УДК 519.712.2

Новая верхняя оценка для $(n, 3)$-MAX-SAT. Близнец И. А. — В кн.: Теория сложности вычислений. X. (Зап. научн. семин. ПОМИ, т. 399), СПб., 2012, с. 5–14.

До сих пор неизвестно, решаются ли задачи выполнимости или максимальной выполнимости за время $poly(F)c^n$, для $c < 2$, где c – константа, n – число переменных, F – входная формула. Подобные оценки известны, однако, для некоторых частных случаев, когда ограничены длина дизъюнктов, максимальное количество вхождений переменных или длина формулы. В данной работе рассматривается задача $(n, 3)$-MAX-SAT – частный случай задачи MAX-SAT, где каждая переменная встречается не более трех раз. Мы представляем простой алгоритм со временем работы $O^*(2^{\frac{n}{3}})$. Также приводится полиномиально разрешимый подкласс формул. Библ. – 13 назв.

УДК 510.52

Оптимальные эвристические алгоритмы для образа инъективной функции. Гирш Э. А., Ицыксон Д. М., Николаенко В. О., Смаль А. В. — В кн.: Теория сложности вычислений. X. (Зап. научн. семин. ПОМИ, т. 399), СПб., 2012, с. 15–31.

К настоящему моменту ни для какого *языка* из $\mathbf{NP} \setminus \mathbf{P}$ не известно оптимального алгоритма для задачи его распознавания. В данной статье рассматривается задача проверки принадлежности образу инъективной функции. Предложена конструкция *эвристического* алгоритма для этой задачи в вероятностном и в детерминированном случаях (эвристический алгоритм может ошибаться на небольшой доле $\frac{1}{d}$ всех входов; параметр d также передаётся алгоритму). Для данной задачи это улучшает раннее предложенную конструкцию оптимального вероятностного эвристического аксептора (который является оптимальным только на дополнении языка). Библ. – 12 назв.

УДК 510.52

Крипотографические примитивы, доказуемо надёжные в слабом смысле. Гирш Э. А., Меланич О. Ю., Николенко С. И. — В кн.: Теория сложности вычислений. X. (Зап. научн. семин. ПОМИ, т. 399), СПб., 2012, с. 32–64.

В 1992 г. А. Хильтген построил первые конструкции доказуемо (слабо) надёжных криптографических примитивов, а именно односторонних функций. Эти функции доказуемо сложнее обратить, чем вычислить, но сложность (схемная сложность в базисе из произвольных бинарных гейтов) увеличивается лишь в константное число раз (в конструкциях Хильтгена этот показатель приближается к 2). В традиционной криптографии, односторонние функции являются основными примитивами для схем с секретным ключом, а схемы с открытым ключом конструируются на основе функций с секретом. Мы развиваем идеи работ Хильтгена и строим примеры функций с секретом, доказуемо надёжных в слабом смысле, в которых схема противника гарантированно больше, чем схемы честных участников (тоже в константное число раз). Мы строим примеры как (более простых) линейных, так и (более надёжных) нелинейных конструкций. Библ. – 25 назв.

УДК 519.6

Схемная сложность линейных функций: метод исключения гейтов и надежность в слабом смысле. Давыдов А. П., Николенко С. И. — В кн.: Теория сложности вычислений. X. (Зап. научн. семин. ПОМИ, т. 399), СПб., 2012, с. 65–87.

Работа посвящена исследованиям в области схемной сложности в контексте доказуемо надёжных криптографических конструкций. Основываясь на идеях доказуемо надёжных функций с секретом, ранее разработанных в (Hirsch, Nikolenko, 2009; Melanich, 2009), мы представляем новую линейную конструкцию доказуемо надёжной функции с секретом, имеющую порядок надёжности 5/4, а также проводим подробный общий анализ метода исключения гейтов (gate elimination) для случая линейных функций. В работе также приводится неконструктивное доказательство нелинейных нижних оценок схемной сложности на линейные булевы функции и верхние оценки на реализацию линейных булевых функций схемами с уточнёнными константами. Библ. – 53 назв.

УДК 510.52

Сложность обращения явной функции Голдрейха DPLL алгоритмами. Ицыксон Д. М., Соколов Д. О. — В кн.: Теория сложности вычислений. X. (Зап. научн. семин. ПОМИ, т. 399), СПб., 2012, с. 88–108.

Функция Голдрейха отображает бинарную строку длины n в бинарную строку длины n. Каждый бит выхода зависит от d битов входа и вычисляется по фиксированному d-местному предикату. Каждая функция Голдрейха задается графом зависимостей G и предикатом P. В 2000 году О. Голдрейх выдвинул гипотезу, что если граф зависимости является экспандером, а предикат случайный, то такая функция является односторонней. В этой статье мы приводим простое доказательство экспоненциальной нижней оценки на сложность обращения функции Голдрейха близорукими DPLL алгоритмами. Граф зависимости G в нашей конструкции может быть основан на произвольном экспандере, в частности возможно использовать явную конструкции экспандера, в то время как все предыдущие результаты были основаны на случайном графе зависимости. Предикат P может быть линейным или немного нелинейным. Наша конструкция может быть использована и для доказательства нижней оценки для “пьяных” DPLL алгоритмов. Библ. – 18 назв.

УДК 510.52, 519.6

Диофантова иерархия. Кноп А. А. — В кн.: Теория сложности вычислений. X. (Зап. научн. семин. ПОМИ, т. 399), СПб., 2012, с. 109–127.

Класс языков D, определённый в работе L. Adelman и K. Manders (1975), является диофантовым аналогом класса NP. Язык L принадлежит классу D тогда и тогда, когда существует многочлен P, такой, что x принадлежит L если и только если существуют числа y_i полиномиальной длины, такие, что $P(x, y_1, ..., y_m) = 0$.

Вопрос об равенстве классов D и NP открыт. В работе определяется иерархия на основе класса D, аналогичная традиционной полиномиальной иерархии (на основе класса NP) и доказывается связь между двумя иерархиями (в частности, NP содержится во втором уровне диофантовой иерархии). Библ. – 6 назв.