МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
Омский государственный технический университет
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
Омский государственный университет им. Ф. М. Достоевского
Омский филиал
Федерального государственного бюджетного учреждения науки
Института математики им. С. Л. Соболева
Сибирского отделения Российской академии наук

АППРОКСИМАЦИЯ ЛОГИЧЕСКИХ МОДЕЛЕЙ, АЛГОРИТМОВ И ЗАДАЧ – АЛМАЗ'2

Тезисы докладов
Международной конференции,
Омск, 27–30 апреля 2015 г.

ОМСК
Издательство ОмГТУ
2015

УДК 5:004
ББК 22.1+32.97
А76

Ответственный редактор
В. А. Романьков, доктор физ.-мат. наук, профессор

А76 **Аппроксимация логических моделей, алгоритмов и задач – АЛМАЗ'2**: тез. докл. Междунар. конф. (Омск, 27-30 апреля 2015 г.)/ Минобрнауки России, ОмГТУ, ОмГУ им. Ф.М. Достоевского, ОФ ИМ СО РАН; [отв. ред. В.А. Романьков]. – Омск: Изд-во ОмГТУ, 2015. - 76 с.; ил.

ISBN 978-5-8149-2067-6

Сборник содержит тезисы докладов, в которых изложены аспекты теории аппроксимации логических моделей и их теорий, а также вопросы информационной безопасности. Ряд докладов посвящен различным практическим применениям результатов, полученных в данной области исследований.

Издание предназначено для математиков, информатиков, а также студентов и аспирантов, изучающих эти предметы. Оно может быть полезным тем, кто разрабатывает информационные технологии и реализует их на практике.

УДК 5:004
ББК 22.1+32.97

Научное издание

АППРОКСИМАЦИЯ ЛОГИЧЕСКИХ МОДЕЛЕЙ, АЛГОРИТМОВ И ЗАДАЧ – АЛМАЗ'2

Тезисы докладов
Международной конференции
(Омск, 27-30 апреля 2015 г.)

Печатается в авторской редакции
Подписано в печать 16.07.2015. Формат 60 × $84\frac{1}{16}$. Бумага офсетная.
Отпечатано на дупликаторе. Усл. печ. л. 4,75. Уч.-изд. л. 4,75.
Тираж 50 экз. Заказ 413

Издательство ОмГТУ. 644050, г. Омск, пр. Мира, 11, т. 23-02-12
Типография ОмГТУ

ISBN 978-5-8149-2067-6

© ОмГТУ, 2015

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ РЕДАКТОРА

Международная конференция "Аппроксимация логических моделей, алгоритмов и задач – АЛМАЗ'2" продолжает предыдущие конференции, прошедшие в Омске: "Алгебра, алгоритмы и вычисления на суперкомпьютерах" 2012 года и "Математические проблемы информатики" 2013 года. На этих конференциях затрагивается широкий спектр современных проблем математики в их связи с проблемами информатики. Доклады представляют как чисто теоретические исследования, так и практически направленные работы в обозначенной области. В работе конференций принимают участие как известные ученые, так и молодые исследователи.

С пленарными докладами выступили: С.Н. Артемов, Ю.Ш. Гуревич, А.В. Николаев (США), М. Казалс-Руис (Испания), Е. Френкель (Москва и Италия), А.М. Райгородский (Москва), М.Ю. Хачай (Екатеринбург), Э.Х. Гимади, А.В. Кельманов, Д.Е. Пальчунов, С.О. Сперанский (Новосибирск), В.М. Гичев, Э.Ю. Даниярова, А.В. Еремеев, С.В. Зыкин, А.А. Мищенко, Г.А. Носков, В.Н. Ремесленников, А.Н. Рыбалов, А.В. Трейер, А.Н. Шевляков (ОФ ИМ СОРАН, Омск), Е.В. Щерба (ОмГТУ, Омск), В.П. Ильев, В.А. Романьков (ОмГУ, Омск).

Активное участие в работе конференции приняли преподаватели и аспиранты ОмГТУ: М.С. Астахов, Д.А. Волков, П.С. Ложников, Ю.Ю. Огородников, В.А. Соловьев, А.Е. Сулавко, И.В. Торопченко, И.В. Широков, А.В. Шутенко, ОмГУПС: А.В. Еременко, а также И. Казачков (Испания).

В работе конференции участвовали молодые исследователи: М.В. Малов, М.А. Вахрамеев, Н.А. Журавлева, А.В. Ильев, П.А. Уляшев (ОФ ИМ СО РАН), А.Ю. Никитин (ОмГУ), П.О. Мартынов (ОГПУ) и др.

Ряд докладов (более точно – восемь пленарных докладов) сделан дистанционно. Качество связи было хорошее, что позволило не только видеть и слышать выступающего (из США, Германии, Москвы, Новосибирска), но и вести с ним активный диалог. Опыт дистанционных докладов, приобретенный на предыдущей и настоящей конференциях следует признать удачным. Это отмечалось не только слушателями, но и самими докладчиками.

Основной темой настоящей конференции являлось обсуждение идеи аппроксимации в ее классических и современных аспектах. Традиционные методы аппроксимации величин, функций и объектов в настоящее время дополняются новыми методами, связанными с понятиями аппроксимации классов моделей и их теорий. Рассматривались проблемы и достижения в теории графов, комбинаторной оптимизации, теории групп Ли. Представлена и другая тематика, включающая квантовую механику, логические основы теории игр, теоремы Рамсея, вероятностные логики, защиту информации, в частности – криптографию и т.д.

В. Романьков
31.05.2015

УДК 519.17

ВЫВОД ФОРМУЛЫ ДЛЯ ПОДСЧЕТА ЧИСЛА ПРОСТЫХ ЦИКЛОВ ЗАДАННОЙ ДЛИНЫ В ПРОСТОМ ГРАФЕ

М. С. Астахов, И. В. Широков, А. В. Шутенко[1]
Омский государственный технический университет
г. Омск

Постановка задачи

Пусть G — простой граф с n вершинами, A — его матрица смежности, a_{ij} — ее матричные элементы[1]. Введем обозначение $\mathcal{C}_s(G)$ — количество простых циклов длины s[2].

Модифицируем формулу для следа степени матрицы:

$$\tilde{\mathrm{tr}}\, A^s = \sum_{i_1,\dots i_s;\ i_j \neq i_k} a_{i_1 i_2} a_{i_2 i_3} \dots a_{i_s i_1} \tag{1}$$

Используя это обозначение, получим

$$\mathcal{C}_s(G) = \tilde{\mathrm{tr}}\, A^s / 2s \tag{2}$$

Таким образом, задача подсчета числа простых циклов $\mathcal{C}_s(G)$ сводится к получению формулы для вычисления модифицированного следа (1).

Неравенства $i_j \neq i_k$ в формуле (1) будем называть *препятствиями*. Основной прием для избавления от препятствий заключается в применении очевидного равенства:

$$\sum_{i,\ i \neq j} B_i = \sum_i B_i - B_j. \tag{3}$$

В настоящей работе представлен алгоритм получения универсальной формулы, зависящей от матрицы A и числа s для вычисления модифицированного следа (1), что согласно (2) эквивалентно формуле вычисления числа простых циклов длины s.

Вывод формулы для модифицированного следа

Для сокращения записи введем обозначения

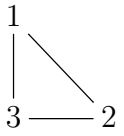
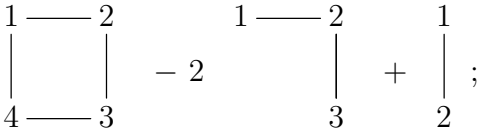
$$\sum_{i_1,\dots i_s;\ i_j \neq i_k} a_{i_1 i_2} a_{i_2 i_3} \dots a_{i_s i_1} \to (1,2)(2,3)\dots(s,1)\,. \tag{4}$$
$$\phantom{\sum_{i_1,\dots i_s;\ i_j \neq i_k}} \quad j \neq k$$

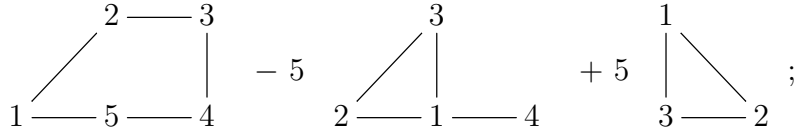
Выражению вида $(i_1, i_2)(i_3, i_4)\dots(i_{l-1}, i_l)$ (индексы могут повторяться) поставим в соответствие простой граф $H(V, E)$ (s–угольник) с множеством вершин $V = \{i_1, \dots, i_l\}$ и множеством ребер $E = \{(i_1, i_2), (i_3, i_4), \dots, (i_{l-1}, i_l)\}$. Такие графы будем называть *формальными*. Формула (1) в этих обозначениях примет вид

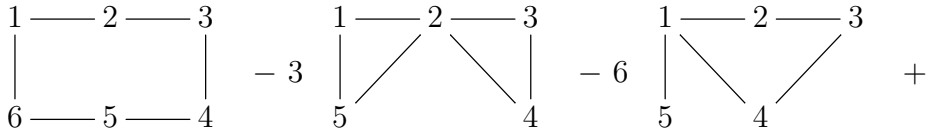
$$\tilde{\mathrm{tr}}\, A^s = \sum_{\alpha=1}^{N(s)} H_\alpha(A). \tag{5}$$

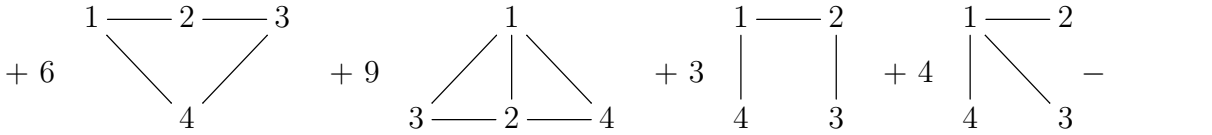
[1] aro_x@mail.ru

Приведем формулы для вычисления модифицированного следа в графическом виде для случаев $s < 7$.

$\tilde{\mathrm{tr}}\, A^3 =$  ; $\tilde{\mathrm{tr}}\, A^4 =$  ;

$\tilde{\mathrm{tr}}\, A^5 =$  ;

$\tilde{\mathrm{tr}}\, A^6 =$ 

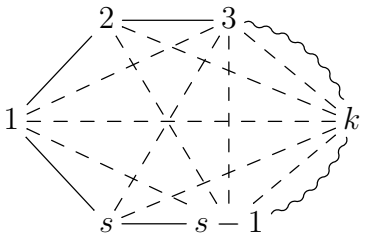


Графический метод позволяет не только представлять конечный результат, но и производить вывод формулы для вычисления модифицированного следа.

Сумме

$$\sum_{\substack{i_1,i_2,\ldots,i_l,\\ i_k\neq i_r}} a_{i_1 i_2}\ldots a_{i_{l-1} i_l} \longleftrightarrow \underset{i_k\neq i_r}{(i_1,i_2)\ldots(i_{l-1} i_l)}$$

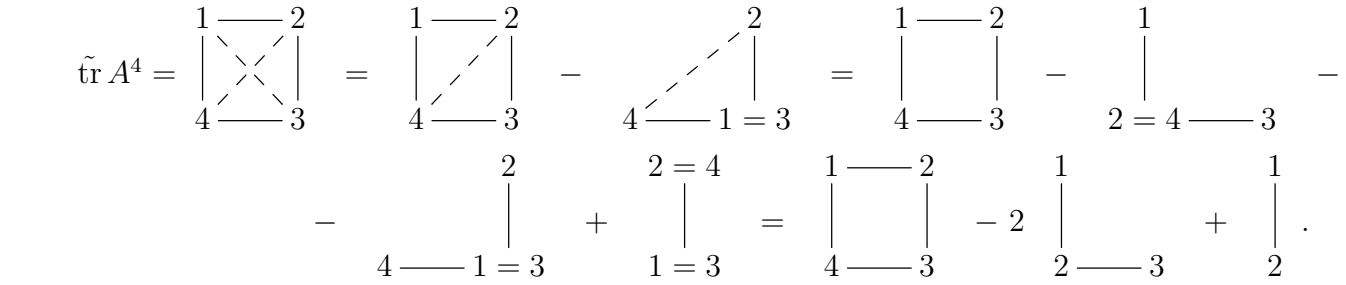
поставим во взаимно однозначное соответствие взвешенный граф с множеством вершин $V = \{i_1, \ldots, i_l\}$, множеством ребер с весом 1: $E^+ = \{(i_1, i_2), \ldots, (i_{l-1}, i_l)\}$ (эти ребра будем как и прежде изображать сплошной линией) и множеством ребер веса (-1): $E^- = \{(i_k, i_r)\}$, т.е. препятствиям будут соответствовать ребра отрицательного веса (эти ребра будем изображать пунктирными линиями). Тогда модифицированному следу степени матрицы (1) будет соответствовать граф, который мы будем называть *базовым*

$\tilde{\mathrm{tr}}\, A^s \longleftrightarrow$  (6)

Алгоритм получения формулы для модифицированного следа состоит из представления базового графа через графы без ребер с отрицательными весами. А именно, формула

(3) в этих терминах выглядит следующим образом: у исходного графа удаляется ребро отрицательного веса (т.е. удаляется одно препятствие) и "отнимается" граф, получающийся из исходного *склейкой* двух вершин, инцидентных выбранному ребру (склейка — это отождествление двух вершин, если при этом получается двойное ребро, то оно заменяется одинарным).

Проиллюстрируем вышесказанное простейшим примером — случаем $s = 4$.



Данный пример наглядно демонстрирует, что коэффициенты стоящие при графах в конечной формуле это число изоморфных графов, получающихся из базового графа путем всевозможных склеек.

Предположим, что для интересующего нас числа s формула для модифицированного следа нам известна. Пусть требуется для заданного графа G с матрицей смежности A определить значение $\mathcal{C}_s(G)$. Оставим пока в стороне вопрос о вычислении величин $H_i(A)$, поскольку основная сложность алгоритма обусловлена скоростью роста числа слагаемых $N(s)$ формуле (5) при возрастании значения s.

Грубые оценки дают экспоненциальный рост функции $N(s)$, что приводит к выводу о практической бесполезности предлагаемого подхода. Этот вывод изначально вполне очевиден в силу сложности рассматриваемой задачи. Однако, если ограничить класс рассматриваемых графов, то ситуация может измениться.

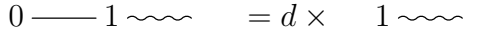
Действительно, совсем не обязательно получать универсальную формулу для $\mathcal{C}_s$, а затем применять ее к рассматриваемому классу графов. Можно использовать свойства графа уже в процессе вывода формулы, что, возможно, значительно сократит вычисления. Основная задача, которую мы здесь ставим — сократить количество формальных графов, фигурирующих в формуле (5). Разумеется, получившаяся формула будет иметь не универсальный характер и будет применима только к данному классу графов.

Формула для специальных классов графов

Если граф G принадлежит к специальному классу, то возможно, что некоторые слагаемые в формуле (5) дают нулевой вклад. Ниже мы рассмотрим несколько таких классов и приведем без доказательства влияния их свойств на вид универсальной формулы.

Регулярные графы

Утверждение 1. Для регулярных графов со степенью вершин d в формальных графах можно удалить все вершины степени 1 и инцидентные им ребра[3]:

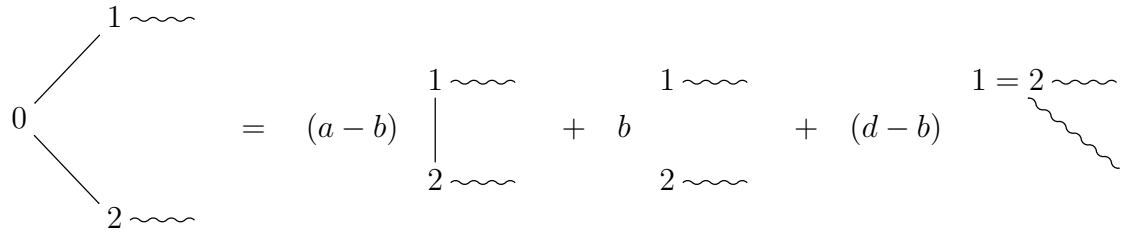


Сильно регулярные графы

Сильно регулярный граф характеризуется следующим набором параметров: (n, d, a, b), где n — число вершин, d — общая для всех вершин степень, a — количество вершин,

смежных двум смежным вершинам, b — количество вершин, смежных двум не смежным вершинам.

Утверждение 2. Для сильно регулярных графов с параметрами (n, d, a, b) в формальных графах можно удалить все вершины степени 2 и инцидентные им ребра:



Используя Утверждения 1 и 2, нетрудно получить:

$$
\begin{aligned}
\mathcal{C}_3(G) &= nda/6; \qquad \mathcal{C}_4(G) = n(d + a^2d - bd - abd - d^2 + bd^2)/8;\\
\mathcal{C}_5(G) &= n(5ad + a^3d - 2abd - 2a^2bd + b^2d + ab^2d - 3ad^2 - bd^2 + abd^2 - b^2d^2 + bd^3)/10;\\
\mathcal{C}_6(G) &= n(4d - 4ad + 15a^2d + a^4d - 6bd - 6abd - 3a^2bd - 3a^3bd + b^2d + 4ab^2d +\\
&\quad +3a^2b^2d - b^3d - ab^3d - 6d^2 - 6a^2d^2 + 10bd^2 + 2abd^2 + a^2bd^2 - 2ab^2d^2 +\\
&\quad +b^3d^2 + 2d^3 - 5bd^3 + abd^3 - b^2d^3 + bd^4)/12;
\end{aligned}
$$

Гипотеза. *Пусть G — сильно регулярный граф, тогда $\mathcal{C}_s(G)$ — полиномиальная функция степени s от параметров графа.*

Если высказанная выше гипотеза верна, то $\mathcal{C}_s$ — полином от параметров сильно регулярных графов, состоящий из $O(s^4)$ слагаемых, т.е. задача вычисления числа простых циклов полиномиальна от длины цикла. В частности, проблема гамильтоновости сильно регулярного графа имеет полиномиальную сложность.

Двудольные графы

Утверждение 3. Для двудольных графов из универсальной формулы можно удалить формальные графы, содержащие циклы нечетной длины [4].

Графы, с ограниченной степенью вершин

Утверждение 4. Если степень вершин графа не превосходит числа d, то из универсальной формулы можно исключить все формальные графы, содержащие вершины степени больше чем d.

Сложность вычисления числа $\mathcal{C}_s(G)$ для таких графов оценивается как $O(s^d)$.

Следствие 1. Если степень вершин графа не превосходит числа d, то задача вычисления числа гамильтоновых циклов полиномиальна.

Для иллюстрации приведем таблицу.

s	$N(s)$	$N_3(s)$	$N_4(s)$
5	3	3	3
6	10	9	10
7	12	9	12
8	35	24	34
9	58	28	53
10	160	67	141
11	341	90	275
12	954	205	718
13	2437	316	1644

Здесь $N_d(s)$ — количество формальных графов в универсальной формуле, не содержащих вершин степени больше, чем d.

Список литературы

[1] Березина Л.Ю. Графы и их применение. – М.: Просвещение, 1979. – 144 с.

[2] Оре О. Графы и их применение. – М.: Мир, 1965. – 175 с.

[3] Cameron P.J., Van Lint J.H. Graph theory, Coding Theory and Block Design. – Cambridge: Cambridge University Press (London Mathematical Society Lecture Note Series 19), 1980. – 140 с.

[4] Меличев В.А., Мельничков О.И., Сарванов В.И., Тышкевич Р.И. Лекции по теории графов. – М.: Наука, 1990. – 384 с.

УДК 512.7

АСИМПТОТИЧЕСКАЯ ПЛОТНОСТЬ СОВМЕСТНЫХ УРАВНЕНИЙ НАД СВОБОДНОЙ ПОЛУРЕШЕТКОЙ

М. А. Вахрамеев[2]
Институт математики им. С. Л. Соболева СО РАН (Омский филиал)
г. Омск

Генерация случайных алгебраических объектов и изучение их свойств является одним из значимых направлений современной математики. Порождение случайных групповых уравнений рассматривалось в работах [1-4]. В данных работах изучалась асимптотическая плотность множества совместных уравнений над различными классами групп. С помощью работ [5-6] понятие уравнения можно определить не только для группы, но и для произвольной алгебраической системы функционального языка. Таким образом, проблему вычисления асимптотической плотности множества совместных уравнений можно сформулировать не только для групп, а для многих классов алгебраических систем.

В данной работе изучаются уравнения над свободной полурешеткой и вычисляется асимптотическая плотность множества совместных уравнений от произвольного числа переменных. Было доказано, что асимптотическая плотность (относительно некоторой естественной стратификации) множества совместных уравнений от m переменных равна $1 - \frac{2}{3^m}$.

Список литературы

[1] Gilman R., Myasnikov A., Roman'kov V. *Random equations in nilpotent groups* // Journal of Algebra. – 2012. – Т. 352. – № 1. – С. 192–214.

[2] Gilman R., Myasnikov A., Roman'kov V. *Random equations in free groups* // Groups, Complexity, Cryptol.. – 2011. – Т. 3. – № 2. – С. 257–284.

[3] Antolin Y., Ciobanu L., Viles N. *On the asymptotics of visible elements and homogeneous equations in surface groups* // Groups Geom. Dyn.. – 2012. – V. 6. – № 4. – P. 619–638.

[4] Меньшов А.В. *Случайные системы уравнений в свободных абелевых группах* // Сиб. матем. журн.. – 2014. – Т. 55. – № 3. – С. 540–552.

[5] Daniyarova E., Miasnikov A., Remeslennikov V. *Unification theorems in algebraic geometry* // Algebra and Discrete Mathematics. – 2008. – V. 1. – P. 80–112.

[6] Даниярова Э.Ю., Мясников А.Г., Ремесленников В.Н. *Алгебраическая геометрия над алгебраическими системами. II. Основания* // Фундаментальная и прикладная математика. – 2012. – Т. 17. – № 1. – С. 65–106.

[2] vahrmih@yandex.ru

УДК 515.122.4; 514.1

О СРЕДНИХ ЗНАЧЕНИЯХ ОБЪЕМОВ УЗЛОВЫХ МНОЖЕСТВ РАЗЛИЧНЫХ ИНВАРИАНТНЫХ СЛУЧАЙНЫХ ПОЛИНОМОВ

В. М. Гичев[3]
Институт математики им. С. Л. Соболева СО РАН (Омский филиал)
г. Омск

Пусть M — изотропно неприводимое однородное риманово многообразие компактной группы Ли G, E — конечномерное G-инвариантное пространство гладких функций на M, в котором задана вероятностная мера σ. Будем называть функции из E полиномами, а меру σ считать G-инвариантной. Риманов объем множества нулей полинома из E является случайной величиной, математическое ожидание которой зависит от σ, но слабо: оно однозначно определяется евклидовой структурой $L^2(\sigma)$ в E. Точнее, G-инвариантное скалярное произведение задает эквивариантное погружение M в единичную сферу $S \subset E$, которое является локальным метрическим подобием, от коэффициента которого (и только от него при фиксированном M) зависит средний объем. Все возможные варианты можно получить, выбирая в качестве σ стандартную (нормализованную) меру на S или же гауссовскую меру с плотностью $\pi^{-\frac{d}{2}} e^{-|u|^2}$ на E, где $d = \dim E$. Более того, если E неприводимо, то коэффициент (обозначим его через s) от σ не зависит, а если $E = E_1 \oplus \cdots \oplus E_k$, где компоненты G-инвариантны и неприводимы, то $s^2 = \sum_{j=1}^k \nu_j s_j^2$, где s_j отвечает E_j, $\nu_j > 0$ и $\sum_{j=1}^k \nu_j = 1$.

Пусть P_n — пространство однородных вещественных полиномов степени n на сфере $S^m = \mathrm{SO}(m+1)/\mathrm{SO}(m)$. В нем можно задать скалярное произведение соотношением $|x^\alpha|^2 = \alpha!$ для мономов x^α и условием ортогональности различных мономов (модель Костлана–Шуба–Смейла). Другая евклидова структура наследуется из пространства $L^2(S^m)$. Средние объемы для них имеют порядок $\sqrt{n}$ и n (это следует из результатов [1] и [2] соответственно). Неприводимые компоненты — пространства сферических гармоник степеней той же четности, что и n. Коэффициенты ν_j для модели Костлана–Шуба–Смейла имеют острый пик вблизи $\sqrt{(m-1)n}$. Видимо, это означает, что компоненты степеней порядка $\sqrt{n}$ вносят основной вклад в результат, однако механизм этого пока неясен.

Список литературы

[1] Kostlan E. *On the distribution of roots of random polynomials*// In: *From Topology to Computation: Proceedings of the Smalefest.* – New York: Springer–Verlag, 1993. – P. 419–431.

[2] Gichev V.M. *Metric properties in the mean of polynomials on compact isotropy irreducible homogeneous spaces*// Analysis and Mathematical Physics. –V. 3. –№ 2. – P. 119–144.

[3] gichev@ofim.oscsbras.ru

УДК 003.26

КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ ПРОТОКОЛА АУТЕНТИФИКАЦИИ УШАКОВА-ШПИЛЬРАЙНА, ОСНОВАННОГО НА ПРОБЛЕМЕ БИНАРНО СКРУЧЕННОЙ СОПРЯЖЕННОСТИ[4]

М.Н. Горнова, Е.Г. Кукина, В.А. Романьков[5]
Омский государственный университет им. Ф.М. Достоевского,
г. Омск

Введение

Приводится криптографический анализ протокола аутентификации Ушакова-Шпильрайна, базирующегося на проблеме бинарно скрученной сопряженности относительно пары эндоморфизмов полугруппы 2×2-матриц над кольцом срезанных многочленов с коэффициентами из поля $\mathbf{F}_2$.. Показано, что закрытый ключ протокола может быть вычислен путём решения системы линейных уравнений над полем $\mathbf{F}_2$. Представлена теоретическая оценка сложности данного криптографического анализа и практические результаты, полученные с помощью подготовленной программы. Показано, что предложенный протокол аутентификации является теоретически и практически нестойким.

В современной алгебраической криптографии примитивы, схемы, протоколы и системы строятся на алгебраических структурах (платформах). Наиболее развита в этом смысле криптография на бесконечных группах, относительно которой см. монографии [1] и [2]. Предположения секретности при этом, как правило, базируются на трудноразрешимых и неразрешимых алгоритмических проблемах. Среди последних чаще всего фигурирует проблема сопряженности, но также встречаются схемы, использующие проблемы равенства, вхождения и т.п. Анализ таких схем ведётся с точки зрения теории сложности. При этом кроме классического понятия "сложности в худшем случае" используются понятия "сложности в среднем" и "генерической сложности". См. по этому поводу [1]-[4].

В настоящей работе рассматривается протокол аутентификации из [5], для которого в качестве платформы предлагается использовать полугруппу 2×2-матриц над срезанными многочленами от одной переменной над полем $\mathbf{F}_2$, состоящим из двух элементов. В качестве базовой трудноразрешимой проблемы фигурирует проблема бинарно скрученной сопряженности. Перейдём к определениям.

Пусть G – группа, φ – её эндоморфизм. Говорят, что элементы $u, v \in G$ *скрученно сопряжены* относительно φ, или, более кратко, *φ-сопряжены*, если существует элемент $x \in G$ такой, что выполняется равенство

$$\varphi(x)u = vx.$$

Легко проверить, что свойство быть *φ-сопряжёнными* является отношением эквивалентности на основном множестве группы G. Понятие скрученной сопряженности обобщает понятие сопряженности, соответствующее тождественному эндоморфизму $\varphi = id$. Его появление в начале 20-го столетия мотивировано топологической теорией фиксированных точек отображений Нильсена-Райдемайстера. Впоследствии это понятие нашло

[4]Работа выполнена при финансовой поддержке РФФИ (проект 15-41-04312
[5]romankov48@mail.ru

своё применение в различных областях математики: теории представлений бесконечных групп, теории динамических систем, алгебраической геометрии и т.п. Свойство скрученной сопряженности интересно и с чисто алгебраической точки зрения. См. по этому поводу [6]–[11]. Имеются попытки использования понятия скрученной сопряженности для алгебраических приложений. В данной работе мы рассмотрим одну из таких попыток из [5], в которой фигурирует даже более общее понятие бинарно скрученной сопряженности, к изложению которого мы сейчас переходим.

Пусть G – группа, φ, ψ – её эндоморфизмы. Говорят, что элементы $u, v \in G$ *скручено сопряжены* относительно φ, ψ, или, более кратко, φ, ψ-*сопряжены*, если существует элемент $x \in G$ такой, что выполняется равенство

$$\varphi(x)u = v\psi(x).$$

.

Свойство быть φ, ψ-*сопряжёнными* также является отношением эквивалентности на основном множестве группы G. Понятие бинарно скрученной сопряженности обобщает понятие скрученной сопряженности, в котором энодоморфизм φ произвольный, а ψ тождественный

В криптографии на бесконечных группах предположения секретности обычно связывают с *поисковой алгоритмической проблемой*. Считается, что трудноразрешимым алгоритмическим проблемам для данной группы соответствуют трудноразрешимые поисковые алгоритмические проблемы. Нахождение и интерпретация таких проблем и соответствующих групп является одной из основных проблем криптографии на бесконечных группах. В этой связи следует заметить, что в [4] и [12] приведены многочисленные примеры раскрытия передаваемых секретных сообщений без вычисления закрытых ключей шифрования, т.е. без решения поисковых алгоритмических проблем, на трудности решения которых базируются предположения секретности. Это заставляет пересмотреть общее мнение о построении систем такого вида. Дальнейший криптографический анализ, основанный на разработанном в [4] методе линейного разложения, можно найти в [13]-[15].

В [5] в качестве платформы для построения протокола аутентификации предлагается использовать полугруппу 2×2-матриц над кольцом K_n n-срезанных многочленов от одной переменной x с коэффициентами из поля $\mathbf{F}_2$ порядка 2. Здесь n – натуральное число. Более точно $K_n = \mathbf{F}_2[x]/I_n$ означает фактор кольцо кольца многочленов $\mathbf{F}_2[x]$ по идеалу $I_n = ideal(x^n)$, порождённому элементом x^n. Произвольный элемент $f(x)$ кольца K_n однозначно записывается в виде $a_0 + a_1x + ... + a_{n-1}x^{n-1}$. Сложение таких нормальных форм обычное, умножение отличается от обычного тем, что все степени x^k при $k \geq n$ равны нулю в K_n, поэтому они не фигурируют в нормальной форме.

Протокол аутентификации Ушакова-Шпильрайна

В этом разделе приводится описание одного раунда протокола аутентификации Ушакова-Шпильрайна из [5]. Подобно классической схеме Фиата-Шамира предполагается k-кратное повторение раундов при одной сессии аутентификации. В каждом из этих раундов вероятность правильного прохождения при незнании секретного ключа равна $1/2$. Значит, вероятность прохождения при незнании секретного ключа в k последовательных раундах не более, чем $(1/2)^k$.

Предположим, что один из корреспондентов, скажем, Алиса, доказывает своё право на аутентификацию, а другой, назовём его Боб, осуществляет проверку её права на аутен-

тификацию. При этом они открыто договариваются о выборе полугруппы G в качестве платформы для протокола аутентификации и двух эндоморфизмов φ и ψ полугруппы G, участвующих в установке этого протокола.

- Алиса выбирает в качестве закрытого ключа элемент s полугруппы G. Затем она выбирает элемент $w \in G$ и вычисляет $t = \psi(s^{-1})w\varphi(s)$. Открытым ключом Алисы служит пара (t, w).

- При очередной сессии аутентификации Алиса выбирает сессионный закрытый ключ r, с помощью которого она вычисляет $u = \psi(r^{-1})t\varphi(r)$, после чего посылает u Бобу.

- Боб выбирает с вероятностью $1/2$ один из битов $b = 0$ или $b = 1$ и посылает его Алисе.

- Если Алиса получает $b = 0$, она должна отправить Бобу сессионный ключ $v = r$. При его получении Боб проверяет выполнимость равенства $u = \psi(v^{-1})t\varphi(v)$. Условием прохождения раунда является справедливость этого равенства.

  Если Алиса получает $b = 1$, она должна вычислить и отправить Бобу элемент $v = sr$. При его получении Боб проверяет выполнимость равенства $u = \psi(v^{-1})w\varphi(v)$. Условием прохождения раунда является справедливость этого равенства.

Непосредственно проверяется, что при правильном элементе v указанные равенства действительно справедливы. В то же время любой, кто захочет выдать себя за Алису, сможет это сделать в случае, если угадает значение ответного бита Боба.

Действительно, если он угадает ответ $b = 0$, то ему достаточно выбрать произвольный ключ r, а затем вычислить и передать элемент $u = \psi(r^{-1})t\varphi(r)$. При угаданном ответе $b = 0$ передается $v = r$. Но если ответом будет 1, необходимо будет передать элемент $v = rs$, что равносильно раскрытию закрытого ключа s.

Если обманщик угадает ответ $b = 1$, он также может успешно завершить данный раунд процесса аутентификации. Для этого он должен выбрать любой элемент $z \in G$, вычислить и передать Бобу элемент $u = \psi(z^{-1})w\varphi(z)$. При ответе $b = 1$ он просто отправляет Бобу элемент $v = z$ и таким образом проходит проверку. Но при ответе $b = 0$ ему для прохождения проверки нужно будет передать такой элемент v, что будет выполнено равенство $u = \psi(v^{-1})t\varphi(v)$. Подходит элемент $v = s^{-1}z$, знание которого позволяет раскрыть s.

Криптостойкость приведённого выше протокола обеспечивается трудноразрешимостью проблемы бинарно скрученной сопряженности в выбранной полугруппе G. Действительно, если кому-либо удалось бы найти по элементам t и w закрытый ключ s, то таким образом был бы раскрыт весь протокол. Если по элементам u и t удалось бы вычислить сессионный ключ r, то при ответе $b = 1$ также удалось бы вычислить закрытый ключ s.

Заметим, что достаточно было бы вычислить такой элемент s', для которого выполнено равенство $t = \psi(s')w\varphi(u)$. С помощью s' также можно проходить аутентификацию, как и с оригинальным закрытым ключом s. Если вычислить элемент $r' \in G$ такой, что $\psi(r')t\varphi(r') = u$, то можно, зная sr, определить элемент $s' = (sr)(r')^{-1}$. Тогда

$$\psi((s')^{-1})w\varphi(s') = \psi(r'r^{-1})(\psi(s)w\varphi(s))\varphi(r(r')^{-1}) =$$
$$= \psi(r')(\psi(r^{-1}t\varphi(r)\varphi((r')^{-1}) = \psi(r')u\varphi((r')^{-1}) = t.$$

Тогда s' также играет роль закрытого ключа s. Вычислить s' можно наблюдая передаваемый Алисой элемент $v = sr$ при ответе Боба $b = 1$.

В [5] в качестве платформы протокола предлагается использовать полугруппу G всех 2×2-матриц над кольцом срезанных многочленов K_n, где n – число порядка 300. Любое отображение $\phi : K_n \to K_n$, для которого $\phi(x) = h$, где $h = h(x)$ – многочлен с нулевым свободным членом, однозначно продолжается до эндоморфизма кольца K_n, рассматриваемого как алгебра над $\mathbf{F}_2$. Обозначим такой эндоморфизм через ϕ_h. Действительно, $\mathbf{F}_2[x]$ – свободная коммутативная ассоциативная алгебра над $\mathbf{F}_2$ размерности один со свободным порождающим x. Поэтому любое отображение $x \mapsto h$, где h – произвольный многочлен из $\mathbf{F}_2[x]$, однозначно продолжается до ее эндоморфизма. Если h – многочлен с нулевым свободным членом, то идеал I_n инвариантен относительно этого эндоморфизма. В этом случае данный эндоморфизм индуцирует эндоморфизм ϕ_h кольца K_n. Любой эндоморфизм кольца K_n естественным образом распространяется на полугруппу G, действуя соответствующим образом на элементы матриц. В [5] в качестве фигурирующих в протоколе аутентификации φ и ψ предлагается выбирать соответствующие распространения на G эндоморфизмов кольца K_n вида ϕ_h, где $h \in K_n$ имеет нулевой свободный член. Для этих распространений сохраняются обозначения ϕ_h.

Криптографический анализ протокола аутентификации Ушакова-Шпильрайна

Рассмотрим уравнение

$$t = \psi(s^{-1})w\varphi(s),$$

в котором неизвестной является матрица $s = (s(ij)), s(ij) \in K_n, i, j = 1, 2$. Считаем, как это предлагается авторами протокола в [5], что каждый из эндоморфизмов ψ и φ имеет вид ϕ_h для соответствующих многочленов без свободных членов $h \in K_n$, как это объяснено выше. Умножим уравнение слева на $\psi(s)$. В результате получим равносильное уравнение

$$\psi(s)t = w\varphi(s).$$

Запишем элементы матрицы s в нормальной форме с неопределенными коэффициентами из поля $\mathbf{F}_2$:

$$s(ij) = s(ij)_0 + s(ij)_1 x + ... + s(ij)_{n-1} x^{n-1}.$$

Применив к матрице s эндоморфизмы φ и ψ, получим равносильную систему линейных уравнений от $4n$ переменных $s(ij)_l$ $(i, j = 1, 2; l = 0, 1, ..., n-1)$ над полем $\mathbf{F}_2$. Остается найти такое решение данной системы линейных уравнений, для которого соответствующая ему матрица s будет обратимой. Значительно облегчает эту задачу то обстоятельство, что матрица s обратима тогда и только тогда, когда обратима матрица s_1, являющаяся образом s относительно гомоморфизма специализации, при котором x отображается в 1. Действительно, имеется всего 4 обратимых 2×2 матрицы над $\mathbf{F}_2$. Следовательно, достаточно рассмотреть четыре различных случая и хотя бы в одном из них найти решение s, которое уже будет обратимым.

Список литературы

[1] Myasnikov A., Shpilrain V., Ushakov A. Group-based cryptography. (Advances courses in Math., CRM, Barselona). – Basel-Berlin-New York: Birkhäuser Verlag, 2008, – 183 p.

[2] Myasnikov A., Shpilrain V., Ushakov A. Non-commutative cryptography and complexity of group-theoretic problems. (Amer. Math. Soc. Surveys and Monographs). – Providence R.I.: Amer. Math. Soc., 2011, – 385 p.

[3] Романьков В.А. *Диофантова криптография на бесконечных группах*// Прикладная дискретная математика. – 2012. – № 2(16). – С. 15–42.

[4] Романьков В.А. Алгебраическая криптография. – Омск: ОмГУ, 2013. –135 с.

[5] Shpilrain V., Ushakov A. *An autentication scheme based on the twisted conjugacy problem*// In: *ACNS 2008, Lecture Notes Comp. Sc.,* – V. 5037, – 2008. – P. 366–372.

[6] Fel'shtyn A., Troitsky E. *Twisted Burnside-Frobenius theory for discrete groups*// J. Reine Angew. Math. – 2007. – V. 613. – P. 193–210.

[7] Goncalves D., Wong P. *Twisted conjugacy classes in nilpotent groups*// J. Reine Angew. Math. – 2009. – V. 633. – P. 11–27.

[8] Roman'kov V. *The twisted conjugacy problem in polycyclic groups*// J. Group Theory. – 2010. –V. 13. – №3. – P. 353–364.

[9] Вентура Э., Романьков В.А. *Проблема скрученной сопряжённости для эндоморфизмов метабелевых групп*// Алгебра и логика. – 2009. – V. 48. –№ 2. – С. 157–173.

[10] Roman'kov V. *Twisted conjugacy classes in nilpotent groups*// J. Pure and Applied Algebra – 2011. –V. 215. –№ 4. – P. 664–671.

[11] Fel'shtyn A., Goncalves D.L. *Reidemeister spectrum for metabelian groups*// International Journal of Algebra and Computation. –2011. – V. 21. –№ 3. – P. 1–16.

[12] Романьков В.А. *Криптографический анализ некоторых схем шифрования, использующих автоморфизмы*// Прикладная дискретная математика. –2013. – №3 (21). – С. 36–51.

[13] Roman'kov V., Myasnikov A. *A linear decomposition attack*// Groups-Complexity-Cryptology. – 2015. – V. 7. – № 1. – P. 81–94.

[14] Roman'kov V. *A polynomial time algorithm for the braid double shielded public key cryptosystem*// arXiv: 1412.5277v1 [math. GH] 17 Dec. 2014.

[15] Roman'kov V. *Linear decomposition attack on public key exchange protocols using semidirect products of (semi)groups*// arXiv: 1501.0052v1 [math. CR] 6 Jan. 2015.

УДК 512.7

АЛГЕБРАИЧЕСКАЯ ГЕОМЕТРИЯ НАД СВОБОДНОЙ МЕТАБЕЛЕВОЙ АЛГЕБРОЙ ЛИ[6]

Э. Ю. Даниярова[7]
Институт математики им. С. Л. Соболева СО РАН (Омский филиал),
г. Омск

Пусть F_r — свободная метабелева алгебра Ли ранга $r \geqslant 2$ над полем k, $\mathrm{char}(k) \neq 2$. Поставим задачу построения алгебраической геометрии над F_r как над алгебраической системой языка $\mathtt{L} = \{+^{(2)},\ \circ^{(2)},\ \{k_\alpha^{(1)} \mid \alpha \in k\},\ c_a, a \in F_r\}$ с естественной интерпретацией операций сложения, лиева умножения, умножения на коэффициенты поля k и константных символов, соответствующих всем элементам из F_r.

Напомним, что основной задачей алгебраической геометрии является задача классификации алгебраических множеств с точностью до изоморфизма, что эквивалентно классификации координатных алгебр алгебраических множеств. Алгебра F_r нётерова по уравнениям, а в этом случае выделяется задача классификации неприводимых алгебраических множеств (и/или неприводимых координатных алгебр), поскольку произвольное алгебраическое множество представимо в виде конечного объединения неприводимых, причём это представление однозначно с точностью до перестановки неприводимых компонент и исключения лишних. Стандартно структурное описание неприводимых координатных алгебр удобно получать параллельно с их описанием на языке универсальных аксиом в силу следующей теоремы.

Теорема 1 [1]. *Для любой конечно порождённой F_r-алгебры Ли A над полем k следующие условия эквивалентны:*

1. *Алгебра A является координатной алгеброй некоторого неприводимого алгебраического множества над F_r.*
2. *$A \in F_r - \mathrm{ucl}(F_r)$.*
3. *Алгебра A F_r-дискриминируется алгеброй F_r.*

Согласно этой теореме, для классификации неприводимых координатных алгебр над F_r, нужно найти свойства алгебры F_r, записывающиеся универсальными предложениями языка $\mathtt{L}$, обладая которыми конечно порождённая F_r-алгебра Ли будет дискриминироваться алгеброй F_r. Пути такого поиска приводят к развилке: случай конечного основного поля k и случай бесконечного k существенно различаются. Для конечного поля k была доказана следующая теорема.

Теорема 2 [2]. *Для произвольной конечно порождённой F_r-алгебры Ли A над конечным полем k следующие условия эквивалентны:*

1. *A является координатной алгеброй некоторого неприводимого алгебраического множества над F_r.*

[6]Работа выполнена при финансовой поддержке РФФИ (проект 14-01-00068-а)
[7]evelina.omsk@list.ru

2. *A удовлетворяет списку универсальных аксиом Φ_r языка* $\mathtt{L}$.

3. *радикал Фиттинга* $\mathrm{Fit}(A)$

   - *абелев,*
   - *имеет коразмерность r:* $\dim A/\mathrm{Fit}(A) = r$,
   - *как модуль над кольцом многочленов $R = k[x_1, \ldots, x_r]$ не имеет кручения,*
   - *подмодуль* $\mathrm{Fit}(F_r)$ *выделяется в* $\mathrm{Fit}(A)$ *прямым слагаемым;*

4. *A F_r-изоморфна алгебре $F_r \oplus M$ для некоторого конечно порождённого модуля без кручения M над кольцом многочленов $R = k[x_1, \ldots, x_r]$.*

Таким образом, если поле k конечно, то произвольная неприводимая координатная алгебра над F_r получается из F_r с помощью операции расширения радикала Фиттинга путём прямого присоединения некоторого модуля M без кручения над кольцом многочленов R. Если же поле k бесконечно, то в радикале Фиттинга неприводимой координатной алгебры над F_r появление кручения возможно, причём в качестве такого кручения может выступать радикал любого проективного многообразия над полем k.

Теорема 3. *Для произвольной конечно порождённой F_r-алгебры Ли A над бесконечным полем k следующие условия эквивалентны:*

1. *A является координатной алгеброй некоторого неприводимого алгебраического множества над F_r.*

2. *A удовлетворяет списку универсальных аксиом Φ_r^∞ языка* $\mathtt{L}$.

3. *радикал Фиттинга* $\mathrm{Fit}(A)$

   - *абелев,*
   - *как модуль над кольцом многочленов $R_{F_r} = k[x_1, \ldots, x_r]$ не имеет кручения,*
   - *как модуль над кольцом многочленов R_A либо не имеет кручения, либо имеет такое кручение, что аннуляторы всех его ненулевых элементов совпадают и равны радикалу I некоторого невырожденного проективного многообразия над полем k,*
   - *в каждом конечно порождённом R_{F_r}-подмодуле* $\mathrm{Fit}(F_r) \subseteq M \subseteq \mathrm{Fit}(A)$ *подмодуль* $\mathrm{Fit}(F_r)$ *выделяется прямым слагаемым,*
   - *любые R_{F_r}-независимые элементы из* $\mathrm{Fit}(F_r)$ *являются R_A/I-независимыми в* $\mathrm{Fit}(A)$.

Список литературы

[1] Даниярова Э. Ю., Мясников А. Г., Ремесленников В. Н., *Алгебраическая геометрия над алгебраическими системами II: Основания* // Фундаментальная и прикладная математика. – 2012. – Т. 17. – № 1. – С. 65–106.

[2] Даниярова Э. Ю., Казачков И. В., Ремесленников В. Н., *Алгебраическая геометрия над свободной метабелевой алгеброй Ли II: Случай конечного поля* // Фундаментальная и прикладная математика. – 2003. – Т. 9. – № 3. – С. 65–87.

УДК 519.85

ПРИБЛИЖЕННОЕ РЕШЕНИЕ ЗАДАЧИ УПРАВЛЕНИЯ ПОСТАВКАМИ

А. В. Еремеев[8]
Институт математики им. С. Л. Соболева СО РАН (Омский филиал)
г. Омск

В настоящей работе приводится обзор алгоритмов с гарантированной оценкой точности для приближенного решения задачи управления поставками. Рассматриваемая задача состоит в минимизации стоимости доставки продукции от множества поставщиков до одного потребителя. При этом допустимый размер каждой открытой поставки ограничен снизу и сверху, а суммарный размер потребления ограничен снизу. Задача имеет следующую формальную постановку.

$$\min \quad \sum_{i=1}^{m} c_i(x_i),$$

$$\sum_{i=1}^{m} x_i \geq A,$$

$$x_i \in \{0\} \cup [l_i, u_i], \ i = 1, ..., m.$$

Здесь m – число поставщиков; A – минимальное количество продукта, требуемое потребителю; l_i – минимальное количество продукта, которое поставщик i готов доставить потребителю; u_i – максимальное общее количество продукта, которое поставщик i может доставить. Переменными являются объемы поставок x_i от поставщика i, $i = 1, \ldots, m$, а стоимости доставки продукции от поставщика i выражены функциями $c_i(\cdot)$, $i = 1, \ldots, m$. Предполагается, что функции $c_i(\cdot)$ эффективно вычислимы.

Поставленная задача представляет собой задачу математического программирования с несвязной областью допустимых решений и является NP-трудной, т.к. к ней полиномиально сводится задача РАЗБИЕНИЕ (см., например, [3]).

В [2] для случая вогнутых неубывающих функций функций $c_i(\cdot)$ на $[0, u_i]$, $i = 1, \ldots, m$, предложен 2-приближенный жадный алгоритм трудоемкости $O(m^2)$. В [3] построена вполне полиномиальная аппроксимационная схема (FPTAS), пригодная для непрерывных функций $c_i(\cdot)$, $c_i(l_i) = \Omega(1)$, $i = 1, \ldots, m$, и основанная на подходе, изложенном в [5]. Несколько позднее близкая по свойствам FPTAS была разработана в [4]. Во многих случаях оценка трудоемкости алгоритма [4] оказывается ниже соответствующей оценки алгоритма из [3].

В [1] предложен $(1 + \varepsilon)$-приближенный алгоритм для случая, когда объем поставки от каждого поставщика принадлежит объединению конечного числа отрезков, а функции стоимости поставок являются вогнутыми и неубывающими в пределах каждого из допустимых интервалов. Упомянутые выше FPTAS из работ [3] и [4] имеют на порядок бóльшую трудоемкость относительно величины $1/\varepsilon$ по сравнению со схемой, предложенной в [1].

[8]eremeev@ofim.oscsbras.ru

Список литературы

[1] Еремеев А.В., Ковалев М.Я., Кузнецов П.М. *Приближенное решение задачи управления поставками со многими интервалами и вогнутыми функциями стоимости*// Автомат. и телемех. – 2008. – № 7. – С. 90–97.

[2] Еремеев А.В., Романова А.А., Сервах В.В., Чаухан С.С. *Приближенное решение одной задачи управления поставками*// Дискретный анализ и исследование операций. Сер. 2. – 2006. – Т. 13. – № 1. – С. 27–39.

[3] Chauhan S.S., Eremeev A.V., Romanova A.A., Servakh V.V., Woeginger G.J. *Approximation of the supply scheduling problem* // Oper. Res. Lett. – 2005. – V. 33. – N 3. – P. 249–254.

[4] Ng C.T., Kovalyov M.Y., Cheng T.C.E. *An FPTAS for a supply scheduling problem with non-monotone cost functions*// Naval Res. Logistics. – 2008. – V. 55. – P. 194–199.

[5] Woeginger G.J. *When does a dynamic programming formulation guarantee the existence of a fully polynomial time approximation scheme (FPTAS)?* // INFORMS J. Comput. – 2000. – V. 12. – № 1. – P. 57–74.

УДК 004.056.55; 003.26

ГЕНЕРАЦИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ НА ОСНОВЕ ПОДПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ КОМПЬЮТЕРНЫХ СИСТЕМ[9]

А.В. Еременко[10], В.Б. Майков, К.О. Ступко, О.Е. Мироненко
Омский государственный университет путей сообщения,
г. Омск

Существует множество способов идентификации личности. Одним из таких способов является идентификация личности по почерку и динамике подписи. Подпись – это уникальный атрибут человека, как и его физиологические характеристики. Современный уровень технологий позволяет злоумышленникам создавать из отпечатка пальца муляж, который будет принят системой сканирования за «живой» образец, а также подделывать другие физиологические признаки. Преимуществом подписи или рукописного пароля является невозможность предъявления и изготовления «муляжа», системы идентификации личности по рукописным паролям и автографу удобны и перспективны [1]. Однако актуальной остается проблема защиты биометрического эталона пользователя, хранящегося на удаленном сервере. Каким образом можно защитить конфиденциальную информацию биометрическими методами, обеспечив при этом защищенность биометрических данных? Вариант решения обозначенной выше проблемы рассмотрен в [2]. Решение заключается в получении из биометрических данных пользователей криптографических ключей, что позволяет объединить преимущества от использования биометрических технологий и криптографических методов, а также защитить биометрические данные пользователей при выполнении сервисных процедур.

В настоящей работе предлагается способ освобождения криптографических ключей, основанный на методе из работы [2], а также использовании статических и динамических характеристик подписи субъекта.

Для проведения исследований была собрана база, состоящая из подписей двадцати человек. Рассмотрим подпись в системе координат, где x, y – координаты подписи, p – давление пера на планшет. Далее необходимо выделить признаки, на основе которых может быть сгенерирован криптографический ключ.

Расстояние между двумя точками на плоскости не изменяется при их синхронном сдвиге и повороте. Это свойство можно использовать при построении инвариантов контурных образов на бинарных отображениях. Рассматриваемый здесь класс инвариантов вычисляется как расстояния между координатами контурного образа.

Весь процесс вычисления инварианта, основанного на матрице расстояний, можно разделить на этапы:

1. Отбросим начальные и конечные значения всех точек с нулевым давлением.

2. Произведем одномерное преобразование Фурье для x, y и p.

[9]Работа выполнена при финансовой поддержке РФФИ (проект 15-07-09053)
[10]nexus-@mail.ru

3. Произведем обратное преобразование Фурье, учитывая, что размерность на выходе должна соответствовать числу, которое является ближайшим меньшим кратным степени 2.

4. Вычисляем шаг: $h = \frac{N}{R_h}$, где N – количество точек после обратного преобразования Фурье, R_h – желаемая размерность матрицы кратная степени 2.

5. Вычисляем матрицу расстояний для всей совокупности координат:

$$R = \begin{pmatrix} r_{11} & \dots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{n1} & \dots & r_{nn} \end{pmatrix}, \tag{1}$$

где r_{ij} – расстояние между i-ой и j-ой координатами, вычисляемое по формуле:

$$r_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (p_i - p_j)^2}. \tag{2}$$

Поскольку при расчете получается слишком много элементов, необходимо производить вычисления с шагом h.

6. Нормируем полученную матрицу:

$$R' = \begin{pmatrix} r'_{11} & \dots & r'_{1n} \\ \vdots & \ddots & \vdots \\ r'_{n1} & \dots & r'_{nn} \end{pmatrix}, \tag{3}$$

где r'_{ij} - нормированное расстояние между i-ой и j-ой координатами.

$$r'_{ij} = \frac{r_{ij}}{r_{12} + r_{23} + ... + r_{n-1n}}. \tag{4}$$

Элементы полученной матрицы до и после нормирования будут являться признаками для идентификации подписи. После расчета матрицы необходимо рассчитать следующие характеристики подписи, которые также являются признаками:

1. Отношение длины подписи к ее ширине (это наиболее простая характеристика):

$$S = \frac{max_{i=1,\dots,n}(x_i) - min_{j=1,\dots,n}(x_j)}{max_{i=1,\dots,n}(y_i) - min_{j=1,\dots,n}(y_j)}. \tag{5}$$

2. Центр подписи, описываемый координатами C_X,C_Y и C_P. Для вычисления данной характеристики необходимо найти сумму координат по оси O_x и O_y, а потом разделить на количество точек в подписи:

$$C_X = \frac{1}{n}\sum_{i=1}^{n} x_i, C_Y = \frac{1}{n}\sum_{i=1}^{n} y_i, C_P = \frac{1}{n}\sum_{i=1}^{n} p_i. \tag{6}$$

3. Угол наклона подписи. Под углом подписи понимается – косинус среднего угла наклона ломаной траектории линии подписи к оси абсцисс:

$$Q = \frac{1}{n-1}\sum_{i=1}^{n} \frac{x_{i+1} - x_i}{\sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}}. \tag{7}$$

4. Угол наклона между центрами половин подписи. После того как был найден центр подписи C_x, разобьем множество (X,Y,Z)=$[(x_i, y_i, p_i)]$ на два подмножества: L=$[(x_i, y_i, p_i)|x_i \leq C_x]$ и R=$[((x_i, y_i, p_i)|x_i > C_x]$. Найдем центры полученных множеств L и R:

$$C_{X_L} = \frac{1}{|L|}\sum_{x_i \in L}^{n} x_i, C_{Y_L} = \frac{1}{|L|}\sum_{y_i \in L}^{n} y_i, C_{P_L} = \frac{1}{|L|}\sum_{p_i \in L}^{n} p_i, \tag{8}$$

$$C_{X_R} = \frac{1}{|R|}\sum_{x_i \in R}^{n} x_i, C_{Y_R} = \frac{1}{|R|}\sum_{y_i \in R}^{n} y_i, C_{P_R} = \frac{1}{|R|}\sum_{p_i \in R}^{n} p_i. \tag{9}$$

Для создания эталона подписи, пользователь несколько раз воспроизводит ее на графическом планшете. Из каждой реализации подписи путем указанных выше преобразований вычисляются все описанные параметры: r'_{ij}, S, C_X, C_Y, C_P, Q, C_{X_L}, C_{Y_L}, C_{P_L}, C_{X_R}, C_{Y_R}, C_{P_R}.После этого производится расчет средних значений указанных параметров по всем реализациям. Полученный вектор значений является эталоном подписи. Затем эталонные значения признаков округляются до целых и представляются в виде последовательности m бит A_m.

Далее случайным образом генерируется равномерно распределенная битовая последовательность, которая кодируется помехоустойчивым кодом Рида-Соломона с исправляющей способностью d таким образом, что на выходе получаем последовательность m бит B_m. Далее A_m и B_m складываются по модулю 2. Закодированная последовательность Z_m называется открытой строкой, данную строку можно хранить в открытом доступе [3].

При осуществлении дешифрования информации, зашифрованной на ключе Bm, пользователю необходимо ввести подпись, которая будет обработана по описанному принципу и преобразована в строку A^*_m. Данная строка будет незначительно отличаться от эталонной строки A_m, если пользователь воспроизвел свою подпись корректно. Получение одинаковых образцов подписи технически невозможно при их повторном воспроизведении. Из

Авторы	Вероятность ошибки 1-го рода	Вероятность ошибки 2-го рода	Условия тестирования
Santos et. al. [5]	57,3%	1,18%	126 испытуемых из базы данных рукописных паролей MCYTX
Maiorana and Campisi [7]	9%	9%	126 испытуемых из базы данных рукописных паролей MCYTX
Разрабатываемый способ освобождения ключа	6%	1%	Проведено 400 опытов (включая 200 попыток подделки) с участием 20 испытуемых

Таблица 1: Сравнение достигнутых показателей

Z_m при помощи операции сложения по модулю 2 «вычитается» строка A^*_m, результатом этой операции является строка B^*_m. Если количество ошибочных значений признаков не превышает исправляющей способности кода d, то применяя код, исправляющий ошибки Рида-Соломона, можно получить исходную последовательность B_m [4], и операция дешифрования будет успешной. В противном случае (при попытке подделки подписи другим пользователем) количество неверных значений признаков превысит d, и полученный ключ шифрования не будет равен Bm. Описанный способ может быть применен для защиты секретных ключей при осуществлении асимметричных алгоритмов шифрования и использовании ЭЦП.

Проведена предварительная оценка эффективности предложенного способа освобождения ключа, по результатам которой ошибки 1-ого и 2-ого рода составили 0,06 и 0,01. Сравнение полученных результатов с достигнутыми ранее приведено в таблице 1.

Список литературы

[1] Ложников П. С., Еременко А. В. *Идентификация личности по рукописным паролям* // Мир измерений. – 2009. – № 4(98). – С. 11–17.

[2] Еременко А.В., Сулавко А.Е. *Исследование алгоритма генерации криптографических ключей из биометрической информации пользователей компьютерных систем* // Информационные технологии. – 2013. – № 11. – С. 47–51.

[3] Dodis Y., Reyzin L., Smith A. *Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data* // In: *Proceedings from Advances in Cryptology. EuroCrypt.* – 2004.

[4] Morelos-Zaragoza R.H. The art of error correcting coding. John Wiley & Sons, 2006. – 320 p.

[5] Santos M. F., Aguilar J. F., Garcia J. O. *Cryptographic key generation using handwritten signature* // In: *Proceedings of SPIE, Orlando, Fla, USA, Apr. 2006.* – 2006. – V. 6202. – P. 225–231.

[6] Maiorana E., Campisi P. *Fuzzy commitment for function based signature template protection* // In: *IEEE Signal Processing Letters.* – 2010. – V. 17. – P. 249–252.

УДК 512.7; 510.6

ОБ ОБЪЕДИНЕНИИ АЛГЕБРАИЧЕСКИХ МНОЖЕСТВ В ФУНКЦИОНАЛЬНЫХ И ПРЕДИКАТНЫХ ЯЗЫКАХ

Н. П. Журавлёва[11]
Институт математики им. С. Л. Соболева СО РАН (Омский филиал),
г. Омск

Следуя работам [1,2,3], понятие уравнения можно определить для произвольной алгебраической системы $\mathcal{A}$ произвольного языка $\mathcal{L}$. С помощью понятия уравнения над $\mathcal{A}$ естественным образом определяются алгебраические множества как решения систем уравнений над $\mathcal{A}$. Объединение даже конечного числа алгебраических множеств не всегда снова является алгебраическим множеством. По этой причине в работах [3,4] было введено понятие эквациональной области как алгебраической системы, в которой любое конечное объединение алгебраических множеств снова является алгебраическим. Возникает следующий вопрос: можно ли построить нетривиальную (то есть состоящую более чем из одного элемента) алгебраическую систему, которая является эквациональной областью в языке с очень бедным множеством термов.

В данной работе указанная выше проблема решается отрицательно для алгебраических систем языка $\mathcal{L}_f$ (язык, состоящий из произвольного числа одноместных функций и констант) и для алгебраических систем языка $\mathcal{L}_p$ (язык, состоящий из конечного числа предикатных символов) при условии, что существует предикатный символ из $\mathcal{L}_p$, который интерпретируется не как тождественно ложный или тождественно истинный предикат.

Теорема 1. *Пусть $\mathcal{A} =< A|\mathcal{L}_f >$ – алгебраическая система языка $\mathcal{L}_f$ и $|A| > 1$. Тогда $\mathcal{A}$ не является эквациональной областью.*

Теорема 2. *Пусть $\mathcal{A} =< A|\mathcal{L}_p >$ – алгебраическая система языка $\mathcal{L}_p$ и в $\mathcal{A}$ существует предикатный символ, который интерпретируется не как тождественно истинный и не как тождественно ложный. Тогда $\mathcal{A}$ не является эквациональной областью.*

Теорема 3. *Пусть $\mathcal{A} =< A|\mathcal{L}_p >$ – алгебраическая система языка $\mathcal{L}_p$ и каждый предикат языка интерпретируется на $\mathcal{A}$ как тождественно истинный или тождественно ложный. Тогда $\mathcal{A}$ является эквациональной областью.*

Список литературы

[1] Daniyarova E., Miasnikov A., Remeslennikov V., *Unification theorems in algebraic geometry* // Algebra and Discrete Mathematics. – 2008. – № 1. – С. 80–112.

[2] Даниярова Э. Ю., Мясников А. Г., Ремесленников В. Н., *Алгебраическая геометрия над алгебраическими системами. II. Основания* // Фундаментальная и прикладная математика. – 2012. – Т. 17. – № 1. – С. 65–106.

[3] Даниярова Э.Ю., Мясников А.Г., Ремесленников В.Н. *Алгебраическая геометрия над алгебраическими системами. V. Случай произвольной сигнатуры* // Алгебра и логика. – 2012. – Т. 51. – № 1. – С. 41–60.

[11] zhuravlyova.nataly@gmail.com

[4] Даниярова Э.Ю., Мясников А.Г., Ремесленников В.Н. *Алгебраическая геометрия над алгебраическими системами. IV. Эквациональные области и ко-области* // Алгебра и логика. – 2010. – Т. 49. – № 6. – С. 715–756.

УДК 510.223; 004.65

АКСИОМАТИКА ФУНКЦИОНАЛЬНЫХ ЗАВИСИМОСТЕЙ С НЕОПРЕДЕЛЕННЫМИ ЗНАЧЕНИЯМИ В БАЗАХ ДАННЫХ

С. В. Зыкин[12]
Институт математики им. С. Л. Соболева СО РАН (Омский филиал),
г. Омск

Основой проектирования структуры реляционной базы данных (БД) являются зависимости. Исторически первыми были исследованы функциональные зависимости (ФЗ). Рассмотрим их формальное определение. Задано отношение (таблица) R, определенное на множестве атрибутов $U = \{A_1, A_2, \ldots, A_n\}$.

Определение 1. *Пусть X и Y – некоторые подмножества из множества атрибутов U. Будем говорить, что X функционально определяет Y и записывать $X \to Y$, если в любой реализации отношения R не могут присутствовать два кортежа $t, u \in R$, такие что $t[X] = u[X]$ и $t[Y] \neq u[Y]$.*

В определении 1 $t[X]$ – значения атрибутов множества X в кортеже t, условие $t[X] = u[X]$ означает совпадение значений одноименных атрибутов, а условие $t[Y] \neq u[Y]$ означает неравенство значений хотя бы для одного атрибута.

ФЗ в последствии явились основой формальной теории проектирования схем баз данных [1, 2], эту теорию в данной работе мы будем называть классической.

Проблема неопределенных значений рассматривалась в работах [3, 4, 5, 6, 7]. В этих работах сформулированы различные системы аксиом совместно для сильных и слабых ФЗ. Для них рассматривается полнота и надежность. Однако, полученные системы аксиом сильно отличаются от аксиом классической теории, следовательно, эти теории не является обобщением классической: если удалить из рассмотрения значение $Null$, то не получим аксиомы классической теории. Основная причина – допущение наличия неопределенности в левой части ФЗ и отождествление двух неопределенных значений и, как следствие, отсутствие транзитивности. С точки зрения приложений левая часть ФЗ становится ключом отношения и идентификатором объектов. Наличие неопределенности в не ключевых атрибутах это неопределенность характеристики объекта. Тогда как, наличие неопределенности в ключевых атрибутах это неопределенность объекта, что отвергается в существующих технологиях БД. Эта принципиальная разница проигнорирована в указанных работах.

Рассмотрим подход, который является обобщением классической теории: как только исчезнет значение $Null$, то предлагаемая теория будет совпадать с классической.

Дано: произвольная реализация отношения R, множества атрибутов $X, Y \subseteq U$, зависимость $X \to Y$ на R.

Определение 2. *Областью определения атрибутов $dom(X)$ в R является множество кортежей $T_R(X) = \{t_1, t_2, \ldots, t_s\} \in R$, для которых выполнено условие $t[X] \neq Null$.*

Определение 3. *Областью определения зависимости $dom(X \to Y)$ в R является множество кортежей $T_R(X \to Y) = \{t_1, t_2, \ldots, t_s\} \in R$, для которых выполнено условие $t[XY] \neq Null$.*

[12]szykin@mail.ru

Для областей определения выполнены следующие свойства.
П1. (Включение) Если $Y \subseteq X \subseteq U$, то $dom(X) \subseteq dom(Y)$.
П2. (Зависимость) Если $X \to Y$, то $dom(X \to Y) = dom(X) \cap dom(Y)$.
П3. (Объединение) $dom(X \cup Y) = dom(X) \cap dom(Y)$.
П4. (Логическое следствие) $dom(F_1 \models F_2) = dom(F_2|F_1) = dom(F1) \cap dom(F2)$.

Система аксиом ФЗ с областями определения имеет следующий вид.
A*1. (Рефлексвность) Если $Y \subseteq X \subseteq U$, то $X \to Y$ и $dom(X \to Y) = dom(X)$. **A*2**. (Пополнение) Если $X \to Y$ и $Z \subseteq U$, то $XZ \to YZ$ и $dom(XZ \to YZ) = dom(X) \cap dom(Y) \cap dom(Z)$.
A*3. (Транзитивность) Если $X \to Y$ и $Y \to Z$, то $X \to Z$ и $dom(X \to Z) = dom(X) \cap dom(Y) \cap dom(Z)$.

Теорема 1. Аксиомы **A*1 – A*3** надежны (непротиворечивы).

Лемма. Если $X \to Y$ логически следует из F, то для любой области определения $dom(V) \subseteq dom(X \to Y)$, зависимость $X \to Y$ также следует из F.

На основании рассмотренного свойства разработан алгоритм построения замыкания множества атрибутов X_V^+ на множестве зависимостей F в области определения $dom(V)$.

Теорема 2. Зависимость $X \to Y$ выводима из аксиом **A*1 – A*3**, в области $dom(V)$, если $Y \subseteq X_V^+$.

Теорема 3. Система аксиом **A*1 – A*3** полна для конечномерных баз данных.

На основании исследованных свойств разработан алгоритм нормализации отношений.

Исходные данные: Отношение R, определенное на множестве атрибутов:
$U = \{A_1, A_2, \ldots, A_n\}$, $F = \{F_1, F_2, \ldots, F_k\}$ – множество функциональных зависимостей и $D = \{D_1, D_2, \ldots, D_k\}$ – соответствующие области определения зависимостей.
Цикл: Сочетания без повторений из n элементов по m, $m = \overline{1, 2, \ldots, n-1}$.
Для атрибутов X, соответствующих текущему сочетанию, строим замыкания по областям D_i, начиная с минимальных.
Для каждого замыкания, если оно не совпадает со всем множеством U, производим декомпозицию: $[R] = [R] - Y$, $[R*] = XY$.
Конец цикла.

Список литературы

[1] Ullman J. Principles of Database Systems. – New York: Computer Science Press, 1980. – 379 p.

[2] Maier D. The Theory of Relational Databases. – New York: Computer Science Press, 1983. – 637 p.

[3] Zaniolo C. *Database Relations with Null Values* // Journal of Computer and System Sciences. – 1984. – №. 28. – P. 142–166.

[4] Vassiliou Y. *Functional dependencies and incomplete information* // VLDB '80 Proceedings of the sixth international conference on Very Large Data Bases. – 1980. – V. 6. – P. 260–269.

[5] Atzeni P., Morfuni N. *Functional dependencies and constraints on Null values in database relations* // Information and Control. – 1986. – V. 70. – № 1. – P. 1–31.

[6] Levene M., Loizou G. *Axiomatisation of functional dependencies in incomplete relations* // Theoretical Computer Science. – 1998. – V. 206. – № 1-2. – P. 283–300.

[7] Hartmann S., Link S. *The implication problem of data dependencies over SQL table definitions: axiomatic, algorithmic and logical characterizations* // ACM Transactions on Database Systems. – 2012. – V. 37. – № 2. – P. 1–40.

УДК 519.151

АКСИОМАТИЗИРУЕМОСТЬ КЛАССОВ МАТРОИДОВ ПРЕДПИСАННОГО РАНГА

А. В. Ильев[13]
Институт математики им. С. Л. Соболева СО РАН (Омский филиал),
г. Омск

В настоящей работе рассмотрены вопросы универсальной аксиоматизируемости и конечной аксиоматизируемости классов матроидов предписанного ранга.

Пусть $k \in \mathbb{N}$ — фиксированное число. Тогда *матроидом ранга, не превосходящего* k, называется пара $M = (U, \mathcal{I})$, где U — непустое (возможно бесконечное) множество, $\mathcal{I}$ — непустое семейство его *независимых* подмножеств, удовлетворяющее аксиомам:

(I1) $I \in \mathcal{I},\ J \subseteq I \Rightarrow J \in \mathcal{I}$ (аксиома наследственности);

(I2) для любых $I, J \in \mathcal{I}$ таких, что $|J| = |I| + 1$, существует элемент $j \in J \setminus I$, для которого $I \cup \{j\} \in \mathcal{I}$ (аксиома пополнения).

(I3) $|I| \leq k$ для всех $I \in \mathcal{I}$.

Число $r(M)$, равное общей мощности максимальных независимых множеств матроида, называется *рангом матроида* M

Чтобы определить *матроид ранга* $k \in \mathbb{N}$, в приведенном выше определении матроида аксиому (I3) нужно заменить на аксиому (I3′):

(I3′) $r(M) = k$.

Далее определим матроид ранга, не превосходящего k, на языке исчисления предикатов первого порядка с равенством.

Матроид M *ранга, не превосходящего* k, — это алгебраическая система $M = \langle U, \Sigma_I \rangle$, где U — непустое множество, а сигнатура $\Sigma_I = \langle I_0, I_1, ..., I_k, = \rangle$ состоит из $k+1$ предикатов независимости, местность каждого из которых совпадает с его порядковым номером, и предиката равенства, причем предикаты независимости удовлетворяют условиям *неупорядоченности и неповторения элементов, наследственности* и *пополнения*:

1) $\forall x_1 \ldots \forall x_n\ [I_n(x_1, ..., x_n) \to \bigwedge\limits_{\pi} I_n(\pi(x_1), ..., \pi(x_n))]$, где π пробегает по всем перестановкам элементов $x_1, ..., x_n,\ \ n \in \{1, ..., k\}$;

2) $\forall x_1 \ldots \forall x_n\ [I_n(x_1, ..., x_n) \to \bigwedge\limits_{i \neq j} (x_i \neq x_j)],\ \ n \in \{1, ..., k\}$;

3) $\forall x_1 \ldots \forall x_n\ [(I_n(x_1, ..., x_n) \to I_{n-1}(x_2, ..., x_n) \wedge \ldots \wedge I_{n-1}(x_1, ..., x_{n-1})) \wedge I_0],\ n \in \{2, ..., k\}$;

4) $\forall x_1 \ldots \forall x_n\ \ \forall y_1 \ldots \forall y_{n+1}\ \ [\, I_n(x_1, ..., x_n)\ \wedge\ I_{n+1}(y_1, ..., y_{n+1})\ \to$
$\bigvee\limits_{i \in \{1,\ldots,n+1\}} I_{n+1}(x_1, ..., x_n, y_i)],\ \ n \in \{1, ..., k-1\}$.

Таким образом, класс матроидов ранга, не превосходящего заданного $k \in \mathbb{N}$, конечно универсально аксиоматизируем. Кроме того, доказано, что класс матроидов ранга k конечно аксиоматизируем, но не является универсально аксиоматизируемым.

[13]artyom_iljev@mail.ru

УДК 519.723.4; 004.056.5; 621.39

МЕТОД ПОДТВЕРЖДЕНИЯ АУТЕНТИЧНОСТИ ПЕРЕДАВАЕМОЙ ПО СЕТИ ИНФОРМАЦИИ НА ОСНОВЕ БИОМЕТРИЧЕСКИХ ДАННЫХ С НАЛОЖЕНИЕМ ПОМЕХОУСТОЙЧИВОГО КОДА

П. С. Ложников[14], А. Е. Сулавко[15], Д. А. Волков[16]
Омский государственный технический университет,
г. Омск

Введение

С появлением глобальной сети Интернет проблема защиты каналов связи и передаваемой по ним информации стала фундаментальной [1]. Развитие телекоммуникаций влечет за собой увеличение потребности обеспечения аутентичности данных, передаваемых по сети. От случайных или преднамеренных искажений информации при передаче по каналам связи используется помехоустойчивое кодирование [2], аналогичные коды, исправляющие ошибки, можно применить в целях подтверждения аутентичности передаваемой информации (аутентификации субъекта, передающего данные).

На сегодняшний день люди часто имеют дело с виртуальными образами своих партнеров (по бизнесу, по работе и др.). Фальсификация личности в сети Интернет представляет большую опасность с точки зрения наносимого этими действиями финансового ущерба. Оценки финансовых потерь от подобных атак впечатляют [3]. Традиционные процедуры аутентификации основаны на проверке пароля, аппаратного идентификатора или биометрических данных пользователя. Перспективным направлением повышения надежности указанных процедур считается переход на многофакторную аутентификацию [4], часто для этого сочетают парольную защиту (в силу простоты и низкой стоимости реализации) с другими факторами.

Использующиеся на практике протоколы аутентификации в условиях ограниченного доверия сторон обычно основаны на принципе разделения секрета или принципе доказательства с нулевым разглашением. Однако схемы разделения секрета сложно реализовать для биометрических данных, так как биометрические характеристики не связанны между собой закономерностями теории чисел. Цель настоящей работы - разработать метод двухфакторной удаленной аутентификации субъектов в условиях ограниченного доверия сторон с использованием биометрических данных.

В качестве факторов аутентификации предлагается использовать клавиатурный и рукописный пароль. Рукописный пароль (частным случаем является автограф) субъекта относится к тайным динамическим биометрическим образам, преимущества которых заключается в объединении индивидуальных особенностей подсознательных движений человека и секрета (пароля) для получения аутентификатора [5]. При регистрации нового тайного образа и смене аутентификатора, меняются и биометрические характеристики. К недостаткам динамических биометрических признаков относится сравнительно низкая стабильность воспроизведения индивидуальных характеристик, изменчивость с течением

[14]lozhnikov@gmail.com
[15]sulavich@mail.ru
[16]volkovdanil91@gmail.com

времени. Осуществить рукописный ввод пароля можно при помощи специального графического планшета, планшетного компьютера или смартфона.

Основная часть

Предлагаемый метод основан на использовании «нечеткого экстрактора» - алгоритма, выделяющего случайные, равномерно распределенные последовательности битов из биометрических данных в условиях зашумленности [6]. «Нечеткие экстракторы» способны компенсировать ошибки, возникающие вследствие технической невозможности получения одинаковых значений биометрических характеристик при их повторном вводе субъектом. Такие алгоритмы базируются на теории информации и помехоустойчивом кодировании и обычно используются для генерации криптографических ключей без необходимости их хранения в промежутках между обращениями к ним [6]. Общая концепция построения такого генератора заключается в следующем: Изначально случайным образом генерируется битовая последовательность, которая кодируется помехоустойчивым кодом (кодом Адамара, Рида-Соломона, Хемминга и др.) [2], далее данная последовательность объединяется с эталонными характеристиками субъекта. Полученная строка объединяется с закодированной битовой последовательностью. Теоретически способ объединения может быть различным - от простого сложения по модулю 2 до использования сложных алгоритмов. Результатом объединения является открытая строка, которая может храниться на общедоступном сервере. Чтобы получить ключ шифрования или ключ доступа, в зависимости от назначения экстрактора, субъект снова воспроизводит биометрические данные, которые «вычитаются» из открытой строки для «отсоединения» закодированной битовой последовательности (которая будет изменена, вследствие отличия предъявленных данных от эталонных). После применения кода, исправляющего ошибки к полученной строке, в случае высокой степени «схожести» предъявленного биометрического образа и эталонного, будет найдена исходная последовательность битов, которая и является ключевым материалом. Известны работы, в которых описанный подход применялся для генерации криптографических ключей из подписи субъектов [7]. В рамках настоящей работы данный подход был изменен для реализации процедуры двухфакторной аутентификации.

Разработанный метод включает процедуру создания секретного ключа доступа (аналога открытой строки в классическом «нечетком экстракторе») и аутентификации. Одним из отличий предлагаемой процедуры создания ключа доступа является получение битовой последовательности на основе пароля пользователя, путем вычисления значения хеш-функции H. Далее строка H кодируется помехоустойчивым кодом Рида-Соломона, в результате формируется закодированная строка Hc. Помимо строки Hc вычисляется строка Hw, которая представляет собой значение хеш-функции от строки H (требуется для защиты от угрозы предъявления легитимных пароля и биометрических данных, описано далее). В качестве биометрических признаков a_j предлагается использовать: нормированные по энергии амплитудные спектры, полученные при помощи преобразования Фурье, функций $V_{xy}(t)$ скорости пера на поверхности планшета и функции $p(t)$ давления пера на планшет, а также коэффициенты корреляции между функциями $x(t)$, $y(t)$, $p(t)$ рукописного пароля и их производными. Таким образом, количество извлекаемых индивидуальных характеристик (N) из рукописного пароля равно 47 (N = 47, 16 амплитуд низкочастотных гармоник функции $V_{xy}(t)$, 16 амплитуд низкочастотных гармоник функции $p(t)$, 15

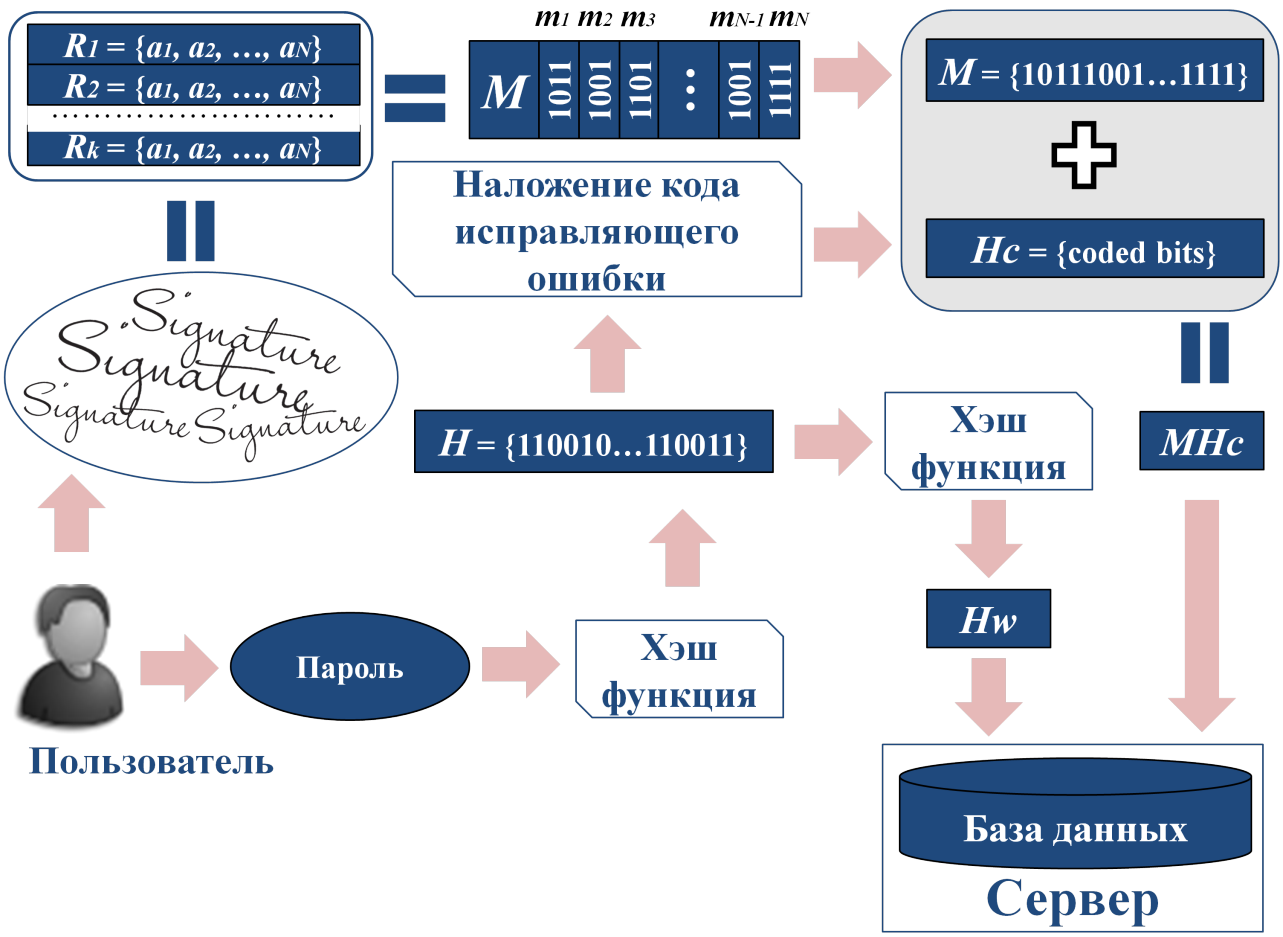


Рис. 1: Формирование ключа доступа пользователя

коэффициентов корреляции). Описанные признаки имеют отношение к динамике воспроизведения рукописного пароля (динамической подписи) [5].

$$V_{xy}(t) = \sqrt{(x(t+\Delta t) - x(t))^2 + (y(t+\Delta t) - y(t))^2},$$

где x и y - координаты точки пера на поверхности планшета, t - время регистрации координат положения пера на планшете, Δt - интервал времени между регистрацией координат положения пера.

При создании ключа доступа пользователь печатает пароль на клавиатуре и несколько раз вводит рукописный пароль на графическом планшете или планшетном компьютере. Каждая реализация рукописного пароля преобразуется в вектор $R_h = \{a_1, a_2, a_3, ..., a_N\}$ значений обозначенных выше признаков a_j. Из k полученных векторов (k - количество введенных реализаций рукописного пароля) формируется вектор $M = \{m_1, m_2, m_3, ..., m_N\}$ средних значений признаков m_j. Чем выше значение k, тем более точно вектор M описывает эталонные значения признаков. Значения m_j округляются до 1 байта. Таким образом, вектор M путем конкатенации значений m_j преобразуется в последовательность из 376 бит. Данная последовательность объединяется с Hc. В результате объединения будет

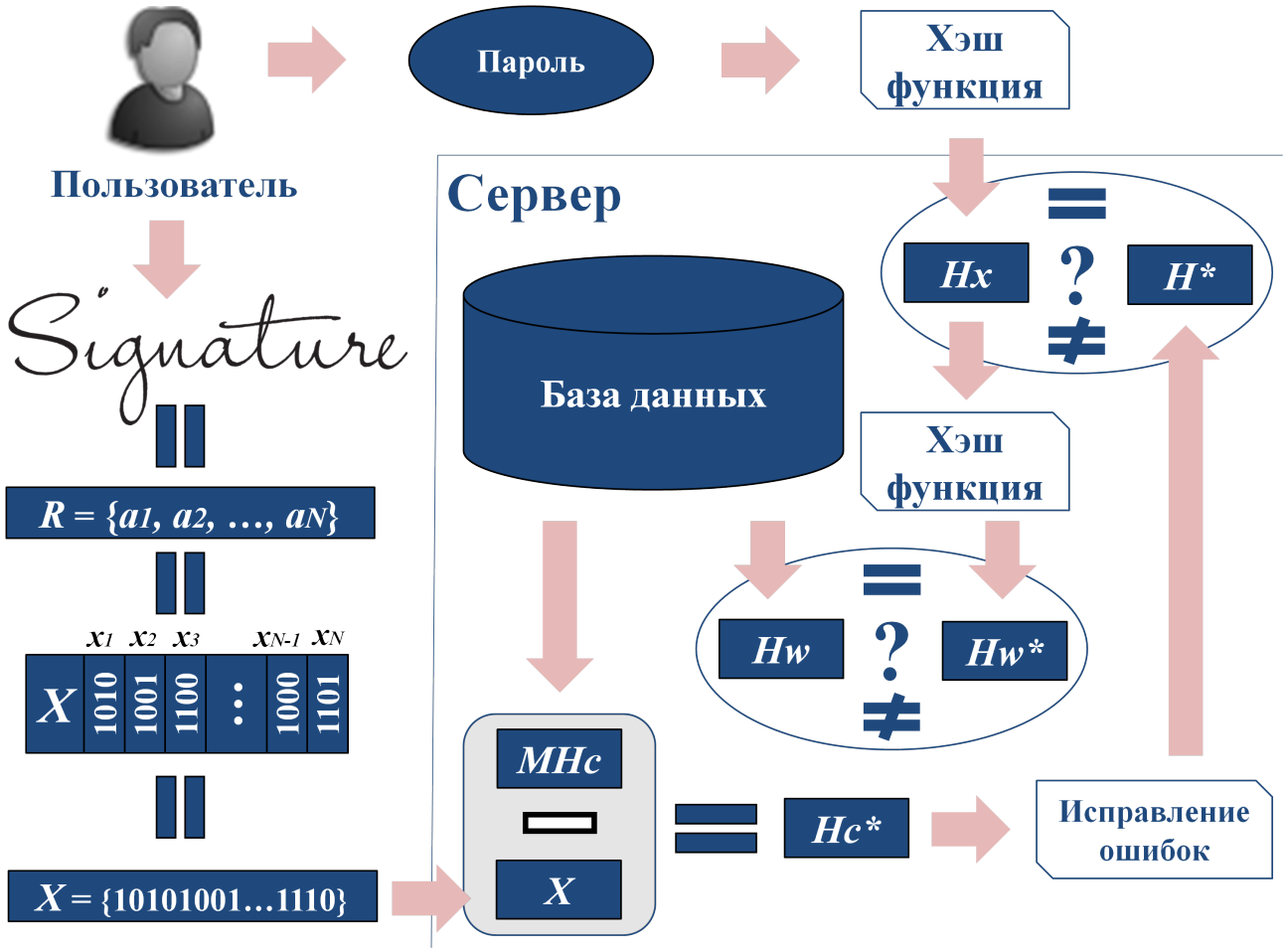


Рис. 2: Аутентификация пользователя

получен секретный ключ доступа - строка MHc. Процесс формирования ключа доступа реализуется на клиенте (на стороне субъекта, проходящего аутентификацию). На сервер отправляется ключ MHc, а также строка Hw. Описанная процедура создания ключа иллюстрируется на рисунке 1. Длина значения хеш-функции пароля после наложения кода, исправляющего ошибки, должна быть не менее 376 бит (длина $Hc \geq 376$ бит).

В процессе аутентификации пользователя компьютерной системы производится следующая последовательность действий. Пользователь вводит пароль на клавиатуре и рукописный пароль. На основе пароля вычисляется строка Hx - значение хеш-функции. Реализация рукописного пароля преобразуется в вектор значений признаков $X = \{a_1, a_2, a_3, ..., a_N\}$. Значения a_j округляются до 1 байта, вектор X преобразуется в последовательность из 376 бит. Строка Hx и битовая последовательность отправляются на сервер вместе с запросом на аутентификацию (по защищенному каналу связи, например, используя протокол SSL). Далее на сервере из ключа «вычитается» битовая последовательность, после чего будет получена строка $Hc*$, которая незначительно отличается от строки Hc, если при аутентификации был передан верный пароль и «правильные» биометрические данные пользователя. К $Hc*$ применяется код Рида-Соломона, исправляющий ошибки, в результате этой

операции получаем строку $H*$. Если $Hx = H*$ - пользователь получает доступ к серверу, т.к. в данном случае $H = Hx$, т.е. пароль верный, а рукописный пароль воспроизведен с достаточной степенью схожести, т.е. вектор X близок к M. В противном случае доступ отклоняется, так как, по крайней мере, одна из составляющих аутентификатора была введена некорректно. В итоге ни пароль, ни его хеш-функция, ни биометрические признаки не нуждаются в хранении, как на сервере, так и на клиентской машине.
Строка Hw необходима для защиты от следующей угрозы. В случае похищения строки MHc злоумышленник может сгенерировать любой аналог строки H и наложить помехоустойчивый код, получив аналог строки Hc, «вычесть» Hc из MHc и получить аналог M. Отправив на сервер H и M, злоумышленник получит доступ. Схожую атаку можно реализовать, сгенерировав любой аналог M. Поэтому помимо сравнения Hx и $H*$ при аутентификации целесообразно осуществлять сравнение Hw и $Hw*$ (значение хеш-функции от строки Hx). Процесс аутентификации изображен на рисунке 2.

При положительной аутентификации нечестный проверяющий (сервер) может сохранить значение хеш-функции пароля, а также обрывочные данные об эталонных значениях биометрических признаков (осуществив «вычитание» Hx из MHc и получив битовую последовательность M). Однако полученные данные не позволяют узнать клавиатурный и рукописный пароль. Битовая последовательность M содержит лишь округленные значения признаков неизвестного рукописного пароля, по которым невозможно его восстановить (т.е. восстановить исходные функции $x(t)$, $y(t)$, $p(t)$). Кроме того, проверяющая сторона даже не может знать о том, какие биометрические признаки используются пользователем, т.к. алгоритм обработки и получения биометрической информации выполняется на клиенте. Например, если заменить данные рукописного пароля на данные изображения лица, сервер об этом ничего «не узнает», если длина векторов M и X будет равна 47 байтам. Предлагаемый метод аутентификации может использовать в своей основе любые биометрические данные, при условии, что длина получаемых битовых последовательностей M и X (векторов) будет удовлетворительной.

Выводы

Эффективность предложенного метода аутентификации напрямую зависит от вероятности ошибок восстановления исходной битовой последовательности H, которая в свою очередь зависит от исправляющей способности кода Рида-Соломона и операций «объединения» и «вычитания» битовой последовательности, а также информативности биометрических признаков. Классический вариант реализации «нечеткого экстрактора» подразумевает использование в качестве этих операций сложение по модулю 2. В настоящей работе планируется использовать операцию нечеткой импликации, адаптировав один из алгоритмов нечеткого вывода (Tsukamoto, Sugeno, Mamdani, Larsen и др.) [8]. При использовании аппарата нечетких множеств удается получить более приемлемые результаты по уменьшению неопределенности исходных данных [8]. Возможно, за счет использования алгоритма нечеткого вывода удастся сократить количество отличающихся бит в строках Hc и $Hc*$ на этапе «вычитания» X из MHc, в тех случаях, когда векторы M и X были получены при обработке идентичных рукописных паролей, введенных одним и тем же пользователем.
По результатам предварительной оценки эффективности метода, при фиксированной ис-

правляющей способности кода Рида-Соломона, вероятность ошибок аутентификации составила менее 0,08. Количество различных субъектов, осуществляющих ввод пароля, в рамках эксперимента было равным 14, каждый из которых использовал 1 определенный рукописный пароль, количество реализаций рукописного пароля каждого субъекта составляло 20, при k=3. При определении оптимальной исправляющей способности кода и использовании модифицированных способов «объединения» и «вычитания» битовой последовательности на основе алгоритма нечеткого вывода, полученная вероятность может быть снижена в несколько раз.

В рамках будущих исследований планируется проведение вычислительного и натурного моделирования процесса генерации ключа доступа с последующим восстановлением строки H для определения оптимальной исправляющей способности кода Рида-Соломона. По результатам моделирования даны оценки вероятности ошибок первого и второго рода. Для более достоверных выводов необходимо сформировать базу данных признаков рукописных паролей с достаточным объемом.

Список литературы

[1] Wagner D., Soto P. *Mimicry Attacks on Host-Based Intrusion Detection Systems* // In: *Proceedings of the 9th ACM Conference on Computer and Communications Security.* IEEE Computer Society. Washington (DC, USA), 2002. – C. 252–264.

[2] Morelos-Zaragoza R.H. The art of error correcting coding. John Wiley & Sons. – 2006. – 320 p.

[3] Epifantsev B.N., Lozhnikov P.S., Kovalchuk A.S. *Hidden identification for operators of information-processing systems by heart rate variability in the course of professional activity* // In: *Dynamics of Systems, Mechanisms and Machines (Dynamics).* – V. 11–13. 2014. – P. 1–4.

[4] Liou J. C. et al. *A Sophisticated RFID Application on Multi-Factor Authentication* // In: *Information Technology: New Generations (ITNG), 2011 Eighth International Conference.* – IEEE, 2011. – C. 180–185.

[5] Ivanov A.I., Lozhnikov P.S., Samotuga A.Ye, *A Hybrid document formation technology* // Cybernetics and Systems Analysis. – 2014. – V. 50. – № 6. – P. 956–959.

[6] Dodis Y., Reyzin L., Smith A. *Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data* // In: *Proceedings from Advances in Cryptology. EuroCrypt.* 2004.

[7] Maiorana E., Campisi P. *Fuzzy commitment for function based signature template protection* // In: IEEE Signal Processing Letters. – 2010. – V. 17. – P. 249–252.

[8] Tsoukalas L. H. Fuzzy and Neural Approaches in Engineering. – New York: John Wiley&Sons.Inc, 1997. – 587 p.

УДК 512.7

О СЛАБОЙ НЕТЕРОВОСТИ СИСТЕМ УРАВНЕНИЙ В НИЖНИХ ПОЛУРЕШЕТКАХ[17]

М. В. Малов[18]
Институт математики им. С. Л. Соболева СО РАН (Омский филиал)
г. Омск

Введение

Понятие нетеровости по уравнениям является одним из основных в универсальной алгебраической геометрии. Одно из обобщений этого свойства – слабая нетеровость – изучалось в статьях А.Н. Шевлякова[1], Ю.С. Дворжецкого[2]. В данной работе изучается слабая нетеровость систем уравнений в классе нижних полурешеток, не содержащих следующей подполурешетки:

Найдены необходимые и достаточные условия слабой нетеровости систем от одной переменной над полурешетками из данного класса. Основные определения приведены в серии статей Э.Ю. Данияровой, А.Г. Мясникова, В.Н. Ремесленникова по универсальной алгебраической геометрии [3, 2, 5].

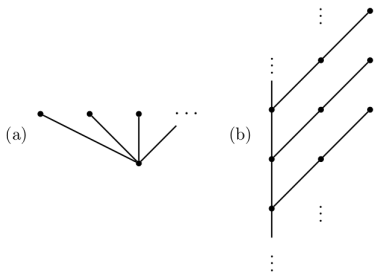
Слабая нетеровость систем уравнений одной переменной

Сформулируем основное определение работы.

Определение. Система уравнений $\mathcal{S}$ называется *слабо нетеровой* над полурешеткой $\mathbf{M}$, если существует эквивалентная конечная система $\mathcal{S}'$, множество решений которой совпадает с множеством решений системы $\mathcal{S}$.

В рассматриваемом классе полурешеток справедлива следующая теорема.

Теорема. *Пусть любые два элемента полурешетки $x,\ y \in \mathbf{M}$ соединены конечной цепью. Любая система от одной переменной над полурешеткой $\mathbf{M}$ будет слабо нетеровой тогда и только тогда, когда она не содержит подполурешеток, которые могут быть графически представлены в следующих видах:*



[17]Работа выполнена при финансовой поддержке РНФ (проект 14-11-00085)
[18]m.malov.v@gmail.com

Список литературы

[1] Шевляков А.Н. Алгебраическая геометрия над коммутативными полугруппами. Автореферат канд. диссертации. Омск, 2010.

[2] Дворжецкий Ю.С. Системы уравнений над алгебраическими системами с порядком. Автореферат канд. диссертации. Омск, 2014.

[3] Даниярова Э. Ю., Мясников А. Г., Ремесленников В. Н. *Алгебраическая геометрия над алгебраическими системами. II. Основания* // Фундаментальная и прикладная математика. – 2011/2012. – Т. 17, – № 1. – С. 65–106.

[4] Daniyarova E., Miasnikov A., Remeslennikov V. *Algebraic geometry over algebraic structures. III. Equationally Noetherian property and compactness* // Southeast Asian Bull. Math. – 2011. – V. 35. – P. 35–68.

[5] Daniyarova E., Miasnikov A., Remeslennikov V. *Unification theorems in algebraic geometry* // Algebra Discrete Math. – 2008. – V. 1. – P. 80–112.

УДК 519.17

КОНЕЧНЫЕ СВОБОДНЫЕ КОММУТАТИВНЫЕ МОНОИДЫ, ДОПУСКАЮЩИЕ ОБОБЩЕННО ВНЕШНЕПЛАНАРНЫЕ ГРАФЫ КЭЛИ

П. О. Мартынов[19]
Омский государственный педагогический университет,
г. Омск

Изучаются конечные свободные коммутативные моноиды, допускающие обобщенно внешнепланарные графы Кэли. Найдено следующее характеристическое свойство.

Теорема. *Граф Кэли конечного свободного коммутативного моноида S с циклическими соотношениями обобщенно внешнепланарен тогда и только тогда, когда выполнено одно из следующих условий:*

1) $S = \langle a \mid a^m = 1\rangle$, где m -любое натуральное число;

2) $S = \langle a, b \mid ab = ba,\ a^{r+m} = a^r,\ b^t = 1\rangle$, либо $S = \langle a, b \mid ab = ba,\ a^m = 1,\ b^t = 1\rangle$, где для натуральных r, m, t выполнено одно из следующих ограничений:

а) $t = 1$; б) $m \leq 2,\ t = 2$;

3) $S = \langle a, b, c \mid ab = ba,\ ac = ca,\ bc = cb,\ a^{r+m} = a^r,\ b^2 = b,\ c = 1\rangle$, где r и m – натуральные числа, причем $m \leq 2$.

Список литературы

[1] Zelinka B. *Graphs of Semigroups* // Casopis. Pest. Mat. – 1981. – V. 106. – P. 407–408.

[2] Харари Ф. Теория графов. – М: Мир, 1973. – 300 с.

[3] Sedlacek J. *On a generalization of outerplanar graphs (in Czech)* // Casopis. Pest. Mat. – 1988. – V. 113. – №2 – P. 213–218.

[4] Sedlacek J. *On local properties of graphs again* // Casopis. Pest. Mat. – 1989. – V. 114. – №4 – P. 381–390.

[5] Caceres J., Marquez A. *A linear algorithm to recognize maximal generalized outerplanar graphs* // Mathematica Bohemica. – 1997. – V. 122. – №3 – P. 225–230.

[6] Соломатин Д.В. *Конечные свободные коммутативные полугруппы с планарными графами Кэли* // В: *Математика и информатика: наука и образование: Межвузовский сборник научных трудов: Ежегодник.* – Омск: Изд-во ОмГПУ. , 2003. – Вып.3. С. – 32–38.

[7] Соломатин Д.В. *Строение полугрупп, допускающих внешнепланарные графы Кэли* // Сибирские Электронные Математические Известия. – 2011. – Т. 8 – С. 191–212.

[8] Соломатин Д.В. *Конечные свободные коммутативные моноиды, допускающие планарный граф Кэли* // Вестник Омского университета. – 2005. – №4. – С. 36–38.

[19] 3mbar90@gmail.com

УДК 512.541

УНИВЕРСАЛЬНЫЕ ИНВАРИАНТЫ ДЛЯ КЛАССОВ АБЕЛЕВЫХ ГРУПП[20]

А. А. Мищенко[21], В. Н. Ремесленников[22], А. В. Трейер[23],
Институт математики им. С. Л. Соболева СО РАН (Омский филиал),
Омский государственный технический университет,
г. Омск

Проблема элементарной эквивалентности абелевых групп решена в статье В. Шмелевой [1]. В этой работе доказан следующий результат: абелевы группы A и B элементарно эквивалентны тогда и только тогда, когда значения элементарных инвариантов группы A совпадают со значениями элементарных инвариантов для группы B. Определения элементарных инвариантов можно найти в [2].

Цель данной работы следующая. Мы заменяем элементарную теорию $\mathrm{Th}(A)$ для абелевой группы A на универсальную теорию этой группы $\mathrm{Th}_\forall(A)$ и вводим универсальный инвариант $\mathrm{UI}(A)$ для группы A как последовательность

$$\mathrm{UI}(A) = (\mathrm{UI}_0(A), \mathrm{UI}_2(A), \mathrm{UI}_3(A), \mathrm{UI}_5(A), \ldots, \mathrm{UI}_{p_n}(A), \ldots),$$

где $\mathrm{UI}_{p_n}(A)$ – вектор составленный из значений элементарных инвариантов, а p_n – простое число, и доказываем аналог теоремы Шмелевой об универсальной эквивалентности абелевых групп:

Теорема 1. *Две абелевы группы A и B универсально эквивалентны тогда и только тогда, когда* $\mathrm{UI}(A) = \mathrm{UI}(B)$.

Далее мы переходим к классам абелевых групп и определяем универсальный инвариант $\mathrm{UI}(\mathcal{K})$ для класса $\mathcal{K}$, и доказываем аналог теоремы Шмелевой для классов абелевых групп:

Теорема 2. *Пусть $\mathcal{K}_1$ и $\mathcal{K}_2$ – два универсально аксиоматизируемых класса абелевых групп. Тогда* $\mathrm{Th}_\forall(\mathcal{K}_1) = \mathrm{Th}_\forall(\mathcal{K}_2)$ *тогда и только тогда, когда* $\mathrm{UI}(\mathcal{K}_1) = \mathrm{UI}(\mathcal{K}_2)$.

Для доказательства основных результатов мы вводим множество канонических абелевых групп CGr, со следующими свойствами:

Теорема 3. *Для групп из класса* CGr *верны следующие утверждения:*

1. *Если $C_1, C_2 \in$ CGr пара неизоморфных групп, то* $\mathrm{Th}_\forall(C_1) \neq \mathrm{Th}_\forall(C_2)$;
2. *Для любой абелевой группы A существует такая единственная группа $C \in$ CGr, что* $\mathrm{Th}_\forall(A) = \mathrm{Th}_\forall(C)$;
3. *Для любого универсального класса абелевых групп $\mathcal{K}$ существует такое однозначно определенное подмножество $C(\mathcal{K})$ множества канонических групп* CGr, *что* $\mathrm{Th}_\forall(\mathcal{K}) = \mathrm{Th}_\forall(C(\mathcal{K}))$.
4. *Если $\mathcal{K}_1$ и $\mathcal{K}_2$ различные универсальные классы, то $C(\mathcal{K}_1) \neq C(\mathcal{K}_2)$.*

[20]Работа выполнена при финансовой поддержке РНФ (проект 14-11-00085)
[21]alexei.mishenko@gmail.com
[22]remesl@ofim.oscsbras.ru
[23]alexander.treyer@gmail.com

Список литературы

[1] Szmielew W. *Elementary properties of Abelian groups.* // Fundamenta Mathematica. – 1955. – V. 41. – P. 203–271.

[2] Ершов Ю.Л. Проблемы разрешимости и конструктивные модели. — М.: Наука, 1980.

УДК 512.541; 511.17

ЭЛЕМЕНТАРНЫЕ ИНВАРИАНТЫ АБЕЛЕВЫХ ГРУПП

А. Ю. Никитин[24]
Омский государственный университет им. Ф.М. Достоевского,
г. Омск

Сначала дадим определение четырех инвариантов Шмелевой для абелевых групп, следуя книге Ю.Л. Ершова [2].

Пусть A – абелева группа, p – простое число,

$A[p]$ – подгруппа в A, состоящая из всех элементов A порядка p или 1 (p-слой),

nA – подгруппа в A, состоящая из всех элементов вида na, где $a \in A$ и $n \in \mathbb{N}$.

Отметим, что p-слои $(p^{k-1}A)[p]\Big/(p^kA)[p]$ и фактор группы $p^{k-1}A\Big/p^kA$ являются группами периода p, поэтому их можно рассматривать как векторные пространства над полем из p элементов, и можно говорить о размерностях dim этих векторных пространств.

$$\alpha_{p,k}(A) = \begin{cases} \dim\left(p^{k-1}A\Big/p^kA\right), \text{ если эта размерность конечная;} \\ \infty, \text{ в противном случае.} \end{cases}$$

$$\beta_{p,k}(A) = \begin{cases} \dim\left((p^{k-1}A)[p]\Big/(p^kA)[p]\right), \text{ если эта размерность конечная;} \\ \infty, \text{ в противном случае.} \end{cases}$$

$$\gamma_{p,k}(A) = \begin{cases} \dim\left((p^kA)[p]\right), \text{ если эта размерность конечная;} \\ \infty, \text{ в противном случае.} \end{cases}$$

$$\delta(A) = \begin{cases} 0, \text{ если группа } A \text{ ограничена;} \\ 1, \text{ в противном случае.} \end{cases}$$

Сформулируем важную теорему для элементарных теорий абелевых групп с использованием инвариантов.

Теорема Шмелёвой. *Абелева группа A элементарно эквивалента абелевой группе B, тогда и только тогда когда все инварианты $\alpha_{p,k}$, $\beta_{p,k}$, $\gamma_{p,k}$ и δ на этих группах совпадают.*

Так же важным является следующее свойство инвариантов абелевых групп, раскладывающихся в прямую сумму.

Теорема 1. *Пусть A и B – абелевы группы. Тогда*

$$\alpha_{p,k}(A \oplus B) = \alpha_{p,k}(A) + \alpha_{p,k}(B),$$

$$\beta_{p,k}(A \oplus B) = \beta_{p,k}(A) + \beta_{p,k}(B),$$

[24]nikitinlexey@gmail.com

$$\gamma_{p,k}(A \oplus B) = \gamma_{p,k}(A) + \gamma_{p,k}(B),$$
$$\delta(A \oplus B) = \max(\delta(A), \delta(B)).$$

Все инварианты являются формульными, то есть им соответствуют формулы логики первого порядка. Некоторые из них можно описать универсальными формулами, как показывает следующее утверждение.

Теорема 2. *Инварианту δ соответствует множество универсальных формул*

$$\Psi = \{\psi_m \mid \psi_m = (\forall x\ mx = 0), m \in \mathbb{N}\},$$

где $x-$ элемент группы.

Инварианту γ вида $\gamma_{p,k}(A) < m$ соответствует универсальная формула

$$\forall x_1 \ldots \forall x_m \in A \left[\bigwedge_{i=1}^{m} p^k \cdot x_i = 0\right] \longrightarrow \bigvee_{\substack{0 \le k_i < p \\ k_1 = k_2 = \cdots = k_m \neq 0}} \left(\sum_{i=1}^{m} k_i \cdot x_i = 0\right)$$

Отметим, что для инварианта γ вида $\gamma_{p,k}(A) > m$ универсальной формулы не найдено.

Список литературы

[1] Мищенко А. А., Ремесленников В. Н., Трейер А. В. *Генерические теории серий конечных абелевых групп//* Алгебра и логика. – 2014. – Т. 53. – № 6. – С. 722–734.

[2] Ершов Ю.Л. Проблемы разрешимости и конструктивные модели. – М.: Мир, 1980. – 416 с.

[3] Фукс Л. Бесконечные абелевы группы Т. 1. – М.: Мир, 1974. – 336 с.

УДК 512.7

ГЕНЕРИЧЕСКИЕ ТЕОРИИ КАК МЕТОД АППРОКСИМАЦИИ ЭЛЕМЕНТАРНЫХ ТЕОРИЙ[25]

В. Н. Ремесленников[26]
Институт математики им. С. Л. Соболева СО РАН (Омский филиал),
г. Омск

В статье А.Г. Мясникова и автора [1] сформулированы основные понятия об аппроксимации элементарных теорий. Доклад на конференции тесно связан с содержанием этой статьи. Напомним несколько определений из нее.

Пусть $S = \{M_i, i \in I\}$ — бесконечное множество алгебраических систем сигнатуры L, и μ — вероятностная мера над I (μ — конечно-аддитивна и $\mu(I) = 1$); B — булева алгебра μ-измеримых подмножеств из I; Φ_L — множество предложений сигнатуры L; $T = \mathrm{Th}(S)$ — элементарная теория множества систем S.

Определение 1. *Генерической теорией множества систем S относительно меры μ называется множество $\mathsf{GTh}(S, \mu)$ всех таких предложений $\varphi \in \Phi_L$, что подмножество*

$$I_\varphi = \{i \in I |\ M_i \models \varphi\}$$

измеримо, и $\mu(I_\varphi) = 1$.

Предложение. *Для любого множества систем S и меры μ теория $\mathsf{GTh}(S, \mu)$ непротиворечива и $\mathsf{GTh}(S, \mu) \supseteq \mathrm{Th}(S)$.*

В докладе приведены примеры генерических теорий для серий следующих алгебраических систем:

1. конечные булевы алгебры,
2. конечные графы,
3. конечные поля,
4. конечные циклические группы,
5. конечные частичные порядки.

Аппроксимацию элементарных теорий мы предлагаем проводить двумя следующими способами:

- с помощью понятия генерического компаньон-оператора для элементарной теории,
- методом построения экзистенциальных моделей для элементарной теории.

Определение 2. *Пусть $T = \mathrm{Th}(\mathcal{K})$, где $\mathcal{K} = \{\mathcal{K}_i, i \in I\}$. Оператор $T \to \mathsf{GTh}(\mathcal{K}, \mu)$ на теориях есть генерический компаньон-оператор, если*

[25]Работа выполнена при финансовой поддержке РНФ (проект 14-11-00085)
[26]remesl@ofim.oscsbras.ru

1. $T_\forall = \mathsf{GTh}_\forall(\mathcal{K}, \mu)$;

2. *мера* $\mu = \mu_F$, *где* F*— неглавный фильтр над множеством* I.

Определение 3. *Если* $\mathsf{GTh}(\mathcal{K}, \mu)$ *есть генерический компаньон-оператор, то будем говорить, что теория* $\mathrm{Th}(\mathcal{K})$ *компаньон-аппроксимируется теорией* $\mathsf{GTh}(\mathcal{K}, \mu)$.

Компаньон-аппроксимируемость выполняется для теорий моделей из приведенных выше пунктов 1– 4.

Что касается серии конечных частичных порядков из 5, то ее генерическая теория построенная с помощью асимптотического фильтра не будет компаньон-аппроксимирующей для теории этой серии.

Список литературы

[1] Мясников А.Г., Ремесленников В.Н. *Генерические теории как метод аппроксимации элементарных теорий* // Алгебра и логика. – 2014. – Т. 53. – № 6. – С. 779–789.

УДК 519.2

ON INVARIANTS OF PROBABILITY SPACES

S. O. Speranski[27]
Sobolev Institute of Mathematics,
Novosibirsk

We start by describing the probability logic QPL with quantifiers over events. (See [1] for some background information.)

Elements of $\mathscr{X} := \{x_i \mid i \in \mathbb{N}\}$ are called *variables*. We define *e-terms* inductively as follows:

- every variable is an e-term;
- if t_1 and t_2 are e-terms, then so are $\overline{t_1}$, $t_1 \cap t_2$ and $t_1 \cup t_2$.

By an *atomic* QPL-*formula* we mean an expression of the form

$$f(\mu(t_1), \ldots, \mu(t_n)) \leqslant g(\mu(t_{n+1}), \ldots, \mu(t_{n+k}))$$

where f and g are polynomials with rational coefficients, μ is a special symbol, and $t_1, \ldots, t_{n+k}$ are e-terms. Let $\wedge$, $\vee$, $\neg$ and $\to$ denote the usual logical connectives. By an *e-quantifier* we mean Qx with $Q \in \{\forall, \exists\}$ and $x \in \mathscr{X}$. Finally, QPL-*formulas* are built up from atomic QPL-formulas using logical connective symbols (i.e. $\wedge, \vee, \neg, \to$) and e-quantifiers in the standard way.

By a QPL-*structure* we simply understand a pair $(\mathscr{P}, v)$ where:

- $\mathscr{P}$ is a probability space, i.e. it has the form $\langle \Omega, \mathscr{A}, \mathsf{P} \rangle$ where
  - $\mathscr{A}$ is a σ-algebra over a non-empty set Ω, and
  - P is a countably additive probability measure on $\mathscr{A}$;
- v is a partial valuation, i.e. a mapping from a subset of $\mathscr{X}$ to $\mathscr{A}$.

It is now easy to define the *satisfiability relation for* QPL, denoted by $\Vdash$. First we inductively assign elements of $\mathscr{A}$ to all e-terms over $\mathrm{dom}(v)$:

$$\begin{aligned} v\left(\overline{t_1}\right) &:= \text{the complement of } v(t_1) \text{ in } \Omega; \\ v(t_1 \cap t_2) &:= \text{the intersection of } v(t_1) \text{ and } v(t_2); \\ v(t_1 \cup t_2) &:= \text{the union of } v(t_1) \text{ and } v(t_2). \end{aligned}$$

For any quantifier-free QPL-formula Ψ whose variables belong to $\mathrm{dom}(v)$, let

$$(\mathscr{P}, v) \Vdash \Psi \iff \begin{array}{l} \text{the result of replacing each } \mu(t) \text{ in} \\ \Psi \text{ by } \mathsf{P}(v(t)) \text{ holds in } \langle \mathbb{R}, +, \times, \leqslant \rangle. \end{array}$$

(Hence if we forget about e-quantifiers, we get a variant of one decidable probability logic studied in [5].) Then I extend this relation to all QPL-formulas whose free variables belong to $\mathrm{dom}(v)$ by requiring that:

[27]katze.tail@gmail.com

- the logical connectives $\wedge$, $\vee$, $\neg$ and $\rightarrow$ behave clasically;
- variables in e-quantifiers range over 'events', viz. elements of $\mathscr{A}$.

We write $\mathscr{P} \Vdash \Phi$ instead of $(\mathscr{P}, \varnothing) \Vdash \Phi$, and use $\mathrm{Th}(\mathscr{P})$ to denote

$$\{\Phi \mid \Phi \text{ is a } \mathsf{QPL}\text{-sentence and } \mathscr{P} \Vdash \Phi\},$$

called the QPL-*theory of* $\mathscr{P}$. In fact all the results below remain true even if we add quantifiers over reals to QPL (appropriately modifying the notion of a formula).

Consider an arbitrary probability space $\mathscr{P} = \langle \Omega, \mathscr{A}, \mathsf{P} \rangle$. Take

$$\Lambda \ := \ \{E \in \mathscr{A} \mid \mathsf{P}(E) = 0\}.$$

Clearly the subset relation and the equality relation on $\mathscr{A}$, modulo Λ, are defined in $\mathscr{P}$ by the QPL-formulas

$$x \preccurlyeq y \ := \ \mu(\overline{x} \cup y) = 1 \quad \text{and} \quad x \sim y \ := \ x \preccurlyeq y \wedge y \preccurlyeq x$$

respectively. Indeed $x \sim y$ gives us a congruence relation on $\langle \mathscr{A}, \preccurlyeq \rangle$. Now let

$$\mathscr{A}_\sim \ := \ \{[\![E]\!] \mid E \in \mathscr{A}\}$$

where $[\![E]\!]$ denotes $\{E' \in \mathscr{A} \mid \mathscr{P} \Vdash E \sim E'\}$. Naturally we introduce Boolean operations on $\mathscr{A}_\sim$ by

$$\begin{aligned} \neg[\![E_1]\!] \ &:= \ [\![\Omega \setminus E_1]\!], \\ [\![E_1]\!] \wedge [\![E_2]\!] \ &:= \ [\![E_1 \cap E_2]\!], \\ [\![E_1]\!] \vee [\![E_2]\!] \ &:= \ [\![E_1 \cup E_2]\!]. \end{aligned}$$

So we obtain an 'abstract' σ-algebra (leaving $\Omega_\sim$ unspecified). Further, the function $\mathsf{P}_\sim : [\![E]\!] \mapsto \mathsf{P}(E)$ can be viewed as a countably additive probability measure on $\mathscr{A}_\sim$ — take $\mathscr{P}_\sim$ to be $\langle \mathscr{A}_\sim, \mathsf{P}_\sim \rangle$. Of course, it is easy to adapt the initial QPL-semantics to deal with such 'abstract' spaces. Moreover one readily checks that for every QPL-formula $\Phi(x_1, \ldots, x_n)$ and every $\{E_1, \ldots, E_n\} \subseteq \mathscr{A}$,

$$\mathscr{P} \Vdash \Phi(E_1, \ldots, E_n) \quad \Longleftrightarrow \quad \mathscr{P}_\sim \Vdash \Phi([\![E_1]\!], \ldots, [\![E_n]\!]).$$

On the other hand the predicate '$[\![x]\!]$ is an atom of $\mathscr{A}_\sim$' is defined in $\mathscr{P}$ by

$$At(x) \ := \ \mu(x) > 0 \wedge \forall y\,((y \preccurlyeq x \wedge \mu(y) > 0) \rightarrow y \sim x).$$

Let $\mathscr{D}$ denote $\{[\![E]\!] \in \mathscr{A}_\sim \mid \mathscr{P} \Vdash At(E)\}$. This collection is at most countable; hence the supremum of $\mathscr{D}$ in $\mathscr{A}_\sim$ exists. Actually each probability space turns out to be in a sense equivalent to a convex sum of a discrete space and an atomless space.

By the *invariant of* $\mathscr{P}$ we mean the function $\sharp_{\mathscr{P}}$ from $\mathbb{R}$ into $\mathbb{N}$ given by

$$\sharp_{\mathscr{P}}(r) \ := \ \text{the cardinality of } \{[\![E]\!] \in \mathscr{D} \mid \mathsf{P}(E) = r\}.$$

(Notice that $\sharp_{\mathscr{P}}(r) \leqslant \lfloor r^{-1} \rfloor$ if $r > 0$, and $\sharp_{\mathscr{P}}(r) = 0$ otherwise.) E.g., $\mathscr{P}$ is atomless — or more formally, $\mathscr{P} \Vdash \neg\exists x\, At(x)$ — iff $\sharp_{\mathscr{P}}$ is the zero function.

Theorem 1. *For any two probability spaces $\mathscr{P}_1$ and $\mathscr{P}_2$,*

$$\sharp_{\mathscr{P}_1} \;=\; \sharp_{\mathscr{P}_2} \quad\Longleftrightarrow\quad \mathrm{Th}(\mathscr{P}_1) \;=\; \mathrm{Th}(\mathscr{P}_2).$$

In particular, all atomless spaces have the same QPL-theory, that of the Lebesgue measure $\mathscr{L}$ on the unit interval.

Theorem 2. $\mathrm{Th}(\mathscr{L})$ *is decidable.*

Clearly we can view $\sharp_{\mathscr{P}}$ as a 'structural representation' of $\mathscr{P}$, but not of its QPL-theory. For instance, it is relatively easy to show the following.

Proposition. *Given an integer $n \geqslant 2$, take $\mathscr{P}$ to be a space for which*

$$\sharp_{\mathscr{P}}(r) \;=\; \begin{cases} 1 & \text{if } r = n^{-k-1} \text{ for some } k \in \mathbb{N} \\ 0 & \text{otherwise.} \end{cases}$$

Then $\mathrm{Th}(\mathscr{P})$ *is* Π^1_∞*-complete (viz. one-one equivalent to the second-order theory of the standard model* $\langle \mathbb{N}, +, \times, = \rangle$ *of arithmetic).*

Thus, even when we deal with quite simple invariants/representations, their theories may turn out to be very complex. That Π^1_∞ appears here is no accident:

Theorem 3. *The validity problem for* QPL *is* Π^1_∞*-complete.*

Furthermore there are a partial function γ from the powerset of $\mathbb{N}$ onto the set of all invariants and a computable function τ translating any sentence Φ of QPL into a formula $\Phi^\tau(X)$ of monadic second-order arithmetic, such that for every $A \subseteq \mathbb{N}$,

$$\langle \mathbb{N}, +, \times, = \rangle \models \Phi^\tau(A) \quad\Longleftrightarrow\quad \begin{array}{c} \text{there exists a probability space } \mathscr{P} \\ \text{for which } \sharp_{\mathscr{P}} = \gamma(A) \text{ and } \mathscr{P} \Vdash \Phi. \end{array}$$

(Actually the relation 'X belongs to $\mathrm{dom}(\gamma)$' is even arithmetically definable.)

We conclude with several remarks. The mathematical machinery behind the Π^1_∞-hardness results can be found in [2]. A probability logic related to QPL has been investigated in [4, 3]. Yet it does not share some very nice properties with QPL and is in fact much less attractive from the structural viewpoint we presented here.

Список литературы

[1] Speranski S. O., *Quantifying over events in probability logic: an introduction*// Mathematical Structures in Computer Science. — 2015. — Cambridge: Cambridge University Press (accepted).

[2] Speranski S.O., *A note on definability in fragments of arithmetic with free unary predicates* // Archive for Mathematical Logic. — 2013. — V. 52. — № 5–6. — P. 507–516.

[3] Speranski S.O. *Complexity for probability logic with quantifiers over propositions* // Journal of Logic and Computation. — 2013. — V. 23. — № 5. — P. 1035–1055.

[4] Speranski S. O., *Quantification over propositional formulas in probability logic: decidability issues* // Algebra and Logic. — 2011. — V. 50. — № 4. — P. 365–374.

[5] Fagin R., Halpern J.Y., Megiddo N. *A logic for reasoning about probabilities* // Information and Computation. — 1990. — V. 87. — № 1–2. — P. 78–128.

УДК 004.056.5; 004.5

НЕПРЕРЫВНАЯ СКРЫТАЯ ИДЕНТИФИКАЦИЯ СУБЪЕКТОВ НА ОСНОВЕ СТАНДАРТНОГО ПЕРИФЕРИЙНОГО ОБОРУДОВАНИЯ[28]

А. Е. Сулавко*[29], А. В. Еременко**[30]
* Омский государственный технический университет,
**Омский государственный университет путей сообщения,
г. Омск

Вопросы защиты информации от несанкционированного доступа всегда были и остаются актуальными. Со временем изменяются лишь типы правонарушений, совершаемых в данной области. Аналитические исследования показывают, что большая часть рисков информационной безопасности обусловлена деятельностью инсайдеров - внутренних нарушителей, собственных сотрудников, нашедших способы прохождения всех рубежей авторизации и получивших санкционированный доступ к корпоративной информации за пределами своей компетенции. В соответствии с The Global State of Information Security Survey 2014 – глобальным исследованием информационной безопасности, проведенным фирмой PwC и журналами CIO и CSO, основной причиной инцидентов, связанных с нарушением безопасности, являются сотрудники (31%) и бывшие сотрудники компаний (27%). По данным Zecurion Analytics суммарный ущерб от деятельности внутренних нарушителей в мире за 2013 и 2014 годы составил более 42 млрд. долл., и с каждым годом оценки ущерба растут [1]. Использующиеся на практике процедуры аутентификации выполняют функцию разграничения понятий «свой» и «чужой», не учитывая, что авторизованный пользователь, являющийся штатным сотрудником, может также оказаться нарушителем. Процедура аутентификации, как правило, строится на основе предъявления секрета (пароля, ключа и т.д.) или биометрических образов. Пароли взламывают (имеется множество способов – от социальной инженерии до перебора по словарю), а открытые биометрические образы (отпечаток пальца, радужка и т.д.) можно подделать. Последнее отнюдь не тривиальная задача, но если злоумышленник обладает технологией изготовления муляжа, целевая система защиты (и любая аналогичная) будет скомпрометирована. Предлагается сделать процедуру идентификации скрытой, и проводить ее непрерывно в процессе работы пользователя в компьютерной системе, параллельно осуществляя распознавание нелояльного (потенциально опасного для информационной безопасности) поведения.

Настоящая работа посвящена проверке на истинность двух гипотез:

1. Данные, полученные в процессе мониторинга работы пользователя с периферийным оборудованием (клавиатурой и мышью), позволяют проводить скрытую непрерывную аутентификацию/идентификацию пользователя, получившего доступ к компьютерной системе, с достаточной для потребителя надежностью.

2. Информация о действиях пользователя в компьютерной системе, в частности, особенности работы с оконными приложениями, используемые сочетания клавиш, ха-

[28]Работа выполнена при финансовой поддержке РФФИ (проект 15-37-50269)
[29]sulavich@mail.ru
[30]nexus-@mail.ru

рактер работы с мышью и клавиатурой позволит распознать нелояльное поведение и предотвратить реализацию внутренней угрозы информационной безопасности.

Спланировано и проведено в разное время 2 эксперимента по скрытому мониторингу и регистрации действий пользователей компьютерных систем:

1. «Без возможности нарушения режима безопасности». Проводился на протяжении двух недель, каждый день по 1 часу кроме выходных + один день в течение всего рабочего дня. Количество испытуемых – 10 человек. Таким образом, при формировании базы признаков лояльных сотрудников учитывались изменения портрета работы субъектов во времени.

2. «С возможностью нарушения режима безопасности». Общее количество испытуемых – 30 человек (10 из которых принимали участие в предыдущем эксперименте). Эксперимент длился в течение двух часов. По окончанию эксперимента часть испытуемых совершила нарушения (12 человек), оставшаяся часть нет.

Анализировались следующие действия пользователя:

- частота запуска приложений;
- частота нажатий «горячих» клавиш;
- количество производимых операций с файлами различных разрешений (чтение, изменение, удаление);
- времена удержания клавиш при вводе текста на клавиатуре (характеризует клавиатурный почерк);
- паузы между нажатием клавиш при вводе текста на клавиатуре (характеризует клавиатурный почерк);
- средняя скорость перемещения курсора мыши от одного элемента интерфейса к другому;
- время задержки перед осуществлением перемещения курсора мыши от одного элемента интерфейса к другому в миллисекундах;
- максимальное и среднее отклонения в пикселях от кратчайшего пути перемещения курсора мыши от одного элемента интерфейса к другому.

Первые три характеристики были признаны неинформативными как для целей идентификации, так и для определения нелояльного поведения. Спонтанное отклонение дисперсии количества произошедших событий безопасности (операции с файлами, запуск программ, использование «горячих» клавиш) в определенное время суток от их среднего числа, полученного в результате многократных наблюдений в это же время суток, может свидетельствовать как о реализации атаки, так и об изменении характера выполняемых задач.

Сделана попытка адаптации закона Фиттса [2] для его использования в целях получения количественных оценок особенностей работы субъектов с мышью. Данный закон

касается сенсорно-моторных процессов человека и связывает время движения субъекта к наблюдаемой цели с точностью движения и с расстоянием перемещения. Чем дальше или точнее выполняется движение субъекта, тем больше коррекции необходимо для его выполнения, и соответственно, больше времени требуется субъекту для внесения этой коррекции. При внесении коррекции движений проявляются индивидуальные особенности человека. Нормирование скорости перемещения курсора мыши между элементами интерфейса производится по формуле

$$V_{mid} = \frac{T}{log_2(\frac{D}{W}+1)}, \tag{1}$$

где T – время, которое было затрачено на перемещение курсора мыши от одного элемента интерфейса к другому в миллисекундах, D – дистанция от точки начала движения до центра элемента интерфейса, к которому направляется курсор (в пикселях), W – ширина элемента интерфейса, к которому направляется курсор, измеренная вдоль оси движения в пикселях.

Формула (1) является производной от той, что приводится в работе [2]. Признаки, характеризующие индивидуальность клавиатурного почерка и особенностей работы с мышью субъекта имеют нормальное распределение. Проверка гипотезы о распределении выполнялась с помощью критерия Хи-квадрат.

Формирование эталона субъекта осуществляется в процессе работы за компьютером. При увеличении базы данных признаков хранение всех значений указанных величин становится нецелесообразным. Поэтому более удобным при реализации процедуры создания эталона является рекуррентное вычисление оценочных значений параметров нормального закона распределения – математического ожидания и среднеквадратичного отклонения по следующим формулам, приведенным в [3].

$$M_K = \frac{K-1}{K} \cdot M_{K-1} + \frac{X_K}{K}, \tag{2}$$

где X – значение биометрического признака, K – количество значений признака, использованных ранее для обучения.

$$\sigma_K = \sqrt{\frac{K-2}{K-1} \cdot \sigma^2_{K-1} + \frac{(X_K - M_K)^2}{K-1}}, \tag{3}$$

где X – значение биометрического признака, K – количество значений признака, использованных ранее для обучения, M_K – оценка математического ожидания на основании K значений признака.

При формировании эталона в реальном времени вычисляются значения признаков, но сохраняется только общее число уже использованных примеров и текущее значение математического ожидания.

Решения о предоставлении доступа принимаются в процессе работы субъекта на компьютере на основе усовершенствованной стратегии Байеса, учитывающей параметры и взаимное расположение функций плотностей вероятности значений признаков [4]. Метод последовательного применения формулы Байеса заключается в вычислении интегральных апостериорных вероятностей гипотез за некоторое число шагов при помощи формулы гипотез Байеса [5]. В [4] приводится модифицированная формула Байеса, при помощи которой удалось достигнуть наиболее высоких результатов в задаче распознавания пользователей компьютерных систем по подписи и клавиатурному почерку. Аналогичный подход было решено применить в данном исследовании с использованием формулы

$$P_j(H_i|A) = P_{j-1}(H_i|A) + \left[\frac{P_{j-1}(H_i|A)P(A_j|H_i)}{\sum_{i=1}^{n} P_{j-1}(H_i|A)P(A_j|H_i)} - P_{j-1}(H_i|A)\right] \cdot (W_j), \tag{4}$$

где W_j – вес j-го признака, $P(H_i/A_j)$ – апостериорная вероятность i-ой гипотезы, вычис-

ляемая на j-ом шаге при поступлении j-ого признака, $P(A_j/H_i)$ – условная вероятность i-ой гипотезы при поступлении признака A_j. Вес признака W_j вычисляется исходя из информативности признака, при $W_j = 1$ данная формула эквивалентна обычной формуле Байеса, подробно данный вопрос раскрывается в [4].

Каждая гипотеза подразумевает, что предъявляемые данные о подсознательных движениях принадлежат определенному субъекту, т.е. каждая гипотеза ассоциируется с определенным эталоном субъекта. На каждом шаге за априорную вероятность принимается апостериорная вероятность, вычисленная на предыдущем шаге. Новый шаг алгоритма воспроизводится в тот момент, когда происходит событие, при котором поступает новая информация о пользователе (нажатие клавиши, движение курсора мыши от одного элемента интерфейса к другому и т.д.), в формулу Байеса поступают данные о том признаке, с которым связано произошедшее событие. На первом шаге все гипотезы (субъекты) считаются равновероятными, т.е. $P_0(H_i/A) = 1/n$, где n – количество гипотез (пользователей). Условные вероятности вычисляются исходя из закона распределения значений признаков (в данном случае нормального). Чтобы отличить известного пользователя от неизвестного системе устанавливается пороговое значение апостериорных вероятностей гипотез, которое по аналогии с [4] было установлено равным 0,99. При преодолении данного значения определенной гипотезой, субъект, ассоциируемый с данной гипотезой считается идентифицированным.

Проведен натурный эксперимент, в ходе которого на основе созданных эталонов производилась идентификация работающих на компьютерах субъектов. В течение 7 минут все зарегистрированные в системе испытуемые (10 человек) были идентифицированы. В системе также работали лица, не имеющие эталон (20 человек). Через 10 минут доступ к ресурсу был заблокирован всем не имеющим эталона субъектам. Эксперимент был повторен 10 раз. Таким образом, было проведено 100 опытов по распознаванию известных (имеющих эталон) субъектов и 200 опытов по распознаванию неизвестных субъектов. Каждый эксперимент длился максимум 10 минут. Количество ошибок составило 6 (3 случая неверной классификации неизвестного пользователя, как известного и 6 случаев ошибочного не распознавания известного субъекта в течение 10 минут работы, т.е. отказ в доступе). Таким образом, по результатам проведения 300 опытов вероятность правильной классификации составила 0,97. Оценить полученные результаты в сравнении с достигнутыми ранее можно по таблице 2. В таблице 2 FRR означает вероятность ошибки 1-ого рода (ложный отказ в допуске), FAR – вероятность ошибки 2-ого рода (ложный допуск), P – вероятность правильного распознавания.

В заключительной части работы был проведен вычислительный эксперимент, в ходе которого на основе эталонов полученных до и после совершения нарушений генерировались значения признаков методом Монте-Карло. Далее эти значения признаков сравнивались с эталонами, полученными до совершения нарушений, при помощи стратегии Байеса. Количество значений каждого признака от каждого эталона составило 1000, что определяет приемлемую достоверность результатов. Анализ данных, полученных в рамках описанных выше экспериментов показал, что количество ошибок идентификации субъектов в состоянии после (во время) совершения нарушений режима доступа к информации увеличилось в среднем на 26%. Таким образом, информативность клавиатурного почерка и особенностей работы с мышью для задач непрерывной идентификации субъекта снижается при реализации им противоправных действий по отношению к информационным

Таблица 2: Сравнение полученных результатов с достигнутыми ранее

Технология	Кол-во испытуемых	Кол-во опытов	FRR	FAR	P
Нейронные сети [6]	32	320	—	—	0,97
Нейронные сети [7]	>100	5440	0,08	0,01	—
Статистические алгоритмы [8]	30	553	0,015	0,019	—
Статистические алгоритмы [9]	100	5000	0,014	0,014	0,986
Байесовские сети [10]	33	873	—	—	0,959
Нечеткая логика [11]	10	200	0,034	0,029	—
Разработанный метод	30	300	0,01	0,02	0,97

ресурсам. При выполнении заданий в условиях конкуренции степень неопределенности значений признаков клавиатурного почерка возрастает (в проведенных опытах величина дисперсии возрастала для каждого признака). При совершении нарушений режима доступа, неопределенность также значительно возрастает у большинства испытуемых (у 9 из 12). Возможно, это вызвано волнением. Чем больше субъект взволнован, тем более нестабилен клавиатурный почерк субъекта. Логично, что при совершении правонарушений волнение значительно усиливается, что отражается на динамических биометрических признаках субъекта. Однако это характерно не для всех испытуемых. Аналогичные заключения сделаны относительно особенностей работы испытуемых с мышью.

Список литературы

[1] Утечки конфиденциальной информации. Предварительные итоги 2014 года. – Zecurion Analytics. 2015 г. – http://www.zecurion.ru/upload/iblock/fe3/Zecurion_Data_leaks_2015.pdf.

[2] Раскин Д. Интерфейс: новые направления в проектировании компьютерных систем. – СПб: Символ-плюс, 2010. – 272 с.

[3] Брюхомицкий Ю.А., Казарин М.Н. Учебно-методическое пособие к циклу лабораторных работ «Исследование биометрических систем динамической аутентификации пользователей ПК по рукописному и клавиатурному почеркам» по курсу: «Защита информационных процессов в компьютерных системах». – Таганрог: Изд-во ТРТУ, 2004. – 38 с.

[4] Епифанцев Б.,Н., Ложников П.С., Сулавко А.Е. *Алгоритм идентификации гипотез в пространстве малоинформативных признаков на основе последовательного применения формулы Байеса//* В: *Межотраслевая информационная служба.* – ФГУП «ВИМИ». – 2013. – № 2. – С. 57–62.

[5] Вапник В.Н., Червоненкис А.Я. Теория распознавания образов (статистические проблемы обучения). – М.: Наука, 1974. – 416 с.

[6] Harun N., Woo W.L., Dlay S.S. *Performance of keystroke biometrics authentication system using artificial neural network (ann) and distance classifier method* // In: *Computer and Communication Engineering (ICCCE), 2010 International Conference.* – May 2010. – P. 1–6.

[7] Pavaday N., Soyjaudah K. *Investigating performance of neural networks in authentication using keystroke dynamics* // In: *AFRICON 2007.* – Sept. 2007. – P. 1–8.

[8] Ara'ujo L., Jr L.S., Ling L., Yabu-Uti J. *User authentication through typing biometrics features* // IEEE Transactions on Signal Processing. – Feb. 2005. – V. 53(2) – P. 851–855.

[9] Lv H.R., Wang W.Y. *Biologic verification based on pressure sensor keyboards and classifier fusion techniques* // IEEE Transactions on Consumer Electronics. – Aug. 2006. – V. 52(3) – P. 1057–1063.

[10] Balagani K.S., Phoha V.V., Ray A., Phoha S. *On the Discriminability of Keystroke Feature Vectors Used in Fixed Text Keystroke Authentication* // Pattern Recognition Letters. – 2011. – V. 32 – P. 1070–1080.

[11] Ara'ujo F., M L.C., Liz'arraga Gustavo, Sucupira L., Rabelo, Yabu-uti J., Tadanobu, Lee L.L. *Typing Biometrics User Authentication based on Fuzzy Logic* // IEEE Latin America Transactions. – March 2004. – V. 2(1) – P. 69–74.

УДК 004.056.5; 004.056.5

ВОЗМОЖНОСТЬ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПО ОСОБЕННОСТЯМ РАБОТЫ С МЫШЬЮ [31]

А. Е. Сулавко*[32], В. Ю. Писаренко*[33], А. И. Голева*[34], Н. Р. Стороженко*[35], Д. Н. Зверев**[36]

*Омский государственный технический университет,

** Омский государственный университет путей сообщения

г. Омск

Повсеместная информатизация и введение компьютеров в различные сферы деятельности приводит к массовому переходу на электронный документооборот. Поэтому актуализация вопросов защиты компьютерных ресурсов от несанкционированного доступа является закономерным явлением. Потеря, искажение, нарушение конфиденциальности информации наносит финансовый ущерб ее собственнику. По данным аналитических исследований компании *InfoWatch* основная доля этого ущерба (55%) обусловлена деятельностью инсайдеров – внутренних нелояльных по отношению к организации сотрудников [1]. В связи с этим требуется проводить скрытый мониторинг деятельности пользователя за компьютером, его непрерывную аутентификацию и распознавание опасных с точки зрения информационной безопасности действий. Современные средства аутентификации основаны на проверке паролей, смарт-карт и биометрических характеристик. Последний вариант позволяет привязать аутентификатор к личности человека, поэтому является предпочтительным. Основная проблема создания биометрических систем идентификации/аутентификации состоит в выделении информативных признаков. Наиболее надежными в этом плане являются открытые биометрические образы – отпечатки пальцев, радужная оболочка. Однако эти признаки находятся «на виду», существует множество способов их хищения незаметно для владельца. Кроме того, реализовать скрытую процедуру аутентификации с их использованием проблематично (если вообще возможно). В рамках данной работы предлагается подход для разграничения доступа в компьютерной системе на основе особенностей работы пользователя с мышью. Данные, полученные при работе пользователя с мышью, используются для аутентификации пользователя, получившего доступ к компьютерной системе. Это возможно в связи с тем, что у каждого пользователя существует собственная манера управления манипулятором «мышь» [2].

Прежде всего, необходимо выделить устойчивые признаки и создать эталон пользователя. Эталонная информация должна быть характерно различимой у разных людей, а образцы одного человека, должны быть схожи. Один из потенциальных признаков основан на оценке среднего времени перемещения курсора мыши между элементами интерфейса при помощи адаптированной для данной задачи формулы (1) закона Фиттса [3]. Закон связывает время движения субъекта к наблюдаемой цели с точностью движения и с расстоянием перемещения. Чем дальше или точнее выполняется движение руки (кисти, ноги

[31]Работа выполнена при финансовой поддержке РФФИ (проект 15-37-50269)

[32]sulavich@mail.ru

[33]xperia.v.j.p@gmail.com

[34]frybkf07.93@mail.ru

[35]snikr@bk.ru

[36]zverkjjl@mail.ru

и др.) субъекта, тем больше коррекции необходимо для его выполнения, и соответственно, больше времени требуется субъекту для внесения этой коррекции. При внесении коррекции движений проявляются индивидуальные особенности человека.

$$T = V_{mid} \cdot \log_2(\frac{D}{W} + 1), \tag{1}$$

где V_{mid} — средняя скорость движения курсора мыши между элементами интерфейса в пикселях в секунду, D — дистанция перемещения курсора между элементами интерфейса (в пикселях), W — ширина элемента интерфейса, к которому направляется курсор. V_{mid} вычисляется для каждой пары возникающих кнопок (элементов интерфейса) как среднее значений, рассчитанных по формуле (2). В качестве признаков также предлагается использовать амплитуды первых десяти низкочастотных гармоник функции $V_{mid}(t)$, вычисляемой по формуле (2). Разложение функции производится с помощью преобразования Фурье. Также признаками являются максимальное Cmax и среднее C_{mid} отклонения (в пикселях) от кратчайшего пути перемещения курсора между двумя элементами.

$$V_{xy}(t) = \sqrt{(x(t + \triangle t - x(t))^2 + (y(t + \triangle t) - y(t))^2}, \tag{2}$$

где x и y – координаты курсора, t – время регистрации координат курсора, $\triangle t$ – интервал времени между регистрацией координат курсора.

Для предварительной оценки информативности признаков разработан программный модуль. Элементы интерфейса, относительно которых производится измерение признаков – кнопки различных размеров, появляющиеся в случайно определенных областях экрана. Пользователю предлагается нажимать на данные кнопки.

На основании критерия Хи-квадрат установлено, что распределения описанных признаков близко к нормальному. Поэтому для создания эталонов были рассчитаны параметры данного закона распределения – математические ожидания и среднеквадратичные отклонения значений каждого признака. Эти параметры представляют собой эталон. Была собрана база, состоящая из набора 100 реализаций каждого признака шести испытуемых, т.е. создано шесть эталонов по данным о 100 перемещениях курсора для каждого пользователя.

В качестве способа принятия решений решено использовать стратегию Байеса [4], основанную на последовательном применении формулы гипотез Байеса (3). Каждая гипотеза подразумевает, что данные о движениях принадлежат определенному субъекту, то есть каждая гипотеза ассоциируется с определенным эталоном пользователя.

$$P_j(H_i/A) = \frac{P_{j-1}(H_i/A)P(A_j/H_i)}{\sum_{i=1}^{n} P_{j-1}(H_i/A)P(A_j/H_i)}, \tag{3}$$

где $P_j(H_i/A)$– апостериорная вероятность i-ой гипотезы, вычисляемая при поступлении j-ого признака, $P(A_j/H_i)$ – условная вероятность i-ой гипотезы при поступлении j-ого признака. Таким образом, на каждом шаге за априорную вероятность принимается апостериорная вероятность, вычисленная на предыдущем шаге. В режиме идентификации разработанного программного модуля при каждом перемещении курсора измеряются значения признаков и рассчитываются апостериорные вероятности гипотез по формуле (3) за

13 шагов.До осуществления перемещений курсора (на нулевом шаге) все гипотезы равновероятны, то есть, $P_0(H_i/A) = 1/n$, где n – количество гипотез (пользователей). Условные вероятности вычисляются исходя из закона распределения признаков (в данном случае нормального), как плотности вероятности поступающих значений признаков.

По результатам предварительной оценки при наличии 6 эталонов на основе разработанного программного модуля процент верных решений при идентификации пользователей составил 87%.

Список литературы

[1] Исследование утечек конфиденциальной информации: отчет InfoWatch. – 2014. – http://www.infowatch.ru/report2014. - (дата обращения 03.03.2015).

[2] Диденко С. М., Шапцев В. А. *Исследование динамики работы пользователя с манипулятором мышь* // В: *Математическое и информационное моделирование.* Тюмень: Изд-во Тюм. ун-та, 2004. – С. 295–304

[3] Раскин Д. Интерфейс: новые направления в проектировании компьютерных систем. – СПб: Символ-плюс, 2010. – 272 с.

[4] Епифанцев Б.Н., Ложников П.С., Сулавко А.Е. Алгоритм идентификации гипотез в пространстве малоинформативных признаков на основе последовательного применения формулы Байеса // *Межотраслевая информационная служба.* ФГУП «ВИМИ». – 2013. – № 2. – С. 57–62.

УДК 519.854.2

КОМБИНАТОРНЫЕ ЗАДАЧИ ДЛЯ НИЛЬПОТЕНТНЫХ И МЕТАБЕЛЕВЫХ ГРУПП[37]

А. В. Трейер[38]
Институт математики им. С. Л. Соболева СО РАН (Омский филиал),
Омский государственный технический университет,
г. Омск

В дискретной комбинаторной оптимизации широко известны задача о рюкзаке (имеется ввиду распознавательный вариант задачи) и задача о сумме подмножеств. Аналогичные по формулировке проблемы можно определить на группах. Пусть группа G задана представлением $G = \langle X | r_i(X) = 1, i \in I \rangle$, где $X = \{x_1, \ldots, x_n\}$ – конечное множество и на группе G разрешима проблема равенства слов в представлении выше.

Сформулируем задачу о рюкзаке для группы G:

Задача о рюкзаке. *Пусть $g_1, \ldots, g_k, g$ – слова в алфавите $X \cup X^{-1}$. Существуют ли неотрицательные целые числа $\varepsilon_1, \ldots, \varepsilon_k$, такие, что экспоненциальное групповое уравнение $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k} = g$ разрешимо в группе G.*

Приведем формулировку задачи о сумме подмножеств для группы G:

Задача о сумме подмножеств. *Пусть $g_1, \ldots, g_k, g$ – слова в алфавите $X \cup X^{-1}$. Существуют ли целые числа $\eta_1, \ldots, \eta_k \in \{0, 1\}$, такие, что экспоненциальное групповое уравнение $g_1^{\eta_1} \ldots g_k^{\eta_k} = g$ разрешимо в группе G.*

Так же как и в классической дискретной оптимизации, для задач выше, сформулированных над группами, можно исследовать вопрос о разрешимости этих задач и вопрос о принадлежности проблемы тому или иному классу сложности, в случае, если задача разрешима.

Два основных результата доклада, полученных в этом направлении, следующие: проблема о рюкзаке неразрешима для нильпотентных групп и проблема о сумме подмножеств для группы фонарщика NP-полна. Приведем строгие формулировки полученных результатов:

Теорема 1(А.А.Мищенко, А.В.Трейер). *Для любого натурального числа $c \geq 2$ существует конечно порожденная группа G ступени нильпотентности c такая, что задача о рюкзаке неразрешима на группе G.*

Теорема 2. *Пусть группа G задана представлением $G = \langle a, t | [t^{-m} a t^m, t^{-n} a t^n] = 1, a^2 = 1,\ m, n \in \mathbb{Z} \rangle$, тогда проблема о сумме подмножеств для группы G NP-полна.*

Исходя из геометрических свойств группы G из теоремы 2, некоторые авторы называют ее группой фонарщика или по-английски, "lamplighter group".

[37]Работа выполнена при финансовой поддержке РНФ (проект №14-11-00085)
[38]alexander.treyer@gmail.com

УДК 512.7

ЭЛЕМЕНТЫ АЛГЕБРАИЧЕСКОЙ ГЕОМЕТРИИ НАД НЕКОТОРЫМИ КЛАССАМИ ВПОЛНЕ ПРОСТЫХ ПОЛУГРУПП[39]

П. А. Уляшев[40]
Институт математики им. С. Л. Соболева СО РАН (Омский филиал),
г. Омск

Пусть S — произвольная полугруппа, I и Λ — непустые множества индексов и P — матрица элементов из S размера $|\Lambda| \times |I|$. Матричной полугруппой Риса $\mathcal{M}(S; I; \Lambda; P)$ называется множество $I \times S \times \Lambda$ с заданной на нем операцией умножения

$$(i, s, \lambda)(j, t, \mu) = (i, sp_{\lambda j}t, \mu).$$

Согласно классической теореме Риса (см. [1]) любая вполне простая полугруппа изоморфна некоторой матричной полугруппе Риса над группой.

В работе рассматриваются классы вполне простых полугрупп с ограничениями на матрицу P. При помощи методов, описанных в [2], получены критерии, определяющие координатные полугруппы алгебраических множеств.

Список литературы

[1] Howie J. Fundamentals of semigroup theory. The Clarendon Press, Oxford University Press, London Mathematical Society Monographs. NewSeries, – V. 12, 1995, 351 p.

[2] Даниярова Э.Ю., Мясников А.Г., Ремесленников В.Н. *Алгебраическая геометрия над алгебраическими системами. II. Основания*// Фундаментальная и прикладная математика. – 2011/2012. – Т. 17. – № 1. – С. 65–106.

[39]Работа выполнена при финансовой поддержке РНФ (проект 14-11-00085)
[40]p.ulyashev@gmail.com

УДК 512.53

CONES AND THICK MONOIDS IN FREE GROUPS[41]

E. Frenkel*[42], V. N. Remeslennikov**[43]
* Moscow State University, Moscow, Universita' degli Studi di Firenze, Florence, Italy,
Sobolev Institute of Mathematics (Omsk branch),
Omsk

In this paper we are going to expose some recent results obtained by authors on regular subsets of free groups, thick subsets and, in particular, thick monoids; we also prepare a detailed version of the current paper. Regular sets and their algorithmic properties together with thick subsets was previously studied by authors and their coauthors in a series of papers [1], [2], and [3]. In the present paper we are interested in more subtle classification of thick sets and their structure. To fulfill this task, we use the so-called cones (i.e. subsets of free groups with a fixed prefix or postfix) and double based cones (i.e. cones with both ends being fixed, see p. 66 for precise definitions), as well as thick monoids. The latter term appears as a product of decomposition of an arbitrary set into sets of the special form and constitute the heart of the problem from computational and algorithmic points of view. We apply such measuring tools as $\lambda-$measure and generating functions (defined on p. 65). Our methods allow also to calculate generating functions and therefore Cesaro measures of cones and thick monoids directly without laborious computations involved in standard linear algorithm (cited on p. 65; see Lemma 5 and Theorem 6 for results).

Regular subsets. We start from basics on regular sets and proceed with the main definitions on the asymptotic characteristics of regular sets (see, for example, the papers above for more details). Let $X = \{x_1, \ldots, x_m\}$ be an alphabet and define Σ to be the letters of X with their formal inverses: $\Sigma = X \cup X^{-1}$. Let $F = F(X)$ be the free group generated by X.

Now we are going to introduce the machinery to deal with such subclass of subsets in F as regular sets. Namely, a *finite state automaton* $\mathcal{A}$ is a quintuple $(S, \Sigma, \delta, I, Z)$, where S is a finite set of states, Σ is an alphabet, $I \subset S$ is the (non-empty) set of initial states, $Z \subseteq S$ is the set of final states, and δ is a set of arrows with labels in the enlarged alphabet $\Sigma \cup \varepsilon$ (here ε is assumed not to lie in Σ). Further, a *deterministic automaton* can be considered a special case of a finite state automaton with no arrows labelled ε, the only one initial state and each state being the source of exactly one arrow with any given label from Σ.

By the Kleene-Rabin-Scott theorem, all *regular* subsets over Σ (i.e. the closure of finite subsets of free monoid over Σ under the rational operations) are exactly the sets accepted by a finite state automaton over $\Sigma \cup \epsilon$, or, equivalently, accepted by a deterministic automaton over Σ. The language accepted by an automaton $\mathcal{A}$ we shall denote by $L = L(\mathcal{A})$.

For a subset R of F, denote by $f_k(R) = \frac{|R \cap S_k|}{|S_k|}$ the *frequency* of elements from R among the words of length k in F. The frequencies of elements in a subset will help us to define the $\lambda-$measure and the generating function of this set.

[41]The work is supported by the RFBR (project 14-01-00068-a)
[42]lizzy.frenkel@gmail.com
[43]remesl@ofim.oscsbras.ru

$\lambda-$ **measure.** An important measuring tool in F is the so-called $\lambda-$*measure*. By definition,

$$\lambda(R) = \sum_{k=0}^{\infty} f_k(R).$$

A subset $R \subseteq F$ is called λ-*measurable*, if $\lambda(R) < \infty$, and *exponentially* $\lambda-$*measurable* if there exists a positive constant $\delta < 1$ such that $f_k(R) < \delta^k$ for big enough k. We adjuste this measure to obtain $\lambda^*(R) = \frac{2m}{2m-1}\lambda(R)$.

Generating function. Another widely used characteristic is the so-called generating function of a set. The *generating function* for R is a formal series:

$$g_R(t) = \sum_{k=0}^{\infty} f_k(R)t^k.$$

We shall also use the *adjusted* version of this function: $g_R^*(t) = \frac{2m}{2m-1} \cdot g_R(t)$. In case of regular subsets of F the generating function can be described in a very concise form:

Theorem 1. *For a regular set $R \subseteq F$ the function $g_R(t)$ is a rational function of t with rational coefficients and either*

- *has no singularity at $t = 1$ (in this case R is exponentially $\lambda-$measurable) or*
- *has a simple pole at $t = 1$ (in this case R is thick).*

In particular,

$$Res_1 g_R(t) = -\mu_0(R).$$

It remains to say that a regular set is called *thick* if the parameter $\mu_0(R)$ defined by formula above is strictly positive. This parameter $\mu_0(R)$ is called *Cesaro density* of R. Moreover, for every regular set R the function $g_R(t)$ can be computed algorithmically. Here we cite a standard algorithm, that given automaton $\mathcal{A}$ such that $L(\mathcal{A}) = R$ output the function $g_R(t)$:

Algorithm I computing the frequency generating function $g_R(t)$ for a regular set R. Let $\mathcal{A} = (S, \Sigma, \delta, I, Z)$ be an automaton such that $|S| = n$ and let A be it's adjacency matrix, i.e. $n \times n$ matrix such that a_{ij} corresponds to the number of arrows from the state i to the state j. Let $R = L(\mathcal{A})$.

1. Given an automaton $\mathcal{A}$, compute the adjacency matrix A.
2. Compute the fundamental matrix $B = tA(E - tA)^{-1}$ of $\mathcal{A}$.
3. The generating function $g_R(t)$ is equal to $\sum\limits_{i \in I, j \in Z} b_{ij}$.

Unfortunately, this algorithm involves the matrix inversion and therefore hardly implementable whenever the size of automaton n is big enough. One of our main goals is to provide more direct and suitable for practical purposes methods of calculation of $g_R(t)$.

We are going to split regular subsets of free groups into special pieces such that the measures of these new subsets can be computed directly. Now we recall the notions of such regular sets as cones, introduced in [1] and investigated in further papers [2] and [3].

A *cone* $C(w)$ with the handle w is a set of all elements in F containing the given word w as initial segment. A cone with a *right-hand side handle*, i.e. the set of all words in F that *terminates* with w (we denote this sort of cones by $C[w]$). A *double-based cone* with handles w_1, w_2, is a set of all elements in F of the form $w_1 \circ f \circ w_2$, $f \in F$.

Further, let us define one of the crucial for our purposes notions: the notion of a special automaton. It appears in similar form at [1]; here we improve this machinery and compute the asymptotic characteristics of the obtained automata explicitly.

Let $\mathcal{A} = (S, X \cup X^{-1}, \delta, i_0, Z)$ be a deterministic automaton. Then $\mathcal{A}$ is called *special* over F if

a. The initial vertex has no inedges;

b. There is only one final state $z_0 \in Z$;

c. $\mathcal{A}$ does not contain inaccessible states;

d. For every state $s \in S$ there is a direct path from s to the final state z_0;

e. For any state $s \in S$, all arrows which enter s have the same label $x \in X \cup X^{-1}$. We shall say in this situation that *s has type x*.

f. For any state s of type x in $\mathcal{A}$, all arrows exiting from s cannot have label x^{-1}.

The following theorem explains relation between the class of all regular sets and the special automata.

Theorem 2. *Let L be a regular language in F. Then there exist a finite number of special automata $\mathcal{A}_1, \ldots, \mathcal{A}_k$ such that L is a disjoint union of languages $L_0 = L(\mathcal{A}_0), \ldots, L_k = L(\mathcal{A}_k)$ in F: $L = L_0 \sqcup L_2 \sqcup \ldots \sqcup L_k$.*

Notice also, that, generally speaking, this decomposition is not unique.

Continuing the procedure of splitting of the special automata, we obtain the following lemma.

Lemma 3. *Let $R = R(\mathcal{A})$ and $\mathcal{A} = (S, X \cup X^{-1}, \delta, i_0, z_0)$ be a special automaton over F. Then there exist regular languages R_1, R_2, R_3 in F such that $R_j = L(\mathcal{A}_|)$, with $\mathcal{A}_j = (S_j, X \cup X^{-1}, \delta_j, i_j, z_j)$, $j = 1, 2, 3$; $\mathcal{A}_1$ being special, and*

1. *if $\mathcal{A}$ has at least one arrow exiting z_0, then R_2 is non-empty, $i_2 = z_2$, $i_3 \neq z_3$ and*

$$R = R_1 \circ R_2 \text{ is unambiguos};$$
$$R_2 = 1 \sqcup R_3 \sqcup (R_3 \circ R_3) \sqcup (R_3 \circ R_3 \circ R_3) \sqcup \cdots;$$
$$g_R(t) = g_{R_1}(t) g^*_{R_2}(t); \quad \lambda(R) = \lambda(R_1)\lambda^*(R_2).$$

2. *if there is no arrows exiting z_0, then $R_2 = R_3 = \emptyset$, $R = R_1$, $\lambda(R) = \lambda(R_1)$, and $g_R(t) = g_{R_1}(t)$.*

It turns out that for regular sets accepted by special automaton their thickness can be easily checked.

An automaton $\mathcal{A}$ with $i_0 = z_0$ is called $X-$*complete* if for every state $s \in S$ of type x all arrows labeled by $X \cup X^{-1} \setminus \{x^{-1}\}$ exit from s.

Proposition 4. *Let $\mathcal{A}$ be a special automaton, and $R = L(\mathcal{A})$ be a set such that $R = R_1 \circ R_2$ is the splitting of the form described above, with $R_2 = L(\mathcal{A}_2)$. If $\mathcal{A}_2$ is not X-complete, then R is exponentially $\lambda-$ measurable.*

The proposition above makes the computation of generating function for R easy; recall that $\mu_0(R)$ in this case is 0.

Therefore, it remains to analyze the case where the automaton $\mathcal{A}_2$ obtained in the decomposition of R is $X-$complete. Indeed, let R_2 be a regular subset of F of second type accepted by the automaton $\mathcal{A}_2$. Then R_2 forms a monoid, and if $\mathcal{A}_2$ is $X-$complete, then the *monoid* R_2 we shall call *thick*. An interesting fact about thick monoids is that we can describe them in terms of double-based cones. In turns, one can compute precisely the values of the generating function and Cesaro density of double-based cones (see Lemma 5 and Theorem 6 below); therefore, it can be made precisely for thick monoids.

Lemma 5. *Let $C(a, b)$ be a double-based cone with both handles a, b in $X \cup X^{-1}$. Then following holds:*

1. *$f_k(C(a, b)) = f_k(C(c, d))$ and therefore $g_{C(a,b)}(t) = g_{C(c,d)}(t)$ for all a, b, c, d in $X \cup X^{-1}$ such that $ab \neq 1$, $cd \neq 1$. Further, $f_k(C(a, a^{-1})) = f_k(C(b, b^{-1}))$ for arbitrary $a, b \in X \cup X^{-1}$.*

2. $f_k(C(a, a^{-1})) = (2m-1)f_k(C(a, a)) - \dfrac{1}{2m(2m-1)^{k-1}}$, *for* $k \geq 3$,

3. $g_{C(a,a)}(t) = \dfrac{t^2}{4m^2(1-t)} + \dfrac{t^2}{4m^2(2m-1)} + \dfrac{t^3}{2m(2m-1)(2m-1-t)}$,

   and

   $g_{C(a,a^{-1})}(t) = \dfrac{t^2}{4m^2(1-t)} - \dfrac{t^2}{4m^2} - \dfrac{t^3}{2m(2m-1-t)}$,

4. $\mu_0(C(a, b)) = \mu_0(C(c, d)) = \dfrac{1}{4m^2}$ *for all* $a, b, c, d \in X \cup X^{-1}$.

The generating function and Cesaro density of the arbitrary double-based cone are provided in the following theorem:

Theorem 6. *Let $R = C(u, v)$ be a double-based cone with handles u, v in F such that $u = u_0 \circ a$, $v = b \circ v_0$, where $u_0, v_0 \in F$ and $a, b \in X \cup X^{-1}$. Then*

1. $g_R(t) = g_{C(a,b)}(t) \cdot \lambda^*(u_0) \cdot \lambda^*(v_0)$;

2. $\mu_0(R) = \dfrac{\lambda^*(u_0) \cdot \lambda^*(v_0)}{4m^2}$.

We want to conclude this paper with another result that reveals importance of the thick monoids. Indeed, the following classification of regular subsets was known from [1]:

Theorem 7. *Let F be a free group and R be a regular subset of F. Then*

1. *every regular subset in F is either thick or exponentially negligible;*

2. *a regular subset in F is thick if and only if its prefix closure contains a cone.*

This powerful statement on regular subsets is practically inconvenient in its claim 2: instead of characterisation of the set itself we describe its prefix closure. Fortunately, we can save the situation using precisely the notion of a thick monoid:

Theorem 8. *A regular subset R of F is thick if and only if it contains a thick monoid.*

Список литературы

[1] Borovik A.V., Myasnikov A.G., Remeslennikov V.N. *Multiplicative measures on free groups* // Intern. J. of Algebra and Computation, – 2003. – V.13. – №6. – P. 705–731.

[2] Frenkel E., Myasnikov A.G., Remeslennikov V.N. *Regular sets and counting in free groups*// In: *Combinatorial and Geometric Group Theory.* Series "Trends in Mathematics". Basel: Birkhauser-Verlag, 2010, – P. 93–118.

[3] Frenkel E., Remeslennikov V.N. *Double cosets in free groups* // International Journal of Algebra and Computation. —2013. – V. 23. – № 5. – P. 1225–1241.

УДК 512.53

О ПОДПОЛУГРУППАХ СВОБОДНОЙ ЛЕВОРЕГУЛЯРНОЙ ПОЛУГРУППЫ[44]

А. Н. Шевляков[45]
Институт математики им. С. Л. Соболева СО РАН (Омский филиал),
г. Омск

Многообразие леворегулярных полугрупп задается тождествами $xx = x$ (идемпотентность) и $xyx = xy$ (левая регулярность). Обозначим через $\mathcal{F}_n$ свободную леворегулярную полугруппу ранга n. В докладе предложено описание всех конечных леворегулярных полугрупп вложимых в $\mathcal{F}_n$ при подходящем значении n.

[44]Работа выполнена при финансовой поддержке РНФ (проект 14-11-00085)
[45]a_shevl@mail.ru

УДК 519.178; 004.7; 004.056.5

ЗАДАЧА О МАКСИМАЛЬНОМ ПОТОКЕ В БУЛЕВОЗНАЧНОЙ СЕТИ И ЕЕ ПРИЛОЖЕНИЯ

Е. В. Щерба[46], В. А. Соловьев
Омский государственный технический университет,
г. Омск

Одной из классических задач алгоритмической теории графов является задача отыскания максимального потока в транспортной сети. Под транспортной сетью понимается ориентированный граф, дугам которого приписаны некоторые положительные числа (веса). Различные методы и алгоритмы для решения указанной задачи в разное время были предложены Фордом и Фалкерсоном [1], Диницем [2], Карзановым [3] и другими исследователями (см. [4]). Указанная задача имеет важное практическое значение в области телекоммуникаций. В частности, её решение можно использовать для балансировки потоков при маршрутизации, максимизации количества передаваемых пакетов между узлами, поиска «узких» мест в распределенной компьютерной сети.

Вместе с тем, актуальные потребности в новых сетевых протоколах и технологиях зачастую связаны с проблемами информационной безопасности. Для разграничения доступа и повышения безопасности в глобальных телекоммуникационных сетях широко применяется процедура межсетевого экранирования (фильтрация различных типов сетевого трафика).

Рассмотрим следующую задачу. Пусть задана маршрутизируемая сеть передачи данных, отправитель и получатель в которой предопределены. Данные, передаваемые по сети, относятся к некоторому конкретному типу, и число различных типов конечно. В качестве примера, различные типы данных могут быть ассоциированы с различными сетевыми протоколами, адресами сетей и узлов, номерами сетевых портов, метками безопасности или с пересечениями по указанным селекторам. Каждый маршрутизатор в сети может ограничивать передачу данных определенного типа, т.е. функционирует как пакетный фильтр. Множество разрешенных типов данных для каждого канала связи определяется двумя маршрутизаторами, связанными непосредственно при помощи данного канала.

[46]evscherba@gmail.com

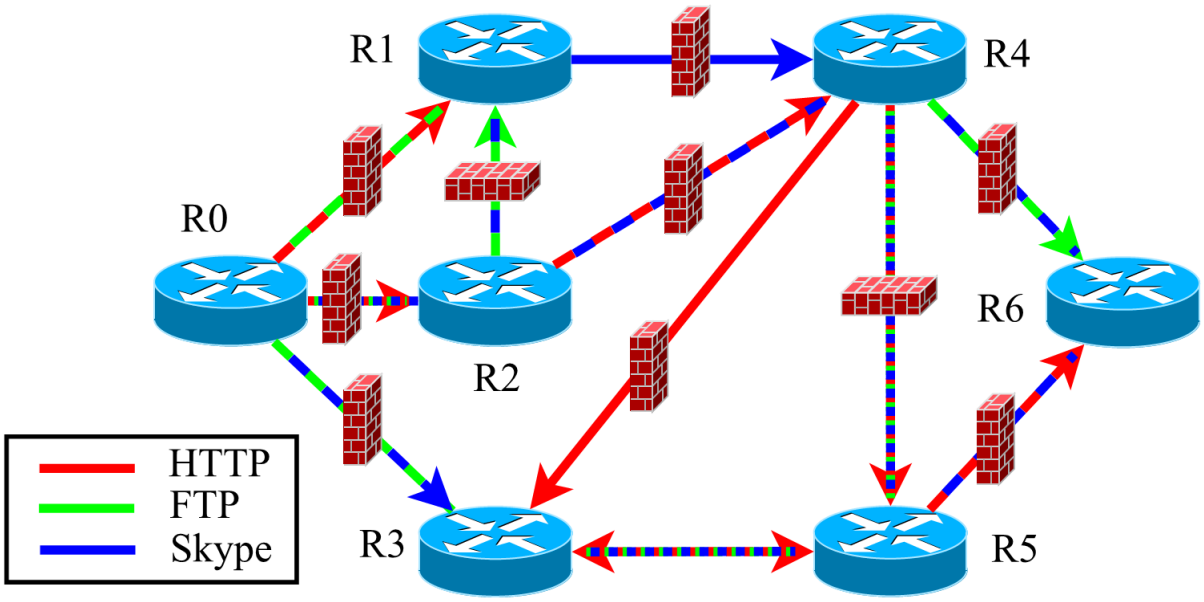


Рис. 3: Пример телекоммуникационной сети с пакетной фильтрацией

Пример сети, соответствующей описанной модели, представлен на рис. 3. В рассматриваемом примере представлено три типа данных (HTTP, FTP и Skype). Для каждого канала определены разрешенные типы данных. Множество всех разрешенных типов данных, доступных для передачи от маршрутизатора *R0* к маршрутизатору *R6* состоит из двух элементов {HTTP, Skype}, поскольку тип данных {FTP} фильтруется.

В общем случае существует проблема определения множества всех разрешенных типов данных, которые могут быть переданы по сети от источника к получателю, и путей для их передачи. Классические методы не могут быть напрямую использованы для решения этой задачи, поскольку используется не количественная, а качественная характеристика данных и каналов связи, и требуется найти максимальный логический поток.

Для формализации представленной задачи, используем определение булевозначной сети, предложенное В.Н. Салием [5]. Под булевозначной сетью понимается ориентированный мультиграф, каждой дуге которого приписан некоторый элемент из фиксированной конечной булевой алгебры B.

Пусть M - это конечное множество всех возможных типов данных, передаваемых по сети, $P(M)$ - множество всех подмножеств множества M. Булева алгебра B определяется как $\langle P(M)|\vee,\wedge,\neg,0,1\rangle$. Пусть V - конечное множество маршрутизаторов, E - конечное множество каналов связи, соединяющих маршрутизаторы, для каждого канала задана пропускная способность (множество разрешенных типов данных). Таким образом определена булевозначная сеть $G=(V,E)$ с функцией пропускных способностей $c: E \to B$.

Далее будем рассматривать двухполюсную булевозначную сеть, в которой вершина s ассоциирована с источником информации и является источником в данной сети, а вершина t ассоциирована с получателем информации и является стоком.

Для исходного примера $M=\{a_1,a_2,a_3\}, P(M)=\{0,a_1,a_2,a_3,a_1a_2,a_1a_3,a_2a_3,1\}$. Булевозначная сеть, соответствующая исходной модели, представлена на рис. 2. Для дальнейшей формализации задачи потребуется ввести несколько определений.

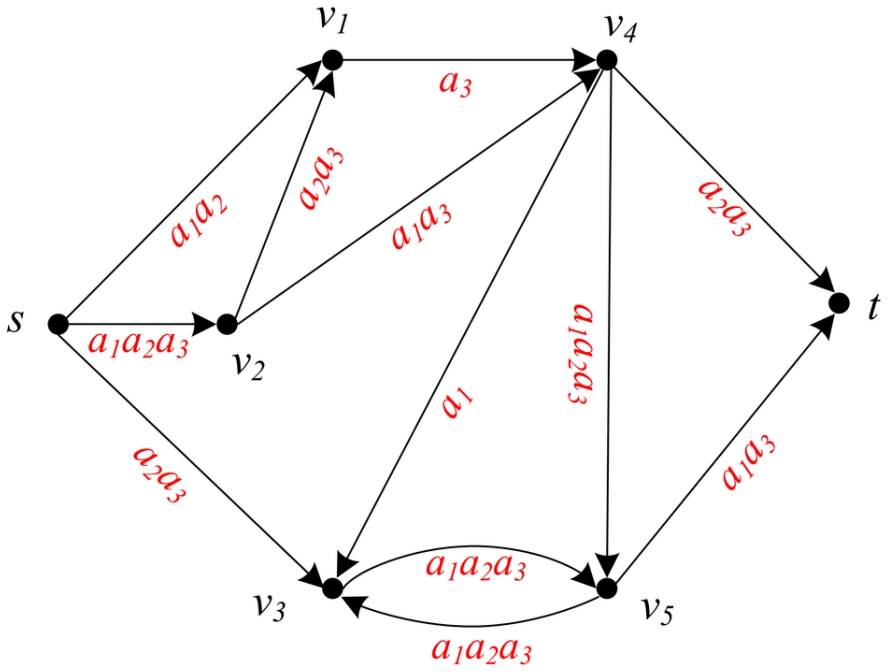


Рис. 4: Пример булевозначной сети, соответствующей исходной модели

Определение 1. Пусть задана булевозначная B-сеть $G = (V, E)$ с источником s, стоком t, функцией пропускных способностей $c : E \to B$. Потоком из s в t в данной сети назовём функцию $f : E \to B$, удовлетворяющую следующим условиям:

1) $0 \leq f(e) \leq c(e)$ для всех $e \in E$;

2) $\bigvee\limits_{u \in V} f(u, v) = \bigvee\limits_{u \in V} f(v, u)$ для всех $v \in V \setminus \{s, t\}$;

3) $\bigvee\limits_{u \in V} f(s, u) = \bigvee\limits_{v \in V} f(v, t)$.

Определение 2. Величиной потока f будем называть элемент булевой алгебры $b \in B$:

$$b(f) = \bigvee_{v \in V} f(s, v).$$

Определение 3. Мощностью потока $|b(f)|$ будем называть число атомов (элементов множества M), содержащихся в его величине.

Определение 4. Поток f^* называется максимальным, если

$$|b(f^*)| = \max_f |b(f)|.$$

Определение 5. Пропускной способностью разреза $(W, \overline{W})$ будем называть элемент

булевой алгебры $c \in B$:

$$c(W, \overline{W}) = \bigvee_{e \in (W, \overline{W})} c(e).$$

Определение 6. Мощностью разреза $|c(W, \overline{W})|$ будем называть число атомов (элементов множества M), содержащихся в его пропускной способности.

Определение 7. Среди всех разрезов, разделяющих s и t, разрез с минимальной мощностью называется минимальным.

Утверждение. *В любой конечной булевозначной сети $G = (V, E)$ величина максимального потока f из s в t не превосходит пропускную способность минимального разреза $(W, \overline{W})$, разделяющего s и t:*

$$b(f) \leq c(W, \overline{W}).$$

Таким образом, для решения исходной задачи необходимо найти максимальный поток f из s в t в заданной булевозначной сети $G = (V, E)$ с функцией пропускных способностей $c : E \to B$. Для нахождения максимального потока в булевозначной сети можно использовать интуитивный алгоритм с оценкой сложности $O(|M||V|^2)$. Идея алгоритма состоит в том, чтобы найти путь из s в t для каждого атома булевой алгебры B, и если этот путь существует, добавить данный атом к значению потока для каждой дуги, входящей в найденный путь.

Определение 8. Пусть задана булевозначная B-сеть $G = (V, E)$ с источником s, стоком t, функцией пропускных способностей $c : E \to B$. Предпотоком из s в t в данной сети назовём функцию $f^* : E \to B$, удовлетворяющую следующим условиям:

1) $0 \leq f^*(e) \leq c(e)$ для всех $e \in E$;

2) $\bigvee\limits_{u \in V} f^*(u, v) \geq \bigvee\limits_{u \in V} f^*(v, u)$ для всех $v \in V \setminus \{s\}$.

В результате адаптации метода проталкивания предпотока в транспортных сетях для булевозначных сетей, был предложен более эффективный алгоритм нахождения максимального потока в булевозначной сети. Дополнительные обозначения: A - список активных вершин, A^* - вспомогательный список, $f_i(v)$ - совокупный предпоток, входящий в вершину v. Описание алгоритма см. в конце статьи после списка литературы.

Идея алгоритма состоит в итеративном проталкивании максимального предпотока от источника к стоку. По завершении проталкивания, объединение предпотоков, входящих в сток, будет соответствовать максимальному потоку в данной сети. Второй этап алгоритма предназначен для итеративного приведения предпотока к максимальному потоку от стока к источнику.

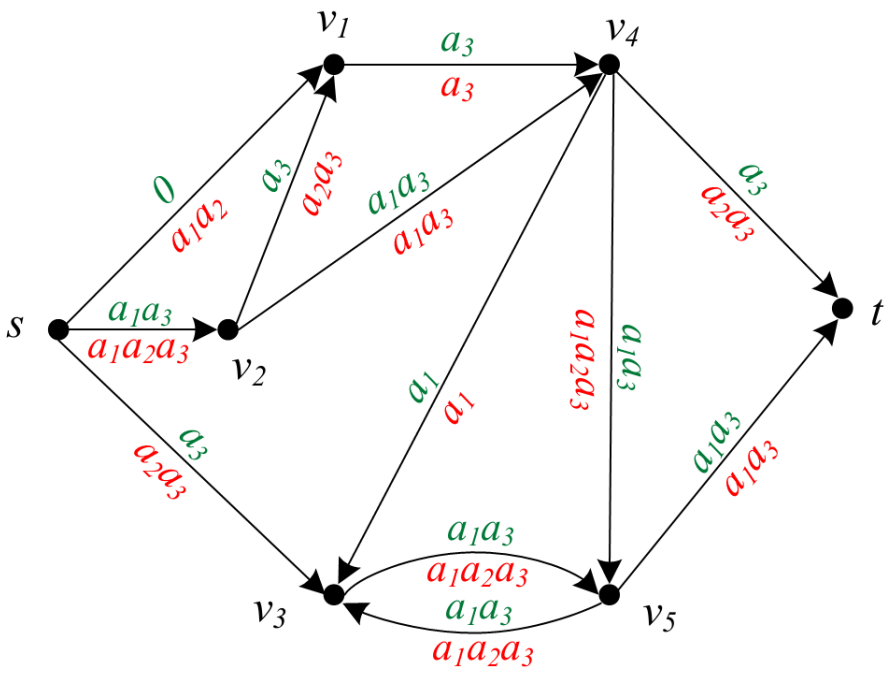


Рис. 5: Пример определения максимального потока в заданной сети

Применяя представленный выше алгоритм к булевозначной сети, представленной на рис. 4, можно определить значение максимального потока из s в t в данной сети (рис. 5) и его величину $\{a_1a_3\}$, т.е. множество всех разрешенных типов данных, которые могут быть переданы по сети от источника к получателю, в исходной постановке задачи.

Таким образом, в работе рассмотрена актуальная задача сетевой безопасности, представлена соответствующая ей формальная задача о максимальном потоке в булевозначной сети и предложен эффективный алгоритм для её решения. В целом, применение моделей булевозначных сетей открывает новые возможности для решения важных сетевых проблем, а разработка новых протоколов и технологий на базе этого подхода представляет перспективную область исследований.

Список литературы

[1] Ford L.R., Fulkerson D.R., *Maximal flow through a network* // Canadian Journal of Mathematics. – 1956. – V. 8. – P. 399–403.

[2] Диниц Е.А., *Алгоритм решения задачи о максимальном потоке в сети со степенной оценкой* // Доклады АН СССР. – 1970. – Т. 194. – № 4. – С. 754–757.

[3] Карзанов А.А., *Нахождение максимального потока в сети методом предпотоков* // Доклады АН СССР. – 1974. – Т. 215. – № 1. – С. 49–53.

[4] Goldberg A.V., Tarjan R.E., *Efficient Maximum Flow Algorithms* // Communications of the ACM. – 2014. – V. 57. – № 8. – P. 82–89.

[5] Салий В.Н., *Оптимизация в булевозначных сетях* // Дискретная математика. – 2005. – Т. 17. – № 1. – С. 141–146.

Algorithm 1 Алгоритм нахождения максимального потока в булевозначной сети

```
procedure PushMaxFlowBoolean(G, M, c, s, t)
    A ← {s}, A* ← {∅}, f_i(s) ← {1}                ▷ Проталкивание предпотока к стоку
    for all v ∈ V(G)\{s} do
        f_i(v) ← {∅}
    end for
    while A ≠ {∅} do
        for all u ∈ A do
            for all v ∈ V(G) do
                f_i*(v) ← f_i(v)
                if (u, v) ∈ E(G) then
                    f*(u, v) ← (f_i(u) ∧ c(u, v))
                    f_i(v) ← (f_i(v) ∨ f*(u, v))
                    if f_i*(v) ≠ f_i(v) then
                        A* ← A* ∨ {v}
                    end if
                end if
            end for
        end for
        A ← A*, A* ← {∅}
    end while
    A ← {t}, A* ← {∅}                              ▷ Приведение предпотока к максимальному потоку
    for all v ∈ V(G)\{t} do
        f_i(v) ← {∅}
    end for
    while A ≠ {∅} do
        for all u ∈ A do
            for all v ∈ V(G) do
                f_i*(v) ← f_i(v)
                if (v, u) ∈ E(G) then
                    f(v, u) ← (f_i(u) ∧ f*(v, u))
                    f_i(v) ← (f_i(v) ∨ f(v, u))
                    if f_i*(v) ≠ f_i(v) then
                        A* ← A* ∨ {v}
                    end if
                end if
            end for
        end for
        A ← A*, A* ← {∅}
    end while
    return f
end procedure
```