

Министерство науки и высшего образования РФ
Ярославский государственный университет им. П. Г. Демидова
Математический факультет



ПУТЬ В НАУКУ. МАТЕМАТИКА

Тезисы докладов конференции

Всероссийская молодежная конференция

11-14 мая 2022 г.

Ярославский государственный университет им. П. Г. Демидова

Ярославль
Филигрань
2022

УДК 51(063)
ББК 22.1я431
П90

*Печатается в соответствии с решением оргкомитета
Всероссийской молодежной конференции*

П 90 Путь в науку. Математика : тезисы докладов конференции : Всероссийская молодежная конференция, 11-14 мая 2022 г., Ярославль/ Яросл. гос. ун-т им. П. Г. Демидова ; под. ред. А. А. Кащенко, И. С. Кащенко; – Ярославль : Филигрань, 2022. – 64 с. – ISBN 978-5-6048593-9-1.

В сборнике представлены материалы и тезисы докладов Всероссийской молодежной конференции «Путь в науку. Математика», проходившей 11-14 мая 2022 г. в Ярославском государственном университете им. П. Г. Демидова.

УДК 51(063)
ББК 22.1я431

Организатор конференции:

Ярославский государственный университет им. П. Г. Демидова

Редакционная коллегия:

И. С. Кащенко – д-р физ.-мат. наук, доц., ЯрГУ
А. А. Кащенко – канд. физ.-мат. наук, ЯрГУ
И. Н. Маслеников – ЯрГУ

ISBN 978-5-6048593-9-1

©авторы, 2022
©ЯрГУ, 2022

Содержание

Секция чистая и прикладная алгебра	5
<i>Безуглова И. И.</i> Код Рида – Маллера	5
Секция дифференциальные уравнения	8
<i>Никитина А. А.</i> Преобразования Дарбу и отображения Янга – Бакстера	8
<i>Фролов Д. Г.</i> Устойчивость состояния равновесия у двух взаимодействующих экономик в математической модели Кейнса	11
<i>Хорошева Е. В.</i> Анализ одной из версий математической модели Кейнса	14
Секция проблемы разработки и защиты программ и данных	16
<i>Баулина А. А.</i> Десериализация. Проблемы безопасности	16
<i>Большаков Д. А.</i> Криптографически стойкие системы электронного голосования	19
<i>Иванов И. О.</i> Исследование BRCA	22
<i>Никешина А. С.</i> Изучение уязвимостей веб-приложений	25
<i>Развалов Н. А.</i> Распределение биоматериала для проведения ПЦР	28
<i>Тетерин Т. А.</i> Алгоритм геометрического упрощения картографических объектов на основе коэффициентов Фурье	30
<i>Горшков В. Г.</i> Исследование модели топологических отношений пространственных объектов	34

Секция математический анализ	39
<i>Богомолова Н. С.</i> Квадратичная интерполяция и задача о поглощении треугольником параболического сектора	39
<i>Воробьев П. А.</i> Анализ эффективности баз данных .	41
<i>Зеленова В. К.</i> Периодические решения в предельном обобщенном уравнении Мэки – Гласса с n запаздываниями	44
<i>Хохлова А. А.</i> Вычисление числовых характеристик n -мерного симплекса	46
Секция математическое моделирование	49
<i>Ежов Д. М., Храмов А. Н., Боровкова Е. И.</i> Анализ и сравнение возможных схмотехнических реализаций носимого монитора дыхания для системы с биологической обратной связью	49
<i>Костерин Д. С.</i> Ступенчатые решения квазинормальных форм одной распределенной краевой задачи	51
<i>Курбако А. В., Сказкина В. В., Боровкова Е. И.</i> Методы расчета кардиоинтервалограммы из сигнала фотоплетизмограммы для анализа синхронизации контуров вегетативного контроля	54
<i>Маслеников И. Н.</i> Исследование локальной динамики одного дифференциального уравнения второго порядка с запаздыванием в производной . . .	57
<i>Погребняк М. А.</i> Моделирование движения транспортного потока	58
<i>Семенюта Е. Ю.</i> Влияние электрических связей на экстремальные события в ансамбле двух нейронов Хиндмарш – Роуз с химическими связями	60

Секция чистая и прикладная алгебра

Код Рида – Маллера

*И. И. Безуглова (ЯрГУ им. П. Г. Демидова,
Ярославль)*

Научный руководитель: д.ф.-м.н., проф. Л. С. Казарин

Код Рида – Маллера — это линейный код над полем $GF(2)$, способный обнаруживать и исправлять ошибки. Данный код обладает простым описанием и декодированием, осуществляемым методом простого голосования. Код Рида – Маллера обозначается как $RM(r, m)$, и характеризуется несколькими параметрами: r — порядок кода, $0 \leq r \leq m$; m — некоторое число, которое задаёт длину кода; $n = 2^m$ — длина кода; $d_0 = 2^{m-r}$ — минимальная длина кода.

Задача данной работы состоит в изучении и исследовании кода Рида – Маллера.

Применение. Маринер-9

Код Рида – Маллера с параметрами: $r = 1$; $m = 5$; $n = 2^m = 32$; $k = m + 1 = 6$ — длина кодируемого сообщения; $d_0 = 2^{m-r} = 16$; применялся на спутнике «Маринер 9» (1971 год) для получения фотографий Марса. Каждая точка на фотографиях задавала один из 64 уровней градации черного цвета и кодировалась двоичным словом длины 32.

Корректирующая способность

Корректирующая способность — характеристика, которая показывает может ли код исправлять ошибки. Она описывается минимальным расстоянием Хэмминга $\rho(u, v)$ — числом несовпадающих компонент векторов.

Пусть у нас есть код с минимальным расстоянием d_0 . Мы получили закодированное сообщение. Есть два случая:

1) Переданное сообщение принадлежит коду. Мы можем сделать этот вывод, если полученное сообщение не совпадает с другими кодовыми словами, т. е. содержит не более чем $d_0 - 1$ изменений.

2) Переданное сообщение не принадлежит коду. В данном случае мы можем исправить слово, если в нём допущено меньше половины ошибок от минимальной длины: $\lfloor (d_0 - 1)/2 \rfloor$.

Таким образом при декодировании мы можем обнаружить до $2^{m-r} - 1$ ошибок и исправить $2^{m-r-1} - 1$ ошибку.

Порождающая матрица

Код Рида – Маллера определяется через порождающую матрицу $G(r, m)$. Рассмотрим построение данной матрицы:

- 1) Порождающая матрица нулевого порядка всегда задаётся одинаково: $G(0, m)$ — строка из 2^m единиц.
- 2) Для порождающей матрицы первого порядка $G(1, m)$ нужно в столбики записать двоичные представления чисел от 0 до 2^m . Длина столбика должна равняться m , поэтому, если длина двоичного числа меньше m , то мы дополняем его сверху нулями.

Ещё один вариант построения данной матрицы: в каждой i -ой строке, где $i = 1, 2, \dots, m$, чередовать по 2^{m-i} нулей и единиц.

- 3) Для построения порождающих матриц более высоких порядков $G(r, m)$ мы берем возрастающие наборы чисел длины r от 1 до m , и перемножаем поэлементно соответствующие строки из порождающей матрицы первого порядка.

- 4) Порождающая матрица кода Рида – Маллера $G(r, m)$ представляет собой записанные друг под другом порождающие матрицы наименьших порядков.

Кодирование

Для того чтобы закодировать слово, нам необходимо умножить это слово на порождающую матрицу:

$$x = y * G(r, m). \quad (1)$$

Как мы знаем, матрица G состоит из линейно независимых строк длины n , т. е. код Рида – Маллера представляет собой линейное пространство с базисом, состоящим из строк порождающей матрицы G .

Закодированное слово передаётся по каналу связи, принимается получателем и декодируется. Во время передачи возможны помехи, которые «искажают» слова. У закодированного слова длина больше, чем у исходного, т. е. оно обладает некой «избыточностью», благодаря которой с большей вероятностью удаётся обнаружить ошибки и впоследствии их исправить.

Скорость кодирования: $k*n$, т. к. при кодировании мы умножаем вектор длины k на матрицу длины $n = 2^m$.

Декодирование

Для того, чтобы декодировать полученное слово, нужно решить систему уравнений (1) относительно y .

Для удобства разобьём информацию на $r + 1$ сегмент:

$$y[N] = x[K(r)] * G[K(r), N], \quad (2)$$

где $K(r) = K(0) \cup K(1) \cup \dots \cup K(r)$ — множество индексов строк матрицы G ; $N = \{0, 1, \dots, 2^m - 1\}$ — множество индексов столбцов матрицы G .

$K(r)$ можно представить в виде $K(r) = K(r - 1) \cup K(r)$, поэтому нашу систему (2) можно переписать как:

$$y[N] = x[K(r - 1)] * G[K(r - 1), N] + x[K(r)] * G[K(r), N]. \quad (3)$$

Для того, чтобы решить данную систему, сначала нам необходимо найти вектор $x[K(r)]$. Каждую его компоненту x_i , $i \in K(r)$, можно выразить с помощью 2^{m-r} уравнений β_j , которые будут содержать по 2^r слагаемых. Если для определённой компоненты x_i , все значения β равны, то x_i будет равно этому значению. Но такая ситуация бывает не всегда, т. к. возможны ошибки. В таком случае значение x_i выбирают по принципу голосования: выбирается наиболее часто встречающееся значение из β .

Когда мы вычислили $x[K(r)]$, мы можем посчитать:

$$y^{(r-1)}[N] = y[N] + x[K(r)] * G[K(r), N],$$

где $y[N]$ — полученное слово; $G[K(r), N]$ — порождающая матрица r -того порядка. После этого можно преобразовать нашу систему (3): $y^{(r-1)}[N] = x[K(r - 1)] * G[K(r - 1), N]$. В этой системе мы определяем $x[K(r - 1)]$, и понижаем количество неизвестных и уравнений, как это было сделано ранее. И так далее, пока мы не дойдём до $x[0]$.

Скорость декодирования зависит от r . Пусть $t = 1 + C_1^m + \dots + C_m^r$. Для каждого r -го блока «голосования» у нас будет 2^{m-r} проверочных сумм по 2^r бит.

Литература

- [1] Питерсон У. У. Коды, исправляющие ошибки. М.: Мир, 1976.
- [2] Морелос-Сарагоса Р. Х. Мир связи. М.: Техносфера, 2005.

Секция дифференциальные уравнения

Преобразования Дарбу и отображения Янга – Бакстера

**А. А. Никитина (ЯрГУ им. П.Г. Демидова,
Ярославль)**

Научный руководитель: PhD С. Г. Константинову-Ризос

Уравнение Янга – Бакстера является одним из фундаментальных уравнений в математической физике. В данной работе кратко расскажем, как с помощью преобразования Дарбу построить новые решения уравнения, содержащие некоммутативные переменные.

Определим отображение Янга – Бакстера Y на некотором множестве A :

$$Y : A \times A \rightarrow A \times A, \quad (x, y) \rightarrow (u(x, y), v(x, y)). \quad (1)$$

Уравнение Янга-Бакстера : $Y^{12} \circ Y^{13} \circ Y^{23} = Y^{23} \circ Y^{13} \circ Y^{12}$, где $Y^{ij} : A \times A \times A \rightarrow A \times A \times A, i \neq j, i < j$. Элемент Y^{ij} действует на ij переменные набора (x, y, z) , как отображение (1), а на третью переменную тождественно. Например, $Y^{12}(x, y, z) = (u(x, y), v(x, y), z)$. Если присвоить переменным x, y и z параметры a, b и $c \in \mathbb{C}$, соответственно, тогда можно рассматривать параметрическое отображение Янга – Бакстера следующего вида: $Y_{ab} : (A \times \mathbb{C}) \times (A \times \mathbb{C}) \rightarrow (A \times \mathbb{C}) \times (A \times \mathbb{C})$.

Параметрическое уравнение Янга – Бакстера:

$$Y_{ab}^{12} \circ Y_{ac}^{13} \circ Y_{bc}^{23} = Y_{bc}^{23} \circ Y_{ac}^{13} \circ Y_{ab}^{12}, \quad (2)$$

Определение 1. [1] Пусть задана квадратная матрица $L = L(x; a, \lambda) = L_a(x)$, где x — переменная, a — параметр, λ — спектральный параметр. Матрица L называется матрицей Лакса для отображения $(x, y) \xrightarrow{Y_{a,b}} (u(x, y; a, b), v(x, y; a, b))$, если удовлетворяет задаче «матричной рефакторизации»:

$$L(u; a, \lambda)L(v; b, \lambda) = L(y; b, \lambda)L(x; a, \lambda). \quad (3)$$

Утверждение 1. [2,3] Если из задачи матричной трифакторизации $L(u, a)L(v, b)L(w, c) = L(x, a)L(y, b)L(z, c)$ следует, что $u = x, v = y, w = z$, то отображение $Y_{a,b}$, которое определяется уравнением (3), является отображением Янга – Бакстера.

Определение 2. Пусть $L = D_x + U(u; \lambda)$ — дифференциальный оператор, где $U(u; \lambda)$ принадлежит алгебре \mathfrak{sl}_2 . Преобразование Дарбу — это преобразование вида MLM^{-1} , которое оставляет оператор L ковариантным. Т. е. $MLM^{-1} = \tilde{L}$, где $\tilde{L} = D_x + U(\tilde{u}; \lambda)$.

Из $MLM^{-1} = \tilde{L}$ следует $ML = \tilde{L}M$, которое является задачей матричной рефакторизации, как (3). Это наводит на мысль рассматривать задачу матричной рефакторизации для конкретных матриц Дарбу M , чтобы построить отображения Янга – Бакстера. Подробнее узнать про построение отображений с коммутативными переменными с использованием преобразования Дарбу можно в [4,5]. Далее, кратко расскажем идею построения через преобразования Дарбу новых отображений, содержащих некоммутативные переменные.

Пусть \mathbb{D} — кольцо с единицей, в котором каждый ненулевой элемент обратим. Элементы \mathbb{D} будем обозначать так: $\mathbf{x}, \mathbf{y}, \mathbf{z}$. Значит, $\mathbf{x}\mathbf{y} \neq \mathbf{y}\mathbf{x}$, для любых $\mathbf{x}, \mathbf{y} \in \mathbb{D}$.

Для построения первого отображения Янга – Бакстера возьмём матрицу Дарбу для оператора NLS (связан с нелинейным уравнением Шрёдингера):

$$M(\mathbf{x}_1, \mathbf{x}_2; a) = \lambda \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a + \mathbf{x}_1\mathbf{x}_2 & \mathbf{x}_1 \\ \mathbf{x}_2 & 1 \end{pmatrix}. \quad (4)$$

Подставим эту матрицу в задачу матричной рефакторизации:

$$M(\mathbf{u}_1, \mathbf{u}_2; a) M(\mathbf{v}_1, \mathbf{v}_2; b) = M(\mathbf{y}_1, \mathbf{y}_2; b) M(\mathbf{x}_1, \mathbf{x}_2; a). \quad (5)$$

Получится система полиномиальных уравнений. Мы собираем коэффициенты разных степеней параметра λ и получаем систему полиномиальных уравнений для $\mathbf{x}_i, \mathbf{y}_i, \mathbf{v}_i$ и $\mathbf{u}_i, i = 1, 2$.

Решаем эту систему для $\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}_1, \mathbf{v}_2$. Получится решение:

$$(\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_1, \mathbf{y}_2) \xrightarrow{Y_{a,b}} \begin{pmatrix} ((b-a)\mathbf{x}_1(\mathbf{y}_2\mathbf{x}_1+1)^{-1} + \mathbf{y}_1, \\ \mathbf{y}_2, \mathbf{x}_1, (\mathbf{y}_2\mathbf{x}_1+1)^{-1}\mathbf{y}_2(a-b) + \mathbf{x}_2). \end{pmatrix} \quad (6)$$

Для построения второго отображения Янга – Бакстера возьмём матрицу Дарбу для оператора dNLS:

$$M(\mathbf{x}_1, \mathbf{x}_2; a) = \lambda^2 \begin{pmatrix} a + \mathbf{x}_1\mathbf{x}_2 & 0 \\ 0 & 0 \end{pmatrix} + \lambda \begin{pmatrix} 0 & \mathbf{x}_1 \\ \mathbf{x}_2 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad (7)$$

По аналогии с предыдущим примером, подставляем матрицу (7) в задачу матричной рефакторизации, получаем другую систему полиномиальных уравнений относительно степеней λ . Решением этой системы будет:

$$(\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_1, \mathbf{y}_2) \xrightarrow{Y_{a,b}} \begin{pmatrix} \mathbf{x}_1 + \mathbf{y}_1 - (b - \mathbf{x}_1\mathbf{y}_2)\mathbf{x}_1(a - \mathbf{y}_2\mathbf{x}_1)^{-1}, \\ \mathbf{y}_2\mathbf{x}_1[(b - \mathbf{x}_1\mathbf{y}_2)\mathbf{x}_1(a - \mathbf{y}_2\mathbf{x}_1)^{-1}]^{-1}, \\ (b - \mathbf{x}_1\mathbf{y}_2)\mathbf{x}_1(a - \mathbf{y}_2\mathbf{x}_1)^{-1}, \\ \mathbf{y}_2 + \mathbf{x}_2 - \mathbf{y}_2\mathbf{x}_1[(b - \mathbf{x}_1\mathbf{y}_2)\mathbf{x}_1(a - \mathbf{y}_2\mathbf{x}_1)^{-1}]^{-1}. \end{pmatrix} \quad (8)$$

В коммутативном случае легко проверить, является ли данное отображение отображением Янга – Бакстера, путем прямой подстановки в уравнение. Однако для некоммутативных отображений это довольно сложная задача. Поэтому для доказательства, что найденные решения (6) и (8) являются решением уравнения Янга – Бакстера, надо показать, что из задачи матричной трифакторизации следует единственное тождественное решение.

Литература

- [1] Suris Y. B., Veselov A. P. Lax matrices for Yang–Baxter maps // Journal of Nonlinear Mathematical Physics. 2003. V. 10. P. 223–230.
- [2] Veselov. A. P. Yang–Baxter maps and integrable dynamics // Physics Letters A. 2003. V. 314. P. 214–221.
- [3] Kouloukas T. E., Papageorgiou. V. G. Yang–Baxter maps with first-degree-polynomial 2×2 Lax matrices // Journal Physics A. 2009. V. 42. P. 404012.
- [4] Adler V. E., Yamilov R. I. Explicit auto-transformations of integrable

chains // Journal of Physics A. 1994. V. 27. No. 2. P. 477.

[5] Konstantinou-Rizos S., Mikhailov A. V. Darboux transformations, finite reduction groups and related Yang–Baxter maps // Journal of Physics A. 2013. V. 46. P. 425201.

Устойчивость состояния равновесия у двух взаимодействующих экономик в математической модели Кейнса

Д. Г. Фролов (ЯрГУ им. П. Г. Демидова, Ярославль)

Научный руководитель: д.ф.-м.н., доц. А. Н. Куликов

Одной из наиболее известных моделей макроэкономики, по праву, следует считать математическую модель Кейнса бизнес-цикла.

Приведем ее в наиболее простом и нормированном варианте

$$\begin{cases} \dot{x} = \frac{y}{x} - \gamma, \\ \dot{y} = \frac{y^2}{x} - xy, \end{cases} \quad (1)$$

где $x = x(t)$ — нормированная ставка кредита, $y = y(t)$ — доход в изучаемом экономическом субъекте, γ — некоторая положительная постоянная, характеризующая скорости экономических процессов (приведена уже в нормированном виде).

Система дифференциальных уравнений (1) имеет положительное состояние равновесия $S_1 : x = \gamma, y = \gamma^2$. Состояние равновесия S_1 асимптотически устойчиво, если $\gamma \in (0, 1)$ и неустойчиво, если $\gamma \in (1, \infty)$. При $\gamma = 1$ реализуется критический случай в задаче об устойчивости S_1 , когда у соответствующей матрицы Якоби есть пара чисто мнимых собственных значений $\lambda_{1,2} = \pm i$. Если $\gamma = 1 + \varepsilon, \varepsilon \in (0, \varepsilon_0)$, то из теоремы Андронова – Хопфа следует, что система (1) имеет устойчивый предельный цикл (см., например, [1]).

Целью данной работы является изучение устойчивости состояния равновесия системы дифференциальных уравнений,

которая описывает динамику двух экономик с учетом их взаимодействия (конкуренции):

$$\begin{aligned}\dot{x}_1 &= \frac{y_1}{x_1} - \gamma + d_1(x_2 - x_1), \\ \dot{y}_1 &= \frac{y_1^2}{x_1} - x_1 y_1 + d_2(y_2 - y_1), \\ \dot{x}_2 &= \frac{y_2}{x_2} - \gamma + d_1(x_1 - x_2), \\ \dot{y}_2 &= \frac{y_2^2}{x_2} - x_2 y_2 + d_2(y_1 - y_2),\end{aligned}\tag{2}$$

где $\gamma > 0$, $x_1 = x_1(t)$, $x_2 = x_2(t)$, $y_1 = y_1(t)$, $y_2 = y_2(t)$, взаимодействие экономик характеризуют коэффициенты $d_1, d_2 > 0$. Если $d_1 = d_2 = 0$, то имеем две независимые экономики.

Система дифференциальных уравнений (2) имеет положительное состояние равновесия $S_2 : x_1 = \gamma, y_1 = \gamma^2, x_2 = \gamma, y_2 = \gamma^2$. Если $d_1 = d_2 = 0$, то S_2 асимптотически устойчиво при $\gamma \in (0, 1)$ и неустойчиво при $\gamma \in (1, \infty)$.

Ситуация меняется, если $d_1^2 + d_2^2 \neq 0$.

Теорема 1. Если $\gamma \in (1, \infty)$, то S_2 — неустойчивое состояние равновесия системы дифференциальных уравнений (2) при любых d_1, d_2 ($d_1, d_2 \geq 0$).

Для удобства произведем замену $d_1 = \frac{d}{2}, d_2 = \gamma q \frac{d}{2}$, вспомогательный параметр $q = \frac{d_2}{\gamma d_1}$.

Теорема 2. 1. Если $\gamma \in (0, 1), q \in (q_*, \infty)$, где $q_* = 3 - 2\sqrt{2}$, то S_2 асимптотически устойчиво.

2. Если $\gamma \in (0, 1), q \in (0, q_*)$, то S_2 неустойчиво, если $d \in (d_*, d_{**})$, где $d_* = \frac{1-q-\sqrt{q^2-6q+1}}{2q}, d_{**} = \frac{1-q+\sqrt{q^2-6q+1}}{2q}$ и остается устойчивым, если $d \in (0, d_*) \cup (d_{**}, \infty)$.

Пусть $d = d_*$ или $d = d_{**}$, тогда реализуется критический случай в задаче об устойчивости S_2 , когда три собственных значения матрицы Якоби, вычисленной в точке $S_2(\gamma, \gamma^2, \gamma, \gamma^2)$ лежат в левой полуплоскости комплексной плоскости, а одно из собственных чисел этой матрицы равно 0.

Доказательство теорем 1, 2 основано на использовании известной теоремы А. М. Ляпунова об устойчивости по первому (линейному) приближению [2]. Это приводит к необходимости анализа спектра матрицы

$$\begin{pmatrix} -1 - d_1 & \frac{1}{\gamma} & d_1 & 0 \\ -2\gamma^2 & \gamma - d_2 & 0 & d_2 \\ d_1 & 0 & -1 - d_1 & \frac{1}{\gamma} \\ 0 & d_2 & -2\gamma^2 & \gamma - d_2 \end{pmatrix}.$$

При $d = d_* + \gamma\varepsilon$ или $d = d_{**} + \gamma\varepsilon$, где $\varepsilon \in (0, \varepsilon_0)$, т. е. ε — малый неотрицательный параметр, можно доказать следующее утверждение.

Теорема 3. *Существует $\varepsilon_0 > 0$ такое, что при $\varepsilon \in (0, \varepsilon_0)$ система дифференциальных уравнений (2) имеет два состояния равновесия S_3 и S_4 отличные от S_2 .*

При этом $S_3(\varepsilon) = S_3(\eta_1, \eta_2, \eta_3, \eta_4)$, $S_4(\varepsilon) = S_4(\eta_3, \eta_4, \eta_1, \eta_2)$, где $\eta_1 \neq \eta_3, \eta_2 \neq \eta_4$. Доказательство использует такие методы теории динамических систем как метод интегральных многообразий, метод нормальных форм Пуанкаре – Дюлака. Эти методы позволяют в условиях теоремы 3 свести вопрос о существовании состояния равновесия S_3 (S_4) к анализу скалярного уравнения

$$z' = \beta z + lz^3,$$

где $z = z(s)$, $s = \varepsilon t$ — медленное время, $\beta, l \in R$ и определяются в ходе реализации алгоритма построения нормальной формы.

Последнее уравнение имеет:

- а) состояние равновесия $z = z_0 = 0$;
- б) два ненулевых состояния равновесия $z_{1,2} = \pm \sqrt{-\frac{\beta}{l}}, \frac{\beta}{l} < 0$.

Анализ системы (2) показал, что наличие взаимодействия (конкуренции) может привести к потере устойчивости состояния экономического равновесия S_2 при меньших значениях основного параметра γ . В некоторых случаях это приводит к появлению иных состояний равновесия. Для них характерна «неоднородность», когда показатели первой экономики отличаются от показателей второй экономики. Например, одна из них становится эффективней другой.

Литература

[1] Куликов А. Н., Куликов Д. А., Фролов Д. Г. Модель Кейнса делового цикла и задача о диффузной неустойчивости // Итоги науки и техники. Современная математика и ее приложения. (принято к

печати).

[2] Демидович Б. П. Лекции по математической теории устойчивости. М.: Наука, 1967.

Анализ одной из версий математической модели Кейнса

**Е. В. Хорошева (ЯрГУ им. П. Г. Демидова,
Ярославль)**

Научный руководитель: к.ф.-м.н., доц. Д. А. Куликов

Рассматривается система из двух дифференциальных уравнений

$$\begin{aligned}\dot{x} &= \frac{y^2}{x_3} - \gamma, \\ \dot{y} &= \frac{y}{x} - xy,\end{aligned}\tag{1}$$

где γ — положительная постоянная, $x = x(t)$ — нормированная процентная ставка кредита, $y = y(t)$ — нормированный доход экономического субъекта. Например, региона, национальной экономики. Математическая модель (1) — это один из возможных вариантов математической модели Кейнса (см., например, монографии [1,2], а также статью [3]).

Система дифференциальных уравнений (1) имеет состояние равновесия

$$S: x = \gamma, y = \gamma\tag{2}$$

с положительными координатами.

Состояние равновесия S в макроэкономике принято называть «состоянием экономического равновесия». Оно асимптотически устойчиво, если $\gamma \in (0, \frac{1}{2})$ и неустойчиво, если $\gamma \in (\frac{1}{2}, \infty)$. При $\gamma = \frac{1}{2}$ реализуется критический случай пары чисто мнимых собственных значений спектра устойчивости.

В докладе речь идет о том, что при $\gamma = \frac{1}{2}(1 + \varepsilon)$, $\varepsilon \in (0, \varepsilon_0)$, $0 < \varepsilon_0 \ll 1$ система (1) имеет орбитально асимптотически устойчивый цикл Андронова – Хопфа.

Обоснование применимости известной теоремы Андронова – Хопфа основано на использовании метода нормальных форм Пуанкаре – Дюлака. Для построения нормальной формы использована одна из версий алгоритма Крылова – Боголюбова.

Реализация такого подхода позволила ответить на весь комплекс вопросов, возникающий при анализе бифуркационной задачи. В частности, для периодических решений, формирующих цикл, получены асимптотические формулы

$$\begin{aligned}x &= \frac{1}{2}(1 + \varepsilon) \left(1 + 2\varepsilon^{\frac{1}{2}} \cos \left((1 + o(\varepsilon))t + \varphi_0 - \frac{\pi}{4} \right) + o(\varepsilon) \right), \\y &= \frac{1}{2}(1 + \varepsilon) \left(1 + \sqrt{2}\varepsilon^{\frac{1}{2}} \cos((1 + o(\varepsilon))t + \varphi_0) + \right. \\&\quad \left. + \frac{1}{2}\varepsilon (\cos(2(1 + o(\varepsilon))t + 2\varphi_0) - 1) + o(\varepsilon) \right),\end{aligned}\tag{3}$$

где φ_0 — произвольная действительная постоянная. Решение (3) орбитально асимптотически устойчиво.

Итак, анализ системы дифференциальных уравнений (1) показал, что при потере устойчивости состояния равновесия S появляется экономический цикл, характерный для рыночной (капиталистической) экономики.

Литература

- [1] Кейнс Д. М. Общая теория занятости, процента и денег. М.: Юрайт, 2019.
- [2] Занг В. Б. Синергетическая экономика. М.: Мир, 1999.
- [3] Torre V. Existence of limit cycles and control in complete Keynesian systems by theory of bifurcations // *Econometrica*. 1977. V. 45. No. 6. P. 1457–1466.

Секция проблемы разработки и защиты программ и данных

Десериализация. Проблемы безопасности

**А. А. Баулина (ЯрГУ им. П. Г. Демидова,
Ярославль)**

Научный руководитель: к.ф.-м.н. Д. М. Мурин

Сериализация — это процесс преобразования объекта в поток байтов для сохранения или передачи в память, базу данных или файл. Она используется для сохранения состояния объекта, для организации распределенной обработки данных, где объекты передаются из одной виртуальной машины на другую; для реализации восстановления после отказа и выравнивания нагрузки серверов.

К сожалению, нельзя слепо полагаться на механизмы сериализации, которые есть во всех распространенных языках программирования. По данным Национальной базы данных уязвимостей США с начала 2022 года было зарегистрировано уже 25 уязвимостей, возникших в процессе десериализации в различных программных продуктах. В том числе, например, уязвимость в Cisco Webex Meetings, позволяющая злоумышленнику внедрить вредоносный код в приложение [1]. Отсюда целью работы является исследование возможных уязвимостей десериализации в языке Java и разработка способов их решения.

В работе приводятся описания возможных атак на процесс десериализации, часть из них была реализована. Приведем пример некоторых из них.

Приложение, использующее сериализацию Java особенно уязвимо в том случае, если сериализованные объекты передаются по сети. Весь трафик между приложением и сервером основан на передаче сериализованных объектов. Это дает ложное чувство безопасности — весь трафик это неудобочитаемые потоки байтов, сразу не видно, какие данные передаются. На самом деле этот код подвержен атаке по внедрению в имя файла. Т. е. хакер может загрузить любой файл системы. Эта уязвимость существует, потому что при десериализации объекта отсутствует какая-либо валидация. JVM никак не может проверить, что

объект имеет такое же внутреннее состояние, как и в момент сериализации. Вся информация доступная в момент десериализации — это только информация, содержащаяся в потоке. Если изменить содержимое в потоке, то Java слепо доверится ей в процессе десериализации.

Для обхода защитных механизмов, применяемых в процессе сериализации, может быть использовано отложенное выполнение — исполнение кода в момент зачистки объекта. С этой целью используется метод `Object.finalize()`. Вредоносный код, расположенный в одноименных функциях объектов, исполняется сборщиком мусора, когда объект уже больше не используется. Отложенное выполнение основывается на инициализации объекта в процессе десериализации. Даже если в процессе приведения типов будет сгенерировано `ClassCastException`, будет уже поздно. Объект станет целью сборщика мусора, а тот, в процессе «зачистки», вызовет метод `finalize()`, таким образом исполняя вредоносный код.

Для защиты приложения от атак, были изучены существующие рекомендации [2-5] и проведен их анализ. В работе приводится перечень решений, которые должны уменьшить уязвимость программного обеспечения (ПО), и на их основе был разработан собственный метод защиты.

Предлагается десериализовать данные исключительно из доверенных источников, проверяя их целостность. Отсюда реализуем элемент модели безопасности с нулевым доверием. Будем подписывать сериализованные объекты с помощью хеш-функции, проводя таким образом аутентификацию отправителя. Полученный поток байтов может быть проверен получателем перед началом процесса десериализации, чтобы максимально обезопасить код ПО. Таким образом, при проверке хеша можно сказать, был ли изменен изначальный объект. Кроме того, будем использовать шифрование для защиты конфиденциальности.

Из приведенных рассуждений следует логичный вопрос: что делать сначала — подписывать или шифровать? Предположим, сначала мы зашифровали объект, а потом подписали, поместив в `SignedObject`. В таком случае злоумышленник, перехватив `SignedObject`, может извлечь оттуда подпись, заменив на её свою собственную — это пример атаки посредника. Да, зло-

умышленник не сможет прочесть содержимое, но и получатель тоже (расшифровать сообщение можно только после проверки подписи). Адресат не может с уверенностью утверждать, что полученный объект был подписан именно отправителем.

Именно поэтому предлагается использовать следующий алгоритм:

- подписать пересылаемый объект с помощью алгоритма SHA3-512withDSA, поместив его в SignedObject;
- зашифровать SignedObject по ГОСТ 34.12-2018, используя симметричный алгоритм блочного шифрования «Кузнечик» [6].

Для успешной реализации предложенного алгоритма необходимо решить проблему распределения ключей. Будем использовать протокол HTTPS, в котором данные передаются поверх криптографического протокола TLS, основанного на использовании цифровых сертификатов [7].

Для настройки TLS понадобятся OpenSSL и консольная утилита keytool (входит в поставку JDK). С их помощью можно создать самоподписанный сертификат, keystore (хранилище ключей) и truststore (хранилище доверенных сертификатов), чтобы впоследствии использовать их в серверной и клиентской части приложения.

Тестирование проводилось с помощью Postman — инструмента для тестирования API, позволяющего в том числе составлять и отправлять HTTP-запросы и работать с ответами на них. Было проверено, что при отправке HTTP-запроса без сертификата, не удастся даже пройти этап маршрутизации в серверной части приложения. При добавлении корректного сертификата клиента к запросу приложение работает, как и задумывалось.

Литература

- [1] NIST [Электронный ресурс]. – <https://nvd.nist.gov/vuln/search/>.
- [2] Secure Coding Guidelines for Java SE [Электронный ресурс]. – <https://www.oracle.com/java/technologies/javase/seccodeguide.html>.
- [3] Serialization in Java: Examples and Prevention / Sudip Sengupta [Электронный ресурс]. – <https://crashtest-security.com/java-serialization>.
- [4] Java Object Serialization / Ted Neward [Электронный ресурс]. – <https://developer.ibm.com/articles/j-5things1/>.

[5] How to protect your Apps from the Java Serialization Vulnerability [Электронный ресурс]. – <https://www.contrastsecurity.com/security-influencers/protect-your-apps-from-java-serialization-vulnerability>.

[6] ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. Организация и проведение работ по международной стандартизации в Российской Федерации: межгосударственный стандарт : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 4 декабря 2018 г. N 1061-ст. – Москва : Стандартинформ, 2018.

[7] Transport Layer Security [Электронный ресурс]. – https://en.wikipedia.org/wiki/Transport_Layer_Security.

Криптографически стойкие системы электронного голосования

***Д. А. Большаков (ЯрГУ им. П. Г. Демидова,
Ярославль)***

Научный руководитель: д.ф.-м.н., проф. В. Г. Дурнев

Дистанционное электронное голосование (ДЭГ) в России проводится в экспериментальном формате с 2020 года. На выборах 19 сентября 2021 года в семи субъектах РФ (в том числе и в Ярославской области) у избирателей была возможность проголосовать дистанционно. В марте 2022 года в ФЗ «Об основных гарантиях избирательных прав и права на участие в референдумах граждан Российской Федерации» [1] была добавлена статья 64.1, описывающая порядок проведения ДЭГ, следовательно такой способ голосования останется актуальным.

Поскольку всеобщее избирательное право является основой демократического государства, поэтому вопрос безопасности в программно-техническом комплексе (ПТК) ДЭГ является вопросом государственной важности.

Целью работы является изучение устройства федерального ПТК ДЭГ, используемого на выборах 19 сентября 2021 года и оценка безопасности её использования. Рассмотрим основные этапы дистанционного электронного голосования [2]:

1. Пользователь портала ДЭГ проходит процедуру аутентификации и идентификации с использованием ЕСИА, получает

токен идентификации ЕСИА, по которому проверяется наличие в списке участников ДЭГ и получение персональных данных.

2. Участник голосования генерирует ключевую пару электронной подписи, далее формируется подпись вслепую для ключа проверки ЭП, происходит получение идентификатора текущего голосования и открытого ключа шифрования бюллетеней.

3. Факт выдачи подписи фиксируется в списке участников ДЭГ, сохраняется значение маскированной подписи вслепую.

4. Происходит переход в анонимную зону с сохранением ключевой пары ЭП, слепой подписи и с помощью анкор-ссылки.

5. Участник ДЭГ получает бюллетень, заполняет его, шифрует ключом зашифрования бюллетеней, формирует доказательство корректности содержимого с нулевым разглашением.

6. Участник ДЭГ формирует транзакцию, состоящую из зашифрованного бюллетеня, доказательства корректности, ключа проверки ЭП участника, значения слепой подписи. Транзакция подписывается ключом участника и отправляется в избирательный ящик.

В общей сложности на всех этапах ДЭГ используются следующие криптографические алгоритмы [3]:

- электронная подпись по ГОСТ Р 34.10-2012;
- слепая подпись на основе RSA;
- хеш-функция «Стрибог» по ГОСТ Р 34.11-2018;
- схема шифрования Эль-Гамала на эллиптических кривых;
- доказательство корректности по схеме Chaum-Pedersen ZKP;
- протокол разделения закрытого ключа по схеме Шамира.

Из плюсов выделим криптографическую надёжность [4], доказуемое исключение связи голоса с его владельцем, но при этом возможность проверки наличия своего голоса в блокчейне.

Первый минус — клиент-серверная структура системы, обеспечивающая распределённость и защищённость серверов, но при этом не гарантирующая защищённость пользовательских устройств [5]. Для персональных компьютеров актуальна опасность перехвата управления или изменения текста бюллетеня в анонимной зоне (*УБИ.130* и *УБИ.127*, помеченные в «Модели угроз и нарушителя безопасности информации» как «Актуальные и Высоковероятные»)[6]. Для мобильных устройств суще-

ствует опасность перехвата паролей двухэтапной аутентификации и скрытого участия в ботнете (*УБИ.168 и УБИ.171*)[6].

Второй блок проблем связан с доверием к ПТК. В электронном варианте голосования отсутствует возможность убедиться в том, что человек вошёл в систему под своими персональными данными, поэтому существует опасность регистрации фиктивных избирателей. Следующая проблема — у участников голосования нет возможности убедиться, что ПТК реализует протокол в полной мере без отступлений, не имеет программных «закладок» и бэкдоров. Более того, сам блокчейн не гарантирует отсутствия перезаписи, поскольку он строится на централизованной основе и круг серверов строго определён компанией-разработчиком Ростелеком.

Третий блок проблем связан с пониманием избирателями электронной системы. Протокол ДЭГ полон абстрактных математических понятий, требующих знаний в области криптографии для их понимания. «Вера на слово» в случае, когда речь идёт о конституционном праве гражданина на голос однозначно недопустима.

Дистанционные выборы в Эстонии проводятся с 2005 года. В эстонском варианте ДЭГ аутентификация происходит с помощью физических ID-карт или SIM-карт, а сама система имеет развитую систему общественного контроля, но при этом не имеет технической гарантии анонимности, поскольку отсутствует механизм выдачи подписи вслепую. При всём этом, граждане Эстонии доверяют ДЭГ, на что указывает высокий процент его участников – 30-40% от всех голосующих [7].

Подводя итоги, в ходе нашей работы было проанализировано устройство федеральной системы ДЭГ, а также изучена модель угроз и нарушителя безопасности информации ПТК ДЭГ, выявлены как плюсы, так и минусы её массового использования. Реализация избирательного права требует полного обеспечения безопасности волеизъявления, что затруднительно в текущей реализации ДЭГ со всеми её недостатками. Следовательно, система нуждается в технической и смысловой доработке.

Литература

- [1] Об основных гарантиях избирательных прав и права на участие

в референдумах граждан Российской Федерации: Федеральный закон от 12.05.2002 №63-ФЗ// Собрание законодательства. – 2002.

[2] Описание протокола ДЭГ к выборам, голосование на которых состоится 17, 18 и 19 сентября 2021 г. – М.: ЦИК РФ, 2021. – 13 с.

[3] Алферов, А. П., Зубов А. Ю. Основы криптографии. М.: Гелиос, 2005.

[4] Обзор криптографического протокола системы дистанционного электронного голосования [Электронный ресурс]. – <https://habr.com/ru/users/RTteam/posts/page2/>.

[5] «Какая проблема перерисовать данные?» Что случилось с электронным голосованием в Москве [Электронный ресурс]. – <https://www.bbc.com/russian/features-58631126>.

[6] Модель угроз и нарушителя безопасности информации, обрабатываемой в программно-техническом комплексе дистанционного электронного голосования. Выписка. – Москва: ЦИК РФ, 2021. – 44 с.

[7] Россия vs Эстония: сравнение электронных голосований [Электронный ресурс]. – <https://evoting.digitaldem.ru/2021/08/18/evoting-estonia-vs-russia/>.

Исследование BRCA

И. О. Иванов (ЯрГУ им. П. Г. Демидова, Ярославль)

Научный руководитель: к.ф.-м.н., доц. О. П. Якимова

Рак молочной железы (РМЖ) является наиболее распространенным видом рака у женщин во всем мире, а семейный анамнез (сведения об истории болезни, условиях жизни больного, перенесённых им заболеваниях и т. п.) РМЖ является одним из наиболее важных факторов риска заболевания. Около 15–20 % семейного риска РМЖ можно объяснить редкими мутациями в генах BRCA1 или BRCA2. В исследовании 2017 года [1] авторы оценили кумулятивный риск развития рака молочной железы к 80 годам как 72 % для носителей мутации BRCA1 и 69 % для носителей мутаций BRCA2.

Все осложняется тем, что мутации имеют аутосомно-доминантный тип наследования (50 % вероятность передать мутантный ген от родителя вне зависимости от пола) и, т. к. чаще

всего РМЖ развивается уже после рождения детей, мутации в генах BRCA1 и BRCA2 широко представлены в популяции.

Современные методы анализа ДНК, основанные на NGS (next generation sequencing), позволяют с высокой долей вероятности определить носительство тех ли иных мутации у человека. Знание о возможных носительствах позволяют определить, находится ли человек в группе риска. Такие люди получают определенные рекомендации для профилактики возможного заболевания и находятся под наблюдением специалиста.

Целью данной работы является разработка пайплайна обработки данных таргетного секвенирования генов BRCA1 и BRCA2. Результатом работы программы являются данные, содержащие аннотированные варианты, пригодные для интерпретации соответствующими специалистами в лице биоинформатика и врача-генетика.

Весь пайплайн можно разделить на этапы, включающие в себя предобработку сырых данных (обрезка праймеров, выравнивание прочтений, сортировка, удаление ПЦР дубликатов), коллинг вариантов, очистка мусора, и аннотирование вариантов.

После секвенирования в прочтениях остаются специальные праймеры — короткие фрагменты нуклеиновой кислоты, комплементарные ДНК мишени; служат затравкой для синтеза комплементарной цепи с помощью ДНК-полимеразы. Праймеры увеличивают шанс коллинга ложноотрицательных вариантов на концах ампликонов, поэтому хорошей практикой является удаление праймеров после секвенирования. Для обрезки праймеров был реализован свой алгоритм, показывающий хорошую чувствительность (>80 % обрезанных праймеров) и приемлемую скорость работы (150 000 прочтений – 30 с) при допустимом количестве ошибок в 5 %. Однако при увеличении до 15 % скорость падает до 3 мин. Поэтому в качестве альтернативы было принято решение использовать pTrimmer, опубликованный на ресурсе BMC Bioinformatics в 2019 году [2]. Он демонстрирует отличную чувствительность (>89 %) и превосходную скорость работы (11 млн прочтений – 35 секунд) [2].

После обрезки праймеров начинается стандартный этап предобработки данных, включающий в себя выравнивание про-

чтений на референсный геном, сортировку, маркировку ПЦР дубликатов и перекалибровку base quality score. Данная последовательность действий рекомендована GATK [3], создателями haplotypeCaller, который используется в качестве основного коллера вариантов.

После обработки данных следует этап коллинга вариантов – процесс определения отличий в последовательности образца от референсного генома человека. В качестве основного коллера используется HaplotypeCaller, а также дополнительный коллер, поставляемый в пакете инструментов BCFTools. Дополнительный коллер нужен в связи с тем, что HaplotypeCaller имеет плохую чувствительность на концах ампликонов (наблюдение специалистов).

После коллинга вариантов нужно отфильтровать ложные варианты. Для этого были подобраны жесткие фильтры, основанные на статистических данных. Фильтрация происходит по таким полям как ReadPosRankSum, MappingQualityRankSum, MappingQuality, StrandOddsRatio, FisherStrand [4]. Помимо жестких фильтров используется инструмент CNNScoreVariants. Он основан на сверточной нейросети, натренированной на результатах анализа одиночных образцов. Результатом работы является пометка, показывающая прошел ли вариант фильтрацию или должен быть отброшен.

Аннотация полученных вариантов происходит после получения результатов коллинга. Для этого используется специальный инструмент VEP. Среди возможностей можно выделить указание генов и транскриптов, затронутых вариантами, определение расположения вариантов (выше транскрипта, в кодирующей последовательности, в некодирующей РНК, в регуляторных областях), интеграция с базой 1000 Genome Project, а также использование программ предсказателей, предсказывающих возможную патогенность варианта.

Финальным шагом является выставление баллов вариантам, основываясь на разработанной скоринговой модели и фильтрация тех, которые не набрали соответствующего количества баллов. Количество баллов основывается на пометке, полученной после CNNScoreVariants, частоте альтернативного аллеля, а также факте того, является ли вариант инделом (вставкой или делецией). Помимо этого, учитывается то, встречается ли

вариант в специализированных базах (Bic, exLOVD, Enigma), содержащих данных о мутациях в генах BRCA1 и BRCA2, или нет.

Литература

- [1] Risks of Breast, Ovarian, and Contralateral Breast Cancer for BRCA1 and BRCA2 Mutation Carriers [Электронный ресурс]. – <https://pubmed.ncbi.nlm.nih.gov/28632866/>.
- [2] pTrimmer: An efficient tool to trim primers of multiplex deep sequencing data [Электронный ресурс]. – <https://bmcbioinformatics.biomedcentral.com/articles/10.1186/s12859-019-2854-x>.
- [3] Germline short variant discovery [Электронный ресурс]. – <https://gatk.broadinstitute.org/hc/en-us/articles/360035535932-Germline-short-variant-discovery-SNPs-Indels>.
- [4] Hardfiltering germline short variants [Электронный ресурс]. – <https://sites.google.com/a/broadinstitute.org/legacy-gatk-forum-discussions/methods-and-algorithms/11069-Hardfiltering-germline-short-variants>.

Изучение уязвимостей веб-приложений

**А. С. Никешина (ЯрГУ им. П. Г. Демидова,
Ярославль)**

Научный руководитель: к.ф.-м.н., доц. О. П. Якимова

Под безопасностью веб-приложений понимают защитные меры, при которых злоумышленник не сможет нарушить его работоспособность и не сможет получить доступ к конфиденциальным данным как извне при попытке взлома, так и изнутри через нелегитимный доступ.

Согласно исследованиям компании Positive Technologies в 2021 году веб-ресурсы компаний становились объектами атак в 17 % случаев от общего числа атак. Доля хакинга и эксплуатации веб-уязвимостей суммарно составила 43 % среди всех использованных методов в атаках на организации [1].

Основная проблема, с которой сталкиваются сотрудники подразделений информационной безопасности — приоритизация уязвимостей для устранения. Объективной и наиболее популярной классификацией уязвимостей считается OWASP Top 10.

OWASP (Open Web Application Security Project) — международная некоммерческая организация, сосредоточенная на анализе и улучшении безопасности программного обеспечения. OWASP Top 10 — это отчет, в котором перечислены основные проблемы, связанные с безопасностью веб-приложений. Рейтинг составляется на основе консенсуса мнений экспертов по безопасности со всего мира.

Рассмотрим актуальные уязвимости, которые были включены в последний релиз OWASP Top 10, выпущенный в 2021 году [2].

1. Нарушение контроля доступа. Как правило, к данной категории относятся сбои в предоставленных разрешениях или неправильно настроены или отсутствуют ограничения для аутентифицированных пользователей. То есть ситуации, когда пользователь может выполнить действие, на которое у него не должно быть прав.

2. Сбои в криптографии. Иными словами, это проблемы с шифрованием чувствительных данных или его полное отсутствие. Сюда относятся следующие проблемы: передача чувствительных данных в открытом виде, использование устаревших или слабых алгоритмов шифрования, хэширования и др.

3. Внедрение кода. Атаки данной категории позволяют злоумышленнику внедрить исполняемый код, который в дальнейшем будет выполнен на веб-сервере, а также внедрить произвольный SQL-код. Чтобы защититься от данной атаки, следует фильтровать и экранировать пользовательский ввод, использовать параметризованные запросы к базе данных.

4. небезопасная архитектура. Это широкая категория, представляющая различные недостатки, выраженные как «отсутствующий или неэффективный дизайн управления». Плохо продуманная структура проектируемого приложения влечет за собой неспособность определить требуемый уровень безопасности.

5. Неправильная конфигурация. Данная уязвимость относится к неправильной реализации безопасности, предназначенной для защиты данных приложения. Можно сказать, что это ошибки настроек безопасности.

6. Уязвимые и устаревшие компоненты. Данная уязвимость актуальна для приложений, в которых используется устарев-

шее ПО, а также сторонние библиотеки, компоненты или фреймворки с открытым исходным кодом. Злоумышленники уделяют им должное внимание, постоянно анализируют код и ищут «слабые места».

7. Ошибки идентификации и аутентификации. Такие недостатки, как возможность автоматизированного подбора пароля, отсутствие многофакторной аутентификации, слабые требования к паролю, позволяют злоумышленникам заполучить пароли, ключи или сессионные токены, а также эксплуатировать другие ошибки реализации для временного или постоянного перехвата учетных записей пользователей.

8. Нарушение целостности данных и программного обеспечения. К этой категории относятся атаки, нацеленные на критические данные и конвейеры CI/CD. Одной из частых причин, приводящих к возникновению этих уязвимостей, являются автоматические обновления компонентов приложения, которые могут выполняться без проверки достоверности источников, а также небезопасная десериализация.

9. Журнал безопасности и сбой мониторинга. Недостаточное ведение журнала и отсутствие эффективной системы мониторинга приводят к увеличению периода времени от возникновения атаки до ее обнаружения. Важно регистрировать и отслеживать поведение веб-приложения, чтобы своевременно распознать подозрительную активность и предотвратить атаку.

10. Подделка запросов со стороны сервера. Данная атака возможна в случае наличия уязвимости ПО, позволяющей злоумышленнику спровоцировать сервер отправить запрос на произвольный адрес. Если в приложении можно отправлять HTTP запросы, не проверяя URL, то это позволяет делать запросы в локальную сеть сервера, а также сканировать порты на сервере и соседних серверах во внутренней сети.

Большая часть изученных эксплойтов связана с чрезмерным доверием к пользовательскому вводу, поэтому все пользовательские данные должны быть очищены перед отображением или использованием в SQL-запросах и вызовах файловой системы.

Беспокоиться о безопасности веб-приложения необходимо начинать еще на этапе развития идеи. Анализируя возможные

угрозы, связанные с той или иной функциональностью, разрабатывать приложения, руководствуясь лучшими практиками по безопасному кодированию.

Литература

- [1] Positive technologies [Электронный ресурс]. – <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/>.
- [2] OWASP [Электронный ресурс]. – <https://owasp.org/Top10/>.

Распределение биоматериала для проведения ПЦР

**Н. А. Развалов (ЯрГУ им. П. Г. Демидова,
Ярославль)**

Научный руководитель: к.ф.-м.н., доц. О. П. Якимова

Одним из значимых достижений медицины является ПЦР. ПЦР — это реакция, которая позволяет понять содержится ли определенный участок ДНК в исследуемом образце. ПЦР используется во многих областях, таких как: криминалистика, медицинская диагностика заболеваний, клонирование генов.

Для успешного протекания реакции необходимо правильно распределять биоматериал. Этот процесс совершается вручную, поэтому было принято решение его автоматизировать.

ДНК — это двуцепочечная молекула, где каждая цепочка состоит из звеньев-нуклеотидов: аденин, тимин, цитозин и гуанин, обозначаемые А, Т, С и G соответственно. Цепи нуклеотидов расположены в молекуле ДНК антипараллельно. Принцип комплементарности — это когда нуклеотиды образуют водородные связи строго по определённом правилу: «А» соединяется только с «Т», а «G» — с «С». Такие связи сцепляют между собой две цепочки нуклеотидов. Имея одну цепь ДНК, в соответствии с принципом комплементарности, легко построить ее пару. На этом принципе основана ПЦР. Праймер — это искусственно синтезированная короткая цепочка нуклеотидов, необходимая для протекания реакции [1].

В ходе ПЦР некоторые праймеры могут соединяться между собой, тем самым образуя побочный продукт. Такие реакции стоит избегать, для этого праймеры, которые могут взаимодействовать между собой нужно поместить в разные пробирки.

Представим граф, вершинами данного графа будут являться праймеры, а ребра показывают какие праймеры между собой дают побочный продукт. Для решения поставленной задачи необходимо вершины графа распределить на группы таким образом, чтобы вершины, между которыми есть ребра, оказались в разных группах. Как показывает практика достаточно всего двух групп. По этой причине потребуется алгоритм, в котором будет произведена проверка на двудольность графа при помощи быстрых алгоритмов СНМ (системы не пересекающихся множеств). После работы данного алгоритма, мы получаем доли (группы).

Для определения двудольности графа произведём серию поисков в ширину. Иными словами, будем запускать алгоритм поиска в ширину из каждой непосещённой вершины. Вершину, из которой мы начинаем идти, мы помещаем в первую долю. В процессе поиска в ширину, если мы идём в какую-либо новую вершину, то мы помещаем данную вершину в долю, отличную от доли текущей вершины. В противном случае, если мы проходим по ребру в вершину, которая уже посещена, мы проверяем, чтобы данная вершина и текущая вершина находились в разных долях. Получая ответ, убеждаемся, что исходный граф является двудольным, в следствие чего найдем разбиение вершин графа на две доли. Иначе, при отрицательном ответе, рассмотрим следующее решение данной задачи.

В случае, когда граф оказался не двудольным, предлагаете раскрашивать вершины по следующему правилу. Вершины, между которыми есть ребро должны быть раскрашены разными цветами, количество цветов должно быть минимальным. Вершины, имеющие одинаковый цвет, не будут иметь между собой ребер, следовательно могут быть помещены в одну группу. Таким образом мы решили нашу задачу.

Алгоритм раскраски выдает минимальное количество цветов, когда совершит полный перебор всех вершин, что в следствии затрачивает достаточно продолжительное время. Алгоритм, разбивающий граф на две доли, выдает результат за

один проход графа и затрачивает на эту операцию меньшее количество времени, по сравнению с алгоритмом раскраски. Что дает достаточное преимущество алгоритму проверки графа на двудольность, и отвечает на вопрос, зачем мы рассматриваем два алгоритма.

Литература

1. Полимеразная цепная реакция [Электронный ресурс]. – https://ru.wikipedia.org/wiki/Полимеразная_цепная_реакция.

Алгоритм геометрического упрощения картографических объектов на основе коэффициентов Фурье

**Т. А. Тетерин (ЯрГУ им. П. Г. Демидова,
Ярославль)**

Научный руководитель: к.ф.-м.н., доц. О. П. Якимова

За счёт бурного развития техники и появления вычислительных машин, возникает возможность автоматизировать процесс составления карт разных масштабов, опираясь на одну подробную карту большого масштаба. Благодаря этому появляется отдельная наука — геоинформатика, занимающаяся вопросами научного обоснования, проектирования, формирования, эксплуатации и применения географических информационных систем и так же рассматривающая задачу генерализации карт.

Картографическая генерализация — это процесс контроля количества подробной информации (картографических полигональных объектов), отображаемой на карте. Иными словами, если на картах малого масштаба отображались бы все объекты, которые только возможны, то это вызывало бы проблемы анализа карт, их обработки и хранения. Поэтому суть процесса генерализации при уменьшении масштаба карты заключается в уменьшении визуальной детализации данных этой карты за счёт обобщения и упрощения её объектов.

Под картографическим объектом будем понимать некоторую последовательность точек, которая формирует один опре-

деленный объект на карте (река, озеро, дорога, граница региона и др.). Отсюда процесс упрощения заключается в уменьшении количества его точек путём удаления некоторых из них или путём построения новой последовательности точек.

На данный момент существует достаточно много различных алгоритмов картографической генерализации. В апреле 2020 года учеными из Китая был предложен алгоритм упрощения данных, основывающийся на идее представления исходной полилинии в виде ряда Фурье [1]. Целью этой работы является изучение предложенного алгоритма и проведение сравнительного анализа его работы.

Если в геоинформатике объект задается последовательностью точек, то в математике его можно рассматривать как кусочно-заданную функцию. В нашей ситуации ломаная линия представляет собой некоторую периодическую функцию, периодом которой является периметр полигонального объекта, образованного этой ломанной.

Пусть полигональный объект задаётся функцией $y = f(x)$, причем L — период этой функции, а $f(x)$ является кусочно-заданной функцией, в которой каждая часть — это ребро исходной линии, причем каждая её точка будет задаваться в комплексном виде. Тогда такую функцию можно разложить в ряд Фурье, из которого наиболее важный интерес представляют коэффициенты c_i ($i = 0, \pm 1, \pm 2, \dots, \pm n, \dots$), рассчитывающиеся в выражении:

$$c_n = \frac{2}{L} \sum_{k=0}^{N-1} \int_{S_k}^{S_{k+1}} \left\{ x_k + \frac{x_{k+1} - x_k}{S_{k+1} - S_k} (s - S_k) + \right. \\ \left. + i \left[y_k + \frac{y_{k+1} - y_k}{S_{k+1} - S_k} (s - S_k) \right] \right\} e^{-i \frac{2n\pi s}{L}} ds, \quad (1)$$

где N — количество частей функции, описывающей полигональный объект, а L — периметр полигонального объекта.

Заметим, что ломаная, образующая упрощаемый объект, может быть как замкнута, так и незамкнута. Поэтому, чтобы представить в виде ряда Фурье незамкнутый объект, его необходимо достроить до замкнутого. Это можно сделать путём проведения прямой между крайними точками незамкнуто-

го объекта, и относительно этой прямой построить набор симметричных точек.

Для построения упрощенного объекта представим набор коэффициентов выражения (1) в виде вектора

$$V_d = (d_1, d_2, \dots, d_n, \dots), \tag{2}$$

где $d_n = \frac{\|c_n\|}{\|c_1\|}$.

Для оценки предложенной модели упрощения картографических объектов, были проведены эксперименты, в которых предложенная модель сравнивалась с алгоритмами Дугласа – Пекера [2], Ли – Оупеншоу [3], Висвалингам – Уайатта [4] и алгоритмом «sleeve-fitting» [5].

В качестве характеристик для сравнения были выбраны обобщенное расстояние Хаусдорфа (GHD), количество изгибов в линии, отношение длины преобразованной линии к длине исходной.

Таблица 1. Сравнения алгоритмов

Название а-ма.	GHD	Кол-во изгибов	Длина от исх.	GHD	Кол-во изгибов	Длина от исх.
Исходная карта Длина: 3417, Кол-во изгибов: 1254						
50%						
а-м. [1] 300	1341	166	0.74	1759	166	0.73
а-м. [1] 600	856	345	0.83	1536	286	0.8
а-м. [1] 1200	838	532	0.88	2000	284	0.82
а-м. [2]	668	656	0.98	1604	353	0.94
а-м. [3]	1153	389	0.79	1807	210	0.68
а-м. [4]	699	648	0.97	1567	353	0.89
а-м. [5]	654	690	0.98	1470	373	0.92
12,5%						
а-м. [1] 300	3931	134	0.69	6511	74	0.59
а-м. [1] 600	4122	138	0.71	5743	70	0.6
а-м. [1] 1200	5342	134	0.71	5937	72	0.6
а-м. [2]	3166	176	0.87	6405	89	0.77
а-м. [3]	5298	108	0.52	15818	61	0.39
а-м. [4]	3160	170	0.77	6666	96	0.62
а-м. [5]	3223	164	0.77	6834	96	0.64

Проведя анализ результатов, можно заметить, что рассматриваемый в этой работе алгоритм особо хорошо проявляет себя, когда количество точек упрощаемого объекта сокращается в 16 раз. На это указывают характеристики. Так, обобщенное

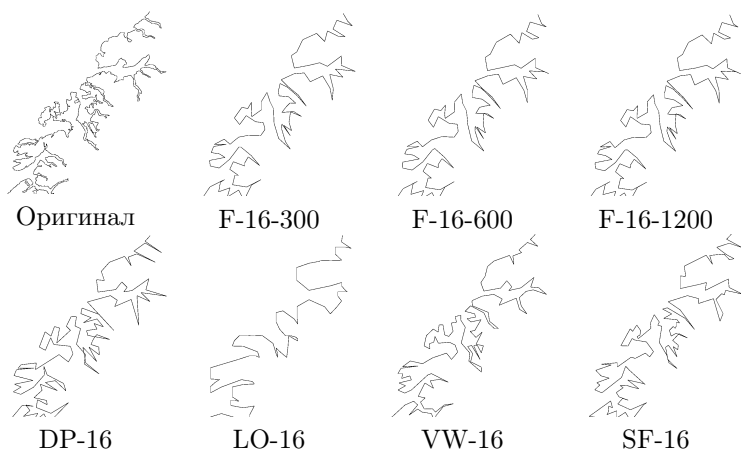


Рис. 1. Примеры упрощения контура норвежской линии фьордов с сокращением количества точек в 2 раза с применением разных алгоритмов: F-16-300, F-16-600, F-16-1200 — упрощение с использованием предложенного алгоритма, DP-16 — упрощение алгоритмом Дугласа – Пекера, LO-16 — упрощение алгоритмом Ли – Оупеншоу, VW-16 — упрощение алгоритмом Висвалингам – Уайатта, SF-16 — упрощение алгоритмом «sleeve-fitting»

расстояние Хаусдорфа показывает насколько приближен упрощенный объект к исходному. На 16-кратном уменьшении числа точек объекта у изучаемого алгоритма оно наименьшее у тех вариантов, когда вычисляется 600 и 1200 членов в ряду. Когда количество точек урезается не так сильно, GHD рассматриваемого алгоритма приближается к среднему значению GHD по остальным алгоритмам, либо не сильно его превышает. Также стоит обратить внимание на коэффициент, показывающий какую часть длины исходного объекта составляет длина преобразованного. На 16-кратном уменьшении числа точек она приближена к средней длине преобразованной линии по остальным алгоритмам.

Литература

- [1] Pengcheng L., Tianyuan X., Jia X., Tinghua A. A multi-scale

representation model of polyline based on head/tail breaks // International Journal of Geographical Information Science. 2020. V. 34. No. 11. P. 2275–2295.

[2] Douglas D. H., Peucker T. K. Algorithms for the reduction of the number of points required to represent a digitized line or its caricature // Canadian Cartographer. 1973. V. 10. No. 2. P. 112–122.

[3] Li Z., Openshaw S. Algorithms for automated line generalization based on a natural principle of objective generalization // International Journal of Geographical Information Systems. 1992. V. 6. No. 5. P. 373–389.

[4] Visvalingham M., Whyatt J. Line generalization by repeated elimination of points // Cartographic Journal. 1993. V. 30. No. 1. P. 46–51.

[5] Zhao Z., Saalfeld A. Linear-time sleeve-fitting polyline simplification algorithms // Proceedings of AutoCarto 13, 1997. P. 214–223.

Исследование модели топологических отношений пространственных объектов

В. Г. Горшков (ЯрГУ им. П. Г. Демидова, Ярославль)

Научные руководители: к.ф.-м.н. Д. М. Мурын,

к.ф.-м.н., доц. О. П. Якимова

Для картографии имеет принципиальное значение сохранение качественных характеристик географических объектов при применении к картам различных преобразований (в первую очередь масштабирования). Например, извилистая река при изменении масштаба должна сохранить свойство «извилистость». Для целей картографии не достаточно только обозначения наличия реки в определенной местности. При этом для обеспечения возможности эффективного хранения и обработки карт применяются различные алгоритмы «упрощения» и «сжатия», что вместе с необходимостью сохранения качественных характеристик объектов часто приводит к нарушению топологических связей между объектами. Например, при упрощении линии реки может оказаться, что близлежащий точечный объект (город, дом и т. п.) перемещается с одного берега на другой (см. рис. 1).

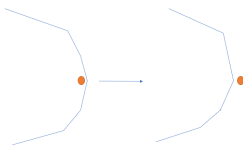
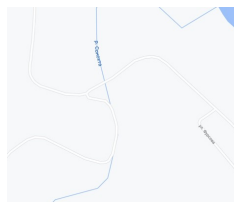


Рис. 1. Некорректное упрощение

Ситуация усугубляется тем, что в современных геоинформационных системах информация хранится «послойно» и применение различных алгоритмов упрощения к различным слоям карты может приводить к появлению топологических конфликтов при наложении различных слоев. Например, на рис. 2 приведен пример топологического конфликта, при котором два различных объекта (река и дорога) накладываются друг на друга, при условии, что на спутниковой карте между этими объектами есть существенное расстояние.



а)



б)

Рис. 2. Топологические конфликты

Целью нашего исследования является разработка алгоритмов преобразований карт (в первую очередь масштабирования и упрощения), сохраняющих существенные качественные географические свойства объектов и топологические отношения между ними.

В работах [1-3] предлагаются алгоритмы, позволяющие определить некоторые топологические отношения между объектами, например, определить пересекаются ли объекты, касаются ли друг друга, покрывается ли один объект другим и т. д. Однако в этих статьях не рассматривается вопрос о взаимном расположении объектов (например, два объекта могут не пе-

```

List<Point> points;
Point P;
Double Distance = infinity;
Bool CanBeGeneralized = false;
Bool FlagPerpendicular = false;
Double angle = 0;
Double totalangle = 0;
for (int i=1; i<points.Count; i++)
    Line line = Line (points[i], points[i-1]);
    //Прямая задается начальной и конечной точкой
    Point perpendicular = line.GetPerpendicular(P)
    // Метод, возвращающий точку основания перпендикуляра.
    if (perpendicular ∈ line)
        if (line.DistanceTo(P) < Distance)
            // Метод, возвращающий расстояние от точки до прямой
            Distance := line.DistanceTo(P) ;
            FlagPerpendicular := true;
            angle := GetAngle(Vector((points[i-1], points[i])), Vector(perpendicular, P))
            //Вектор задается начальным и конечным значением.
            //Угол считается против часовой стрелки
Line l = Line (points [0], points[points.Count-1] )
Point per = l.GetPerpendicular(P);
Totalangle:= GetAngle(Vector(points[0], points[points.Count-1]), Vector(per, P);
if(totalangle ==90 && angle == 90) || (angle ==270 && totalangle ==270)
    if ( FlagPerpendicular == true)
        CanBeGeneralized = true;

else if (FlagPerpendicular ==false)
    CanBeGeneralized = true;

```

Рис. 3. Алгоритм

ресекается, но нельзя сказать лежит ли один левее или правее другого, выше или ниже и т. д.).

Будем рассматривать только точечные и полилинейные объекты (без самопересечений). Приведем предложенный нами алгоритм, позволяющий осуществлять упрощение полилинейного объекта с учетом взаимного расположения с точечным объектом (см. рис. 3).

Входные данные: массив точек линии; координаты точечного объекта.

Анализ работы нашего алгоритма и результаты экспериментов:

1. Скорость работы алгоритма $O(n)$.
2. Идея доказательства: приклеиваем точечный объект к ближайшей к нему стороне полилинейного (к которой строим перпендикуляр) и начинаем стягивать полилинейный объект в вектор от первой точки до последней (по сути распрямляем его).

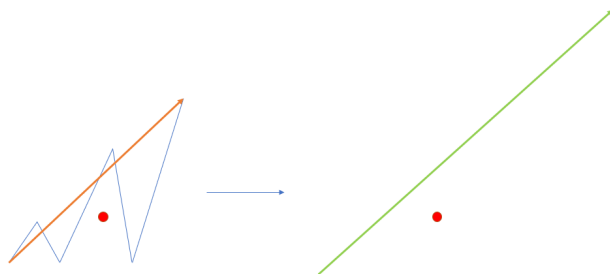


Рис. 4. Пример сглаживания

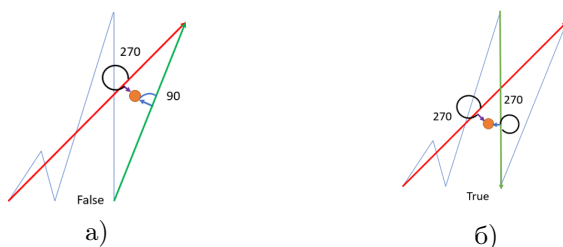


Рис. 5. Результаты экспериментов

Литература

- [1] Clementini E., Sharma J., Egenhofer M. J. Modelling topological spatial relations: Strategies for query processing // Computers&Graphics. 1994. V. 18. No. 6. P. 815–822.

- [2] Zhou X., He H., Hou D., Li R., Zheng H. A RefinedLines/Regions and Lines/Lines Topological Relations Model Based on Whole-Whole Objects Intersection Components // ISPRS Int. J. Geo-Inf. 2021. V. 10. P. 15.
- [3] Liu W. et al. A refined line-line spatial relationship model for spatial conflict detection //International Conference on Conceptual Modeling. 2005. P. 239–248.

Секция математический анализ

**Квадратичная интерполяция и задача
о поглощении треугольником
параболического сектора**

**Н. С. Богомолова (ЯрГУ им. П. Г. Демидова,
Ярославль)**

Научный руководитель: д.ф.-м.н., доц. М. В. Невский

В докладе рассматриваются вопросы, связанные с полиномиальной интерполяцией непрерывных на отрезке функций.

Через $C[a, b]$ обозначим пространство непрерывных функций $f : [a, b] \rightarrow R$ с равномерной нормой $\|f\|_{C[a,b]} = \max_{a \leq x \leq b} |f(x)|$, через Π_n — совокупность алгебраических многочленов одной переменной степени не выше n . Пусть $P : C[a, b] \rightarrow \Pi_n$ — интерполяционный проектор с попарно различными узлами $x_0, \dots, x_n \in [a, b]$. Известно (см. [1]), что норма P как оператора из $C[a, b]$ в $C[a, b]$ может быть вычислена по формуле:

$$\|P\| = \max_{a \leq x \leq b} \sum_{i=0}^n |l_i(x)|, \quad l_i(x) = \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}. \quad (1)$$

В частности, для квадратичной интерполяции на отрезке $[-1, 1]$ имеем

$$\|P\| = \max_{-1 \leq x \leq 1} (|l_0(x)| + |l_1(x)| + |l_2(x)|). \quad (2)$$

Формула (1) была положена в основу вычисления нормы проектора на произвольных наборах узлов. С применением (2) удалось вычислить минимальное значение нормы проектора при $n = 2$. Как оказалось, в этом случае $\min \|P\| = 1.25$, причём это значение при интерполяции на $[-1, 1]$ реализуется только на узлах $-s, 0, s$ при $0.942809... \leq s \leq 1$.

В монографии М. В. Невского [2] был предложен совершенно другой подход к нахождению нормы проектора при квадратичной интерполяции.

Обозначим

$$\Gamma_1 = \{(x, x^2) \in R^2 : -1 \leq x \leq 1\}, \quad (3)$$

$$\Gamma_2 = \{(x, 1) \in R^2 : -1 \leq x \leq 1\}. \quad (4)$$

Пусть D — выпуклая оболочка Γ_1 и Γ_2 , S — треугольник с вершинами на Γ_1 . Введем в рассмотрение величину

$$\xi(S) := \min\{\sigma \geq 1 : D \subset \sigma S\}. \quad (5)$$

Эту величину мы называем коэффициентом поглощения треугольником S параболического сектора D .

Предположим, что $-1 \leq x_0 < x_1 < x_2 \leq 1$, $P : C[-1, 1] \rightarrow \Pi_2$ — интерполяционный проектор с узлами x_0, x_1, x_2 . Рассмотрим треугольник с вершинами (x_0, x_0^2) , (x_1, x_1^2) и (x_2, x_2^2) (см. рис. 1). Как отмечается в [2], имеет место равенство

$$\xi(S) = \frac{3\|P\| - 1}{2}. \quad (6)$$

Коэффициент поглощения $\xi(S)$ можно вычислить, применяя несложные геометрические соображения; после этого норма проектора может быть вычислена с применением (6).

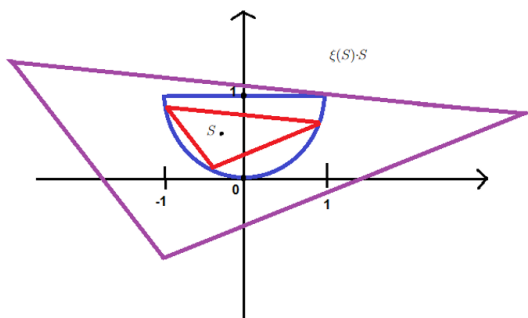


Рис. 1. Поглощение треугольником параболического сектора

Этот подход позволил подтвердить результаты вычисления $\|P\|$ по формуле (2), проверить справедливость равенства (6), а

также получить новым путём результаты о минимальных проекторах. Все вычисления, описанные выше, были реализованы автором на компьютере.

Литература

- [1] Невский М. В., Иродова И. П. Некоторые вопросы теории приближения функций. Ярославль: ЯрГУ, 1999.
- [2] Невский М. В. Геометрические оценки в полиномиальной интерполяции. Ярославль: ЯрГУ, 2012.

Анализ эффективности баз данных П. А. Воробьев (ЯрГУ им. П. Г. Демидова, Ярославль)

Научный руководитель: к.ф.-м.н., доц. А. Ю. Ухалов

Вводится концепция рассмотрения любой программы в виде математической функции вида

$$F : R^n \rightarrow R^m.$$

В качестве входных параметров рассматриваются настройки приложения такие как параметры конфигурационного файла, а в качестве выходных — потребляемые программой ресурсы сервера, время выполнения, параметры отображающие «side-effect».

Рассматривается задача определения алгоритма построения подобной функции для определённых задач возможных при использовании СУБД.

В качестве первой задачи рассматривается поиск максимального количества значений для вставки в PostgreSQL при использовании различных подходов.

Гипотеза 1. *Время вставки данных через единый SQL запрос для всех значений и вставки через один запрос для каждого значения напрямую зависит от количества значений и $F(x)$ — время вставки данных, можно выразить в виде*

$$F(x) = ax + b. \tag{1}$$

Чтобы подтвердить или опровергнуть гипотезу можно либо выполнить множество тестирований и аппроксимировать функцию по множеству точек, либо провести замеры времени при вставке двух значений x_1 и x_2 , получить функцию по двум точкам и проверить принадлежность точки $(x_3, F(x_3))$, где

$$x_3 = \frac{x_1 + x_2}{x_3}.$$

При использовании второго подхода получено, что функция $F(x) \approx 0,0008x + 0,0148$ при использовании запроса для каждого значения, а максимальное количество значений, которое можно вставить за одну секунду равно 1064. Проведя аналогичные действия для вставки единым запросом получаем $F(x) \approx 0.0008x + 0.0077$, а максимальное количество значений — 1240.

Таким образом показано, что для вставки данных через единый SQL запрос для всех значений и вставки через один запрос для каждого значения, время линейно зависит от количества значений.

Определение 1. *Батчем называется множество значений (или наборов значений), которые присутствуют в SQL запросе. Мощность такого множества называется размером батча. Вставка батчами предполагает разбиение множества значений для вставки на подмножества размера N и вставку несколькими SQL запросами.*

Гипотеза 2. *При вставке с использованием батча с несколькими элементами, время вставки данных в PostgreSQL линейно зависит от количества элементов. $F(x, y) = ax + by + c$, где x — количество значений для вставки, y — размер батча.*

Опровергнуть данную гипотезу можно, как минимум, для $y = 10000$. В этом случае, график $F(x, 10000)$ будет подобен параболе, а значит не будет иметь заявленный вид. Минимальное время вставки будет приблизительно равным размеру батча и в случае 10000, минимальное время вставки ниже одной секунды достигнуто при $x = 10500$.

Аналогично можно исследовать методы хранения в СУБД Yandex Clickhouse при использовании таблицы с MergeTree. Поставленная задача требует получить функцию, описывающую

размер данных в таблице. Как и в случае PostgreSQL можно предположить, что искомая функция имеет тип $F(x) = ax + b$. Для подтверждения, выберем $x_1 = 10000$ и $x_2 = 100000$. Проведём вставку x_i значений в таблицу и определим размер данных:

$$F(x_1) = 7561526, F(x_2) = 75585926.$$

Найдём коэффициенты:

$$\begin{cases} k \times 10000 + b = 7561526, \\ k \times 100000 + b = 75585926, \end{cases} \quad F(x) \approx \frac{56687}{75} \times x + \frac{9778}{3}.$$

Проверить данное утверждение можно выполнив вставку 50000 значений. Тогда, общий размер должен быть примерно равен 37794592. Выполнив вставку получено значение:

$$F(50000) = 37761322,$$

что подтверждает теорию о линейности функции F .

Подобным образом можно сформулировать задачу для системы управления Whisper, хранящей данные Graphite в виде дерева. Необходимо получить функцию, описывающую размер файлов внутри СУБД после нескольких итераций сбора данных стека приложений go-graphite. Также необходимо описать количество создаваемых файлов в ходе работы системы.

Так как для каждая метрика Graphite разбивается на элементы, то хранение происходит в виде дерева, где терминальными узлами являются файлы, хранящие метку времени и значение метрики, то с каждой итерацией размер файла увеличивается на 64 бита. Количество создаваемых файлов можно вычислить, перемножив количества всех возможных значений элементов метрики Graphite. Тогда, общий размер файлов Whisper в байтах после x итераций описывается следующей функцией:

$$F(x) = 64xI,$$

где I — количество создаваемых файлов.

Литература

- [1] Шениг Г. PostgreSQL 11. Мастерство разработки. М.: ДМК-Пресс, 2019.

[2] Адельштайн Т., Любанович Б. Системное администрирование в Linux. Санкт-Петербург: Питер, 2010.

[3] Описание СУБД Whisper [Электронный ресурс]. – <https://graphite.readthedocs.io/en/latest/whisper.html>.

Периодические решения в предельном обобщенном уравнении Мэки – Гласса с n запаздываниями

**В. К. Зеленова (ЯрГУ им. П. Г. Демидова,
Ярославль)**

Научный руководитель: к.ф.-м.н. М. М. Преображенская

Данная задача продолжает работу [1], посвященную генераторам Мэки – Гласса. Генератором Мэки – Гласса принято называть [2, 3] электрический генератор, функционирование которого описывается [4] уравнением Мэки – Гласса:

$$\frac{dV}{dt} = -bV + \frac{acV(t - \tau)}{1 + (cV(t - \tau))^\gamma}.$$

Здесь $V(t)$ — это функция напряжения, $a > 0$ — уровень насыщения нелинейности, $b > 0$ — RC -постоянная, $\tau > 0$ — запаздывание по времени, параметр $\gamma > 0$ определяет форму нелинейной функции, $c > 0$ — сила обратной связи.

Назовем обобщенным уравнением Мэки – Гласса:

$$\frac{dV}{dt} = -bV + \frac{ac(V(t - \tau) + \sum_{k=1}^m V(t - r_k))}{1 + (c(V(t - \tau) + \sum_{k=1}^m V(t - r_k)))^\gamma}.$$

Здесь добавлены еще m запаздываний $r_k > 0$.

Введем замены переменных $V = c^{-1}u(\frac{t}{\tau})$, $\beta = b\tau$, $\alpha = a$, $d_k = \frac{r_k}{\tau}$, перенормируем время $t \mapsto \frac{t}{\tau}$ и устремим параметр γ к бесконечности. Получаем следующее предельное уравнение:

$$\begin{aligned} \dot{u} = & -\beta u + \alpha \left(u(t - 1) + \sum_{k=1}^m u(t - d_k) \right) \cdot \\ & \cdot F \left(u(t - 1) + \sum_{k=1}^m u(t - d_k) \right), \end{aligned} \quad (1)$$

где

$$F(w) \stackrel{\text{def}}{=} \lim_{\gamma \rightarrow +\infty} \frac{1}{1+w^\gamma} = \begin{cases} 1, & 0 < w < 1 \\ \frac{1}{2}, & w = 1, \\ 0, & w > 1. \end{cases}$$

Здесь $w(t) = u(t-1) + \sum_{k=1}^m u(t-d_k)$.

В работе отыскиваются периодические решения уравнения (1). Доказан следующий результат.

Теорема 1. Пусть параметры d_k имеют вид $h + k\Delta$, $k = 1, \dots, m$. Тогда существует область параметров α, h, β и такие Δ, u_0 , что уравнение (1) имеет периодическое решение:

$$u_*(t) = \begin{cases} u_0 e^{-\beta t} & \text{при } t \in [0, t_0], \\ e^{-\beta(t-t_0)} \left(\alpha(t-t_0) + \frac{1}{A} \right) & \text{при } t \in [t_0, t_0 + h + \Delta], \\ e^{-\beta(t-t_0)} \left(\frac{\alpha^2 e^{\beta(h+\Delta)}}{2} (t-h-\Delta-t_0)^2 + \right. & \\ \quad \left. + \alpha(t-t_0) + \frac{1}{A} \right) & \text{при } t \in [t_0 + h + \Delta, t_1], \\ \tilde{u} e^{-\beta(t-t_1)} & \text{при } t \in [t_1, T_0], \end{cases}$$

$$u_*(t + T_0) = u_*(t),$$

где

$$t_0 = \frac{1}{\beta} \ln(Au_0),$$

t_1 — корень уравнения: $e^{\beta(h+\Delta)} \alpha(t-h-\Delta-t_0) + 1 = e^{\beta(t-t_0)}$,

$$u_0 = u(0), A = e^\beta + \sum_{k=1}^m e^{\beta(h+k\Delta)},$$

$$T_0 = \frac{1}{\beta} \ln(\tilde{u}A) + t_1 - t_0, \tilde{u} = u(t_1).$$

Литература

- [1] Преображенская М. М. Релейная модель Мэки – Гласса с двумя запаздываниями // ТМФ. 2020. Т. 203. № 1. С. 106–118.
 [2] Tateno M., Uchida A. Nonlinear dynamics and chaos synchronization in Mackey-Glass electronic circuits with multiple time-delayed feedback // Nonlinear Theory and Its Applications, IEICE. 2012. Т. 3. №. 2. Р. 155–164. [3] Sano S., Uchida A., Yoshimori S., Roy R. Dual synchronization

of chaos in Mackey-Glass electronic circuits with time-delayed feedback // Phys. Rev. E. 2007. V. 75. P. 016207.

[4] Mackey M. C., Glass L. Oscillation and chaos in physiological control systems // Science. 1977. V. 197. No. 4300. P. 287–289.

Вычисление числовых характеристик n -мерного симплекса

**А. А. Хохлова (ЯрГУ им. П. Г. Демидова,
Ярославль)**

Научный руководитель: д.ф.-м.н., доц. М. В. Невский

В докладе обсуждается компьютерная реализация алгоритмов, связанных с вычислением некоторых числовых характеристик n -мерного симплекса.

Пусть S — невырожденный симплекс в \mathbb{R}^n , вершины которого имеют вид $x^{(j)} = (x_1^{(j)}, \dots, x_n^{(j)})$, $1 \leq j \leq n + 1$. Матрица вершин этого симплекса

$$\mathbf{A} := \begin{pmatrix} x_1^{(1)} & \cdots & x_n^{(1)} & 1 \\ \vdots & \ddots & \vdots & \vdots \\ x_1^{(n+1)} & \cdots & x_n^{(n+1)} & 1 \end{pmatrix}$$

является невырожденной, причем $\text{vol}(S) = \frac{|\det(\mathbf{A})|}{n!}$.

Пусть $\mathbf{A}^{-1} = (l_{ij})$. Линейные многочлены

$$\lambda_j(x) = l_{1,j}x_1 + \dots + l_{n,j}x_n + l_{n+1,j}$$

называются базисными многочленами Лагранжа симплекса S . Именно с применением этих многочленов и их коэффициентов можно вычислить многие характеристики симплекса: осевые диаметры симплекса $d_i(S)$, коэффициенты $\alpha(S)$ и $\xi(S)$ поглощения единичного куба $Q_n = [0, 1]^n$ гомотетическим образом симплекса (с трансляцией и без трансляции), норму соответствующего интерполяционного проектора P на пространство линейных функций и др. Определения этих величин, а также доказательства вычислительных формул приводятся в монографии М. В. Невского [1]; там же даются ссылки на статьи.

Этот материал и был положен в основу компьютерных вычислений.

Более подробно мы остановимся на вычислении так называемых μ -вершин симплекса относительно содержащего его единичного куба. Обозначим через $\Pi_1(\mathbb{R}^n)$ совокупность многочленов степени ≤ 1 от n переменных. Пусть $S \subset Q_n$ $P : C(Q_n) \rightarrow \Pi_1(\mathbb{R}^n)$ — интерполяционный проектор, узлы которого находятся в вершинах S . Как показано в [1], норма P как оператора из $C(Q_n)$ в $C(Q_n)$ может быть вычислена по формуле

$$\|P\| = \max_{x \in \text{ver}(Q_n)} \sum_{j=1}^{n+1} |\lambda_j(x)|.$$

Зафиксируем число $1 \leq \mu \leq n$. Вершина $x \in \text{ver}(Q_n)$ называется μ -вершиной Q_n относительно симплекса S , если для интерполяционного проектора P с узлами в вершинах S выполняется равенство $\|P\| = \sum |\lambda_j(x)|$ и среди чисел $\lambda_j(x)$ имеется ровно μ отрицательных. Понятие μ -вершины является важным в связи со справедливостью некоторых соотношений, связывающих норму P и указанные выше характеристики симплекса S (см. [1]).

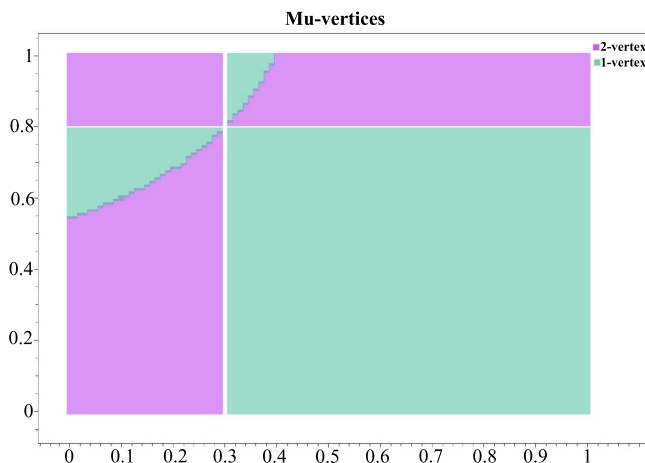


Рис. 1. Пример, разработанный программой

На языке C# была реализована программа вычисления μ -вершин куба относительно находящегося в нём n -мерного симплекса. Для $n = 2$ некоторые результаты были представлены графически. На рис. 1 даётся пример симплекса с вершинами $x^{(1)} = (0.3; 0.8)$, $x^{(2)} = (s; 0.8)$, $x^{(3)} = (0.3; t)$. При $s = 0.82$, $t = 0.36$ были вычислены характеристики: $\text{vol}(S) = 0.11$; $\alpha(S) = 4.20$; $\xi(S) = 7.49$; $\|P\| = 5.33$; $d_1(S) = 0.52$; $d_2 = 0.44$ (значения округлены до двух знаков после запятой). На диаграмме разными цветами изображены μ -вершины. В данном случае найдены 2-вершины и 1-вершины. В правом нижнем углу отмечены 1-вершины.

Литература

- [1] Невский М. В. Геометрические оценки в полиномиальной интерполяции. Ярославль: ЯрГУ, 2012.

Секция математическое моделирование

Анализ и сравнение возможных схмотехнических реализаций носимого монитора дыхания для системы с биологической обратной связью

*Д. М. Ежов (СГУ им. Н. Г. Чернышевского,
Саратов)*

*А. Н. Храмков (СГУ им. Н. Г. Чернышевского,
Саратов)*

*Е. И. Боровкова (СГУ им. Н. Г. Чернышевского,
Саратов)*

Научные руководители: д.ф.-м.н., доц. А. С. Караваев

Ряд исследований [1, 2, 3, 4] отмечают важность кардиореспираторного взаимодействия в процессе регуляции различных систем организма. В последние годы значительный интерес привлекают исследования, использующие активный эксперимент с биологической обратной связью (БОС), обеспечивающей барорефлекторный резонанс в процессе кардиореспираторного взаимодействия. [5, 6]

Такие исследования имеют важное значение для разработки методов диагностики терапии и профилактики патологий кровообращения, дыхания и даже когнитивных расстройств, однако требуют создания аппаратно-программных систем БОС, что является нерешенной задачей и предметом исследования научного сообщества. Организация биологической обратной связи требует контролируемого управления различными параметрами организма, включая частоту и глубину дыхания, соотношение длительности вдоха-выдоха и др., что, в общем случае, является нерешённой задачей [5].

Целью проводимого исследования является анализ и сравнение возможных схмотехнических решений аппаратной части системы с биологической обратной связью — регистратора дыхания. Проблемы при использовании с доступным тензометрическим датчиком — малый размах сигнала датчика и

разное постоянное смещение при использовании с разными испытуемыми. Следовательно, появилась необходимость сравнения разных схмотехнических решений, способных решить эти проблемы.

Были предложены четыре схемы: на основе инструментального усилителя, оригинальная двухкаскадная схема с фильтром высоких частот между каскадами, исследована на возможность применимости в данном случае схема активной компенсации смещения, предложенная в [7] и схема с дифференциальным АЦП высокой разрядности без аналоговой части.

Все схемы были промоделированы в программном пакете NI Multisim, были собраны и протестированы лабораторные образцы трёх схем.

Сопоставление показало, что наилучшими характеристиками в смысле уровня шумов, времени релаксации, смещения постоянной составляющей и др. обладает схема с размещением на выходе тензометрического датчика — моста Уитстона дифференциального АЦП разрешением не ниже 24 бит.

В результате был разработан и создан образец носимого телеметрического аппаратно-программного комплекса с БОС для регистрации и анализа сигнала дыхания испытуемых. Комплекс обеспечивает контроль глубины и частоты дыхания испытуемого по известному закону и используется в проводимых научной группой экспериментальных исследованиях.

Работа выполнена при финансовой поддержке гранта МК-2325.2021.1.2.

Литература

- [1] Shioyai Y., Stefanovska A., McClintock P. V. E. Nonlinear dynamics of cardiovascular ageing // *Physics Reports*. 2010. V. 488. P. 51–110.
- [2] Guyenet P. G. Regulation of Breathing and Autonomic Outflows by Chemoreceptors // *Compr Physiol*. 2014. V. 4. No. 4. P. 1511–1562.
- [3] Schafer C., Rosenblum M. G., Abel H.-H., Kurths J., Synchronization in the Human Cardiorespiratory System // *Physical Review E*. 1999. V. 60. P. 857–870.
- [4] Bartsch R. P., Schumann A. Y., Kantelhardt J. W., Penzel T., Ivanov P. C. Phase transitions in physiologic coupling // *PNAS*. 2012. V. 109. No. 26. P. 10181–10186.
- [5] Shaffer F., Meehan Z. M. A Practical Guide to Resonance Frequency

Assessment for Heart Rate Variability Biofeedback // *Frontiers in Neuroscience*. 2020. V. 14. P. 1055.

[6] Gevirtz R. The Promise of Heart Rate Variability Biofeedback: Evidence-Based Applications // *Biofeedback*. 2013. V. 41. P. 110–120.

[7] Rentyuk V. Use an integrator instead of coupling capacitors // *Electronic Design News*. 2012. V. 57. No. 4. P. 49.

**Ступенчатые решения
квазинормальных форм
одной распределенной краевой задачи**
**Д. С. Костерин (ЯрГУ им. П. Г. Демидова,
Ярославль)**

Научный руководитель: д.ф.-м.н., проф. С. Д. Глызин

Рассматривается система уравнений

$$\frac{\partial u}{\partial t} = (A_0 + \varepsilon A_1)u + F_2(u, u) + F_3(u, u, u) + \\ + \varepsilon D_0 \frac{1}{2\pi} \int_0^{2\pi} u(t, x) dx, \quad (1)$$

где $u = u(t, x) \in \mathbb{R}^n$, A_0 , A_1 , D_0 — $n \times n$ матрицы, $F_2(*, *)$, $F_3(*, *, *)$ — линейные по каждому аргументу вектор-функции, ε — малый положительный параметр.

Система (1) рассматривается с периодическим краевым условием

$$u(t, x + 2\pi) \equiv u(t, x). \quad (2)$$

Будем считать, что матрица A_0 имеет простое нулевое собственное значение, все остальные собственные значения имеют отрицательную вещественную часть. Эта ситуация является критическим случаем в задаче об устойчивости нулевого состояния равновесия краевой задачи (1), (2).

В работе исследуется поведение решений рассматриваемой краевой задачи в достаточно малой и не зависящей от ε окрестности нулевого состояния равновесия. В этом случае динамика

решений описывается одномерной краевой задачей, называемой квазинормальной формой. Рассмотрены решения квазинормальных форм и вопрос об устойчивости этих решений.

В работах [1, 2] были рассмотрены некоторые задачи, связанные с построением таких квазинормальных форм. В настоящей работе используется схожая методика построения и анализа квазинормальных форм.

Решение краевой задачи (1), (2) будем искать в виде асимптотического ряда

$$u(t, x) = \varepsilon \xi(\tau, x)a + \varepsilon^2 u_{20} \xi^2(\tau, x) + \dots, \quad \tau = \varepsilon t.$$

Подставив его в (1) и приравняв коэффициенты при одинаковых степенях ε , получим при ε^2 краевую задачу для определения неизвестной функции $\xi(\tau, x)$:

$$\frac{\partial \xi}{\partial \tau} = \lambda \xi + \delta \xi^2 + \gamma_0 M(\xi), \quad \xi(\tau, x + 2\pi) \equiv \xi(\tau, x), \quad (3)$$

где $M(\xi)$ – среднее значение функции ξ .

С помощью нормировок времени и функции ξ можно считать, что $\lambda = 1$, $\delta = -1$. Справедливы следующие результаты.

Теорема 1. *Краевая задача (3) имеет однородные состояния равновесия $\xi_0 = 0$ и $\xi_1 = 1 + \gamma$. Состояние равновесия ξ_1 является асимптотически устойчивым, если $\gamma > -1$.*

Теорема 2. *Краевая задача (3) имеет однопараметрическое семейство кусочно-постоянных решений вида*

$$\xi(\tau, x) = \begin{cases} \rho, & x \in [0, \alpha), \\ 1 - \rho, & x \in [\alpha, 2\pi), \end{cases}$$

где ρ – решение уравнения

$$\rho^2 - \left(1 + \frac{\gamma(\alpha - \pi)}{\pi}\right) \rho - \frac{\gamma(2\pi - \alpha)}{2\pi} = 0.$$

Решения этого семейства являются неустойчивыми при любых α и γ .

В случае, если в (3) $\delta = 0$, решение краевой задачи (1), (2) ищем в виде асимптотического ряда

$$u(t, x) = \varepsilon^{1/2} \xi(\tau, x) a + \varepsilon u_{20} \xi^2(\tau, x) + \varepsilon^{3/2} u_{30} \xi^3(\tau, x) + \dots, \quad \tau = \varepsilon t.$$

В этом случае квазинормальная форма имеет вид

$$\frac{\partial \xi}{\partial \tau} = \lambda \xi + \delta_1 \xi^3 + \gamma M(\xi), \quad \xi(\tau, x + 2\pi) \equiv \xi(\tau, x). \quad (4)$$

Можно считать, что $\lambda = 1$, $\delta_1 = -1$. Справедливы следующие результаты.

Теорема 3. Краевая задача (4) имеет два ненулевых однородных состояния равновесия $\xi_1 = \sqrt{1 + \gamma}$ и $\xi_2 = -\sqrt{1 + \gamma}$, которые являются асимптотически устойчивыми при $\gamma > -\frac{2}{3}$.

Теорема 4. Краевая задача (4) имеет семейство кусочно-постоянных решений вида

$$\xi(\tau, x) = \begin{cases} \rho_1, & x \in [0, \alpha), \\ \rho_2, & x \in [\alpha, 2\pi), \end{cases}$$

где ρ_1, ρ_2, α — решение алгебраической системы

$$\rho_j - \rho_j^3 + \frac{\gamma}{2\pi} [\rho_1 \alpha + (2\pi - \alpha) \rho_2] = 0, \quad j = 1, 2.$$

Решение такого вида является устойчивым, если

$$\begin{aligned} \rho_j^2 &> \frac{1}{3}, \quad j = 1, 2, \\ 2 - 3(\rho_1^2 + \rho_2^2) + \gamma &< 0, \\ (1 - 3\rho_1^2)(1 - 3\rho_2^2) + \gamma - 3 \left[\rho_1^2 \gamma + \frac{\gamma \alpha}{2\pi} (\rho_2^2 - \rho_1^2) \right] &> 0. \end{aligned}$$

Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 18-29-10055).

Литература

- [1] Кащенко С. А., Григорьева Е. В. Медленные и быстрые колебания в модели оптико-электронного осциллятора с запаздыванием // Доклады Академии наук. 2019. Т. 484. № 1. С. 21–25.
- [2] Глызин С. Д., Колесов А. Ю. Бегущие волны в полносвязных сетях нелинейных осцилляторов // Журнал вычислительной математики и математической физики. 2022. Т. 62. № 1. С. 71–89.

Методы расчета кардиоинтервалограммы из сигнала фотоплетизмограммы для анализа синхронизации контуров вегетативного контроля

*А. В. Курбако (СФ ИРЭ им В.А. Котельникова
РАН, Саратов)*

*В. В. Сказкина (СГУ им. Н. Г. Чернышевского,
Саратов)*

*Е. И. Боровкова (СГУ им. Н. Г. Чернышевского,
Саратов)*

Научный руководитель: д.ф.-м.н., доц. А. С. Караваев

Сердечно-сосудистая система (ССС) является сложной нелинейной системой и важной частью человеческого организма. Отклонения в ее работе занимают лидирующую позицию среди причин инвалидизации и смертности населения в трудоспособном возрасте. Своевременная диагностика и профилактика заболеваний ССС позволяют своевременно назначить подходящее лечение и не допустить патологических отклонений в работе организма. В ряде работ была показана возможность и важность оценки особенностей динамики подсистем нервной регуляции для оценки состояния организма при помощи анализа низкочастотных спектральных составляющих сигналов ССС [1].

Ранее был предложен показатель оценки степени синхронизации 0.1 Гц колебаний по сигналам кардиоинтервалограммы (КИГ) и фотоплетизмограммы (ФПГ): суммарный процент фазовой синхронизации S [2]. Разработанный индекс показал свою эффективность при изучении контуров вегетативной регуляции [3] и практическую значимость для диагностических целей [4]. Однако, использование данного индекса осложнено необходимостью регистрации длительных записей сигналов электрокардиограммы (ЭКГ) для выделения КИГ и ФПГ.

В работе были предложены четыре метода для выделения сигнала КИГ из ФПГ в реальном времени, развивающие идею, предложенную в [5]. Методы 1 и 2 измеряют интервалы между сердечными сокращениями как расстояния между миниму-

мами и минимумами соответственно сигнала ФПГ после узкополосной фильтрации (0.8-1.8 Гц). Методы 3 и 4 используют сигнал ФПГ после узкополосной фильтрации для определения интервала кардиоцикла (для метода 3 кардиоцикл: интервал между минимумами сигнала, для 4 — между максимумами). Далее методы 3 и 4 определяют интервал между сердечными сокращениями как расстояние между максимумами и минимумами соседних кардиоциклов соответственно сигнала ФПГ после широкополосной фильтрации (0.6-6.0 Гц). Значения границ фильтрации для 4-х методов являются параметрами.

Оптимальные параметры для выделения КИГ из ФПГ подбирались при переборе по средствам максимизации вероятности того, что коэффициент фазовой когерентности (КФК) между мгновенными фазами в низкочастотном диапазоне [0.05-0.15] Гц сигналов КИГ по ФПГ и по ЭКГ примет значение больше 0.95. Используя оптимальные параметры были рассчитаны КФК между мгновенными фазами в низкочастотном диапазоне для 4-х методов. Для метода 1 коэффициент составляет 0.83 ± 0.20 (среднее \pm стандартное отклонение), 0.84 ± 0.20 для 2 метода, 0.84 ± 0.21 для третьего и 0.79 ± 0.26 для четвертого.

В ходе проверки работоспособности методов были рассчитаны значения суммарного процента 4 методами по сигналу ФПГ и классическим способом с использованием сигнала ЭКГ (см. рис. 1). Средние по ансамблю значения разности составили: 7.34 ± 9.69 для первой методики, 7.05 ± 7.43 для второй, 7.69 ± 7.84 для третьей, 5.83 ± 6.34 для четвертой. Видно, что лучшее соответствие эталонному методу обеспечивает методика 4, а худшее — методика 3.

Таким образом, предложенные методы показали свою работоспособность и возможность использования единственного сигнала ФПГ для оценки суммарного процента фазовой синхронизации. Предложенные методики обладают низкой вычислительной сложностью и позволяют использовать их в реальном времени, что в совокупности с разработанными ранее методами может позволить рассчитывать суммарный процент фазовой синхронизации в реальном времени с использованием носимых приборов на основе низкопотребляющих микроконтроллеров.

Работа выполнена при финансовой поддержке проектов РФФИ, гранты №20-02-00702 и №20-38-90067, а также в рамках государ-

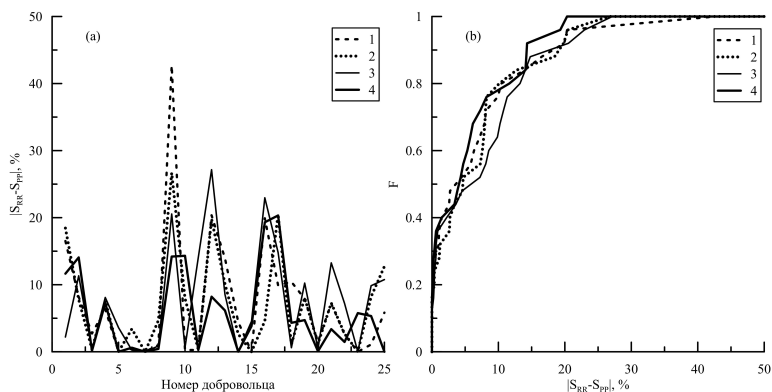


Рис. 1. Сопоставление результатов оценки суммарного процента S , основанной на анализе пары сигналов ЭКГ и ФПГ S_{RR} и четырех используемых методик S_{PP} . Номер на легенде соответствует номеру метода в описании их работы. (a) Модули разности оценок S для всех здоровых добровольцев. (b) Функция распределения модуля разности оценок

ственного задания СФ ИРЭ РАН.

Литература

- [1] Баевский Р. М. и др. Анализ variability сердечного ритма при использовании различных электрокардиографических систем // Вестник аритмологии. 2001. Т. 24. С. 65–87.
- [2] Karavaev A. S. et al. Synchronization of low-frequency oscillations in the human cardiovascular system // Chaos. 2009. V. 19. P. 033112.
- [3] Караваев А. С. и др. Модель сердечно-сосудистой системы человека с автономным контуром регуляции среднего артериального давления // Физиология человека. 2017. Т. 43. № 1. С. 70–80.
- [4] Киселев А. Р. и др. Персонализация подхода к назначению гипотензивной терапии у больных артериальной гипертензией на основе индивидуальных особенностей вегетативной дисфункции сердечно-сосудистой системы // Артериальная гипертензия. 2011. Т. 17. № 4. С. 354–360.
- [5] Кульминский Д. Д. и др. Диагностика синхронизации 0,1 Гц ритмов сердечно-сосудистой системы по унивариантным данным. В кн.:

Тезисы докладов VIII Всероссийской конференции молодых ученых «Нанопотоника, наноэлектроника и нелинейная физика». Саратов: Издательство Саратовского университета. 2013. С. 139–141.

**Исследование локальной динамики одного
дифференциального уравнения второго
порядка с запаздыванием в производной**
**И. Н. Маслеников (ЯрГУ им. П. Г. Демидова,
Ярославль)**

Научный руководитель: д.ф.-м.н., доц. И. С. Кащенко

Рассмотрим дифференциальное уравнение второго порядка с запаздывающей обратной связью:

$$\varepsilon \frac{d^2 y}{dt^2} + \frac{dy}{dt} + \delta y = F \left(\frac{dy}{dt}(t - \tau) \right). \quad (1)$$

Здесь ε и δ — малые и пропорциональные параметры $0 < \varepsilon \ll 1$, $\delta = k\varepsilon$, τ — параметр запаздывания, вещественный и положительный. Функция F достаточно гладкая, не ограничивая общности, можно считать, что $F(0) = 0$. Таким образом, уравнение (1) имеет нулевое состояние равновесия. Рассматриваемая задача является сингулярно возмущенной.

Отметим, что в статье [1] рассмотрена похожая модель опто-электронного осциллятора, в котором параметр δ не является малым.

Характеристический квазиполином линеаризованного в нуле уравнения (1) имеет вид:

$$\varepsilon \lambda^2 + \lambda + k\varepsilon = \lambda \beta_1 e^{-\lambda}. \quad (2)$$

Справедливы следующие результаты.

Теорема 1. *При $|\beta_1| < 1$ и достаточно малом ε , все корни (2) имеют отрицательные вещественные части, нулевое состояние равновесия устойчиво. При $|\beta_1| > 1$ и достаточно малом ε , существуют корни (2), имеющие положительные вещественные части, нулевое состояние равновесия неустойчиво.*

В критических случаях $\beta_1 = \pm 1$ характеристическое уравнение имеет бесконечное количество корней, стремящихся к мнимой оси при $\varepsilon \rightarrow 0$. Таким образом критические случаи имеют бесконечную размерность.

Для исследования поведения решений в случае $\beta_1 = \pm 1$ построены квазинормальные формы — специальные нелинейные уравнения параболического типа, не содержащие малых параметров, решения которых дают главную часть асимптотических по невязке равномерно по $t \geq 0$ решений уравнения (1).

Исследование выполнено при поддержке Российского научного фонда (проект № 21-71-30011).

Литература

- [1] Larger L., Maistrenko Y., Penkovskiy B. Virtual Chimera States for Delayed-Feedback Systems // Physical Review Letters. 2013. V. 111. P. 054103.
- [2] Григорьева Е. В., Кащенко С. А., Глазков Д. В. Особенности локальной динамики модели оптико-электронного осциллятора с запаздыванием // Моделирование и анализ информационных систем. 2018. Т. 25. № 1. С. 71–82.

Моделирование движения транспортного потока

**М. А. Погребняк (ЯрГУ им. П. Г. Демидова,
Ярославль)**

Научный руководитель: д.ф.-м.н., доц. И. С. Кащенко

Работа посвящена математическому моделированию движения транспортного потока. Построена модель, улучшающая результаты работы автора [1] и описывающая ряд новых дорожных ситуаций.

За $x_n(t)$ ($1 \leq n \leq N \in \mathbb{N}$) обозначено положение транспортного средства в момент времени t , а за $\dot{x}_n(t)$ и $\ddot{x}_n(t)$ его скорость и ускорение соответственно. Все автомобили считаются материальными точками, поэтому их внутренняя структура и внешние габариты не учитываются.

В ходе работы была построена математическая модель движения транспортного потока, которая имеет вид системы дифференциальных уравнений с запаздывающим аргументом:

$$\begin{cases} \ddot{x}_n(t) = R_n \left[a_n \left(\frac{v_{max} - \dot{x}_{n-1}(t - \tau)}{1 + e^{k_n(-\Delta x_n(t, \tau) + s_n)}} + \dot{x}_{n-1}(t - \tau) - \dot{x}_n(t) \right) \right] + \\ \quad + (1 - R_n) \left[q_n \left(\frac{\dot{x}_n(t) [\dot{x}_{n-1}(t - \tau) - \dot{x}_n(t)]}{\Delta x_n(t, \tau) - l_{n, \varepsilon}} \right) \right], \\ x_n(t) = \lambda_n, \quad \dot{x}_n(t) = v_n, \quad \text{при } t \in [-\tau, 0], \end{cases}$$

где $\Delta x_n(t, \tau) = x_{n-1}(t - \tau) - x_n(t)$ — расстояние между соседними автомобилями; τ — время реакции водителя; $a_n > 0$ и $q_n > 0$ — коэффициенты, описывающие технические характеристики автомобиля, отвечающие за интенсивность его разгона и торможения соответственно; $v_{max} > 0$ — максимальная желаемая скорость; $l_{n, \varepsilon} > 0$ — безопасное расстояние вида $l_{n, \varepsilon} = l_n - \varepsilon$, где ε — добавка, служащая для предотвращения торможения автомобиля с неограниченной скоростью при $\Delta x_n(t, \tau)$ достаточно близком к l_n ; $k_n > 0$ и $s_n > 0$ — параметры, описывающие поведения водителя: k_n показывает насколько плавно водитель преследующего автомобиля подстраивает свою скорость под впереди идущий, а s_n отражает расстояние, начиная с которого влияние впереди идущего автомобиля перестаёт превалировать; λ_n — начальное положение автомобиля; v_n — начальная скорость автомобиля, а R_n — релейная функция вида:

$$R_n = \begin{cases} 1, & \text{если } \Delta x_n(t, \tau) > \frac{\dot{x}_n^2(t)}{2\mu g} + l_n, \\ 0, & \text{если } \Delta x_n(t, \tau) \leq \frac{\dot{x}_n^2(t)}{2\mu g} + l_n, \end{cases}$$

где μ — коэффициент трения, а g — ускорение свободного падения. Функция R_n описывает переключение «разгон-торможение».

Для модели был проведён анализ устойчивости равномерного режима движения, при котором все автомобили двигаются с одинаковой скоростью v_{max} на расстояниях $\Delta c_n = c_n - c_{n-1}$ друг от друга, где c_n — убывающая последовательность. Для любой убывающей последовательности c_n существует решение системы вида:

$$x_n(t) = c_n + v_{max}t.$$

Устойчивость такого решения зависит от знаков выражений:

$$d_n = -\tau v_{max} + c_n - c_{n-1} - l_{n,\varepsilon}.$$

Справедлива следующая теорема.

Теорема 1. *Если для $\forall n$ выполняется неравенство $d_n > 0$, то равномерный режим устойчив. Если хотя бы при одном каком-то i выполняется неравенство $d_i \leq 0$, то равномерный режим неустойчив.*

Из теоремы 1 следует, что если все автомобили потока движутся на довольно большом расстоянии друг от друга, то такой режим движения устойчив. Устойчивость теряется при увеличении скорости v_{max} , времени реакции водителя τ , безопасного расстояния между автомобилями l_n , или при сокращении расстояния между двумя соседними автомобилями Δc_n .

Литература

[1] Погребняк М. А. Моделирование движения транспортного потока // Тезисы докладов всероссийской молодежной конференции «Путь в науку. Математика» (Ярославль, 2021). Ярославль: ЯрГУ, 2021. С. 81–83.

Влияние электрических связей на экстремальные события в ансамбле двух нейронов Хиндмарш – Роуз с химическими связями

**Е. Ю. Семенюта (ННГУ им. Н. И. Лобачевского,
Нижний Новгород)**

Научный руководитель: к.ф.-м.н., Т. А. Леванова

Экстремальные события (ЭС) — это редкие непериодические отклонения наблюдаемой переменной большой амплитуды от характерного диапазона ее значений при изменении управляющего параметра системы [1]. Редкость ЭС требует характерных масштабов, в первую очередь временных, а интенсивность должна отражать потенциал события, вызывающего кардинальные изменения в системе. Одним из ярких примеров ЭС

в неврологии и медицине являются эпилептические припадки. В предыдущей статье [2] был показан простой ансамбль из двух разрывных нейронов Хиндмарш – Роуз, взаимно связанных с помощью химических синапсов. В этом исследовании мы изучаем ЭС для случая более сложного набора связей. Мы вводим дополнительную электрическую синаптическую связь. Таким образом, наша цель — изучить комплексное влияние различных типов связей на появление и исчезновение ЭС в нейронных ансамблях. Для этого исследуется временная динамика переменной $x_{II} = x_1 + x_2$ для различных комбинаций управляющих параметров k , k_1 и k_2 . Для определения ЭС мы вычисляем уровень $H_s = \mu + 6\sigma$, где μ — среднее значение, а σ — стандартное отклонение всех событий (пиков) на временной диаграмме переменной x_{II} . Этот критерий был впервые введен в [3].

Ансамбль двух нейронов Хиндмарша – Роуза с взаимными химическими синаптическими связями, описывается уравнениями:

$$\begin{cases} \dot{x}_i = y_i + bx_i^2 - ax_i^3 - z_i + I - \\ \quad - k_i(x_i - v_s)\Gamma(x_j) + k(x_j - x_i), \\ \dot{y}_i = c - dx_i^2 - y_i, \\ \dot{z}_i = r[s(x_i - x_R) - z_i], \\ i, j = 1, 2 \ (i \neq j). \end{cases} \quad (1)$$

Здесь переменная x_i описывает мембранный потенциал i -ого нейрона, переменные y_i и z_i соответствуют быстрому и медленному ионным токам, протекающим через мембрану i -ого нейрона. Параметры подобраны так, чтобы каждый нейрон воспроизводил пачечный режим.

Изначально, для случая $k = 0$, наличие ЭС в системе (1) связано с явлением гиперхаоса. На рис. 1 показаны результаты вычисления показателей Ляпунова для различных значений k . Хорошо видно наличие двух положительных показателей Ляпунова при $k = 0$. На рис. 2 видно, что ЭС пропадают в тот момент, когда второй ляпуновский показатель становится меньше нуля.

- Существование ЭС в системе (1) с химическими тормозящими связями связано с гиперхаосом ($\Lambda_1 > \Lambda_2 > 0$).

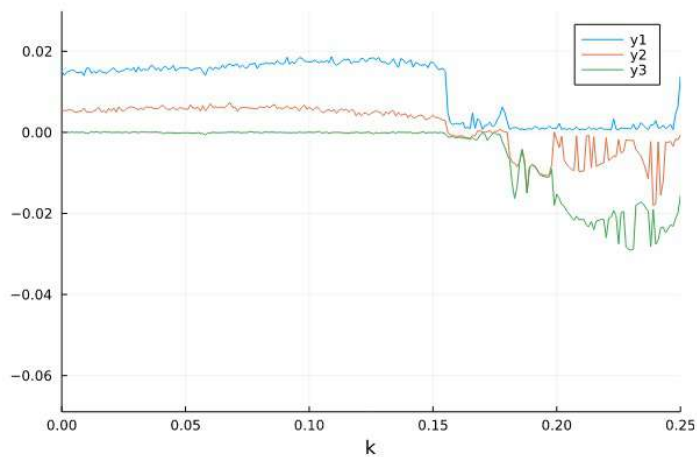


Рис. 1. Три старших показателя Ляпунова в зависимости от k

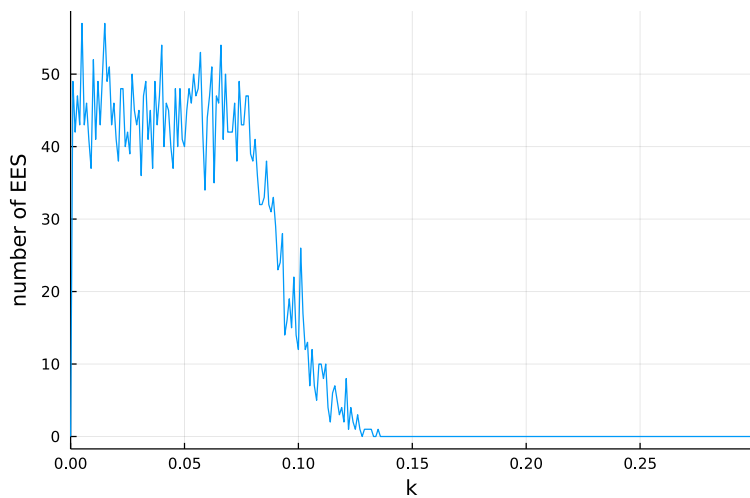


Рис. 2. Количество ЭС в зависимости от k

- Введение слабых электрических связей приводит к уменьшению областей существования ЭС на плоскости параметров (k_1, k_2) и сокращению числа самих событий.
- Введение электрической связи достаточной силы приводит к исчезновению в системе сначала ЭС, а потом и других хаотических режимов (не содержащих ЭС).

Исследование выполнено при финансовой поддержке РНФ в рамках научного проекта No 19-72-10128.

Литература

- [1] Albeverio S., Jentsch V., Kantz H. Extreme events in nature and society. Springer Science & Business Media, 2006.
- [2] Mishra A. et al. Dragon-king-like extreme events in coupled bursting neurons // Physical Review E. 2018. V. 97. No. 6. P. 123–143.
- [3] Dysthe K., Krogstad H. E., Muller P. Oceanic rogue waves // Annu. Rev. Fluid Mech. 2008. V. 40. P. 287–310.

Научное издание

ПУТЬ В НАУКУ. МАТЕМАТИКА

Тезисы докладов конференции

Всероссийская молодежная конференция
11-14 мая 2022 г., Ярославль

Компьютерный набор – авторы
Компьютерная верстка – А. А. Кащенко

Подписано в печать 01.11.2022. Формат 60×90 1/16.
Усл. печ. л. 4,0.
Тираж 24 экз. Заказ № 22131.

Оригинал-макет подготовлен на математическом
факультете ЯрГУ

Отпечатано ООО «Филигрань»,
150049, г. Ярославль, ул. Свободы, 91,
pechataet@bk.ru