# О правильных семействах функций, используемых для задания латинских квадратов

Д. О. Рыков

В работе показано, что *правильность* семейства функций эквивалентна правильности семейств, возникающих на *сильных компонентах* и *блоках* компонент *графа существенной зависимости* семейства функций. Решается задача упрощения семейства, граф существенной зависимости которого содержит *«тривиальный» путь*. При этом упрощении семейства свойство правильности не меняется. Полученные результаты справедливы для семейств функций $k$-значной логики, где $k \geqslant 2$.

**Ключевые слова:** правильные семейства функций, латинские квадраты.

## Введение

В современном мире задачи защиты информации становятся все более актуальными. Появляется необходимость использования *латинских квадратов* для шифрования. Латинским квадратом порядка $n$ называется матрица размера $n \times n$, заполненная элементами некоторого множества $\Omega, |\Omega| = n$, таким образом, что в каждой ее строке и в каждом столбце все элементы различны. Фактически, латинский квадрат является таблицей Кэли (таблицей умножения) квазигруппы, алгебраической системы с бинарной операцией, в которой допускается деление (квазигруппа является некоторым обобщением группы). Латинские квадраты широко применяются во многих областях математики, в частности, в теории кодирования и защите информации. В своей работе о связи в секретных системах [7] К. Шеннон доказал, что шифры, построенные на латинских квадратах, обладают

свойством совершенной секретности. Чтобы не хранить все элементы латинского квадрата, их часто задают функционально, то есть с помощью функции, ставящей в соответствие строке и столбцу элемент, находящийся на их пересечении. В работе [2] приводится способ построения параметрического семейства латинских квадратов с помощью семейства булевых функций, обладающего свойством *правильности*.

Пусть дано семейство булевых функций $f = (f_1(z_1, \ldots, z_n), \ldots, f_n(z_1, \ldots, z_n))$ от $n$ переменных $z_1, \ldots, z_n$. Пусть $\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)$ — семейство булевых функций от двух переменных. Определим систему булевых функций $g = (g_1, \ldots, g_n)$ от $2n$ переменных $x_1, \ldots, x_n, y_1, \ldots, y_n$ соотношениями

$$\begin{gathered} g_1 = x_1 + y_1 + f_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \\ g_2 = x_2 + y_2 + f_2(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \\ \ldots \\ g_n = x_n + y_n + f_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)). \end{gathered}$$

Будем говорить, что семейство булевых функций $f = (f_1, f_2, \ldots, f_n)$ является правильным, если для любых различных наборов переменных $z' = (z'_1, z'_2, \ldots, z'_n)$ и $z'' = (z''_1, z''_2, \ldots, z''_n)$ существует $\alpha \in \overline{1, n}$ такое, что выполнено

$$z'_\alpha \neq z'_\alpha, f_\alpha(z'_1, \ldots, z'_n) = f_\alpha(z''_1, \ldots, z''_n).$$

Оказывается, семейство $g$ задает латинский квадрат при любом семействе функций $\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)$ тогда и только тогда когда семейство $f$ обладает свойством правильности. Таким образом с помощью любого правильного семейства функций $f = (f_1, f_2, \ldots, f_n)$ можно получать различные латинские квадраты, варьируя систему функций-параметров $\pi_1, \pi_2, \ldots, \pi_n$.

Стоит заметить, что схожим способом можно задавать латинские квадраты над векторами элементов $p$-значной логики и абелевых групп. Более подробно об этом можно узнать в статье [4].

Возможность задавать с помощью правильных семейств широкие классы латинских квадратов делает актуальным изучение этих семейств, их свойств, поиск алгоритмов проверки свойства правильности и другие задачи. Этому посвящены работы [1, 2, 3, 4], а также

работа автора [8]. В работе [1] предложен критерий правильности, сводящий задачу проверки правильности к проверке наличия в полиномах Жегалкина всевозможных произведений функций из семейства членов определенного вида. В работе [2] введено понятие *графа существенной зависимости* семейства функций и рядом результатов показано, что структура этого графа имеет большое значение для правильности. Так, семейство функций с ацикличным графом существенной зависимости — правильное, для семейств линейных функций правильность эквивалентна отсутствию циклов в графе. Для семейств мультиаффинных функций правильность эквивалентна тождественному равенству 0 произведения функций по каждому циклу. В работах [3, 4] результаты обобщены на случаи $p$-значной логики.

Имеющиеся результаты о связи правильности с цикловой структурой графа существенной зависимости в случае функций определенных классов навели на идею использования структуры этого графа в случае произвольных функций. В работе автора [8] эта идея была реализована. Показано, что граф существенной зависимости может быть использован для проверки правильности в случае произвольных булевых функций, а именно, проверка правильности сводится к проверке правильности семейств функций, возникающих на сильных компонентах этого графа. Тем не менее, если граф не допускает разложения на сильные компоненты, добиться снижения сложности проверки правильности по сравнению с прямым перебором этим методом не удается.

Целью данной работы является упрощение (по сравнению с предыдущими результатами) задачи проверки правильности (как в случае семейств булевых функций, так и в случае семейств функций $k$-значной логики) с помощью использования информации о структуре графа существенной зависимости, не ограничиваясь случаями семейств функций из определенных классов.

## Правильные семейства функций

Для начала введем основные определения.

**Определение 1.** Семейство функций $f = (f_1, f_2, \ldots, f_n)$ от переменных $x_1, x_2, \ldots, x_n$ называется *правильным*, если для любых двух

различных наборов значений переменных $x' = (x'_1, x'_2, \ldots, x'_n)$ и $x'' = (x''_1, x''_2, \ldots, x''_n)$ существует $\alpha \in \overline{1,n}$ такое, что выполнено

$$x'_\alpha \neq x''_\alpha, \quad f_\alpha(x') = f_\alpha(x'').$$

В данной работе мы не будем ограничиваться случаем булевских функций. Мы будем рассматривать правильные семейства функций над множеством элементов $k$-значной логики, $k \geqslant 2$.

Из определения правильного семейства функций в частности следует, что для любого $i \in \overline{1,n}$ функция $f_i$ не зависит существенно от переменной $x_i$.

Важную роль при изучении правильных семейств играют графы существенной зависимости этих семейств.

**Определение 2.** *Графом существенной зависимости* семейства функций $f = (f_1, \ldots, f_n)$ от переменных $x_1, \ldots, x_n$ называется ориентированный граф $G_f = (V, E)$, где $V = \{1, 2, \ldots, n\}$, а $E = \{(i, j) : f_j$ существенно зависит от $x_i\}$.

По структуре графа существенной зависимости семейства функций (в дальнейшем для краткости будем называть его графом семейства) можно делать определенные выводы о правильности семейства. Так, например, если граф семейства не содержит циклов, то это семейство правильно. Обратное неверно. Также, поскольку функции в правильном семействе не зависят существенно от переменных с тем же индексом, в графе правильного семейства не может быть петель.

Как уже было сказано выше, в работах [2, 3, 4] представлены способы упрощения проверки правильности для семейств функций определенных классов с помощью информации о цикловой структуре графа семейства. В данной работе мы будем рассматривать семейства произвольных функций и увидим, что и в таком случае информация о структуре графа семейства может быть весьма полезной.

Теперь нам понадобятся некоторые понятия из теории графов.

**Определение 3.** Ориентированный граф называется *сильно связным*, или *сильным*, если любые две его вершины взаимно достижимы.

**Определение 4.** *Сильной компонентой* графа называется максимальный сильный подграф.

**Определение 5.** *Конденсацией (факторграфом, графом сильных компонент)* графа $G$ называется граф $G^*$, множеством вершин которого служит множество $\{S_1, S_2, \ldots, S_m\}$ всех сильных компонент графа $G$, а дуга идет из $S_i$ к $S_j$, если в графе $G$ имеется по крайней мере одна дуга, идущая из некоторой вершины компоненты $S_i$ к вершине компоненты $S_j$.

**Определение 6.** Для любого подмножества вершин $S$ графа $G$ *порожденным этим множеством подграфом (вершинным подграфом)* $<S>$ называется максимальный подграф графа $G$, множеством вершин которого является $S$.

Также необходимо напомнить некоторые результаты из теории графов.

**Лемма 1 ([5]).** *Конденсация $G^*$ любого графа $G$ не содержит ориентированных циклов.*

**Лемма 2 ([5]).** *В любом ацикличном графе(графе без циклов) есть вершина, которая не является началом (концом) ни одной из дуг графа.*

Для формулировки следующих результатов обобщим понятие правильного семейства функций следующим образом.

**Определение 7.** Семейство функций $f_I = (f_i)$, $i \in I$, от переменных $x_J = (x_j)$, $j \in J$, $I \subseteq J$, будем называть *правильным*, если при любых значениях вектора $x^0_{J\setminus I} = (x^0_k)$, $k \in J\setminus I$, семейство $\tilde{f}_I = (\tilde{f}_i)$, $i \in I$, где $\tilde{f} = f|_{x_{J\setminus I} = x^0_{J\setminus I}}$, правильно в смысле первоначального определения.

Пусть $I$ — некоторое множество индексов, где $I \subset [1, n]$ и $\varepsilon_I = (\varepsilon_\alpha)$, $\alpha \in I$, $\varepsilon_\alpha \in \{0, 1\}$ — семейство констант с индексами из множества $I$. Определим семейство функций $f^0_{CI} = (f^0_i)$, $i \in CI$, где $CI$ — дополнение множества $I$ в $[1, n]$, полагая для любого $\lambda \in CI$

$$f^0_\lambda(x) = f_\lambda(x)|_{x_\alpha = \varepsilon_\alpha}, \qquad \alpha \in I.$$

Другими словами, $f^0_\lambda$ — это функции семейства $f$ с индексами из множества $CI$, в которых переменные с индексами из $I$ замещены константами семейства $\varepsilon_I$.

**Лемма 3 ([1]).** *Семейство функций $f$ правильно тогда и только тогда, когда для любого множества $I \subset [1,n]$ и любого семейства констант $\varepsilon_I$ семейство $f^0_{CI}$ правильно.*

Проще говоря, если семейство функций правильно, то при фиксации любого набора переменных константами получается правильное семейство функций.

**Следствие 1.** *Если семейство $f = (f_i)$, $i \in I$, правильно в некотором смысле, то для любого подмножества $K \subset I$ семейство $\hat{f} = (f_k)$, $k \in K$, правильно в смысле нового определения.*

Докажем следующую теорему.

**Теорема 1 (Критерий правильности).** *Пусть $f = (f_i)$, $i \in [1,n]$ — семейство функций от переменных $x_1, \ldots, x_n$. $f$ правильно тогда и только тогда, когда $\forall I : <I>$ — сильный граф, правильно семейство $f_I = (f_i)$, $i \in I$.*

**Доказательство.** Необходимость. Если $f$ правильно, то по следствию из леммы правильны также семейства $f_I = (f_i)$, $i \in I$.

Достаточность. Пусть $f_I$ правильно $\forall I : <I>$ — сильный подграф графа $G$. Докажем, что тогда $f$ правильно. Пусть это не так. Пусть свойство правильности нарушается на паре наборов $x'$ и $x''$. Обозначим $I = \{i : x'_i \neq x''_i\}$. Пусть $<I>$ состоит из $k$ сильных компонент $I_1, I_2, \ldots, I_k, k > 1$. Тогда по лемме 2 среди этих $k$ сильных компонент найдется компонента, не являющаяся концом ни одной из дуг в факторграфе $G^*$. Без ограничения общности будем считать, что это компонента $I_1 = \{i_{11}, i_{12}, \ldots, i_{1t_1}\}$. Это означает, что функции семейства $f_{I_1}$ зависят существенно только от переменных $x_{I_1}$. Рассмотрим набор $x''' = (x'''_1, \ldots, x'''_n)$ такой, что $x'''_i = x''_i$ при $i \in I_1$, $x'''_i = x'_i$ при $i \notin I_1$. Очевидно, что $f_i(x''') = f_i(x'')$ при $i \in I_1$, следовательно $\forall i \in [1,n]$, если $x'_i \neq x'''_i$, $f_i(x') \neq f_i(x''')$. Таким образом, свойство правильности нарушается на сильном подграфе $I_1$ графа $G$. Получили противоречие. Теорема доказана.

Из доказательства вышеизложенной теоремы становится понятно, что для проверки правильности по определению не обязательно проверять выполнения свойства правильности на каждой паре наборов. Достаточно проверить только те наборы, которые различаются на вершинах, образующих сильные вершинные подграфы.

Логичным следствием предыдущей теоремы является следующая теорема.

**Теорема 2 (Критерий правильности).** *Пусть* $f = (f_i)$, $i \in [1, n]$, *— семейство функций, конденсация* $G_f^*$ *графа* $G_f$ *состоит из* $k$ *вершин* $I_1, I_2, \ldots, I_k$. *Тогда* $f$ *правильно тогда и только тогда, когда правильны семейства* $f_{I_j} = (f_i)$, $i \in I_j$, $j = 1, \ldots, k$.

Таким образом, с помощью вышеизложенной теоремы проверку правильности большого семейства функций можно свести к проверке семейств на сильных компонентах. Стоит заметить, что теперь для проверки правильности семейств функций на сильных компонентах фиксировать необходимо не все переменные других компонент, а только те, от которых функции компонент могут зависеть существенно. За счет этого можно добиться упрощения задачи проверки правильности. Этот результат приводит нас к задачам построения графа существенной зависимости и поиска сильных компонент в этом графе. В работе [8] описано, как эти задачи могут быть эффективно решены для семейств булевых функций, заданных в виде полинома Жегалкина.

Зададимся вопросом: можно ли задачу проверки правильности упростить еще сильнее и если да, то каким условиям должен удовлетворять граф семейства? Оказывается, можно, в том случае, если сильные компоненты графа допускают разложение на блоки.

**Определение 8.** *Блоком* графа $G$ называется подграф $B$, удовлетворяющий одному из трех условий:

1) $B$ состоит из одной изолированной вершины графа $G$

2) $B$ порождается единственным ребром, которое является перешейком в $G$

3) $B$ является максимальным двухсвязным подграфом графа $G$.

Как известно из теории графов, блоки могут пересекаться только по *шарнирам*. При этом каждая пара блоков может пересекаться только по одному шарниру.

**Определение 9.** *Шарнир* — вершина, после удаления которой из графа число компонент связности графа вырастает.

Предположим, что граф существенной зависимости семейства функций $f$ представляется в виде объединения графов $G_1$ и $G_2$, пе-

ресекающихся по одной вершине. Понятно, что $G_1$ и $G_2$ здесь — объединения нескольких блоков.

$$G = G_1 \cup G_2, G_1 = (V_1, E_1), G_2 = (V_2, E_2),$$
$$V_1 \cap V_2 = \{m\}, V_1 = \{1, 2, \ldots, m\}, V_2 = \{m, \ldots, n\}.$$

Докажем следующее утверждение.

**Утверждение 1.** *Семейство функций* $f = (f_1, f_2, \ldots, f_n)$ *правильно тогда и только тогда, когда правильны семейства* $f^1 = (f_1, f_2, \ldots, f_m)$ *и* $f^2 = (f_m, \ldots, f_n)$.

**Доказательство.** Необходимость очевидна. Докажем достаточность. Пусть $f^1$ и $f^2$ правильные. Предположим, что семейство $f$ не является правильным. Тогда $\exists (x'_1, \ldots, x'_n) = x' \neq x'' = (x''_1, \ldots, x''_n)$: если $x'_\alpha \neq x''_\alpha$, то $f_\alpha(x') \neq f_\alpha(x'')$ . Обозначим $I = \{\alpha : x'_\alpha \neq x''_\alpha\}$

1) $I \subseteq [1, m]$ — противоречие с правильностью $f^1$

2) $I \subseteq [m, n]$ — противоречие с правильностью $f^2$

3) $I \subseteq [1, m-1] \cup [m+1, n]$ Рассмотрим наборы $x'$ и $x''' = (x'_1, \ldots, x'_m, x''_{m+1}, \ldots, x''_n)$. Тогда $f_i(x''') = f_i(x')$ при $i \in [1, \ldots, m-1]$ так как эти функции не зависят существенно от переменных $x_{m+1}, \ldots, x_n$. Рассмотрим множество $J = \{\alpha : x''_\alpha \neq x'''_\alpha\}$. Очевидно, что $J \subseteq [1, m-1], J \subseteq I$. Тогда при $\alpha \in J, f_\alpha(x') \neq f_\alpha(x'') = f_\alpha(x''')$. Получим противоречие с правильностью $f^1$.

4) $I \nsubseteq [1, m], I \nsubseteq [m, n], m \in I$. Рассмотрим следующие наборы:

$$x'$$
$$x''' = (x'_1, \ldots, x'_{m-1}, x'_m, x''_{m+1}, \ldots, x''_n)$$
$$x'''' = (x'_1, \ldots, x'_{m-1}, x''_m, x''_{m+1}, \ldots, x''_n)$$
$$x''$$

Так как $f^1$ — правильное, $f_m(x''') = f_m(x'''')$. Пусть $x'_\alpha \neq x''_\alpha$. Рассмотрим варианты:

а) $\alpha < m$. $f_\alpha(x''') = f_\alpha(x') \neq f_\alpha(x'')$

б) $\alpha > m$. $f_\alpha(x'''') = f_\alpha(x'') \neq f_\alpha(x')$

в) $\alpha = m$. В этом случае справедливо одно из двух: либо $f_m(x'''') = f_m(x''') \neq f_m(x')$, либо $f_m(x'''') = f_m(x''') \neq f_m(x'')$. В первом случае получаем противоречие с правильностью $f^2$. Во втором — противоречие с правильностью $f^1$.

Утверждение доказано.

Прямым следствием доказанного утверждения и предыдущих результатов является следующая теорема.

**Теорема 3.** *Пусть граф $G$ семейства $f$ состоит из $k$ сильных компонент $I_1, I_2, \ldots, I_k$, каждая из которых допускает разложение на $b_1, b_2, \ldots, b_k$ блоков соответственно ($B_{i1} \cup B_{i2} \cup \ldots \cup B_{ib_i} = I_i$). Тогда $f$ правильно $\Leftrightarrow$ $f_{B_{ij}}$ правильно $\forall i, j$.*

Действительно, если мы будем последовательно раскладывать каждую сильную компоненту нашего графа на 2 части, пересекающихся по одной вершине, то в итоге мы получим разложение всех сильных компонент на блоки. Таким образом, мы свели проверку семейства на правильность к проверке на правильность семейств функций на блоках сильных компонент графа семейства.

Этот результат позволяет существенно упростить проверку правильности в случае с большим количеством сильных компонент и/или в случае, если компоненты распадаются на большое количество блоков.

Теперь рассмотрим случай, когда граф семейства имеет определенные «тривиальные» участки, и посмотрим, как можно упростить проверку на правильность в этом случае.

**Определение 10.** *Маршрутом* в ориентированном графе называется чередующаяся последовательность вершин и дуг $v_0, e_1, v_1, \ldots, e_n, v_n$, в которой каждая дуга $e_i$ есть $(v_{i-1}, v_i)$.

**Определение 11.** *Путем* в ориентированном графе называется маршрут, в котором все вершины различны.

**Определение 12.** *Полустепенью исхода $d^-(v)$ (захода $d^+(v)$)* вершины $v$ называется число вершин, смежных из $v$(к $v$).

Итак, мы предположим, что в графе семейства существует путь $i_0, (i_0, i_1), i_1, (i_1, i_2), i_2, \ldots, i_m, (i_m, i_{m+1}), i_{m+1}$ такой, что $d^+(i_j) = d^-(i_j) = 1\ \forall j \in \overline{1, m}$ $(*)$. Тогда каждая из функций $f_1, \ldots, f_m$ зависит существенно только от одной переменной, а функции $f_0, f_{m+1}, \ldots, f_n$ не зависят существенно от переменных $x_1, \ldots, x_{m-1}$. Поэтому можно ввести следующие обозначения:

$$f'_0(x_0, x_{m+1}, \ldots, x_n) = f_0(x_0, x_1, \ldots, x_n),$$

$$f_1'(x_0) = f_1(x_0, x_1, \dots, x_n),$$
$$\dots$$
$$f_m'(x_{m-1}) = f_m(x_0, x_1, \dots, x_n),$$
$$f_{m+1}'(x_0, x_m, x_{m+1}, \dots, x_n) = f_{m+1}(x_0, x_1, \dots, x_n),$$
$$f_{m+2}'(x_0, x_{m+1}, \dots, x_n) = f_{m+2}(x_0, x_1, \dots, x_n),$$
$$f_n'(x_0, x_{m+1}, \dots, x_n) = f_n(x_0, x_1, \dots, x_n).$$

Докажем следующее утверждение (без ограничения общности будем считать, что $i_0 = 0, i_1 = 1, \dots, i_{m+1} = m+1$).

**Утверждение 2.** *Семейство $f = (f_0, \dots, f_n)$ со свойством $(*)$ правильно тогда и только тогда, когда правильно следующее семейство*

$$g = (g_0, g_m, g_{m+1}, \dots, g_n), \text{ где}$$
$$g_0(x_0, x_m, \dots, x_n) = f_0(x_0, x_1, \dots, x_n) = f_0'(x_0, x_{m+1}, \dots, x_n),$$
$$g_m(x_0, x_m, \dots, x_n) = f_1(x_0, x_1, \dots, x_n) = f_1'(x_0),$$
$$g_{m+1}(x_0, x_m, \dots, x_n) = f_{m+1}(x_0, x_1, \dots, x_n) = f_{m+1}'(x_0, x_m, \dots, x_n),$$
$$g_{m+2}(x_0, x_m, \dots, x_n) = f_{m+2}(x_0, x_1, \dots, x_n) = f_{m+2}'(x_0, x_{m+1}, \dots, x_n),$$
$$\vdots$$
$$g_n(x_0, x_m, \dots, x_n) = f_n(x_0, x_1, \dots, x_n) = f_n'(x_0, x_{m+1}, \dots, x_n).$$

**Доказательство.** Необходимость. Пусть $f$ правильно. Докажем, что тогда и $g$ правильно. Предположим, что это не так, то есть $g$ не является правильным. Функции семейства $g$ зависят от переменных $x_0, x_m, x_{m+1}, \dots, x_n$. Рассмотрим пару наборов $x' = (x_0', x_m' \dots, x_n') \neq (x_0'', x_m'', \dots, x_n'') = x''$, на котором нарушается свойство правильности. Пусть $I = \{i \in \{0, m, m+1, \dots, n\} : x_i' \neq x_i''\}$. Рассмотрим наборы $y' = (x_0', x_1', \dots, x_n')$ и $y'' = (x_0'', x_1'', \dots, x_n'')$, которые являются дополненными наборами $x'$ и $x''$. По определению семейства $g$, $\forall i \in \{0, m+1, \dots, n\}$ выполняются $g_i(x') = f_i(y')$ и $g_i(x'') = f_i(y'')$. Следовательно, $\forall i \in I \cap \{0, m+1, \dots, n\}$ выполняется $f_i(y') \neq f_i(y'')$. Тогда остается рассмотреть 2 случая:

а) $m \notin I$. Выбираем $x_1' = x_2' = \dots = x_{m-1}' = x_1'' = x_2'' = \dots = x_{m-1}'' = 0$. Тогда $f$ не являются правильным семейством.

б) $m \in I$. Тогда $x_m' \neq x_m''$, $g_m(x') \neq g_m(x'')$, следовательно, $f_1'(x_0') \neq f'(x_0'')$ и $x_0' \neq x_0''$. Выберем наборы $y'$ и $y''$ таким образом, чтобы выполнялись следующие неравенства:

$$f'_2(x'_1) \neq f'_2(x''_1),$$
$$f'_3(x'_2) \neq f'_3(x''_2),$$
$$\dots$$
$$f'_m(x'_{m-1}) \neq f'_m(x''_{m-1}).$$

Понятно, что такие наборы всегда можно найти. Следовательно, $\forall i \in [1, m], f_i(y') \neq f_i(y'')$. Выше мы уже показали, что $\forall i \in I \cap \{0, m+1, \dots, n\}$, $f_i(y') \neq f_i(y'')$. Таким образом, мы доказали, что $f$ не является правильным. Противоречие. Необходимость доказана.

Достаточность. Предположим, что $g$ — правильное семейство. Докажем, что $f$ также правильно. Пусть это не так, то есть $f$ не является правильным. Пусть это свойство нарушается на паре наборов $x' = (x'_0, x'_1, \dots, x'_n) \neq (x''_0, x''_1, \dots, x''_n) = x''$. Обозначим $y' = (x'_0, x'_m, \dots, x'_n)$, $y'' = (x''_0, x''_m, \dots, x''_n)$. Как уже было сказано выше (в других обозначениях), $\forall i \in \{0, m+1, \dots, n\} g_i(y') = f_i(x'), g_i(y'') = f_i(x'')$. Пусть $I = \{i : x'_i \neq x''_i\}$. Тогда $\forall i \in I \cap \{0, m+1, \dots, n\}$ $g_i(y') \neq g_i(y'')$, так как $f_i(x') \neq f_i(x'')$.

а) $I \cap \{1, \dots, m\} = \varnothing$. Тогда получаем, что $g$ не является правильным семейством. Противоречие.

б) $I \cap \{1, \dots, m\} \neq \varnothing$ Достаточно доказать, что $g_m(y') \neq g_m(y'')$. Предположим что $l \in I \cap \{1, \dots, m\}$. Тогда $f_l(x') \neq f_l(x'')$ и, так как $f_l$ зависит существенно только от $x_{l-1}$, $x'_{l-1} \neq x''_{l-1}$. Поэтому $f_{l-1}(x') \neq f_{l-1}(x'')$, $x'_{l-2} \neq x'_{l-2}$ и т. д. В итоге получаем, что $x'_0 \neq x''_0, f_1(x') \neq f_1(x'')$. Поскольку $g_m(y') = f'_1(x'_0) = f_1(x')$, $g_m(y'') = f'_1(x''_0) = f_1(x'')$, $g_m(y') \neq g_m(y'')$. Таким образом, получаем противоречие с правильностью семейства $g$. Достаточность доказана.

Утверждение доказано.

Таким образом, если в графе семейства существует путь со свойством $(*)$, то такое семейство можно редуцировать с сохранением правильности. Точно так же это семейство можно увеличивать, добавляя новые вершины в цепочку.

## Заключение

В данной работе основное внимание было уделено графическим характеристикам графов семейств и тому, как их можно использо-

вать для проверки правильности. Показано, что в случае, когда граф допускает разложение на сильные компоненты и, в дальнейшем, на блоки, проверка правильности сводится к проверке правильности семейств, возникающих на этих компонентах и блоках компонент. Также решается задача упрощения правильного семейства в случае, если граф семейства содержит некоторый «тривиальный» путь — в этом случае все внутренние точки пути можно заменить на одну. При этом изменении семейства и его графа функция, соответствующая новой точке, наследует функцию одной из точек графа, и свойство правильности семейства не меняется.

Автор выражает благодарность Носову В. А. за научное руководство и постановку задачи.

## Список литературы

[1] Носов В. А. Критерий регулярности булевского неавтономного автомата с разделенным входом // Интеллектуальные системы. — 1998. Т. 3, вып. 3–4. — С. 269–280.

[2] Носов В. А. О построении классов латинских квадратов в булевой базе данных // Интеллектуальные системы. — 1999. Т. 4, вып. 3–4. — С. 307–320.

[3] Носов В. А. Построение параметрического семейства латинских квадратов в векторной базе данных // Интеллектуальные системы. — 2004. Т. 8, вып. 1–4. — С. 517–528.

[4] Носов В. А., Панкратьев А. Е. О функциональном задании латинских квадратов // Интеллектуальные системы. — 2008. Т. 12, вып. 1–4. — С. 317–332.

[5] Харари Ф. Теория графов. — М.: Мир, 1973.

[6] Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2003.

[7] Shannon C. Communication Theory of Secrecy Systems // Bell System Techn. — 1949. J. 28, N 4. — P. 656–715.

[8] Рыков Д. О. Об алгоритмах проверки правильности // Интеллектуальные системы. — 2010. Т. 14, вып. 1–4. — С. 261–276.