УДК 519.7

О ПРЕОБРАЗОВАНИЯХ ЦЕЙТИНА В ЛОГИЧЕСКИХ УРАВНЕНИЯХ

А. А. Семенов

В 1968 г. в журнале «Записки научных семинаров ЛОМИ» вышла статья Григория Самуиловича Цейтина «О сложности вывода в исчислении высказываний» [1]. Сегодня можно с уверенностью сказать, что эта выдающаяся и совершенно новаторская на тот момент работа намного опередила время и предвосхитила целый спектр направлений в логике и теории алгоритмов.

Основным инструментом [1] являются очень простые по своей природе преобразования логических выражений. Далее приведены две цитаты из [1], в которых описаны данные преобразования.

«Исчисления, которыми мы будем пользоваться, направлены на установление противоречивости систем дизъюнкций. Понятие противоречивой системы дизъюнкций служит здесь аналогом понятия тождественно истинной формулы в обычном исчислении высказываний. От вопроса о тождественной истинности заданной формулы исчисления высказываний можно перейти к вопросу о противоречивости некоторой системы дизъюнкций, приведя отрицание данной формулы к конъюнктивной нормальной форме. Однако при таком преобразовании может резко возрасти длина формулы, поэтому мы будем рассматривать другой способ перехода от формулы исчисления высказываний к системе дизъюнкций. Каждой подформуле данной формулы поставим в соответствие свою переменную; двум подформулам будут соответствовать сопряженные переменные[1] в том и только том случае, если одна из этих формул является отрицанием второй. Если некоторая подформула A представляет собой конъюнкцию подформул B и Γ и этим подформулам приписаны соответственно переменные α, β и γ, то припишем подформуле A следующую систему дизъюнкций[2]: $\bar{\alpha}\beta, \bar{\alpha}\gamma, \alpha\bar{\beta}\bar{\gamma}$. Аналогично припишем системы дизъюнкций подформулам, которые представляют собой дизъюнкции и импликации ($\alpha\bar{\beta}, \alpha\bar{\gamma}, \bar{\alpha}\beta\gamma$ для дизъюнкции и $\alpha\beta, \alpha\bar{\gamma}, \bar{\alpha}\bar{\beta}\gamma$ для импликации). Объединим все полученные таким способом системы дизъюнкций и добавим туда еще дизъюнкцию $\bar{\xi}$, где ξ — переменная, соответствующая всей данной формуле. Легко видеть, что полученная система дизъюнкций противоречива в том и только в том случае, если данная формула тождественно истинна».

«Если α, β, γ — какие-нибудь переменные, причем ни α, ни $\bar{\alpha}$ не входят ни в одну из дизъюнкций системы, то систему можно дополнить следующим списком дизъюнкций[3]: $\alpha\beta, \alpha\gamma, \bar{\alpha}\bar{\beta}\bar{\gamma}$».

Первоначальные идеи преобразований, описанных в первой цитате, принадлежат, по-видимому, к категории «фольклорных» — в качестве одного из наиболее ранних примеров Е. Я. Данциным (см. [2]) указывается работа [3]. Вторая цитата дает простейший пример преобразования из класса так называемых «правил расширения». Отметим, что именно в [1] описанные выше преобразования (и первого и второго типов) составили основу «бесспорно нетривиальных» результатов, по сути открывших

[1] Имеется в виду контрарная пара, то есть булева переменная и ее отрицание.

[2] В привычной для нашего времени системе обозначений имеется в виду КНФ $(\bar{\alpha} \vee \beta) \cdot (\bar{\alpha} \vee \gamma) \cdot (\alpha \vee \bar{\beta} \vee \bar{\gamma})$.

[3] Здесь речь идет о КНФ $(\alpha \vee \beta) \cdot (\alpha \vee \gamma) \cdot (\bar{\alpha} \vee \bar{\beta} \vee \bar{\gamma})$. Подразумевается, что дополненная система будет противоречива тогда и только тогда, когда противоречива исходная.

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.