



Международная конференция
**"Современные проблемы математики,
механики и их приложений"**
посвященная 70-летию ректора МГУ
академика В.А.Садовниченко



Материалы конференции

The International Conference
**"Modern problems of mathematics, mechanics and
their applications"**
dedicated to the 70-th anniversary of rector of MSU
acad. V.A.Sadovnichy

Materials of the conference



30 марта – 02 апреля 2009 года
Московский Государственный Университет имени М.В.Ломоносова

Программный комитет:

Академик Ю.С. Осипов (председатель), В.В. Александров, академик А.А. Гончар, Е.П. Долженко, академик С.В. Емельянов, академик Ю.И. Журавлев, академик В.А. Ильин, В.П. Карликов, член-корр. Б.С. Кашин, академик В.В. Козлов, Г.М. Кобельков, академик С.К. Коровин, А.Г. Костюченко, Т.П. Лукашенко, академик Е.И. Моисеев, член-корр. Ю.В. Нестеренко, академик С.М. Никольский, М.К. Потапов, Н.Х. Розов, И.Н. Сергеев, академик А.Т. Фоменко, академик Г.Г. Черный, В.Н. Чубариков, А.С. Шамаев, А.А. Шкаликов.

Организационный комитет:

В.Н. Чубариков (председатель), Т.П. Лукашенко (зам. председателя), В.В. Белокуров, А.В. Боровских, В.В. Галатенко, Д.В. Георгиевский, А.И. Козко, С.Н. Михалев, А.С. Печенцов (зам. председателя), В.Е. Подольский, Т.В. Родионов, А.М. Савчук, К.В. Семенов, Н.В. Семин, И.Н. Сергеев (зам. председателя), С.А. Степин, С.В. Шапошников, А.А. Шкаликов.

Секции конференции

1. Функциональный анализ. Теория операторов.	13
2. Теория функций.	68
3. Дифференциальные уравнения.	110
4. Механика и математическая физика.	264
5. Математика в естествознании.	311
6. Преподавание математики в средней и высшей школе. .	341
7. Интеллектуальные системы и компьютерные науки. ...	351
8. Общие проблемы математики.	383

Конференцию поддержали:

1. Российский фонд фундаментальных исследований
2. Министерство образования и науки РФ
3. Московский Государственный Университет им. М.В.Ломоносова
4. Выпускник механико-математического факультета МГУ О.Д.Звягин
5. Выпускник механико-математического факультета МГУ А.В.Чеглаков

Современные проблемы математики, механики и их приложений. Материалы международной конференции, посвященной 70-летию ректора МГУ академика В.А. Садовниченко. – М.: Издательство «Университетская книга», 2009. – 416с.

Пусть A, B – конечные алфавиты, $|A| = N, |B| = M$. Для $k \in \mathbb{Z}_+$ определим классы языков $L_k(A) = \{L \subseteq A^* \mid \forall \alpha \in L \Rightarrow |\alpha| = k\}$ и $L_{\leq k}(A) = \{L \subseteq A^* \mid \forall \alpha \in L \Rightarrow |\alpha| \leq k\}$.

Пусть $L \subseteq A^*$ – регулярный язык, $s \geq 2, s \in \mathbb{N}$. s -коллекцией языка L назовем семейство языков $\tau(L, s) = \{L_0, \dots, L_{s-1}\}$ таких, что: $L_i \cap L_j = \emptyset, i \neq j, i, j = 0, \dots, s-1$; $\bigcup_{i=1}^{s-1} L_i = L$; $L_0 \stackrel{\text{def}}{=} A^* \setminus L$.

Конечный инициальный автомат $V_{q_0} = (A, B, Q, \varphi, \psi, q_0)$ представляет s -коллекцию языка L $\tau(L, s)$ ($V_q \sim \tau(L, s)$) с помощью системы подмножеств выходного алфавита $\{B_0, \dots, B_{s-1}\}$, $B_i \subset B, B_i \cap B_j = \emptyset, i \neq j, i, j = 0, \dots, s-1$, если

$$\forall \alpha \in L_i \quad \psi(q_0, \alpha) \in B_i, \quad i = 0, \dots, s-1.$$

Пусть $N \geq 2, M \geq 2, K \subseteq A^*$ – класс регулярных языков над алфавитом A . s -сложностью K назовем

$$S_{cc}(K, N, M) = \max_{L \in K} \max_{\tau(L, M)} \min_{V_q \sim \tau(L, M)} S_{ac}(V_q),$$

где $S_{ac}(V_q)$ – число состояний в автомате.

Теорема. $\forall N \geq 2, M \geq 2, \forall k \geq 1$ существует $p \geq 0$, конечный язык $L \in L_k(A)$, коллекция $\tau(L, M)$ и ИКА $V_q(k, N, M) \sim \tau(L, M)$, такие что

$$S_{ac}(V_q(k, N, M)) = S_{cc}(L_k(A), N, M) = \frac{N^{k-p} - 1}{N - 1} + \sum_{i=1}^p (M^{N^i} - p + 1)$$

Следствие. $\forall N \geq 2, M \geq 2$ для $S_{cc}(L_k(A), N, M)$ выполнено

$$\frac{1}{N-1} \cdot \frac{N^k \cdot \log_N M}{k} \lesssim S_{cc}(L_k(A), N, M) \lesssim \frac{N}{N-1} \cdot \frac{N^k \cdot \log_N M}{k}$$

Литература

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. Наука, Москва, 1985.

ОБ АЛГОРИТМЕ ЗАКРЫТОГО СУНДУКА

Хамдамов Р.Х., Кодиров Н.Х.

r.hamdamov@msu.uz, nodir_qodirov@yahoo.com

Алгоритм закрытого сундука основывается на задаче о рюкзаке, которая впервые была предложена 1979 году Ральфом Марклином и Мартином Хеллманом. Тот алгоритм использовал рюкзачные системы и элементы рюкзака передались от одного абонента к другому через открытый канал после использования аппарата модулярной арифметики для каждого элемента рюкзака $/1/$. В предлагаемом новом алгоритме элементы рюкзака (сундука) генерируются каждым абонентом отдельно на основе их закрытого параметра и отсюда происходит названия "алгоритм закрытого сундука". Для генерации закрытых ключей используются псевдослучайные числа, имеющие определенную закономерность распределения.

Предположим абоненты A и B должны обмениваться сообщениями. Здесь абонент B – отправитель, а абонент A – получатель. Для обмена сообщением в данном алгоритме они поступают по следующей вычислительной схеме.

1. Абоненты A и B генерируют общий закрытый параметр $e_A^Z = e_B^Z = e^Z$, используя алгоритм генерации закрытых ключей, например Диффи-Хеллмана.

2. Для шифрования открытого сообщения $X = \{x_1, x_2, \dots, x_l\}$, которое построено в алфавите Z , абонент B на основе общего закрытого параметра e^Z генерирует n – элементы закрытого сундука $K^Z = \{k_1^Z, k_2^Z, \dots, k_n^Z\}$ используя генератор псевдослучайных чисел. После этого берутся коды букв $X = \{x_1, x_2, \dots, x_l\}$ открытого сообщения в алфавите Z , где длина каждого бинарного кода равняется на d . Бинарные коды символов сообщения сливаются в одну последовательность и разбивается на m количество блоков, в котором каждый из них имеет длину n .

$$X' = \{x'_{11}, x'_{12}, \dots, x'_{1n} \quad x'_{21}, x'_{22}, \dots, x'_{2n} \dots x'_{m1}, x'_{m2}, \dots, x'_{mn}\}$$

Скалярно умножив два вектора X' и K^Z , получим вектор – целочисленный шифртекст $S = \{s_1, s_2, \dots, s_m\}$

$$X' = \{1 \ 1 \dots 0 \ 1 \ 0 \dots 1 \dots 0 \ 1 \dots 1\}$$

$$\begin{aligned}
X' &= \{x'_{11} \ x'_{12} \dots x'_{1n} \ x'_{21} \ x'_{22} \dots x'_{2n} \dots x'_{m1} \ x'_{m2} \dots x'_{mn}\} \\
K^Z &= \{k_1^Z \ k_2^Z \dots k_n^Z \ k_1^Z \ k_2^Z \dots k_n^Z \dots k_1^Z \ k_2^Z \dots k_n^Z\} \\
S &= \{x'_{11} \cdot e_1 + \dots + x'_{1n} \cdot e_n = s_1 \quad x'_{21} \cdot e_1 + \dots + x'_{2n} \cdot e_n = s_2 \quad \dots \\
&\quad x'_{m1} \cdot e_1 + \dots + x'_{mn} \cdot e_n = s_m\}
\end{aligned}$$

который отправляется абоненту А.

3. Соблюдая вышеизложенную схему, абонент А аналогичным путем генерирует n элементы $K^Z = \{k_1^Z, k_2^Z, \dots, k_n^Z\}$ сверхвозрастающего закрытого сундука, используя закрытый параметр e_A^Z .

Для получения первоначального открытого текста

$$X' = \{x'_{11} \ x'_{12} \dots x'_{1n} \ x'_{21} \ x'_{22} \dots x'_{2n} \dots x'_{m1} \ x'_{m2} \dots x'_{mn}\}$$

от шифртекста $S = \{s_1, s_2, \dots, s_m\}$ абонент А анализирует элементы $K^Z = \{k_1^Z, k_2^Z, \dots, k_n^Z\}$ один раз справа налево, т.е. для каждого элемента $S_j = \{s_1, s_2, \dots, s_m\}, j = 1, 2, \dots, m$, проверяются условия

$$S_j = \begin{pmatrix} S_j, & \text{если } S_j < k_i^Z \\ S_j - k_i^Z, & \text{если } S_j \geq k_i^Z, i = 1, 2, \dots, n; j = 1, 2, \dots, m \end{pmatrix}$$

Здесь, если выполняется условие $S_j \geq k_i^Z$ (это означает: для формирования шифра $S_j = \{s_1, s_2, \dots, s_m\}, j = 1, 2, \dots, m$ было использовано k_i^Z), то соответствующему индексу $X'_j, j = 1, 2, \dots, m$, присваивается "1", в противном случае, этот индекс равняется "0". Повторяя этот цикл для каждого элемента $S_j = \{s_1, s_2, \dots, s_m\}, j = 1, 2, \dots, m$, получим приведенный открытый текст, где длина их элементов равна n . Последовательно поставив все элементы приведенного текста $X'_j, j = 1, 2, \dots, m$, получим собранное представление открытого текста - X . Разбив его на части, длина которых равно длине бинарного представления букв Z - алфавита получим бинарные коды символов открытого текста. Взяв символы от алфавита соответствующим кодам и поставив их последовательно восстанавливаем открытый текст $X = \{x_1, x_2, \dots, x_l\}$.

Литература

1. Брюс Шнайер, Прикладная криптография, Триумф, 2002.

СИМПЛЕКС-КODOVЫЙ ПОДХОД К РАСПОЗНАВАНИЮ ЗРИТЕЛЬНЫХ ОБРАЗОВ

В. Н. Козлов (Москва, МГУ, мех.-мат. факультет, кафедра МАТИС)

vnkozlov@mail.ru

Изображение - конечное (непустое) множество точек на плоскости (или в трехмерном пространстве, в случае объемных изображений). Содержательным обоснованием этому может служить то, что любое реальное (нецветное) изображение можно аппроксимировать изображением из точек, причем градации серого цвета передаются разной плотностью точек в разных частях изображения. Не закрывает это дорогу и к рассмотрению цветных изображений, поскольку, как известно, цветное изображение можно представить тремя нецветными. Наконец, все, что мы видим, мы видим посредством глаз. Изображение из среды проецируется на сетчатку глаз, что приводит к возбуждению части рецепторных клеток, т.е. в конечном счете - к формированию на сетчатке аналога составленного из точек изображения.

Рассматриваемый подход к распознаванию существенным образом опирается на введение внутренней кодировки изображений, инвариантной к аффинным их преобразованиям.

В плоском и объемном случаях внутренний код изображений, для наглядности - фигур, вводится так. Нумеруются точки фигуры; с учетом ее размерности рассматривается множество всех симплексов, образованных точками фигуры; для каждого симплекса вычисляется мера. Код фигуры образует множество всех троек, состоящих из двух симплексов и числа, являющегося отношением их ненулевых мер.

Для каждой из размерностей доказано, что фигуры с точностью до перенумерации их точек имеют один и тот же код тогда и только тогда, когда они аффинно эквивалентны.

Сравнение (и распознавание) произвольных фигур A и B основывается на следующем. Порождаются множества A^* и B^* всех фигур, получаемых из A и B преобразованиями из некоторого класса (в общем случае аффинными). Рассматривается множество величин $r(A', B')$, где A' из A^* , B' из B^* , являющихся расстоянием между множествами A' и B' (расстояние Хаусдорфа). Показывается, что минимум на этом множестве достигается на конечном его подмножестве, что и позволяет его вычислить. Этот минимум и служит мерой сходства и различия фигур. Содержательно это можно представить как такое наложение

Жуковский Е.С.	18	Кийко И.А.	282
Забелин А.В.	343	Ким В.Э.	158
Заворотинский А.В.	144	Киселев А.Б.	282
Задворнов О.А.	320	Киселев Ю.Н.	311
Задорожный В.Г.	145	Ключанцев М.И.	80
Задорожный А.И.	145	Кобельков Г.М.	322
Зайтов А.А.	26	Ковалев В.Л.	283
Зайцев В.А.	146	Ковалев М.Д.	159
Зайцев Д.В.	358	Ковалишин А.А.	324
Зайцева А.В.	278	Кодзоева Ф.Д.	81
Зайцева О.В.	278	Кодиров Н.Х.	359
Закалюкин В.М.	147	Кожанов А.И.	159
Замонов М.З.	147	Кожанов В.С.	283
Зарубин А.Н.	147	Кожевникова Л.М.	155
Захаров А.В.	391	Козин И.В.	392
Звягин В.Г.	148	Козко А.И.	30
Зейфман А.И.	149	Козлов А.А.	381
Земсков А.В.	272	Козлов В.Н.	360
Зернов А.Е.	149	Козлов И.К.	284
Зинкевич Я.С.	264	Козлов К.Л.	392
Зинченко В.Н.	116	Козловский В.А.	361
Злотник А.А.	150	Козодеров В.В.	322
Зорина Т.Н.	345	Кокшаров И.С.	160
Зубарев В.М.	279	Колпаков Р.М.	393
Зубова С.П.	150	Колпакова Е.А.	160
Ибрагимова Л.С.	151	Колыбасова В.В.	261
Иванов А.В.	103	Комбаров А.П.	393
Иванов А.О.	78	Конев Р.А.	31
Иванов Г.Е.	79	Конечная Н.Н.	31
Иванов М.И.	279	Конограй А.Ф.	81
Игнатъев М.Ю.	151	Конущин А.С.	316
Игошин Д.Е.	280	Конюхова Н.Б.	284
Измоленов В.В.	280	Копачевский Н.Д.	120
Илолов М.И.	152	Кордюков Ю.А.	32
Ильин А.А.	27	Корнев А.А.	323
Илькин В.С.	152	Королев С.А.	161
Имайкин В.М.	153	Корчагина Е.В.	162
Иохвидов Е.И.	27	Костин В.А.	81
Ипатова В.М.	320	Костин Д.В.	162
Ирматов А.А.	354	Костина Т.И.	163
Исламов Г.Г.	153	Кочергин В.В.	394
Исраилов С.М.	321	Кривошеева О.А.	163
Исхоков С.А.	154	Кризский В.Н.	323
Ишкин Х.К.	28	Кропотов Д.А.	316
Ишметов А.Я.	391	Крутицкий П.А.	261
Кадченко С.И.	28	Кручинин П.А.	285
Кайшибаева Г.К.	281	Кубышкин Е.П.	285
Калинин А.И.	275	Кудрявцев В.Б.	361
Калитвин А.С.	29	Кудрявцев В.Б.	361
Калитвин В.А.	29	Кузина Ю.В.	149
Калугин А.Г.	281	Кузьма А.В.	286
Кальменов Т.Ш.	30	Кулжумиева А.А.	203
Кандоба И.Н.	321	Куликов А.Н.	286
Карачик В.В.	155	Куликов Д.А.	164
Каримов Р.Х.	155	Куликовская Н.В.	324
Карликов В.П.	303	Курапов С.В.	394
Карулина Е.С.	156	Курбангалина З.Р.	164
Карюк А.И.	156	Курдюмов В.П.	32
Касымов К.А.	157	Куржанский А.Б.	165
Каюмов И.Р.	79	Курин А.Ф.	165
Каюмов Ш.Ш.	377	Курина Г.А.	166
Кенжебаев К.К.	158	Курочкин С.В.	166
Кибкало М.А.	358	Кусаинова Л.К.	33