Международная конференция

"Современные проблемы математики, механики и их приложений"

посвященная 70-летию ректора МГУ
академика В.А.Садовничего

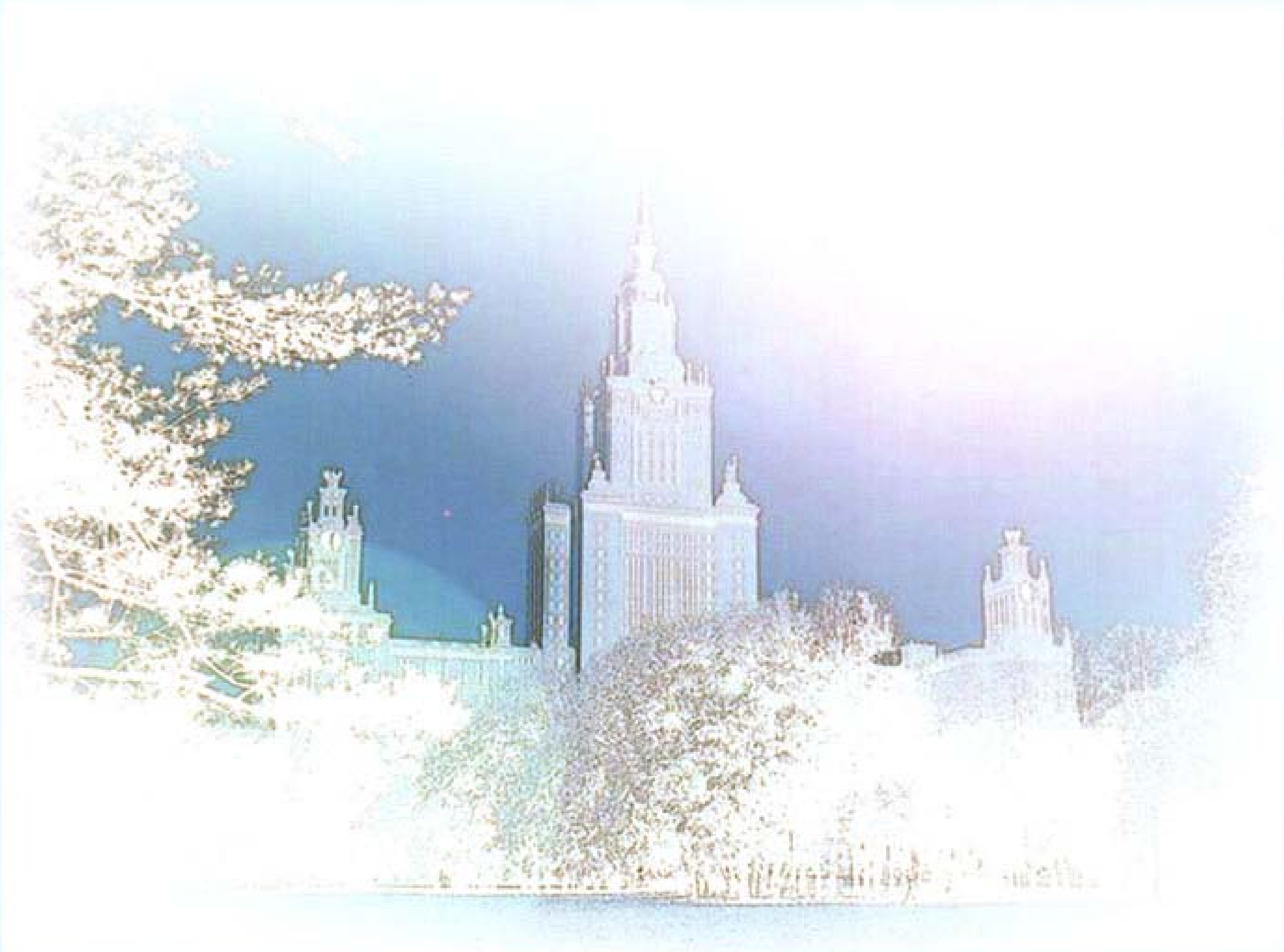
Материалы конференции

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

Секции конференции

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. Садовничего. – М.: Издательство «Университетская книга», 209. – 416с.

ISBN 978-5-91304-078-7

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

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

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 $\{B_0, ..., B_{s-1}\}$,
$B_i \subset B$, $B_i \cap B_j = \varnothing$, $i \neq j$, i, $j = 0, ..., s-1$, если

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

Пусть $N \geqslant 2$, $M \geqslant 2$, $K \subseteq A^*$ – класс регулярных языков над алфавитом A. c–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. *$\forall N \geqslant 2$, $M \geqslant 2$, $\forall k \geqslant 1$ существует $p \geqslant 0$, 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. *$\forall N \geqslant 2$, $M \geqslant 2$ 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 открытий 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 обменяться 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 закрытий параметр $e_A^Z = e_B^Z = e^Z$, используя алгоритм генерации закрытых ключей, например Диффи-Хеллмана.

2. Для шифрования открытого сообщения $X = \{x_1,\ x_2, ..., x_l\}$, которое построено в алфавите - Z, абонент B на основе общего закрытого параметра e^Z генерирует n - элементы закрытого сундука $K^Z = \{k_1^Z, k_2^Z, ..., k_n^Z\}$ используя генератор псевдослучайных чисел. После этого берутся коды букв $X = \{x_1,\ x_2, ..., x_l\}$ 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.

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

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

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

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

$$K^Z = \{k_1^Z\ \ k_2^Z \dots k_n^Z\ \ \ k_1^Z\ \ \ k_2^Z\ \dots\ k_n^Z\ \ \dots\ \ k_1^Z\ \ \ k_2^Z \dots k_n^Z\ \}$$

$$S = \{x'_{11} \cdot e_1 + \dots + x'_{1n} \cdot e_n = s_1\ \ \ x'_{21} \cdot e_1 + \dots + x'_{2n} \cdot e_n = s_2\ \ \dots$$

$$x'_{m1} \cdot e_1 + \dots + x'_{mn} \cdot e_n = s_m\}$$

который отправляется абоненту A.

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

Для получения *первоначального открытого текста*

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

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

$$S_j = \left(\begin{array}{l} S_j,\ \textbf{если}\ S_j < k_i^Z \\ S_j - k_i^Z,\ \textbf{если} S_j \geq k_i^Z, i = 1, 2, ..., n;\ j = 1, 2, ...m \end{array} \right)$$

Здесь, если выполняется условие $S_j \geq k_i^Z$ (это означает: для формирования шифра $S_j = \{s_1,\ s_2, ..., s_m\},\ j = 1, 2, ..., m$ было использовано k_i^Z), то соответствующему индексу $X'_j,\ j = 1, 2, ..., m$, присваивается "1" , в противном случае, этот индекс равняется "0". Повторяя этот цикл для каждого элемента $S_j = \{s_1,\ s_2, ..., s_m\},\ j = 1, 2, ..., m$, получим приведенный открытий текст, где длина их элементов равна - n . Последовательно поставляя все элементы приведенного текста $X'_j,\ j = 1, 2, ..., m$, 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 соответсвуюшим кодам и поставляя их последовательно восставливаем открытий текст $X = \{x_1,\ x_2, ..., x_l\}$.

Литература

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

СИМПЛЕКС-КОДОВЫЙ 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