mathbf{y}, \mathbf{z}) = (0, \mathbf{0}, \mathbf{1})$ перестановкой нуля и единицы в $\mathbf{y}$ и $\mathbf{z}$, и докажем, что $f(\mathbf{x}') = 0$. Действительно, в противном случае функция f не отличается на наборах теста от функции $f(x, \mathbf{y}', \mathbf{z}')$, получаемой из f перестановкой пары переменных из $\mathbf{y}$ и $\mathbf{z}$. Но тогда, поскольку зависимость f от переменных из $\mathbf{y}$ и из $\mathbf{z}$ симметрическая, а не меняющие функцию преобразования образуют группу относительно операции композиции, f должна зависеть симметрическим образом от объединенного набора переменных $(\mathbf{y}, \mathbf{z})$, что невозможно в силу различного характера монотонности $\mathbf{y}$ и $\mathbf{z}$. Следовательно, $f(\mathbf{x}') = 0$.

Заметим теперь, что в силу антимонотонности переменных $\mathbf{y}$ справедливы соотношения $f(0, \mathbf{1}, \mathbf{0}) \leqslant f(0, \mathbf{0}, \mathbf{0}) = 0$. Из них следует, что $f(0, \mathbf{1}, \mathbf{0}) = 0$, а значит, f не отличается на наборах теста от функции $\overline{f}(x, \overline{\mathbf{y}}, \overline{\mathbf{z}})$. По определению теста заключаем отсюда, что подфункции f_0^x и f_1^x являются самодвойственными. В частности, для набора $\mathbf{x}'' = (0, 0, \mathbf{1}, 1, \mathbf{0})$, полученного инвертированием всех компонент набора $\mathbf{x}'$, кроме первой, справедлива цепочка равенств $f(\mathbf{x}'') = \overline{f}(\mathbf{x}') = \overline{0} = 1$.

Снова воспользуемся симметрической зависимостью f от переменных $\mathbf{y}$ и $\mathbf{z}$. Число единиц в $\mathbf{y}$- и $\mathbf{z}$-поднаборах наборов $\mathbf{x}'$ и $\mathbf{x}''$ равно $(1, k-1)$ и $(m-1, 1)$ соответственно. Так как $f(\mathbf{x}') = 0 < 1 = f(\mathbf{x}'')$, а значения x-компоненты в $\mathbf{x}'$ и $\mathbf{x}''$ совпадают, то либо (из антимонотонности f по $\mathbf{y}$) $1 > m-1$, либо (из монотонности f по $\mathbf{z}$) $k-1 < 1$. Следовательно, хотя бы одно из чисел m, k равно единице. Не ограничивая общности рассуждений, рассмотрим случай $m = 1$ (случай

$k = 1$ сводится к данному навешиванием отрицаний на все переменные f). В силу монотонности f по $\mathbf{z}$ и отсутствия неполяризуемых подфункций справедливы следующие соотношения:

$$\begin{array}{lllll} f(1,0,\mathbf{0}) = 1 & \Rightarrow & f(1,0,\mathbf{z}) = 1 \quad \forall \mathbf{z} & \Rightarrow & f(0,0,\mathbf{z}) = 1 \quad \forall \mathbf{z} \neq \mathbf{0}, \\ f(1,1,\mathbf{1}) = 0 & \Rightarrow & f(1,1,\mathbf{z}) = 0 \quad \forall \mathbf{z} & \Rightarrow & f(0,1,\mathbf{z}) = 0 \quad \forall \mathbf{z} \neq \mathbf{1}. \end{array}$$

Следовательно, функция f имеет вид (в обозначениях $y = y_1$)

$$\overline{x}\,\overline{y}\,(z_1 \vee \ldots \vee z_k) \vee \overline{x}\,y\,(z_1 \,\&\, \ldots \,\&\, z_k) \vee x\,\overline{y} = \overline{x}\,(\,\overline{y}\,(z_1 \vee \ldots \vee z_k) \vee z_1 \,\&\, \ldots \,\&\, z_k) \vee x\,\overline{y}.$$

Но тогда, как нетрудно убедиться, f совпадает на наборах теста с функцией

$$\overline{f}(\overline{x}, z_1, y, z_2, \ldots, z_k)$$

и, по определению теста, должна быть ей равна. Переменные $z_2, \ldots, z_k$ в этом случае оказываются одновременно монотонными и антимонотонными, то есть несущественными, что противоречит нашему выбору f при $k \geqslant 2$. Следовательно, $k = 1$ и (в обозначениях $z = z_1$)

$$f = \overline{x}\,(\,\overline{y}\,z \vee z\,) \vee x\,\overline{y} = x\,\overline{y} \vee \overline{x}\,z. \qquad \square$$

Следствие 3. *Если $T(f) \leqslant 5$ для $f(x_1, \ldots, x_n)$ вида (2), то либо $n = 3$, либо $f = \mathrm{XOR}_n$.*

Теорема 3 следует из леммы 6 и следствий 2 и 3.

Работа выполнена при поддержке гранта Президента РФ МД–757.2011.9.

Список литературы

[1] *Вороненко А. А.* О проверяющих тестах для бесповторных функций // Математические вопросы кибернетики. Вып. 11. — М.: Физматлит, 2002. — С. 163–176.

[2] *Вороненко А. А., Чистиков Д. В.* Индивидуальное тестирование бесповторных функций // Ученые записки Казанского государственного университета. Сер. Физико-математические науки. — 2009. — Т. 151, кн. 2. — С. 36–44.

[3] *Бубнов С. Е., Вороненко А. А., Чистиков Д. В.* Некоторые оценки длин тестов для бесповторных функций в базисе $\{\&, \vee\}$ // Прикладная математика и информатика. — 2009. — Вып. 33. — С. 90–100.

[4] *Вороненко А. А.* Тестирование дизъюнкции как бесповторной функции в произвольном бесповторном базисе // Вестник Московского университета. Сер. 15. Вычислительная математика и кибернетика. — 2008. — № 4. — С. 51–52.

[5] *Чистиков Д. В.* Бесповторные функции с труднотестируемыми подфункциями // Вестник Московского университета. Сер. 15. Вычислительная математика и кибернетика. — 2010. — № 4. — С. 38–41.

[6] *Chistikov D. V.* Testing monotone read-once functions // Accepted to IWOCA 2011, to be published in Lecture Notes in Computer Science.

РЕФЕРАТЫ

М. Ф. Абдукаримов. ГРАНИЧНОЕ УПРАВЛЕНИЕ ПРОЦЕССОМ КОЛЕБАНИЙ, ОПИСЫВАЕМЫМ НЕОДНОРОДНЫМ ВОЛНОВЫМ УРАВНЕНИЕМ, ЗА МИНИМАЛЬНЫЙ ПРОМЕЖУТОК ВРЕМЕНИ // СБОРНИК СТАТЕЙ МОЛОДЫХ УЧЕНЫХ факультета ВМК МГУ выпуск №8 (2011 г.), стр. 5–18. В работе получены при $T = l$ необходимые и достаточные условия существования управления на двух концах и предъявлены в явном аналитическом виде эти управления, которые обеспечивают переход колебательного процесса, описываемого неоднородным волновым уравнением, из произвольного начального состояния в наперед заданное финальное состояние.

Библиография 8 раб.

Е. К. Алексеев. ОБ АТАКЕ НА ФИЛЬТРУЮЩИЙ ГЕНЕРАТОР С ФУНКЦИЕЙ УСЛОЖНЕНИЯ БЛИЗКОЙ К АЛГЕБРАИЧЕСКИ ВЫРОЖДЕННОЙ // СБОРНИК СТАТЕЙ МОЛОДЫХ УЧЕНЫХ факультета ВМК МГУ выпуск №8 (2011 г.), стр. 19–32. Рассматривается метод восстановления начального состояния (ключа) фильтрующего генератора по известной выходной последовательности. При этом используется приближение фильтрующей функции алгебраически вырожденной функцией.

Библиография 7 раб.

Н. А. Андреев, В. А. Лапшин, В. В. Науменко. ЭРГОДИЧНОСТЬ ВРЕМЕННОГО РЯДА ОБОБЩЕННОГО ПОКАЗАТЕЛЯ ЛИКВИДНОСТИ // СБОРНИК СТАТЕЙ МОЛОДЫХ УЧЕНЫХ факультета ВМК МГУ выпуск №8 (2011 г.), стр. 33–41. В работе предлагается адаптация существующего статистического теста, позволяющего при некоторых предположениях судить об эргодичности ряда на основании наблюдения траектории. В процессе адаптации рассмотрен случай частичного выполнения условий применимости алгоритма. Полученный алгоритм применяется к реальным данным — динамике некоторого показателя ликвидности финансового рынка.

Библиография 9 раб.

А. И. Аристов. ОЦЕНКИ ВРЕМЕНИ СУЩЕСТВОВАНИЯ ОБОБЩЕННЫХ РЕШЕНИЙ НАЧАЛЬНО-КРАЕВОЙ ЗАДАЧИ ДЛЯ ОДНОГО НЕЛИНЕЙНОГО УРАВНЕНИЯ СОБОЛЕВСКОГО ТИПА // СБОРНИК СТАТЕЙ МОЛОДЫХ УЧЕНЫХ факультета ВМК МГУ выпуск №8 (2011 г.), стр. 42–53. В статье рассмотрена начально-краевая задача для одного нелинейного уравнения соболевского типа. Введено понятие обобщенного решения, доказана однозначная разрешимость задачи, по крайней мере, локально по времени. Найдены достаточные условия для существования решения глобально по времени и для разрушения за конечное время. В случае разрушения решения найдены верхние и нижние оценки времени разрушения в виде явных и квадратурных формул.

Библиография 9 раб.

Е. Г. Дорогуш. МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ТРАНСПОРТНЫХ ПОТОКОВ НА КОЛЬЦЕВОЙ АВТОСТРАДЕ // СБОРНИК СТАТЕЙ МОЛОДЫХ УЧЕНЫХ факультета ВМК МГУ выпуск №8 (2011 г.), стр. 54–68. Анализируются положения равновесия динамической системы, описывающей кольцевую автомагистраль, выясняется их устойчивость. Отдельно исследуется устойчивое положение равновесия, соответствующее полностью загруженной дороге.

Библиография 7 раб.

Д. А. Кронберг. РАСШИРЕНИЕ ОБЛАСТИ СЕКРЕТНОСТИ ПРОТОКОЛА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ФАЗОВО-ВРЕМЕННЫМ КОДИРОВАНИЕМ // СБОРНИК СТАТЕЙ МОЛОДЫХ УЧЕНЫХ факультета ВМК МГУ выпуск №8 (2011 г.), стр. 69–82. Рассмотрены методы увеличения расширения области секретности протокола с фазово-временным кодированием. Эти методы сводятся к классическим действиям над передаваемой

последовательностью данных сразу после согласования базисов и оценки вероятности ошибки в «сыром» ключе. Рассмотрен метод внесения легитимными пользователями дополнительного шума и метод блочного исправления ошибок, а также сочетание этих методов.

Библиография 11 раб.

Т. С. Майская. ОЦЕНКА РАДИУСА ПОКРЫТИЯ МНОГОМЕРНОЙ ЕДИНИЧНОЙ СФЕРЫ МЕТРИЧЕСКОЙ СЕТЬЮ, ПОРОЖДЕННОЙ СФЕРИЧЕСКОЙ СИСТЕМОЙ КООРДИНАТ // СБОРНИК СТАТЕЙ МОЛОДЫХ УЧЕНЫХ факультета ВМК МГУ выпуск №8 (2011 г.), стр. 83–98. В статье даются верхняя и нижняя оценки радиуса покрытия сферы метрической сетью, порожденной сферической системой координат. Показывается, что в асимптотике при стремлении угла к нулю эти оценки совпадают. Проводится сравнение радиуса покрытия изучаемой сети с радиусом покрытия оптимальной метрической сети на единичной сфере.

Библиография 7 раб.

А. С. Мелузов. О КРИПТОАНАЛИЗЕ LILI-128, ОСНОВАННОМ НА ЧАСТИЧНОМ ОПРОБОВАНИИ И МОНОМИАЛЬНОЙ СОВМЕСТНОСТИ СИСТЕМ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ // СБОРНИК СТАТЕЙ МОЛОДЫХ УЧЕНЫХ факультета ВМК МГУ выпуск №8 (2011 г.), стр. 99–107. В работе рассматривается практическое применение алгебраического метода криптографического анализа потокового шифра LILI-128. После построения специальным образом системы булевых алгебраических уравнений, описывающих работу шифратора, проводится частичное опробование k переменных системы, что позволяет получить 2^k различных систем, только одна из которых имеет решение. Последующее исследование на мономиальную совместность полученных систем позволяет быстро отбросить те из них, которые заведомо не имеют решения. В результате метод позволяет с трудоемкостью существенно меньшей, чем при полном переборе, восстановить биты ключа, причем параметры метода могут варьироваться в зависимости от имеющегося количества исходного материала для криптоанализа (битов исходной шифрующей последовательности).

Библиография 23 раб.

А. В. Ничипорчук. МЕТОД БРОЙДЕНА ДЛЯ РЕШЕНИЯ ЗАДАЧ РАВНОВЕСНОГО ПРОГРАММИРОВАНИЯ // СБОРНИК СТАТЕЙ МОЛОДЫХ УЧЕНЫХ факультета ВМК МГУ выпуск №8 (2011 г.), стр. 108–116. Статья посвящена разработке и исследованию вопроса сходимости метода Бройдена для задач равновесного программирования. Этот метод представляет собой аналог известного квазиньютоновского метода Бройдена для решения задач оптимизации.

Библиография 4 раб.

И. А. Самыловский. ПРИМЕНЕНИЕ УСЛОВИЙ ВТОРОГО ПОРЯДКА В ИССЛЕДОВАНИИ ЛОКАЛЬНОЙ ОПТИМАЛЬНОСТИ НЕКОТОРЫХ ТРАЕКТОРИЙ В ЗАДАЧЕ РИДСА-ШЕППА // СБОРНИК СТАТЕЙ МОЛОДЫХ УЧЕНЫХ факультета ВМК МГУ выпуск №8 (2011 г.), стр. 117–122. Статья посвящена применению условий второго порядка в одной задаче оптимального управления. Проводится анализ полученных результатов.

Библиография 5 раб.

В. Г. Саргсян. МАКСИМАЛЬНАЯ МОЩНОСТЬ (k, l)-МНОЖЕСТВА, СВОБОДНОГО ОТ СУММ В ЦИКЛИЧЕСКОЙ ГРУППЕ // СБОРНИК СТАТЕЙ МОЛОДЫХ УЧЕНЫХ факультета ВМК МГУ выпуск №8 (2011 г.), стр. 123–128. В статье найдена максимальная мощность множества, свободного от сумм в циклической группе.

Библиография 10 раб.

О. А. Старунова. СОЗДАНИЕ ПРОГРАММНОЙ СРЕДЫ ДЛЯ СТАТИСТИЧЕСКОЙ ОБРАБОТКИ ДАННЫХ БИОИМПЕДАНСНЫХ ИЗМЕРЕНИЙ // СБОРНИК СТАТЕЙ МОЛОДЫХ УЧЕНЫХ факультета ВМК МГУ выпуск №8 (2011 г.), стр. 129–134. В статье содержится описание интерфейса и возможностей программы BIAStatistica для обработки данных

биоимпедансных измерений состава тела. Программа позволяет строить кривые нормальной изменчивости параметров биоимпеданса и состава тела, получать основные статистические характеристики распределений, анализировать зависимости между признаками.

Библиография 14 раб.

Д. В. Чистиков. БЕСПОВТОРНЫЕ ФУНКЦИИ НАИМЕНЬШЕЙ ТЕСТОВОЙ СЛОЖНОСТИ // СБОРНИК СТАТЕЙ МОЛОДЫХ УЧЕНЫХ факультета ВМК МГУ выпуск №8 (2011 г.), стр. 135–144. В работе описываются все бесповторные функции наименьшей тестовой сложности.

Библиография 6 раб.
