О некоторых новых классах правильных семейств

А. В. ГАЛАТЕНКО
Московский государственный университет им. М. В. Ломоносова
e-mail: agalat@msu.ru

В. А. НОСОВ
Московский государственный университет им. М. В. Ломоносова
e-mail: vnosov40@mail.ru

А. Е. ПАНКРАТЬЕВ
Московский государственный университет им. М. В. Ломоносова
e-mail: apankrat@intsys.msu.ru

К. Д. ЦАРЕГОРОДЦЕВ
Московский государственный университет им. М. В. Ломоносова
e-mail: kirill94_12@mail.ru

УДК 519.716.32

Ключевые слова: правильные семейства функций, последовательности Люка, граф существенной зависимости.

Аннотация

Правильные семейства функций являются удобным средством для задания больших параметрических множеств квазигрупп и n-квазигрупп. В работе описывается обобщение двух известных классов правильных семейств: семейств на основе перемножения перестановочных многочленов и треугольных семейств.

Abstract

A. V. Galatenko, V. A. Nosov, A. E. Pankratiev, K. D. Tsaregorodtsev, Some new classes of proper families, Fundamentalnaya i prikladnaya matematika, vol. 25 (2025), no. 4, pp. 79—93.

Proper families of functions are a convenient framework for specifying large parametric sets of quasigroups and n-quasigroups. The paper describes a generalization of two known classes of proper families: families based on a product of permutation polynomials and triangular families.

Фундаментальная и прикладная математика, 2025, том 25, № 4, с. 79—93.

Памяти Евгения Васильевича Панкратьева

1. Введение

Тематика данной работы относится к сфере компьютерной алгебры, которая являлась основным предметом исследований Евгения Васильевича Панкратьева [1, 9, 20]. В круг его интересов входили различные алгебраические вопросы, в том числе имеющие непосредственное приложение к проблемам защиты информации.

Конечные квазигруппы становятся популярной платформой для реализации различных криптографических функций. В работе К. Шеннона [27] было показано, что табличное гаммирование на основе таблицы Кэли квазигруппы является совершенным шифром. Квазигрупповые алгоритмы NaSHA [21] и EDON-R′ [19] участвовали в конкурсе NIST по выбору стандарта хэширования SHA-3; алгоритмы GAGE и InGAGE [18] были выставлены на конкурс по выбору стандарта низкоресурсной криптографии. Подробный обзор состояния предметной области представлен в [15].

Квазигруппы небольшого порядка могут быть эффективно заданы таблицей Кэли, однако если порядок велик (например, в алгоритме NaSHA используются квазигруппы порядка 2^{64}), табличное задание становится неприемлемым с практической точки зрения. В качестве альтернативы выступают рекурсивные обобщённые сети Фейстеля [23], ортоморфизмы абелевых групп [14] и правильные семейства функций [17].

Правильные семейства булевых функций были введены В. А. Носовым в [4], в [5] было показано, как с помощью правильных семейств булевых функций можно задавать большие классы квазигрупп. Затем В. А. Носов и А. Е. Панкратьев обобщили конструкцию на семейства функций логик произвольной значности [7]. К настоящему моменту известен ряд примеров правильных семейств функций, однако эти примеры покрывают лишь малую долю правильных семейств. Как следствие, актуальна задача расширения спектра примеров. При этом желательно, чтобы выполнялся ряд дополнительных свойств, таких как возможность задания короткими формулами (для обеспечения эффективности по памяти) и большая мощность образа (для обеспечения большой мощности класса порождаемых квазигрупп, см. [2]).

В данной работе обсуждается обобщение двух известных классов правильных семейств: семейств на основе перестановочных многочленов из [6] и треугольных семейств. Дальнейшее изложение имеет следующую структуру. В разделе 2 вводятся необходимые определения. В разделе 3 описывается обобщение семейств из работы [6], доказывается правильность нового класса, а также вычисляется мощность образа. В разделе 4 изучаются рекурсивно треугольные и локально треугольные семейства. Раздел 5 является заключением.

2. Основные определения и обозначения

Пусть $k, n \in \mathbb{N}$, $k \geqslant 2$. Обозначим множество $\{0, 1, \ldots, k-1\}$ через E_k. Пусть P_k^m — множество всех функций из E_k^m в E_k (в частности, P_k^0 — множество всех констант). Будем считать, что на множестве E_k введена структура абелевой группы $(E_k, +)$ (например, с помощью сложения по модулю k). Группу подстановок на множестве $\{1, \ldots, n\}$ обозначим через $\mathcal{S}_n$.

Определение 1. Пусть $f_1, \ldots, f_n \in P_k^n$. Семейство $\mathcal{F}_n = (f_1, \ldots, f_n)$ называется правильным, если для любых наборов $\alpha, \beta \in E_k^n$, $\alpha \neq \beta$, $\alpha = (a_1, \ldots, a_n)$, $\beta = (b_1, \ldots, b_n)$, найдётся индекс i, $1 \leqslant i \leqslant n$, такой что $a_i \neq b_i$, но $f_i(\alpha) = f_i(\beta)$.

Приведём два примера правильных семейств.

Пример 1 [6]. Пусть k простое, $n \geqslant 3$, $g \in P_k^1$ — произвольная биекция,

$$\begin{aligned}
f_1 &= g(x_2+1)\cdot g(x_2+2)\cdot \ldots \cdot g(x_2+k-1)\cdot g(x_3) \mod k,\\
f_2 &= g(x_3+1)\cdot g(x_3+2)\cdot \ldots \cdot g(x_3+k-1)\cdot g(x_4) \mod k,\\
&\vdots\\
f_n &= g(x_1+1)\cdot g(x_1+2)\cdot \ldots \cdot g(x_1+k-1)\cdot g(x_2) \mod k.
\end{aligned}$$

Семейство является правильным тогда и только тогда, когда n нечётно [6, теорема 5].

Для изложения второго примера потребуется сперва дать следующее определение.

Определение 2. Для пары подстановок $\sigma, \tau \in \mathcal{S}_n$ и семейства $\mathcal{F}_n \colon E_k^n \to E_k^n$ размера n рассмотрим семейство $(\sigma, \tau)(\mathcal{F}_n)$, которое получено из $\mathcal{F}_n$ с помощью перестановки индексов переменных и перестановки индексов входящих в семейство функций:

$$(\sigma, \tau)(\mathcal{F}_n) = \begin{bmatrix} f_{\sigma^{-1}(1)}\left(x_{\tau^{-1}(1)}, \ldots, x_{\tau^{-1}(n)}\right) \\ \vdots \\ f_{\sigma^{-1}(n)}\left(x_{\tau^{-1}(1)}, \ldots, x_{\tau^{-1}(n)}\right) \end{bmatrix},$$

т. е. функция с номером i переходит на место функции с номером $\sigma(i)$, а переменная с номером i переходит на место переменной с номером $\tau(i)$.

Введём также преобразование $\sigma(\mathcal{F}_n)$ следующим образом:

$$\sigma(\mathcal{F}_n) = (\sigma, \sigma)(\mathcal{F}_n).$$

Другими словами, $\sigma(\mathcal{F}_n)$ — семейство, полученное применением подстановки σ как к индексам функций, так и к индексам координат. Введённое таким образом преобразование будем называть *согласованной перестановкой* или *согласованной перенумерацией семейства*.

Пример 2. Пусть с точностью до согласованной перенумерации переменных и функций $f_j = f_j(x_1, \ldots, x_{j-1})$, т. е. функция может существенно зависеть

только от переменных с меньшими номерами. Семейства такого вида называются треугольными. Для того чтобы показать, что треугольное семейство правильное, достаточно рассмотреть произвольную пару различных наборов α и β, в качестве i выбрать первый индекс, на котором эти наборы различаются, и заметить, что $f_i(\alpha) = f_i(\beta)$.

Определение 3. Пусть $\mathcal{F}_n = (f_1, \ldots, f_n)$, $f_i \in P_k^n$, является семейством размера n. Под проекцией семейства $\Pi_i^a(\mathcal{F}_n)$, где $a \in E_k$, будем понимать семейство $\mathcal{G}_{n-1}$, полученное из $\mathcal{F}_n$ подстановкой вместо x_i константы a и вычёркиванием функции f_i:

$$\mathcal{G}_{n-1}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = \Pi_i^a(\mathcal{F}_n) = \\ = \begin{bmatrix} f_1(x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n) \\ \vdots \\ f_{i-1}(x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n) \\ f_{i+1}(x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n) \\ \vdots \\ f_n(x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n) \end{bmatrix}.$$

В [8] было введено следующее определение.

Определение 4. Графом существенной зависимости семейства функций $\mathcal{F}_n$ будем называть ориентированный граф $G_{\mathcal{F}} = (V, E)$, множество вершин которого равно $V = \{1, \ldots, n\}$ и ребро (i, j) принадлежит E в том и только в том случае, когда функция f_j существенно зависит от x_i.

Определение 5. Введём частную производную $\partial_i \mathcal{F}(x) \in \{0, 1\}$ отображения $\mathcal{F}\colon E_k^n \to E_k^n$ в точке $x = (x_1, \ldots, x_n)$, $1 \leqslant i \leqslant n$:

$$\partial_i \mathcal{F}(x) = \begin{cases} 1, & \text{если существует } q \in E_k, \text{ такое что} \\ & \mathcal{F}(x_1, \ldots, x_{i-1}, q, x_{i+1}, \ldots, x_n) \neq \\ & \neq \mathcal{F}(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n), \\ 0 & \text{в противном случае.} \end{cases}$$

3. Обобщение конструкции с перестановочным многочленом

Определение 6. Пусть $c, d \in E_k$, $h \in P_k^k$. Функция h обладает (c, d)-свойством, если на любом входном наборе, содержащем значение c, она принимает значение d.

Например, функции min и умножение по модулю k обладают $(0, 0)$-свойством, а функция $\max - (k-1, k-1)$-свойством.

Пусть $n \geqslant 3$, индексы $1, 2, \ldots, n$ «скручены в кольцо»: за n следует 1, перед единицей идёт n. Пусть $g \in P_k^1$, функции $h_i \in P_k^k$, $i = 1, \ldots, n$, обладают

(c,d)-свойством, $c \in \mathrm{Im}(g)$, $I_1 = (c_1,\dots,c_t)$, $I_2 = (c_{t+1},\dots,c_k)$ — два непустых упорядоченных набора элементов E_k, все компоненты которых попарно различны и в объединении дают всё E_k. Рассмотрим семейство $(f_1,\dots,f_n)$, определённое следующим соотношением:

$$f_i = h_i\big(g(x_{i+1}+c_1),\dots,g(x_{i+1}+c_t),g(x_{i+2}+c_{t+1}),\dots,g(x_{i+2}+c_k)\big). \qquad (1)$$

Несложно заметить, что в случае $n=1$ соотношения (1) вырождаются в константу d, в случае $n=2$ возникает семейство

$$f_1 = h_1\big(g(x_2+c_1),\dots,g(x_2+c_t),g(x_1+c_{t+1}),\dots,g(x_1+c_k)\big),$$
$$f_2 = h_2\big(g(x_1+c_1),\dots,g(x_1+c_t),g(x_2+c_{t+1}),\dots,g(x_2+c_k)\big).$$

Замечание 1. Построенное семейство является обобщением семейства из работы [6]. В этой работе предполагалось, что k простое, функции h_i являются умножением по модулю k, функция g — произвольная биекция, $I_1 = (1,\dots,k-1)$, $I_2 = (0)$.

Замечание 2. Результаты раздела остаются верными при замене операции сложения в определении семейства (1) на любую другую операцию, задающую структуру квазигруппы на множестве E_k.

Теорема 1. *Семейство* (1) *является правильным при нечётном* n.

Доказательство. Случай $n=1$ является тривиальным, так как по условию функция f_1 тождественно равна d. В дальнейшем будем считать, что $n \geqslant 3$.

Заметим, что если на каком-то наборе $\alpha \in E_k^n$ функция f_i принимает значение, отличное от d, то по построению $f_{i-1}(\alpha) = f_{i+1}(\alpha) = d$. В силу нечётности n отсюда следует, что на любом входном наборе по крайней мере $(n+1)/2$ функций f_i примут значение d и для любой пары входных наборов α, β найдётся индекс i_0, такой что $f_{i_0}(\alpha) = f_{i_0}(\beta) = d$.

Предположим, что семейство (1) не является правильным, то есть существует пара наборов $\alpha = (a_1,\dots,a_n)$, $\beta = (b_1,\dots,b_n)$, $\alpha \neq \beta$, таких что для любого i, для которого $a_i \neq b_i$, выполнено $f_i(\alpha) \neq f_i(\beta)$. Рассмотрим индекс i_0, такой что $f_{i_0}(\alpha) = f_{i_0}(\beta) = d$. По предположению $a_{i_0} = b_{i_0}$. Если среди элементов $g(a_{i_0}+c_{t+1}),\dots,g(a_{i_0}+c_k)$ найдётся значение c, то по определению семейства f выполнено равенство $f_{i_0-2}(\alpha) = f_{i_0-2}(\beta) = d$. Значит, по предположению $a_{i_0-2} = b_{i_0-2}$. В противном случае значение c встречается среди $g(a_{i_0}+c_1),\dots,g(a_{i_0}+c_t)$, откуда следует, что $f_{i_0-1}(\alpha) = f_{i_0-1}(\beta) = d$, что влечёт равенства $a_{i_0-1} = b_{i_0-1}$. Таким образом, $f_{i_0-2}(\alpha) = f_{i_0-2}(\beta)$, так как все аргументы, подставляемые в функцию f_{i_0-2}, покомпонентно совпадают; следовательно, $a_{i_0-2} = b_{i_0-2}$. Продолжая рассуждения, в силу нечётности n получаем, что наборы α и β совпадают. Противоречие. □

Теорема 2. *Пусть функции* h_i, $i = 1,\dots,n$, *и* g *таковы, что*

$$h_i\big(g(x+c_1),\dots,g(x+c_t),g(y+c_{t+1}),\dots,g(y+c_k)\big)$$

принимает все значения из некоторого множества $M \subseteq E_k$, $|M| = m$. *Тогда мощность образа семейства* (1) *равна*

$$\frac{\left(1+\sqrt{4m-3}\right)^n + \left(1-\sqrt{4m-3}\right)^n}{2^n}.$$

Доказательство. Сперва докажем верхнюю оценку. Заметим, что из определения семейства (1) следует, что если на наборе $\alpha \in E_k^n$ функция f_i принимает значение, отличное от d, то с учётом закольцованности индексов $f_{i-1}(\alpha) = f_{i+1}(\alpha) = d$. Значит, в образе семейства не содержится закольцованных наборов, содержащих два последовательных элемента, отличных от d, и мощность образа не превосходит мощности множества $C_m(n)$ наборов длины n с элементами из M, таких что ни один циклический сдвиг набора не содержит два подряд элемента, отличных от d. Рассмотрим величину $c_m(n)$, определённую следующим соотношением:

$$c_m(n) = \begin{cases} 1 & \text{при } n = 1; \\ 2m-1 & \text{при } n = 2; \\ |C_m(n)| & \text{в оставшихся случаях.} \end{cases}$$

Легко увидеть, что мощность образа семейства (1) не превосходит $c_m(n)$.

Выведем рекуррентное соотношение на $c_m(n)$ при $n \geqslant 3$. Обозначим через $D_m(n)$ множество всех наборов длины n с элементами из M, таких что в любых двух идущих подряд компонентах присутствует значение d, $d_m(n) = |D_m(n)|$. Пусть $\beta = (b_1, \ldots, b_n) \in C_m(n)$. Если $b_1 = d$, то в качестве $(b_2, \ldots, b_n)$ можно выбрать любой набор из $D_m(n-1)$. Если $b_1 \neq d$ ($m-1$ вариантов), то $b_2 = b_n = d$, а в качестве $(b_3, \ldots, b_{n-1})$ можно выбрать любой набор из $D_m(n-3)$. Заметим, что $d_m(1) = m$, $d_m(2) = 2m-1$. Дополнительно положим $d_m(0) = 1$. Мы показали, что при $n \geqslant 3$ выполнено следующее равенство:

$$c_m(n) = d_m(n-1) + (m-1)d_m(n-3). \tag{2}$$

Выпишем аналогичное соотношение на $d_m(n)$ при $n \geqslant 3$. Если набор начинается с d, то его можно продолжить любым набором из $D_m(n-1)$. Если же первый элемент отличен от d ($m-1$ вариант), то следующий элемент непременно равен d, а потом следует произвольный набор из $D_m(n-2)$. Таким образом, при $n \geqslant 3$ выполнено следующее равенство:

$$d_m(n) = d_m(n-1) + (m-1)d_m(n-2). \tag{3}$$

Из соотношения (3) и начальных условий на $d_m(n)$ следует, что $d_m(n)$ является сдвинутой последовательностью Люка $U\big(1, -(m-1)\big)$, то есть $d_m(n) = U_{n+2}\big(1, -(m-1)\big)$ (см., например, [29]). Таким образом, соотношение (2) принимает вид

$$c_m(n) = U_{n+1}\big(1, -(m-1)\big) + (m-1)U_{n-1}\big(1, -(m-1)\big)$$

(причём при $n = 1, 2$ оно тоже выполнено), откуда следует, что $c_m(n)$ совпадает с последовательностью Люка $V_n\big(1, -(m-1)\big)$, то есть удовлетворяет

соотношению

$$c_m(n) = \begin{cases} 1 & \text{при } n = 1; \\ 2m-1 & \text{при } n = 2; \\ c_m(n-1) + (m-1)c_m(n-2) & \text{в остальных случаях.} \end{cases}$$

Следовательно,

$$c_m(n) = 2^{-n} \cdot \left(\left(\sqrt{4m-3}+1\right)^n + \left(1-\sqrt{4m-3}\right)^n \right)$$

(это равенство несложно доказать по индукции).

Теперь установим, что оценка достигается. Для $n = 1$ мощность образа всегда равна 1. Покажем, что при всех других значениях $n \in \mathbb{N}$ образ семейства содержит все элементы множества $C_m(n)$. Пусть $(b_1, \ldots, b_n) \in C_m(n)$. Если $b_i \neq d$, по условию можно подобрать значения a_{i+1} и a_{i+2} в наборе $\alpha = (a_1, \ldots, a_n) \in E_k^n$ так, что $f_i(\alpha) = b_i$. При этом $f_{i-1}(\alpha) = f_{i+1}(\alpha) = d$. Продолжая процесс, зафиксируем компоненты α так, что равенство $f_j(\alpha) = b_j$ выполнено для всех $b_j \neq d$, при этом $f_{j-1}(\alpha) = f_{j+1}(\alpha) = d$. Заметим, что к этому моменту зафиксированы значения α_{j+1} и α_{j+2}, а все существенные переменные функций f_l, таких что равенство $f_l(\alpha) = b_l = d$ пока не обеспечено, остаются свободными. Обеспечим равенство $f_l(\alpha) = b_l = d$, зафиксировав значение a_{l+1} (это всегда можно сделать в силу условия на функции g и h_l). Легко увидеть, что набор $(d, \ldots, d)$ также лежит в образе. В результате обеспечивается нужное значение семейства на наборе α, то есть все элементы $C_m(n)$ принадлежат образу. □

Следствие 1. *Пусть функции h_i, $i = 1, \ldots, n$, и g таковы, что функции*

$$h_i\big(g(x+c_1), \ldots, g(x+c_t), g(y+c_{t+1}), \ldots, g(y+c_k)\big)$$

принимают все k значений. Тогда мощность образа семейства (1) *равна*

$$\frac{\left(\sqrt{4k-3}+1\right)^n + \left(1-\sqrt{4k-3}\right)^n}{2^n}.$$

Рассмотрим несколько примеров семейств, на которых достигается максимум мощности образа. Легко увидеть, что таким свойством обладают исходные семейства из работы [6]. Ещё один пример, работающий для произвольного $k \geqslant 2$, получается, если в качестве g рассмотреть произвольную биекцию, взять $t = 1$ и h_i, равную нулю, если хотя бы один из аргументов равен нулю, и совпадающую с первым аргументом в противном случае.

В общем случае функция h_i с требуемыми свойствами может быть построена следующим образом. После выбора значений c и d значения на всех наборах, имеющих компоненту c, полагаются равными d. Затем выделяются наборы вида $(a+c_1, \ldots, a+c_t, b+c_{t+1}, \ldots, b+c_k)$, все компоненты которых отличны от c. Из построения следует, что значение a может быть выбрано $k-t$ способами, значение b может быть выбрано t способами, что даёт общее число $(k-t) \cdot t \geqslant k-1$ вариантов. На этих наборах функция определяется так, чтобы область значений

имела мощность $k-1$ (исключая значение d; это можно сделать $(k-1)!\cdot\left\{{(k-t)\cdot t \atop k-1}\right\}$ способами, где $\left\{{(k-t)\cdot t \atop k-1}\right\}$ — число Стирлинга второго рода) или k (эта возможность реализуется при $t \neq 1, k-1$; здесь число вариантов равно $k!\cdot\left\{{(k-t)\cdot t \atop k}\right\}$). На остальных наборах h_i доопределяется произвольным образом.

Замечание 3. Оценка мощности класса правильных семейств, введённых в данном разделе, является направлением дальнейших исследований.

4. Рекурсивно и локально треугольные семейства

Определение треугольного семейства допускает следующие обобщения.

Определение 7. Назовём семейство $\mathcal{F}_n$, заданное на E_k^n, рекурсивно треугольным, если существует координата i, такая что $f_i = q \in E_k$ (константа), и каждое из семейств вида $\Pi_i^a(\mathcal{F}_n)$ также является рекурсивно треугольным.

Замечание 4. Треугольные семейства являются частным случаем рекурсивно треугольных: треугольные семейства являются такими рекурсивно треугольными, что каждая из проекций $\Pi_i^a(\mathcal{F}_n)$ постоянна вдоль одного и того же направления j.

Замечание 5. Класс рекурсивно треугольных семейств вкладывается в класс локально треугольных семейств (см. определение 9). Как будет показано далее, локально треугольные семейства являются правильными, а следовательно, и рекурсивно треугольные семейства также являются правильными.

Обозначим через $\Delta_k^{\mathsf{rec}}(n)$ число рекурсивно треугольных семейств k-значной логики размера n.

Лемма 1. *Для числа рекурсивно треугольных семейств $\mathcal{F}_n\colon E_k^n \to E_k^n$ справедлива формула*

$$\Delta_k^{\mathsf{rec}}(n) = \sum_{j=1}^{n}(-1)^{j+1}\cdot k^j \cdot \binom{n}{j}\left(\Delta_k^{\mathsf{rec}}(n-j)\right)^{k^j},$$

где $\Delta_k^{\mathsf{rec}}(0) = 1$.

Доказательство. Утверждение следует напрямую из формулы включений-исключений (см., например, [11, ч. II, § 3]). Существует $\binom{n}{j}$ способов выбрать j «фиктивных направлений», для которых $f_\ell = \mathrm{const}$, и k^j способов зафиксировать значения j фиктивных функций. Каждая из проекций должна образовывать рекурсивно треугольное семейство размера $n-j$, и различные рекурсивно треугольные семейства в проекциях могут выбираться независимо друг от друга, что даёт итоговый вклад $\left(\Delta_k^{\mathsf{rec}}(n-j)\right)^{k^j}$. □

Замечание 6. Для $k = 2$ число рекурсивно треугольных семейств размера n совпадает с числом рекурсивных ориентаций куба $G(E_2^n)$ [24, A141770].

Теорема 3. *Доля булевых рекурсивно треугольных семейств размера n в классе всех булевых правильных семейств размера n стремится к 0 при $n \to \infty$.*

Доказательство. Для числа рекурсивно треугольных семейств справедливо неравенство

$$\Delta_k^{\mathsf{rec}}(n) \leqslant n \cdot k \cdot \left(\Delta_k^{\mathsf{rec}}(n-1)\right)^k.$$

Применяя неравенство рекурсивно и используя равенство $\Delta_k^{\mathsf{rec}}(0) = 1$, можно получить оценку

$$\Delta_k^{\mathsf{rec}}(n) \leqslant \left(n^{k^0} \cdot (n-1)^{k^1} \cdot (n-2)^{k^2} \times \ldots \times \left(n-(n-1)\right)^{k^{n-1}}\right) \cdot k^{(k^n-1)/(k-1)}.$$

Обозначим через $S(n,k)$ число вида

$$S(n,k) = \prod_{i=0}^{n-1} (n-i)^{k^i},$$

тогда согласно полученному неравенству имеем

$$\Delta_k^{\mathsf{rec}}(n) \leqslant S(n,k) \cdot k^{(k^n-1)/(k-1)}.$$

Для $S(n,2)$ верна следующая асимптотика при $n \to \infty$ [16, раздел 6.10]:

$$S(n,2) \sim \frac{s^{2^n}}{n}, \quad s = \sqrt{1 \cdot \sqrt{2 \cdot \sqrt{3 \cdot \ldots}}} \approx 1{,}661688.$$

Таким образом, для величины $\Delta_2^{\mathsf{rec}}(n)$ справедливо асимптотическое неравенство

$$\Delta_2^{\mathsf{rec}}(n) \lesssim \frac{(2s)^{2^n}}{2n},$$

а для доли рекурсивно треугольных с учётом неравенства на число правильных булевых семейств размера n (см. [10]) выполняется

$$\frac{\Delta_2^{\mathsf{rec}}(n)}{T(n)} \lesssim \frac{1}{2n} \cdot \left(\frac{2s}{n}\right)^{2^n}.$$

Полученная величина стремится к 0 при $n \to \infty$. □

Замечание 7. В общем случае для чисел $S(n,k)$ верна асимптотика [30]

$$S(n,k) \sim \frac{(A_k)^{k^n}}{n^{1/(1-k)}},$$

где A_k — некоторая константа, зависящая только от k.

В [28] было введено понятие локального графа взаимодействия для семейства $\mathcal{F}$ в точке x. По сути, это понятие определяет «локализованный» в точке x граф существенной зависимости семейства $\mathcal{F}$, а именно, он показывает, как локальные изменения аргумента в точке x влияют на поведение функции.

Определение 8. Определим локальный граф взаимодействий $G_{\mathcal{F}}(x)$ семейства $\mathcal{F}$ в точке x как ориентированный граф на множестве вершин $V =$

$= \{1, 2, \ldots, n\}$ со множеством рёбер E, имеющим следующий вид: $(i, j) \in E$ тогда и только тогда, когда $\partial_i f_j(x) \neq 0$.

Замечание 8. Граф существенной зависимости семейства $\mathcal{F}$ представляет собой объединение локальных графов взаимодействий $G_{\mathcal{F}}(x)$ по всем точкам $x \in E_k^n$.

В [25] было показано, что если граф существенной зависимости (в работе он назывался глобальным графом взаимодействия) $G_{\mathcal{F}}$ булева семейства $\mathcal{F}$ является ациклическим, то семейство $\mathcal{F}$ задаёт HUPF-сеть. По сути, было показано, что треугольные семейства являются правильными. Обобщение указанного результата приведено в [28], где было показано, что если локальный граф взаимодействия булева семейства $\mathcal{F}$ для каждой точки x является ациклическим, то семейство задаёт HUPF-сеть. Мы можем обобщить указанное наблюдение на любые (не только булевы) семейства $\mathcal{F}$ (см. лемму 5). Дадим предварительные определения.

Определение 9. Назовём семейство $\mathcal{F}$, заданное на E_k^n, локально треугольным в точке x, если существует такая согласованная перестановка σ семейства $\mathcal{F}$, что после её применения мы получим семейство $\mathcal{G}$, для которого $\partial_i g_j(x) = 0$ для всех $1 \leqslant j \leqslant i \leqslant n$.

Лемма 2. *Семейство $\mathcal{F}$ локально треугольно в точке x тогда и только тогда, когда $G_{\mathcal{F}}(x)$ является ориентированным ациклическим графом.*

Доказательство. Перейдём к семейству $\mathcal{G}$. Для переставленного семейства $\mathcal{G}$ первая функция g_1 локально постоянна по любому из направлений, функция g_2 локально постоянна по направлениям $x_2, \ldots, x_n$ и так далее. Это значит, что из вершины с номером i в графе $G_{\mathcal{G}}(x)$ могут выходить рёбра только к вершинам с номерами $j < i$. Если в графе $G_{\mathcal{G}}(x)$ существует цикл $i_1 \to i_2 \to i_k \to i_1$, то указанное свойство нарушается: достаточно рассмотреть вершину с наибольшим номером в цикле. По указанному выше свойству рёбра к этой вершине могут идти только от вершин с бóльшими номерами, но все оставшиеся номера в цикле меньше, чем у рассматриваемой вершины. Мы пришли к противоречию, которое доказывает, что в графе $G_{\mathcal{G}}(x)$ не может быть ориентированных циклов. Поскольку согласованная перестановка семейства только меняет метки у вершин графа $G_{\mathcal{F}}(x)$, то и в исходном графе не может быть циклов.

Докажем в обратную сторону: пусть в $G_{\mathcal{F}}(x)$ нет циклов. Тогда существует топологическая сортировка графа $G_{\mathcal{F}}(x)$ (см., например, [3, раздел 22.4]), т. е. такая перенумерация вершин σ, что после неё в графе остаются только такие рёбра $(i, j) \in E$, для которых $i < j$. Если применить σ к семейству $\mathcal{F}$ как согласованную перенумерацию, то функция f_n не будет зависеть существенно в точке x ни от какой из переменных, функция f_{n-1} может зависеть только от x_n и так далее. Поскольку это верно для каждой точки x, то по определению $\mathcal{F}$ является локально треугольным семейством. □

Лемма 3. *Пусть $\mathcal{F}$ — локально треугольное семейство, $\mathcal{G}$ — некоторая его проекция. Тогда $\mathcal{G}$ также является локально треугольным семейством.*

Доказательство. Без ограничения общности рассмотрим проекцию вида

$$\mathcal{G} = \Pi_i^a(\mathcal{F}).$$

Тогда граф $G_{\mathcal{G}}(x)$ для точки $x = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in E_k^{n-1}$ совпадает с графом $G_{\mathcal{F}}\big((x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n)\big)$ с удалённой i-й вершиной (и всеми инцидентными ей рёбрами). При удалении вершины новых циклов появиться не может, а значит, графы $G_{\mathcal{G}}(x)$ остаются ациклическими для каждой точки x. Следовательно, $\mathcal{G}$ локально треугольно. □

Лемма 4. *Пусть $v, y \in E_k^n$, $v = (v_1, \ldots, v_n)$, $y = (y_1, \ldots, y_n)$, $v_1 \neq y_1, \ldots, v_n \neq y_n$, $\mathcal{F}_n$ локально треугольное. Тогда найдётся такой индекс i, что $f_i(v) = f_i(y)$.*

Доказательство. Проведём доказательство индукцией по n — размеру семейства.

База индукции: при $n = 1$ локально треугольными семействами размера 1 будут только константы: $\mathcal{F}_1 = \big[a\big]$.

Индуктивный переход: рассмотрим $n \geqslant 2$. Так как $\mathcal{F}_n$ локально треугольно в точке v, то найдётся такая координата (без ограничения общности можем предполагать, что её номер равен n), что при варьировании соответствующей переменной при остальных фиксированных координатах никакая из функций не поменяется.

Рассмотрим проекцию вида $\mathcal{G} = \Pi_n^{y_n}(\mathcal{F}_n)$. В таком случае мы переходим к локально треугольному (см. лемму 3) семейству $\mathcal{G}$ размера $n-1$, по предположению индукции найдётся индекс $j < n$, такой что

$$f_j(v_1, \ldots, v_{n-1}, y_n) = g_j(v_1, \ldots, v_{n-1}) = g_j(y_1, \ldots, y_{n-1}) = f_j(y_1, \ldots, y_{n-1}, y_n).$$

Но поскольку исходное семейство $\mathcal{F}_n$ локально постоянно вдоль направления x_n в точке v, то

$$f_j(v_1, \ldots, v_{n-1}, v_n) = f_j(v_1, \ldots, v_{n-1}, y_n) = f_j(y_1, \ldots, y_{n-1}, y_n),$$

что и требовалось доказать. □

Лемма 5. *Пусть $\mathcal{F}$ — заданное на E_k^n локально треугольное семейство. Тогда $\mathcal{F}$ является правильным.*

Доказательство. Для любых двух неравных наборов $x, y \in E_k^n$, $x \neq y$, рассмотрим проекцию $\mathcal{G}$ исходного семейства $\mathcal{F}$ на совпадающие координаты (легко увидеть, что результат не зависит от порядка проецирования). Проекция $\mathcal{G}$ будет локально треугольным семейством по лемме 3. К семейству $\mathcal{G}$ можно применить лемму 4 и получить индекс i, для которого значения функций g_i совпадают. Тогда индекс i является тем индексом, существование которого требуется в определении правильности. □

Замечание 9. Множество булевых локально треугольных семейств шире множества треугольных семейств. Так, например, булевы семейства

$$\begin{bmatrix} 0 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_1x_2 \end{bmatrix}, \quad \begin{bmatrix} x_2x_3x_4 \\ x_1 \oplus x_1x_3 \\ x_2 \oplus x_1x_2 \oplus x_2x_4 \oplus x_1x_2x_4 \\ x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_2x_3 \end{bmatrix} \tag{4}$$

являются локально треугольными, но не треугольными.

Покажем, что рекурсивно треугольные семейства (см. определение 7) являются локально треугольными (а следовательно, правильными).

Утверждение 1. *Пусть $\mathcal{F}_n$ — рекурсивно треугольное семейство на E_k^n. Тогда $\mathcal{F}_n$ является локально треугольным семейством.*

Доказательство. Покажем, что для каждой точки v граф $G_{\mathcal{F}}(v)$ является ациклическим. Для рекурсивно треугольных семейств размера $n = 1$ и $n = 2$ утверждение проверяется напрямую.

Пусть $\mathcal{F}_n$ — рекурсивно треугольное семейство размера n. По свойству рекурсивной треугольности найдётся такой индекс i, что $f_i \equiv \mathrm{const}$, а следовательно, вершина i в графе $G_{\mathcal{F}}(v)$ является истоком (в неё не входит рёбер, так как f_i не зависит ни от одного x_j существенным образом). Следовательно, вершина i не может входить ни в какой из циклов.

Рассмотрим какую-либо проекцию $\mathcal{G} = \Pi_i^a(\mathcal{F})$ и её локальный граф взаимодействий в точке $\tilde{v} = (v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$. Граф $G_{\mathcal{G}}(\tilde{v})$ является подграфом графа $G_{\mathcal{F}}(v)$. При этом если в графе $G_{\mathcal{F}}(v)$ был цикл, то он останется хотя бы в одном из $G_{\mathcal{G}}(\tilde{v})$. Но каждое из семейств $\mathcal{G}$ также является рекурсивно треугольным (меньшего размера), а значит, по предположению индукции, в графах $G_{\mathcal{G}}(\tilde{v})$ нет циклов. □

Замечание 10. Свойство рекурсивной треугольности, вообще говоря, слабее свойства локальной треугольности (см., например, семейство размера 4 из замечания 9: в нём нет константы).

Фактически из рекурсивной треугольности следует, что *для всех* графов $G_{\mathcal{F}}(v)$ найдётся одна и та же вершина i, являющаяся истоком. Для $n = 1, 2, 3$ множества локально треугольных и рекурсивно треугольных семейств совпадают. Для $n = 4$ количество локально треугольных семейств $\Delta^{\mathsf{loc}}(4) = 3\,349\,488$ превышает число рекурсивно треугольных семейств $\Delta^{\mathsf{rec}}(4) = 3\,209\,712$ (см. табл. 1).

Множество локально треугольных семейств шире, чем множество треугольных семейств.

Замечание 11. Треугольные семейства являются и рекурсивно треугольными, и локально треугольными. Известно, что в классе треугольных семейств принимаются всевозможные значения мощности образа правильных семейств [2]. Значит, аналогичным свойством обладают рекурсивно треугольные и локально треугольные семейства.

4.1. Число различных семейств

Введём обозначения:

- $\Delta(n)$ — количество булевых треугольных семейств размера n;
- $\Delta^{\mathsf{loc}}(n)$ — количество булевых локально треугольных семейств размера n;
- $\Delta^{\mathsf{rec}}(n)$ — количество булевых рекурсивно треугольных семейств размера n;
- $T(n)$ — количество булевых правильных семейств размера n.

Таблица 1. Число треугольных, рекурсивно, локально треугольных и правильных булевых семейств размера n

n	$\Delta(n)$	$\Delta^{\mathsf{rec}}(n)$	$\Delta^{\mathsf{loc}}(n)$	$T(n)$
$n=1$	2	2	2	2
$n=2$	12	12	12	12
$n=3$	488	680	680	744
$n=4$	481 776	3 209 712	3 349 488	5 541 744
$n=5$	157 549 032 992	94 504 354 122 272	...	638 560 878 292 512

Число треугольных семейства размера $n=5$ получено в [12] (число CP-сетей размера $n=5$). Число правильных семейств размера $n=5$ получено в [22] (для числа классов эквивалентности замощений пространства), а также в [13, 26] (для числа одностоковых ориентаций). Заполнение ячейки, помеченной многоточием, является одним из направлений дальнейших исследований.

5. Заключение

В работе описаны новые классы правильных семейств: обобщение конструкции на основе перестановочных многочленов и обобщение треугольных семейств. Изучена мощность образа семейств из новых классов, являющаяся важной характеристикой с точки зрения мощности множества порождаемых квазигрупп. Направлениями дальнейших исследований являются оценка мощности первого из обобщений, а также изучение возможности переноса свойств рекурсивной и локальной треугольности на случай треугольных расширений правильных семейств (см., например, [6]).

Литература

[1] Абрамов С. А., Кондратьева М. В., Латышев В. Н., Михалёв А. В. Памяти Евгения Васильевича Панкратьева // Программирование. — 2008. — Т. 34, № 4. — С. 78—80.

[2] Галатенко А. В., Носов В. А., Панкратьев А. Е., Царегородцев К. Д. О порождении n-квазигрупп с помощью правильных семейств функций // Дискрет. матем. — 2023. — Т. 35, № 1. — С. 35—53.

[3] Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы. Построение и анализ. — Вильямс, 2009.

[4] Носов В. А. Критерий регулярности булевского неавтономного автомата с разделённым входом // Интеллект. сист. — 1998. — Т. 3, № 3-4. — С. 269—280.

[5] Носов В. А. Построение классов латинских квадратов в булевой базе данных // Интеллект. сист. — 1999. — Т. 4, № 3-4. — С. 307—320.

[6] Носов В. А. Построение параметрического семейства латинских квадратов в векторной базе данных // Интеллект. сист. — 2006. — Т. 8, № 1-4. — С. 517—529.

[7] Носов В. А., Панкратьев А. Е. Латинские квадраты над абелевыми группами // Фундамент. и прикл. матем. — 2006. — Т. 12, вып. 3. — С. 65—71.

[8] Носов В. А., Панкратьев А. Е. О функциональном задании латинских квадратов // Интеллект. сист. — 2008. — Т. 12, № 1-4. — С. 317—332.

[9] Памяти Евгения Васильевича Панкратьева // Фундамент. и прикл. матем. — 2008. — Т. 14, № 4. — С. 3—14.

[10] Царегородцев К. Д. О взаимно однозначном соответствии между правильными семействами булевых функций и рёберными ориентациями булевых кубов // Прикл. дискрет. матем. — 2020 — № 48. — С. 16—21.

[11] Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.

[12] Allen T. E., Goldsmith J., Mattei N. Counting, ranking, and randomly generating CP-nets // Workshops at the Twenty-Eighth AAAI Conf. on Artificial Intelligence, 2014.

[13] Bosshard V., Gärtner B. Pseudo unique sink orientations. — 2017. — `https://arxiv.org/abs/1704.08481`.

[14] Chakrabarti S., Galatenko A. V., Nosov V. A., Pankratiev A. E., Tiwari S. K. Quasigroups generated by shift registers and Feistel networks // Quasigroups and Relat. Syst. — 2023. — Vol. 31, no. 2. — P. 207—220.

[15] Chauhan D., Gupta I., Verma R. Quasigroups and their applications in cryptography // Cryptologia. — 2021. — Vol. 45, no. 3. — P. 227—265.

[16] Finch S. R. Mathematical Constants. — Cambridge Univ. Press, 2003.

[17] Galatenko A. V., Nosov V. A., Pankratiev A. E., Tsaregorodtsev K. D. Proper families of functions and their applications // Матем. вопр. криптографии. — 2023. — Т. 14, № 2. — С. 43—58.

[18] Gligoroski D., Mihajloska H., Otte D., El-Hadedy M. GAGE and InGAGE. — 2023. — `http://gageingage.org/upload/GAGEandInGAGEv1.03.pdf`.

[19] Gligoroski D., Ødegård R. S., Mihova M., Knapskog S. J., Drapal A., Klima V., Amundsen J., El-Hadedy M. Cryptographic hash function EDON-R′ // Proc. of the 1st Int. Workshop on Security and Communication Networks. — 2009. — P. 1—9.

[20] In Memoriam Eugeny Pankratiev: Faculty of Mechanics and Mathematics, Moscow State University, Moscow, Russia // ACM Commun. Algebra. — 2008. — Vol. 42, no. 1-2. — P. 23—26.

[21] Markovski S., Mileva A. NaSHA — family of cryptographic hash functions // The First SHA-3 Candidate Conf. — Leuven, 2009.

[22] Mathew K. A., Östergård P. R. J., Popa A. Enumerating cube tilings // Discrete Comput. Geom. — 2013. — Vol. 50, no. 4. — P. 1112—1122.

[23] Mileva A., Markovski S. Shapeless quasigroups derived by Feistel orthomorphisms // Glasnik Mat. — 2012. — Vol. 47. — P. 333—349.

[24] OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. — `http://oeis.org` (2008).

[25] Robert F. Iterations sur des ensembles finis et automates cellulaires contractants // Linear Algebra Its Appl. — 1980. — Vol. 29. — P. 393—412.

[26] Schurr I. Unique Sink Orientations of Cubes. — ETH Zurich, 2004.

[27] Shannon C. Communication theory of secrecy systems // The Bell Syst. Tech. J. — 1949. — Vol. 28, no. 2. — P. 656—715.

[28] Shih M.-H., Dong J.-L. A combinatorial analogue of the Jacobian problem in automata networks // Adv. Appl. Math. — 2005. — Vol. 34, no. 1. — P. 30—46.

[29] Vajda S. Fibonacci and Lucas Numbers, and the Golden Section: Theory and Applications. — Ellis Horwood Ltd., 1989.

[30] Xu A. Asymptotic expansion related to the generalized Somos recurrence constant // Int. J. Number Theory. — 2019. — Vol. 15, no. 10. — P. 2043—2055.