Отчёт за 2009 г. по гранту фонда «Династия»

Э.А.Гирш

Санкт-Петербургское отделение Математического института им. В.А.Стеклова РАН

Санкт-Петербургский государственный университет

Академический физико-технологический университет РАН

1 Научная деятельность

Оптимальная полуразрешающая процедура для языка булевых тавтологий — это алгоритм, принимающий этот язык и работающий на каждой тавтологии не более, чем в полином раз дольше, чем любой другой алгоритм. Я.Крайчек и П.Пудлак (1989) показали, что существование такой процедуры эквивалентно важному открытому вопросу теории сложности: существованию p-оптимальной системы доказательств. Недавно Х.Монро (2009) доказал отсутствие такой процедуры при некоторых дополнительных предположениях. Тем не менее, нами построена оптимальная полуразрешающая *эвристическая* процедура.

Статья, содержащая этот результат, **принята на конференцию STACS-2010 и будет опубликована в её трудах**, а пока является препринтом:

E.A.Hirsch, D.M.Itsykson, *On optimal heuristic randomized semidecision procedures, with application to proof complexity,* arXiv.org, no. 0908.2707, 2009.

Также опубликованы статьи с ранее полученными результатами:

Э.А.Гирш, Д.М.Ицыксон, *Бесконечно часто односторонняя функция, основанная на предположении о сложности в среднем случае,* Алгебра и анализ, том 21, номер 3, стр. 130–144, 2009 г.

E.A.Hirsch, S.I.Nikolenko, *A feebly secure trapdoor function,* Lecture Notes in Computer Science, Vol. 5675, Springer, 2009 г.

2 Преподавательская деятельность

Под моим руководством трое аспирантов защитили в 2009 г. кандидатские диссертации, защита четвёртого должна состояться 28 декабря 2009 г. Я продолжаю руководить ещё тремя аспирантами и несколькими студентами, читаю лекции по сложности вычислений на мат-мехе СПбГУ и в Академическом физико-технологическом университете РАН, веду специализированные студенческие семинары. В этом году кафедра математических

и информационных технологий АФТУ РАН, где я являюсь заместителем заведующего кафедрой по научным вопросам, провела первый организованный приём в магистратуру.

3 Участие в конференциях

Доклады:

- E.A.Hirsch, S.I.Nikolenko. A feebly secure trapdoor function. Устный доклад на международной конференции CSR-2009, Новосибирск, август 2009 г.
- E.A.Hirsch. Propositional proof complexity (tutorial). Обзорный доклад на семинаре Estonian Theory Days, Эстония, октябрь 2009 г.
- E.A.Hirsch, D.M.Itsykson. On optimal heuristic proof systems. Устный доклад на совместном российско-австрийском семинаре "Логика конечного и бесконечного: арифметика, сложность и анализ ординалов", Вена, Австрия, июнь 2009 г.
- Последний доклад принят на конференцию STACS-2010, Нанси, Франция, март 2010 г.
- 16-18 декабря 2009 г. планируется совместный семинар ПОМИ-МИАН в Москве, где я планирую сделать обзорный доклад об оптимальных системах доказательств.
- Я также приглашён выступить на конференции TAMC-2010, Прага, Чехия, июнь 2010 г.
- Я руководил (совместно с Эрнстом Майром) курсом "Propositional Proof Complexity" на российско-немецкой студенческой школе JASS-2009.

Организационная работа:

- все эти годы я являюсь членом наблюдательного совета серии CSR (International Computer Science Symposium in Russia),
- участвовал в работе программных комитетов ESA-2007, CSR-2007, SAT-2007, CSR-2008, IWPEC-2009, в будущем году MFCS-2010.

4 Итоги за 2007-2009 гг., сравнение с заявкой

Научные результаты:

Алгоритмы для задачи пропозициональной выполнимости. Как и предполагалось, моё участие в этой области ограничилось двумя обзорными статьями, подводящими итог работе за предыдущие годы — в Encyclopedia of Algorithms (Springer) и Handbook of Satisfiability (IOS Press).

Универсальные объекты и теоремы об иерархии для семантических классов. Эта тема в заявке называлась "Теоремы об иерархии и криптографические примитивы". Речь шла о результатах о внутренней структуре классов объектов, для которых неизвестно эффективной процедуры перечисления, их связи с классическими сложностными классами. Несколько интересных результатов было получено мной и моими учениками, и эта работа активно продолжается:

- доказана связь между обращением функции "в среднем" и криптографическим обращением (совместно с Д.М.Ицыксоном: доклад на WoLLiC-2008 и журнальный вариант в журнале «Алгебра и анализ»);
- построена универсальная (оптимальная) полуразрешающая процедура для любого рекурсивно-перечислимого языка в классе эвристических алгоритмов с любым полиномиально-генерируемым распределением (совместно с Д.М.Ицыксоном, принято на STACS-2010);
- Д.М.Ицыксон в своей диссертации построил универсальные (полные) задачи для вероятностных и эвристических вычислений в среднем;
- С.И.Николенко в своей диссертации предложил несколько универсальных комбинаторных односторонних функций.

Пропозициональные поуалгебраические системы доказательств. В этой области новых результатов получено не было.

Доказуемо надёжные в слабом смысле криптографические примитивы. Эта тематика не планировалась в заявке. Была сконструирована «функция с секретом», обращение которой в 25/22 раз труднее, чем вычисление (совместно с С.И.Николенко, доклад на CSR-2009). Исследования были продолжены О.Ю.Меланич под моим руководством, и в её дипломной работе построены новые примеры таких нелинейных функций.

Научное руководство:

Кандидатские диссертации:

1. Кожевников Арист Александрович. Сложность пропозициональных систем доказательств, оперирующих неравенствами, 2007.
2. Николенко Сергей Игоревич. Новые конструкции криптографических примитивов, основанные на полугруппах, группах и линейной алгебре, 2009.
3. Первышев Константин Вячеславович. Иерархии по времени для некоторых классов эвристик, алгоритмов с подсказкой, криптографических примитивов, 2009.
4. Куликов Александр Сергеевич. Построение алгоритмов для задач булевой логики при помощи автоматизации, комбинированных мер сложности и запоминания дизъюнктов, 2009.

5. Ицыксон Дмитрий Михайлович. Сложность в среднем случае вероятностных вычислений с ограниченной ошибкой, 2009 (планируется 28.12).

Дипломные работы и магистерские диссертации:

1. Смаль Александр Владимирович. Автоматические доказательства в системе Секущие плоскости, 2008.
2. Антипов Дмитрий Юрьевич. Непересекающиеся NP-пары с подсказкой, 2009.
3. Меланич Ольга Юрьевна. Нелинейные функции, односторонние в слабом смысле, 2009.

Преподавание: Как и планировалось, я продолжил работу на мат-мехе СПбГУ. Мы также создали новую кафедру «математических и информационных технологий» в Академическом физико-технологическом университете РАН и начали обучение в магистратуре.