

Представление

Константина Вячеславовича Первышева

на премию СПбМО «Молодому математику» за 2007 год
(за цикл работ о семантических сложностных классах).

Представляемые работы К. В. Первышева 2005-2007 гг. посвящены доказательству классических (и фундаментальных) для теоретической информатики фактов: наличие иерархии по времени для классов вычислительных задач. Доказательства таких фактов для «синтаксических» классов (то есть тех, где вычислительные устройства можно эффективно перечислить) известны давно (как правило, они получаются благодаря диагонализации, использующей такое эффективное перечисление). Работы К. В. Первышева посвящены тому, что можно доказать для «семантических» (т.е. *не* синтаксических) классов. К таким семантическим классам относятся классы вычислений, использующих случайные числа (в частности, взлом криптосистем с открытым ключом), и многие другие.

Всегда ли при помощи большего количества времени (или других ресурсов) можно решить большее количество задач? Для классических вычислений этот вопрос был исследован в середине прошлого века: например, увеличение времени работы более чем в логарифмическое количество раз дает гарантированный выигрыш, а вот увеличение количества использованной памяти с константы до $O(\log \log n)$ никакого выигрыша не дает. Решен этот вопрос был и для других синтаксических классов (например, недетерминированных вычислений).

Для вычислений, использующих случайные числа, равно как и для других семантических классов, этот вопрос открыт и по сей день. Не так давно Л. Фортноу (Lance Fortnow) и др. было показано наличие иерархии по времени для вероятностных вычислений с *ограниченной ошибкой* (**BPP**) при наличии *подсказки в один бит для каждой длины входа*. Им, однако, не удалось достичь такого же результата для других похожих классов языков (например, вероятностных вычислений без ошибки и интерактивных протоколов) — для них Л. Фортноу и др. показали наличие иерархии только с $O(\log n \cdot \log \log n)$ битов подсказки. В своей первой работе К. В. Первышев [3] значительно упростил предыдущие доказательства и доказал наличие иерархии по времени с *подсказкой в один бит для всех семантических классов, удовлетворяющих некоторым довольно общим ограничениям*; в том числе — для вероятностных вычислений без ошибки (**ZPP**), недетерминированных вычислений с единственной правильной подсказкой (**UP**) и для интерактивных протоколов. Последующая работа [1] с соавтором (Dieter van Melkebeek) дает другое доказательство для этих фактов, позволяющее в дальнейшем получать теоремы об (еще более точной) иерархии для новых классов языков «единообразно».

Другой результат номинанта — построение иерархии по времени для *эвристических* алгоритмов, т.е., алгоритмов, которые решают задачу на многих, но не на всех входах.

Л. Фортноу и Р. Сантанам (Rasul Santhanam) показали наличие такой иерархии внутри **ВРР** и оставили вопрос открытым для других вычислительных моделей. К. В. Первышев [2] доказал наличие такой иерархии для широкого класса моделей, включающего двухраундовые интерактивные доказательства и недетерминированные вычисления; он также усилил предыдущий результат для **ВРР**. Для этого был применён новый метод «диагонализации с исправлением ошибок».

Методы, предложенные К. В. Первышевым для семантических классов языков, оказались полезными и для криптографических задач. Вопрос об иерархии по времени для обращения односторонних (one-way) функций формулируется следующим образом: можем ли мы обратить («взломать») большее количество (труднообратимых) функций за большее время? В совместной работе [4] со старшими коллегами (Д. Ю. Григорьевым и научным руководителем Э. А. Гиршем) К. В. Первышев доказывает, что такую теорему об иерархии можно доказать, используя один бит подсказки для каждой длины входа.

Все работы К. В. Первышева хорошо известны зарубежным и отечественным специалистам и активно обсуждаются ими. Они решают *важные* и *непростые* задачи и являются самостоятельными научными исследованиями; в том числе, в совместных работах со старшими коллегами К. В. Первышеву безусловно принадлежит ключевая роль в доказательстве новых результатов.

Уровень результатов К. В. Первышева крайне высок и необычен для столь молодого исследователя. У Константина Вячеславовича безусловно большое будущее и будет очень уместно удостоить его премии «Молодому математику» СПбМО.

Член правления СПбМО,
старший научный сотрудник ПОМИ РАН,
к.ф.-м.н.

Э. А. Гирш

Вице-президент СПбМО,
зав.лаб. мат.логики ПОМИ РАН,
чл.-корр. РАН

Ю. В. Матиясевич

Приложение: список работ К. В. Первышева, представляемых на соискание премии

- [1] **A Generic Time Hierarchy with One Bit of Advice.** *Computational Complexity* 16(2): 139-179 (2007) (with D.van Melkebeek).
- [2] **On Heuristic Time Hierarchies.** *IEEE Conference on Computational Complexity 2007*: 347-358
- [3] **Time hierarchies for computations with a bit of advice,** *Electronic Colloquium on Computational Complexity*, 05-054, ISSN 1433-8092, 2006, 13 pp.
<http://eccc.hpi-web.de/eccc-reports/2005/TR05-054/index.html>
- [4] **Time hierarchies for cryptographic function inversion with advice,** *Electronic Colloquium on Computational Complexity*, 05-076, ISSN 1433-8092, 2006, 14 pp. (with D.Grigoriev and E.A.Hirsch).
<http://eccc.hpi-web.de/eccc-reports/2005/TR05-076/index.html>