Отчёт по гранту "Молодая математика России" за 2017 год

Милованов Алексей

13 декабря 2017 г.

1 Результаты, полученные в этом году

Основные результаты, полученные в этом году посвящены алгоритмической статистике с ограничением на ресурсы.

Нестохастические слова в алгоритмической статистике с ограничением времени

Пример 1. Пусть дано n-битовое число x, являющееся полным квадратом, и не имеющее никаких особенностей, отличающих его от других n-битовых квадратов. Какие статистические гипотезы о происхождении этого числа мы склонны считать правдоподобными? Одной из подходящих гипотез будет такая: это число было получено случайным выбором по равномерному распределению среди всех n-битовых чисел, являющихся полными квадратами (гипотеза μ_1). А явно неподходящей будет такая гипотеза μ_2: это число было получено посредством случайного выбора с равномерным распределением среди всех n-битовых чисел. Почему мы отвергаем вторую гипотезу? Потому, что мы можем указать свойство (быть полным квадратом), которым обладает x, наличие которого легко проверить и которым обладает лишь ничтожная часть всех n-битовых чисел.

Можно возразить, что на этом основании можно отвергнуть и первую гипотезу, поскольку мы можем указать свойство «быть равным x», также выполненное для ничтожной части всех слов по распределению μ_1. Однако, в отличие от свойства «быть полным квадратом», это свойство не является простым — для него нет короткой и быстрой программы, которая проверяет наличие этого свойства. А для свойства «быть полным квадратом» такая программа есть.

Обобщая этот пример, дадим следующее определение подходящей статистической гипотезы для x. Распределение вероятностей μ на двоичных словах называется *приемлемой (acceptable)* гипотезой о происхождении двоичного слова x, если x не принадлежит никакому *простому* множеству слов T, вероятность которого по распределению μ ничтожна. Будем считать множество простым, если оно задается короткой детерминированной

программой, быстро распознающей принадлежность этому множеству, как в Примере 1.

Мы будем называть слово x *стохастическим*, если для него есть приемлемая простая гипотеза. Как измерять простоту гипотезы, то есть, распределения вероятностей μ? Так же, как мы измеряли простоту опровергающего теста T: распределения вероятностей считается простым, если существует короткая программа вероятностной машины без входа, которая за небольшое время порождает это распределение. Мы считаем, что *машина M порождает распределение μ*, если для всех слов x вероятность события [выход M равен x] равна $\mu(x)$. Время работы измеряется как максимум по всех результатам бросаний времени работы M при этих результатах бросаний.

Кроме этих уточнений, определение приемлемой гипотезы μ нуждается в задании следующих трех числовых параметров: верхняя оценка длины программы распознавания T, верхняя оценка времени работы этой программы, верхняя оценка на $\mu(T)$ (насколько малой должна быть вероятность, чтобы быть признанной «ничтожной»). Чем больше все три параметра, тем сильнее требования к приемлемым гипотезам и стохастичности. А определение простой статистической гипотезы μ нуждается в задании двух числовых параметров: верхняя оценка на длину программы, порождающей μ, и верхняя оценка на время работы этой программы. Чем меньше эти параметры, тем сильнее требования к простым гипотезам.

Основной вопрос, интересующий нас: при каких значениях параметров существуют слова, не имеющие простых приемлемых объяснений? Такие слова мы будем называть *нестохастическими*. Главные результат состоит в том, что в предположении NE $\neq$ RE *доказано существование нестохастических слов для полиномиальных ограничений на время и вероятность и логарифмических ограничений на длину программ (Теорема 1).*

Сформулируем приведённые выше понятия и утверждения более формально.

Определение 1. Пусть даны три натуральных параметра t, α, β. Мы называем t, α, β-*приемлемой* гипотезой для слова x такое распределение вероятностей μ, что $\mu(T) \geq 2^{-\beta}$ для любого множества $T \ni x$, распознаваемого детерминированной программой длины менее α и временем работы не больше t на всех входах той же длины, что и x.

Чем больше t, α и меньше β, тем сильнее определение t, α, β-приемлемости. Для любого слова x распределение вероятностей, сосредоточенное на x, будет будет t, α, β-приемлемой гипотезой для x при любых значениях параметров t, α, β. Мы, однако, заинтересованы в простых объяснениях.

Определение 2. Распределение вероятностей μ называется t, α-*простым*, если оно может быть порождено некоторой вероятностной машиной без входа с программой длины менее α и временем работы не более t, и кроме того, функция $x \mapsto \mu(x)$ может быть вычислена программой длины α за время t. функция (Напомним, что машина M порождает μ, если для всех слов x вероятность события [выход M равен x] равна $\mu(x)$.)

Слова, для которых существует t_1, α_1-простая t_2, α_2, β-приемлемая статистическая гипотеза для небольших t_1, α_1, β и больших t_2, α_2 неформально называются стохастическими, а иначе они называются нестохастическими. Чем меньше параметры t_1, α_1, β и больше t_2, α_2, тем сильнее требования к стохастичности и слабее требования к нестохастичности.

Определение 3. Распределение вероятностей μ является t, γ-*правдоподобной* гипотезой для x, если для любого множества $T \ni x$, которое распознается детерминированной машиной с программой длины l и временем работы на входах той же длины, что у x, не больше t, выполнено $\mu(T) > 2^{-\gamma-l}$.

Основной результат утверждает существование *не*стохастических слов длины n для полиномиальных значений t_1, t_2 и логарифмических значениях остальных параметров в следующем предположении:

Гипотеза 1. NE $\neq$ RE. Здесь NE — класс языков, распознаваемых недетерминированными машинами Тьюринга за время $2^{O(n)}$, RE — класс языков, распознаваемых полиномиальными вероятностными машинами Тьюринга за время $2^{O(n)}$ с вероятностью ошибки не более $1/2$ на входах из языка, и не ошибающихся на входах вне языка. Поскольку RE $\subset$ NE, различие классов означает, что NE $\not\subset$ RE. Последнее равносильно существованию языка над однобуквенным алфавитом, принадлежащего NP $\setminus$ RP.

Теорема 1. *Предположим, что* NE $\neq$ RE. *Тогда существует многочлен* t_2 *и константа* α_2 *такие, что для любого многочлена* t_1 *и любой константы* d *для бесконечно многих* n *существует слово длины* n*, для которого нет* $t_1(n), d\log n$*-простых* $t_2(n), \alpha_2, d\log n$*-приемлемых гипотез.*

Дерандомизация PIT для схем глубины 4

В работе “Algebraic Geometric Techniques for Depth-4 PIT Sylvester-Gallai Conjectures for Varieties” Анкит Гупта (Ankit Gupta) доказал существание детерминированного полиномиального алгоритма, решающий проблему равенства нулю многочлена для важного класса алгебраических схем по модулю некоторой гипотезы. Эта гипотеза представляет собой обобщение теоремы Сильвестра-Галлаи (точнее, теоремы Келли, т.к. действие происходит над полем $\mathbb{C}$) для более сложных объектов чем точки и прямые. Нам удалось доказать эту гипотезу для очень частных случаев Мы не будем подробно останавливаться на этих результатах, ввиду их скромности. Предполагаемая работа в этом направлении ещё далека от завершения.

2 Опубликованные работы

1. Milovanov A. On Algorithmic Statistics for Space-Bounded Algorithms, in: Computer Science – Theory and Applications: 12th International Computer Science Symposium in Russia (CSR 2017) Vol. **10304**, Luxemburg : Springer Science and Business Media, 2017, p. 232-244.

2. Milovanov A. Some Properties of Antistochastic Strings, Theory of Computing Systems. 2017. Vol. **61**. No. 2. P. 521-535.

3. Vereshchagin N., Milovanov A. Stochasticity in Algorithmic Statistics for Polynomial Time, in: 32nd Computational Complexity Conference. Вадерн : Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, 2017, **79** p. 17:1-17:18.

Диссертация

Подготовка и защита диссертации по теме "О нестохастических по Колмогорову словах" под руководством Н.К.Верещагина. Защита состоялась 8.12.2017.

3 Участие в конференциях

1. The 12th International Computer Science Symposium in Russia (Казань).

   Доклад: On Algorithmic Statistics for Space-Bounded Algorithms.

2. Twelfth International Conference on Computability, Complexity and Randomness (Майсор, Индия).

   Доклад: Stochasticity in Algorithmic Statistics for Polynomial Time.

4 Работа в научных центрах и международных группах

Работаю стажёром-исследователем в Международной лаборатории теоретической информатики НИУ ВШЭ.

5 Педагогическая деятельность

Весенний семестр

1. Курс "Сложность вычислений" в Школе Анализа Данных

   (ведение семинаров);

2. научное руководство бакалаврской работы Дмитрия Пашментова

   (ФИВТ МФТИ).

Осенний семестр

1. Курс "Математическая логика и теория алгоритмов" на факультете ФАЛТ МФТИ (чтение лекций и ведение семинаров);

2. Курс “Математическая логика и теория алгоритмов” на факультете ФИВТ МФТИ (ведение семинаров);

3. Курс “Дискретная математика-2” на факультете ФКН НИУ ВШЭ (ведение семинаров);

4. Курс “Computability and Complexity” программа “Math in Moscow” (ведение семинаров).