# Правильные семейства булевых функций с симметрическим слагаемым

М. А. Осипова*

Рассматривается обобщение известного квадратично-линейного семейства булевых функций: к линейной треугольной части добавляется произвольная симметрическая булева функция от всех переменных, кроме одноимённой. Доказано, что такое семейство является правильным и имеет максимально возможную мощность образа. Тем самым новое семейство сохраняет ключевое свойство известного частного случая.

**Ключевые слова:** правильное семейство функций, булевы функции, симметрическая функция, квазигруппа, мощность образа.

## 1. Введение

Квазигруппы — аналоги групп без требования ассоциативности — активно рассматриваются как структуры для построения криптографических примитивов: многие известные атаки существенно используют ассоциативность. Прямое табличное задание квазигруппы большого порядка практически неэффективно, поэтому естественным является переход к функциональному заданию квазигруппы.

Один из таких подходов предложен В. А. Носовым [1] и основан на *правильных семействах функций*. Семейство функций задаёт параметрический класс латинских квадратов, а условие правильности является необходимым и достаточным условием того, что получаемая операция является квазигрупповой при произвольном выборе параметрических функций.

В работе рассматривается обобщение известного квадратично-линейного семейства: к линейной треугольной части добавляется произвольная симметрическая булева функция от всех переменных, кроме одноимённой. Основной результат: такое семейство является правильным и имеет максимально возможную мощность образа.

* *Осипова Марина Андреевна* — студентка каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: marina-a-o@yandex.ru.

*Osipova Marina Andreevna* — student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intelligent Systems.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

## 2. Основные понятия и известные результаты

**Определение 1.** Конечная $n$-квазигруппа ($n \geq 2$) — пара $(Q, f)$, где $Q$ — конечное множество, а $f\colon Q^n \to Q$ является биекцией при произвольной фиксации любых $n-1$ переменных.

Пусть $E_k = \{0, 1, \ldots, k-1\}$, $P_k^m$ — множество всех дискретных функций $m$ аргументов $f\colon E_k^m \to E_k$.

**Определение 2.** Семейство $G = (g_1, \ldots, g_m)$, $g_i \in P_k^m$, называется *правильным*, если для любой пары различных $s, t \in E_k^m$ найдётся индекс $i$, $1 \leq i \leq m$, такой, что $s_i \neq t_i$, но $g_i(s) = g_i(t)$.

В работе [2] предложен способ порождения $n$-квазигрупп с помощью правильных семейств; доказано, что конструкция порождает не менее $M^{k^n}$ попарно различных $n$-квазигрупп, где $M$ — мощность образа правильного семейства. Поэтому мощность образа является важной характеристикой.

**Квадратично-линейное семейство.** Пусть $k = 2$. Известно, что для любого $m \geq 1$ семейство

$$f_s(x_1, \ldots, x_m) = \bigoplus_{i<s} x_i \ \oplus \bigoplus_{\substack{1\leq i<j\leq m \\ i,j\neq s}} x_i x_j, \qquad s = 1, \ldots, m,$$

является правильным [3] и имеет максимальную возможную мощность образа $2^{m-1}$ [2].

Логичным шагом является обобщение этой конструкции: добавление к линейной треугольной части произвольной симметрической функции от $m-1$ переменной.

**Определение 3.** Для $l \geq 0$ булева функция $H\colon \{0,1\}^l \to \{0,1\}$ называется *симметрической*, если существует функция $h\colon \{0, \ldots, l\} \to E_2$ такая, что для всякого $z = (z_1, \ldots, z_l) \in \{0,1\}^l$

$$H(z) = h(|z|), \qquad |z| = z_1 + \cdots + z_l$$

(сумма понимается как обычное целое число).

## 3. Основные результаты

**Теорема 1** (Правильность)**.** *Пусть $m \geq 1$, и пусть $H\colon \{0,1\}^{m-1} \to \{0,1\}$ — произвольная симметрическая булева функция. Для $s = 1, \ldots, m$*

*зададим*

$$f_s(x_1,\dots,x_m) = \bigoplus_{i<s} x_i \ \oplus \ H(x_1,\dots,x_{s-1},x_{s+1},\dots,x_m).$$

*Тогда семейство $F = (f_1,\dots,f_m)$ является правильным.*

**Теорема 2** (Максимальная мощность образа)**.** *В условиях теоремы 1*

$$|\operatorname{Im} F| = 2^{m-1}.$$

*В частности, мощность образа – максимально возможная среди правильных булевых семейств размера $m$.*

## 4. Заключение

Доказано, что семейство булевых функций, получаемое добавлением произвольной симметрической функции от $m-1$ переменной к линейной треугольной части, является правильным (теорема 1) и имеет максимально возможную мощность образа $2^{m-1}$ (теорема 2). Тем самым новое семейство сохраняет ключевое свойство известного квадратично-линейного частного случая. Полученные результаты дают новые примеры правильных семейств, пригодные для функционального задания квазигрупп большого порядка, и могут быть использованы в конструкции порождения $n$-квазигрупп.

Направление дальнейшей работы – обобщение конструкции для функций $k$-значной логики.

## Список литературы

[1] Носов В. А., “О построении классов латинских квадратов в булевой базе данных”, *Интеллектуальные системы. Теория и приложения*, **4**:3–4 (1999), 307–320.

[2] Галатенко А. В., Носов В. А., Панкратьев А. Е., Царегородцев К. Д., “О порождении $n$-квазигрупп с помощью правильных семейств функций”, *Дискретная математика*, **35**:1 (2023), 35–53. DOI: 10.4213/dm1749.

[3] Царегородцев К. Д., “О свойствах правильных семейств булевых функций”, *Дискретная математика*, **33**:1 (2021), 91–102. DOI: 10.4213/dm1634.

Статья поступила 8 ноября 2026 г.

**Proper families of Boolean functions with a symmetric summand**

M. A. Osipova

We consider a generalization of the well-known quadratic-linear family of Boolean functions: an arbitrary symmetric Boolean function of all variables except the one with the same index is added to the linear triangular part. It is proved that this family is proper and has the maximum possible image cardinality. Thus, the new family preserves the key property of the known particular case.

**Keywords:** proper family of functions, Boolean functions, symmetric function, quasigroup, image cardinality.

# References

[1] Nosov V. A., "On the construction of classes of Latin squares in a Boolean database", *Intellektual'nye Sistemy*, **4**:3–4 (1999), 307–320 (In Russian).

[2] Galatenko A. V., Nosov V. A., Pankratiev A. E., Tsaregorodtsev K. D., "Generation of $n$-quasigroups using proper families of functions", *Discrete Mathematics and Applications*, **35**:4 (2025), 203–217. DOI: 10.1515/dma-2025-0015.

[3] Tsaregorodtsev K. D., "Properties of proper families of Boolean functions", *Discrete Mathematics and Applications*, **32**:5 (2022), 369–378. DOI: 10.1515/dma-2022-0030.

Received on November 8, 2026