ЛИТЕРАТУРА

1. *Погорелов Б. А., Пудовкина М. А.* О комбинаторных свойствах группы, порождённой X, L-слоями // Прикладная дискретная математика. Приложение. 2012. № 5. С. 22–23.
2. *Пудовкина М. А.* Линейные структуры групп подстановок над конечным модулем // Прикладная дискретная математика. 2008. № 1. С. 25–28.

УДК 519.7

СОВЕРШЕННАЯ УРАВНОВЕШЕННОСТЬ ДИСКРЕТНЫХ ФУНКЦИЙ И УСЛОВИЕ ГОЛИЧА

С. В. Смышляев

Для всяких $n \geqslant 1$, $k \geqslant 2$ через E_k будем обозначать множество $\{0, 1, \ldots, k-1\}$, через $\mathrm{P}_k^{(n)}$ — множество k-значных функций n переменных $f\colon \mathrm{E}_k^n \to \mathrm{E}_k$; $\mathrm{P}_k = \bigcup\limits_{n=0}^{\infty} \mathrm{P}_k^{(n)}$. Для всякого натурального l и всякой функции $f \in \mathrm{P}_k^{(n)}$ будем рассматривать отображение $f_l\colon \mathrm{E}_k^{l+n-1} \to \mathrm{E}_k^l$, $f_l(x_1, x_2, \ldots, x_{l+n-1}) = (f(x_1, \ldots, x_n), \ldots, f(x_l, \ldots, x_{l+n-1}))$.

Определение 1. Функция $f \in \mathrm{P}_k^{(n)}$ называется совершенно уравновешенной (обозначение $f \in \mathcal{PB}_k^{(n)}$), если для всякого натурального l и всякого $y \in \mathrm{E}_k^l$ верно равенство $\left|f_l^{-1}(y)\right| = k^{n-1}$.

Определение 2. Функция $f \in \mathrm{P}_k^{(n)}$ имеет правый барьер длины $b \geqslant 1$, если из равенства $f_b(x_1, x_2, \ldots, x_{n-1}, x'_n, \ldots, x'_{b+n-1}) = f_b(x_1, x_2, \ldots, x_{n-1}, x''_n, \ldots, x''_{b+n-1})$ следует $x'_n = x''_n$.

Абсолютно аналогично случаю $k = 2$ (см. [1]) для произвольного $k \geqslant 2$ доказывается, что наличие барьера влечет совершенную уравновешенность в P_k.

Й. Голичем в работе [2] в 1996 г. рассмотрен (при $k = 2$) вопрос о важном для используемых в фильтрующих генераторах функций свойстве, являющемся естественным усилением свойства совершенной уравновешенности.

Определение 3. Функция $f \in \mathcal{PB}_k^{(n)}$ называется сильно совершенно уравновешенной, если при добавлении любого числа фиктивных переменных между существенными она сохраняет совершенную уравновешенность.

Нетрудно показать, что перестановочность дискретной функции по первой или последней существенной переменной влечет за собой сильную совершенную уравновешенность. Голич в работе [2] предположил, что верно и обратное; данная гипотеза позже, начиная с работы М. Дихтла [3], стала называться гипотезой Голича.

Гипотеза 1 [2]. При $k = 2$ из сильной совершенной уравновешенности некоторой k-значной функции следует её перестановочность (т. е. линейность) по первой или последней существенной переменной.

Косвенное подтверждение справедливости гипотезы Голича было впервые получено в [1] (2008 г.). В работе [4] (2012 г.) гипотеза Голича полностью доказана. Таким образом, известно, что невозможно построить кодирующее устройство на основе регистра сдвига и фильтрующей функции (над алфавитом $\{0, 1\}$), обеспечивающее сохранение истинной случайности битовой последовательности при любом выборе точек входа (см. [2]). Интересен вопрос о возможности построения таких кодирующих

устройств над алфавитом большей мощности — в особенности в случае алфавита мощности $k = 2^m$, $m \geqslant 2$, т. е. в случае рассмотрения кодирующих устройств, преобразующих входную битовую последовательность блоками длины m.

Условие Голича. Сильная совершенная уравновешенность в P_k эквивалентна перестановочности по первой или последней существенной переменной.

Из результатов работ [2, 4] следует, что условие Голича выполнено в P_2. Настоящая работа посвящена рассмотрению следующего обобщения гипотезы Голича, связывающего справедливость условия Голича в P_k с простотой числа k.

Гипотеза 2. Условие Голича выполнено в P_k тогда и только тогда, когда k — простое.

Теорема 1. Для всякого составного k существует функция $f \in \mathcal{PB}_k^{(2)}$, существенно зависящая от обеих переменных и не перестановочная ни по одной из них.

Следствие 1. Если k — составное, то условие Голича не выполнено в P_k.

Теорема 2. Для всякого составного k существует функция $f \in \mathrm{P}_k$ с правым барьером длины 2, существенно зависящая от последней переменной и не перестановочная по ней.

Теорема 3. Для всякого составного k и всякого $n \geqslant 2$ существует сильно совершенно уравновешенная функция $f \in \mathrm{P}_k^{(n)}$, существенно зависящая от всех n переменных, которая не является перестановочной ни по первой, ни по последней переменной, но является сильно совершенно уравновешенной.

Теорема 4. Пусть k — простое и функция $f \in \mathrm{P}_k^{(n)}$ имеет правый барьер длины 2. Тогда f не зависит существенно от последней переменной и перестановочна по предпоследней.

Следствие 2. При простом k условие Голича не нарушается на функциях с барьером длины 2.

Следствие 3. Условие Голича не нарушается на функциях с барьером длины 2 в P_k тогда и только тогда, когда k — простое.

Теорема 5. При $k \in \{2, 3, 5, 7\}$ все совершенно уравновешенные функции из $\mathrm{P}_k^{(2)}$ перестановочны по первой или последней переменной.

Следствие 4. При $k \in \{2, 3, 5, 7\}$ условие Голича не нарушается на функциях из $\mathrm{P}_k^{(2)}$.

Таким образом, гипотеза 2 полностью доказана в части необходимости k быть простым для выполнения условия Голича в P_k. Кроме того, доказан ряд утверждений, косвенно подтверждающих справедливость гипотезы 2 в части достаточности.

ЛИТЕРАТУРА

1. *Logachev O. A., Salnikov A. A., Smyshlyaev S. V., and Yashchenko V. V.* Perfectly Balanced Functions in Symbolic Dynamics // Proc. NATO ARW, Veliko Tarnovo, Bulgaria, 6–9 October 2008. P. 222–233.
2. *Golić J. Dj.* On the Security of Nonlinear Filter Generators // LNCS. 1996. V. 1039. P. 173–188.
3. *Dichtl M.* On nonlinear filter generators // LNCS. 1997. V. 1267. P. 103–106.

4. *Smyshlyaev S. V.* Perfectly Balanced Boolean Functions and Golić Conjecture // J. Cryptology. 2012. No. 25(3). P. 464–483.

УДК 519.7

О РАЗЛОЖЕНИИ БУЛЕВОЙ ФУНКЦИИ В СУММУ БЕНТ-ФУНКЦИЙ[1]

Н. Н. Токарева

Булева функция от чётного числа переменных, максимально удалённая от класса всех аффинных функций, называется *бент-функцией*. В работах [1, 2] исследована связь между вопросом о числе бент-функций и проблемой разложения произвольной булевой функции в сумму двух бент-функций. Была представлена серия гипотез, одна из которых заключается в том, что каждую булеву функцию от n переменных степени не больше $n/2$ можно представить в виде суммы двух бент-функций от n переменных. В [2] с помощью компьютера гипотеза проверена для малых значений $n \leqslant 6$.

В 2011 г. Л. Ку и С. Ли [3] разобрали случай малых n аналитически. В общем случае они доказали, что в виде суммы двух бент-функций может быть представлена любая квадратичная булева функция, любая бент-функция Мак-Фарланда, любая функция частичного расщепления (*partial spread function*).

В данной работе доказан ослабленный вариант гипотезы.

Теорема 1. Любая булева функция от n переменных степени d, где $d \leqslant n/2$, n чётно, может быть представлена в виде суммы не более чем $2\binom{2b}{b}$ бент-функций от n переменных, где b — наименьшее число, $b \geqslant d$, такое, что n делится на $2b$.

Заметим, что разложение, указанное в теореме, можно провести с помощью только бент-функций Мак-Фарланда.

ЛИТЕРАТУРА

1. *Токарева Н. Н.* Гипотезы о числе бент-функций // Прикладная дискретная математика. Приложение. 2011. № 4. С. 21–23.
2. *Tokareva N.* On the number of bent functions from iterative constructions: lower bounds and hypotheses // Adv. in Mathematics of Communications (AMC). 2011. V. 5. No. 4. P. 609–621.
3. *Qu L. and Li C.* Representing a Boolean function as the sum of two Bent functions // Discrete Applied Mathematics. 2012 (to appear).

УДК 681.03

ЛАТИНСКИЕ КВАДРАТЫ И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

М. Э. Тужилин

Подсчёт числа латинских квадратов порядка n — сложная комбинаторная задача, их точное число известно только для n от 1 до 11 [1].

Латинские квадраты находят применение в комбинаторике, алгебре (изучение латинских квадратов тесно связано с изучением квазигрупп), теории кодов, статистике и многих других областях [2].

[1]Исследование выполнено при поддержке РФФИ (проекты 10-01-00424, 11-01-00997) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 г. (гос. контракт 02.740.11.0429).