новое направление в математической логике — теорию сложности формальных доказательств.

Перевод работы [1] на английский язык (см. [4]), выполненный через 15 лет после ее публикации, можно считать заслуженной оценкой фундаментальности. Правда, здесь не обошлось без некоторых «казусных» моментов. Так, авторы работы [5] рассматривают квантифицированный вариант приведенных выше преобразований, указывая в качестве первоисточника свою работу, датированную 1982 годом, и буквально говоря, что «...пропозициональный вариант данных преобразований был предложен Цейтиным в 1983 году (ссылка [4])».

Сложно отследить момент, когда впервые в публикациях стал использоваться термин «преобразования Цейтина» (Tseitin's transformation). Однако на сегодняшний день данный термин прочно укоренился в научной литературе (причем, главным образом, в отношении преобразований, описанных в первой цитате) и фигурирует в работах по сложности формальных доказательств, по верификации дискретных автоматов, по обращению дискретных функций (см., например, [6 – 8] и многие другие).

Настоящая заметка представляет собой введение в обзор, посвященный использованию преобразований Цейтина в ряде областей математической и прикладной логики.

ЛИТЕРАТУРА

1. *Цейтин Г. С.* О сложности вывода в исчислении высказываний // Записки научных семинаров ЛОМИ АН СССР. 1968. Т. 8. С. 234–259.
2. *Данцин Е. Я.* Алгоритмика задачи выполнимости // Вопросы кибернетики. Проблемы сокращения перебора. М.: АН СССР, 1987. С. 7–29.
3. *Waisberg M.* Untersuchungen uber den Aussagen kalkul von Heyting //Wiadomosci Matematyczne. 1938. V. 46. P. 45–101.
4. *Tseitin G.* On the complexity of derivation in propositional calculus // Automat. Reasoning. 1983. V. 2. P. 466–483.
5. *Plaisted D., Greenbaum S.* A Structure-preserving Clause Form Translation // J. Symbolic Computation. 1986. V. 2. P. 293–304.
6. *Groote J. F., Zantema H.* Resolution and binary decision diagrams cannot simulate each other polynomially // J. Discrete Appl. Mathematics. 2003. 130:2. P. 157–171.
7. *Een N., Sorensson N.* Translating Pseudo-Boolean Constraints into SAT // J. Satisfiability, Boolean Modeling and Computation. 2006. No. 2. P. 1–25.
8. *Семенов А. А., Заикин О. С., Беспалов Д. В., Ушаков А. А.* SAT-подход в криптоанализе некоторых систем поточного шифрования // Вычислительные технологии. 2008. Т. 13. № 6. С. 134–150.

УДК 681.03

ПОЧТИ СОВЕРШЕННЫЕ НЕЛИНЕЙНЫЕ ФУНКЦИИ

М. Э. Тужилин

Появление разностного метода вызвало необходимость разработки подходов к построению тех классов S-боксов, которые являются оптимальными для противостояния данному методу. Большое значение приобрело введенное в [1] понятие почти совершенной нелинейной функции (Almost Perfect Nonlinear, или, сокращенно, APN-функции).

Функция $F\colon \mathrm{GF}(p^n) \to \mathrm{GF}(p^n)$ называется *APN-функцией*, если для любых $a \neq 0$ и b из $\mathrm{GF}(p^n)$ уравнение $F(x+a) - F(x) = b$ имеет не более двух решений.

Наибольший интерес исследователей прикован к случаю $p = 2$. Многие свойства APN-функций, заданных на $\mathrm{GF}(2^n)$, описаны в [2].

В силу того, что построение новых APN-функций — довольно сложная задача, имеют важное значение те преобразования функций, при которых сохраняются свойства «быть APN-функцией».

Пусть $F, A, A_1, A_2 : \mathrm{GF}(p^n) \to \mathrm{GF}(p^n)$. Если F — APN-функция, A_1, A_2 — аффинные подстановки и A — аффинная функция, то $F' = A_1 \circ F \circ A_2 + A$ — тоже APN-функция. В этом случае F и F' называются расширенно аффинно эквивалентными (EA-эквивалентными) и аффинно эквивалентными при $A = 0$.

До недавнего времени известны были только такие конструкции APN-функций, которые были EA-эквивалентны степенным функциям $F(x) = x^d$ над конечными полями, они приведены в [3].

В [4] было введено понятие CCZ (Carlet — Charpin — Zinoviev)-эквивалентности.

Отображения F_1 и F_2 поля $\mathrm{GF}(p^n)$ на себя называются *CCZ-эквивалентными*, если графы отображений F_1 и F_2, то есть множества $\{(x, F_1(x)) \mid x \in \mathrm{GF}(p^n)\}$ и $\{(x, F_2(x)) \mid x \in \mathrm{GF}(p^n)\}$ являются аффинно эквивалентными.

CCZ-эквивалентность является более общей, чем EA-эквивалентность (каждый класс CCZ-эквивалентности содержит один или несколько классов EA-эквивалентности), и сохраняет свойства «быть APN-функцией» и «быть AB-функцией».

В [5] приведены серии APN-функций, CCZ-эквивалентных степенным функциям над полем $\mathrm{GF}(p^n)$.

В 2006–2008 годах были построены серии APN-функций, не CCZ-эквивалентных степенным функциям над полем $\mathrm{GF}(p^n)$, большинство из них приведено в [6].

ЛИТЕРАТУРА

1. *Nyberg K., Knudsen L. R.* Provable Security Against Differential Cryptography // LNCS. 1993. V. 740. P. 566–574.
2. *Berger T., Canteaut A., Charpin P., Laigle-Chapuy Y.* On Almost Perfect Nonlinear Functions Over $\mathbb{F}_{2^n}$ // IEEE Transactions on Information Theory. 2006. V. 52. No. 9. P. 4160–4170.
3. *Zeng X., Hu L., Yang Y., Jiang W.* On the inequivalence of Ness-Helleseth APN functions // Cryptology ePrint Archive 2007/379.
4. *Carlet C., Charpin P., Zinoviev V.* Codes, bent functions and permutations suitable for DES-like cryptosystems // Designs, Codes and Cryptography. 1998. V. 15(2). P. 125–156.
5. *Budaghyan L., Carlet C., Pott A.* New Classes of Almost Bent and Almost Perfect Nonlinear Polynomials // Proceedings of the Workshop on Coding and Cryptography. 2005. P. 306–315.
6. *Budaghyan L., Carlet C., Leander G.* Constructing new APN functions from known ones // Cryptology ePrint Archive 2007/063.