Об одном критерии правильности семейства функций

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

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

К. Д. ЦАРЕГОРОДЦЕВ
АО «НПК „Криптонит“»
e-mail: kirill94_12@mail.ru

УДК 519.716.32

Ключевые слова: правильные семейства функций, булевы сети, наследственно единственная неподвижная точка, изометрия, стабилизатор.

Аннотация

Правильные семейства функций являются удобным средством для задания больших параметрических классов квазигрупп и n-квазигрупп. К. Д. Царегородцевым было замечено, что в булевом случае критериальным свойством правильности семейства является существование и единственность неподвижной точки у каждого из отображений, задаваемых самим семейством и каждым его подсемейством. В работе рассматривается обобщение результата на случай логик произвольной значности. Показывается, что композиции возникающих в критерии преобразований-перекодировок и согласованных перенумераций функций и переменных образуют стабилизатор множества правильных семейств заданного размера.

Abstract

A. V. Galatenko, A. E. Pankratiev, K. D. Tsaregorodtsev, A criterion of properness for a family of functions, Fundamentalnaya i prikladnaya matematika, vol. 24 (2023), no. 4, pp. 61—73.

Proper families of functions are a convenient apparatus for specification of large parametric classes of quasigroups and n-quasigroups. K. D. Tsaregorodtsev noticed that in the Boolean case a family is proper if and only if every mapping specified by the family or any of its subfamilies has a unique fixed point. We extend this result to the case of k-valued logics for $k > 2$. We also show that reencoding transformations used in the extended criterion enriched (in terms of composition) with consistent renumbering of variables and functions form the stabilizer of the set of all proper families of the given size.

Фундаментальная и прикладная математика, 2023, том 24, № 4, с. 61—73.

Памяти Александра Васильевича Михалёва

1. Введение

В последние годы растёт интерес к построению различных криптографических примитивов (симметричных и асимметричных шифров, хеш-функций, алгоритмов электронной подписи) на основе конечных квазигрупп (см., например, обзоры [2,8,20]). В ряде разработок авторы используют квазигруппы большого порядка. Так, алгоритм NaSHA [15], участвовавший в конкурсе NIST по выбору стандарта хеширования, основывается на квазигруппах порядка 2^{64}. На практике табличное задание таких квазигрупп невозможно из-за ограничений на память. Возможным выходом из положения представляется переход к функциональному (формульному) заданию квазигруппы. В NaSHA использован подход, основанный на полных отображениях (полных перестановках, перестановках с полным дифференциалом). Пусть $(G,+)$ — конечная абелева группа, σ — перестановка на G, такая что $\sigma(x)-x$ также является перестановкой, $f(x,y)=\sigma(x-y)+y$. Тогда (G,f) — квазигруппа [19]. Авторы алгоритма NaSHA строили полные отображения с помощью вложенных расширенных сетей Фейстеля (подробное описание подхода приведено в [14]). Построение полных отображений на основе обобщённых регистров сдвига с обратной связью предложено в [7].

Правильные семейства функций, введённые В. А. Носовым в [4], являются ещё одной конструкцией для эффективного по памяти задания больших параметрических семейств квазигрупп (см., например, [1,11]). Оказалось, что в булевом случае свойство правильности можно эквивалентным образом описать в терминах других математических моделей. Так, К. Д. Царегородцев заметил, что правильные семейства функций находятся в биективном соответствии с одностоковыми ориентациями булева куба [5]. Ниже будет показано, что семейство является правильным тогда и только тогда, когда оно задаёт булеву сеть с наследственно единственной неподвижной точкой (описание модели и большое количество интересных свойств приведено в [16—18]). Однако при переходе от булева случая к случаю k-значной логики при $k>2$ эквивалентность нарушается: не ясно, как переносить определение одностоковости на случай k-значных кубов, легко строятся примеры k-значных сетей с наследственно единственной неподвижной точкой, не обладающих свойством правильности. В работе доказывается, что критериальным свойством правильности при $k>2$ является наличие наследственно единственной неподвижной точки у самого семейства и всех его перекодировок, порождённых применением биективных преобразований к значениям переменных и значениям функций (теорема 2). Интересно, что перекодировки, обогащённые согласованной перенумерацией переменных и функций (в смысле взятия композиции), являются стабилизатором множества правильных семейств (теорема 3).

Дальнейшее изложение имеет следующую структуру. Раздел 2 содержит основные определения. В разделе 3 формулируется и доказывается критерий правильности семейства в терминах неподвижных точек. Раздел 4 посвящён стабилизатору множества правильных семейств. Наконец, раздел 5 является заключением.

Некоторые из результатов, представленных в данной работе, получены в рамках совместного российско-индийского исследовательского проекта, выполнявшегося под руководством профессора В. А. Артамонова. Ведущим экспертом и научным консультантом проекта являлся профессор А. В. Михалёв.

2. Основные определения

Пусть $k \in \mathbb{N}$, $m \in \mathbb{N} \cup \{0\}$. Обозначим множество $\{0, 1, \ldots, k-1\}$ через E_k, множество всех функций из E_k^m в E_k через P_k^m.

Определение 1. Семейство функций $(f_1, \ldots, f_n)$, $f_i \in P_k^n$, $i = 1, \ldots, n$, $k, n \in \mathbb{N}$, $k \geqslant 2$, называется правильным, если для любых $\alpha, \beta \in E_k^n$, $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$, $\alpha \neq \beta$, найдётся индекс i, такой что $\alpha_i \neq \beta_i$, но $f_i(\alpha) = f_i(\beta)$.

Замечание 1. Из определения очевидным образом следует, что каждая функция правильного семейства фиктивно зависит от одноимённой переменной, т. е. для любого набора $\alpha \in E_k^n$ и любого $a \in E_k$ выполнены равенства $f_i(\alpha) = f_i(\alpha_1, \ldots, \alpha_{i-1}, a, \alpha_{i+1}, \ldots, \alpha_n)$, $i = 1, \ldots, n$.

Примерами правильных семейств являются семейства из констант, а также треугольные семейства, т. е. семейства, в которых f_i фиктивно зависит от переменных $x_i, \ldots, x_n$. Правильность в этих случаях непосредственным образом вытекает из определения. Другие примеры правильных семейств можно найти в [12].

Замечание 2. Правильное семейство $F = (f_1, \ldots, f_n)$, $f_1, \ldots, f_n \in P_k^n$, не может принимать «противоположные» значения (т. е. значения $\alpha, \beta \in E_k^n$ со свойством $\alpha_i \neq \beta_i$, $1 \leqslant i \leqslant n$). В противном случае на соответствующих этим значениям прообразах нарушается свойство правильности.

Определение 2. Булевой сетью размера n, $n \in \mathbb{N}$, называется произвольное семейство функций $(f_1, \ldots, f_n)$, $f_i \in P_2^n$, $i = 1, \ldots, n$.

Булева сеть F размера n естественным образом определяет отображение из E_2^n в E_2^n. Для обозначения этого отображения мы также будем использовать символ F.

Определение 3. Пусть $n, n' \in \mathbb{N}$, $n' < n$, $t = n - n'$, $F = (f_1, \ldots, f_n)$ и $F' = (f'_1, \ldots, f'_{n'})$ — булевы сети, такие что F' получается из F с помощью некоторой фиксации переменных $x_{i_1} = a_1, \ldots, x_{i_t} = a_t$ и исключения функций с номерами $i_1, \ldots, i_t$. Тогда F' называется подсетью булевой сети F.

Определение 4. Булева сеть F имеет наследственно единственную неподвижную точку, если отображение, определяемое сетью F, имеет единственную

неподвижную точку, и для любой сети F', являющейся подсетью сети F, соответствующее отображение также имеет единственную неподвижную точку.

Легко увидеть, что если булева сеть $F = (f_1, \ldots, f_n)$ имеет наследственно единственную неподвижную точку, то зависимость функций f_i от одноимённых переменных фиктивная.

Замечание 3. Понятия сети, подсети и сети с наследственно единственной неподвижной точкой могут быть естественным образом перенесены на случай логики произвольной значности k. Если значность логики больше 2, появляются сети с наследственно единственной неподвижной точкой, в которых функции существенным образом зависят от одноимённых переменных. В качестве очевидного примера можно рассмотреть сеть $F = (f_1)$, в которой $f_1(0) = 0$ и $f_1(x) = x + 1 \pmod k$ при $x \neq 0$.

В дальнейшем для удобства мы будем отождествлять понятия семейства функций и сети, а также подсемейства и подсети.

Определение 5. Пусть $F = (f_1, \ldots, f_n)$ — булева сеть. Наборы $\alpha, \beta \in E_2^n$, $\alpha \neq \beta$, называются зеркальной парой для сети F, если выполнено равенство $F(\alpha) \oplus \alpha = F(\beta) \oplus \beta$, где символ $\oplus$ обозначает покомпонентное сложение по модулю 2.

Теорема 1 [18, предложение 3.1]. *Булева сеть имеет наследственно единственную неподвижную точку тогда и только тогда, когда для неё не существует зеркальных пар.*

Несложно увидеть, что наличие зеркальной пары в точности означает нарушение условия правильности из определения 1. Таким образом, верен следующий факт.

Следствие 1. *Семейство булевых функций $F = (f_1, \ldots, f_n)$ является правильным тогда и только тогда, когда F является булевой сетью с наследственно единственной неподвижной точкой.*

Из лемм 1 и 3 и теоремы 7 работы [11] следует, что в случае логики произвольной значности правильные семейства имеют наследственно единственную неподвижную точку. Однако из замечаний 1 и 3 вытекает, что при $k > 2$ существуют сети с наследственно единственной неподвижной точкой, не являющиеся правильными семействами. Для характеризации правильности в терминах неподвижных точек введём понятие перекодировки семейства.

Определение 6. Пусть $k, n \in \mathbb{N}$, $k \geqslant 2$, $\phi_i \in \mathcal{S}_{E_k}$ — подстановки на множестве E_k. Перекодировкой вектора $x \in E_k^n$ будем называть вектор $y \in E_k^n$ вида $y = \big(\phi_1(x_1), \ldots, \phi_n(x_n)\big)$.

Определение 7. Пусть $k, n \in \mathbb{N}$, $k \geqslant 2$, $f_1, \ldots, f_n \in P_k^n$, $\sigma_1, \ldots, \sigma_n$, $\tau_1, \ldots, \tau_n$ — подстановки на множестве E_k. Семейство $(f_1', \ldots, f_n')$, где

$$f_i'(x_1, \ldots, x_n) = \tau_i\big(f_i\big(\sigma_1(x_1), \ldots, \sigma_n(x_n)\big)\big),$$

называется перекодировкой семейства $(f_1, \ldots, f_n)$.

Замечание 4. Перекодировка семейства является композицией перекодировки аргумента функции и перекодировки полученного вектора значения функции.

Также нам понадобится ещё одно преобразование семейств.

Определение 8. Для подстановки $\sigma \in \mathcal{S}_n$ и элемента $x \in E_k^n$ мы можем рассмотреть преобразование перенумерации

$$x \to \sigma(x) = \left(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}\right),$$

которое переводит компоненту x_i вектора x на место компоненты $x_{\sigma(i)}$.

Введём понятие (согласованной) перенумерации семейства.

Определение 9. Пусть $k, n \in \mathbb{N}$, $k \geqslant 2$, $F = (f_1, \ldots, f_n)$, $f_1, \ldots, f_n \in P_k^n$, $\sigma, \tau \in \mathcal{S}_n$. Рассмотрим семейство $(\sigma, \tau)(F)$, которое получено из семейства F с помощью перестановки индексов переменных и индексов входящих в семейство функций:

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

т. е. функция (переменная) с номером i переходит на место функции (переменной) с номером $\sigma(i)$ ($\tau(i)$). Преобразование $F \to (\sigma, \tau)(F)$ будем называть перенумерацией семейства.

Определение 10. Пусть $k, n \in \mathbb{N}$, $k \geqslant 2$, $F = (f_1, \ldots, f_n)$, $f_1, \ldots, f_n \in P_k^n$, $\sigma, \in \mathcal{S}_n$. Согласованной перенумерацией семейства F будем называть преобразование $F \to \sigma(F) = (\sigma, \sigma)(F)$.

3. Критерий правильности в терминах неподвижных точек

Теорема 2. *Пусть $k, n \in \mathbb{N}$, $k \geqslant 2$, $f_1, \ldots, f_n \in P_k^n$. Семейство $(f_1, \ldots, f_n)$ является правильным тогда и только тогда, когда любая его перекодировка имеет наследственно единственную неподвижную точку.*

Для доказательства теоремы нам потребуется ряд вспомогательных утверждений.

Лемма 1 [11, лемма 1]. *Пусть $(f_1, \ldots, f_n)$ — правильное семейство, $a \in E_k$. Тогда семейство $(f'_1, \ldots, f'_{n-1})$, где $f'_i(x_1, \ldots, x_{n-1}) = f_i(x_1, \ldots, x_{n-1}, a)$, $i = 1, \ldots, n-1$, также правильное.*

Лемма 2 [11, лемма 3]. *Пусть $F = (f_1, \ldots, f_n)$ — правильное семейство, δ — подстановка на множестве $\{1, \ldots, n\}$. Тогда семейство $\delta(F)$, полученное из F согласованной перенумерацией, также является правильным.*

Порождение произвольного подсемейства может быть сведено к согласованной перенумерации, в результате которой фиксируемые переменные станут

последними, и последующей фиксацией этих переменных. Таким образом, из лемм 1 и 2 вытекает следующее утверждение.

Следствие 2. *Все подсемейства правильного семейства являются правильными.*

Лемма 3 [11, теорема 7]. *Пусть F — правильное семейство. Тогда отображение F имеет единственную неподвижную точку.*

Лемма 4. *Пусть $F = (f_1, \ldots, f_n)$ — правильное семейство функций k-значной логики, $F' = (f'_1, \ldots, f'_n)$ — перекодировка семейства F с помощью перестановок $\sigma_1, \ldots, \sigma_n$, $\tau_1, \ldots, \tau_n$. Тогда семейство F' также является правильным.*

Доказательство. Установим правильность семейства F'. Пусть $\alpha', \beta' \in E_k^n$, $\alpha' = (\alpha'_1, \ldots, \alpha'_n)$, $\beta' = (\beta'_1, \ldots, \beta'_n)$, $\alpha' \neq \beta'$. Положим $\alpha_i = \sigma_i(\alpha'_i)$, $\beta_i = \sigma_i(\beta'_i)$, $i = 1, \ldots, n$, и рассмотрим наборы $\alpha = (\alpha_1, \ldots, \alpha_n)$ и $\beta = (\beta_1, \ldots, \beta_n)$. Так как σ_i являются перестановками, компоненты наборов α' и β' отличаются тогда и только тогда, когда отличаются соответствующие компоненты наборов α и β. В частности, $\alpha \neq \beta$. В силу правильности семейства F найдётся индекс i, такой что $\alpha_i \neq \beta_i$, но $f_i(\alpha) = f_i(\beta)$ и, следовательно, $\tau_i\big(f_i(\alpha)\big) = \tau_i\big(f_i(\beta)\big)$. Так как

$$\tau_i\big(f_i(\alpha)\big) = \tau_i\big(f_i(\alpha_1, \ldots, \alpha_n)\big) = \tau_i\big(f_i\big(\sigma_1(\alpha'_1), \ldots, \sigma_n(\alpha'_n)\big)\big) = f'_i(\alpha'),$$
$$\tau_i\big(f_i(\beta)\big) = \tau_i\big(f_i(\beta_1, \ldots, \beta_n)\big) = \tau_i\big(f_i\big(\sigma_1(\beta'_1), \ldots, \sigma_n(\beta'_n)\big)\big) = f'_i(\beta'),$$

семейство F' является правильным по определению. □

Из доказанных утверждений, в частности, следует, что семейство F правильное тогда и только тогда, когда семейство, полученное применением произвольной композиции перекодировки и согласованной перенумерации к F, является правильным.

Доказательство теоремы 2. Пусть семейство F является правильным. Тогда по лемме 4 все его перекодировки также являются правильными. По следствию 2 правильными являются и всевозможные подсемейства. По лемме 3 каждое из них имеет единственную неподвижную точку.

Пусть семейство $F = (f_1, \ldots, f_n)$, где $f_1, \ldots, f_n \in P_k^n$, не является правильным. По определению существуют наборы $\alpha, \beta \in E_k^n$, $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$, $\alpha \neq \beta$, такие что для любого индекса i, для которого $\alpha_i \neq \beta_i$, выполнено $f_i(\alpha) \neq f_i(\beta)$. Обозначим через F' семейство, полученное из F фиксацией $x_i = \alpha_i$ для всех индексов, на которых $\alpha_i = \beta_i$. Пусть $F' = (f'_1, \ldots, f'_{n'})$, а наборы α' и β' получены из α и β выбрасыванием совпадающих компонент. Рассмотрим следующую перекодировку $F'' = (f''_1, \ldots, f''_{n'})$ семейства F'. Перестановки $\sigma_1, \ldots, \sigma_{n'}$ являются тождественными; $\tau_i\big(f'_i(\alpha')\big) = \alpha'_i$, $\tau_i\big(f'_i(\beta')\big) = \beta'_i$, значения τ_i на остальных входах выбираются произвольным образом (в силу неравенств $\alpha'_i \neq \beta'_i$ и $f'_i(\alpha') \neq f'_i(\beta')$ определение τ_i корректно). Выполнены следующие соотношения:

$$f''_i(\alpha') = \tau_i\left(f'_i(\alpha')\right) = \alpha'_i,$$
$$f''_i(\beta') = \tau_i\left(f'_i(\beta')\right) = \beta'_i,$$

и у семейства F'', подсемейства перекодировки F, имеется по крайней мере две неподвижные точки. □

Из доказательства теоремы 2 вытекает следующее утверждение.

Следствие 3. *Семейство $F = (f_1, \ldots, f_n)$, $f_1, \ldots, f_n \in P_k^n$, является правильным тогда и только тогда, когда для любых перестановок $\tau_1, \ldots, \tau_n$ на множестве E_k семейство $\big(\tau_1(f_1), \ldots, \tau_n(f_n)\big)$ имеет наследственно единственную неподвижную точку.*

4. Стабилизатор множества правильных семейств

Выше было показано, что согласованные перенумерации (см. лемму 2) и перекодировки (см. лемму 4) семейства сохраняют свойство семейства «быть правильным». В настоящем разделе мы рассмотрим обратную задачу. Пусть Φ, Ψ — подстановки (биекции) на множестве E_k^n: $\Phi, \Psi \in \mathcal{S}_{E_k^n}$. При каких условиях на Φ, Ψ отображение $x \to \Phi\big(F\big(\Psi(x)\big)\big)$ также будет являться правильным для правильных семейств F? Другими словами, каков стабилизатор для множества $\mathcal{F}_n$ правильных семейств размера n при действии группы $\mathcal{S}_{E_k^n} \times \mathcal{S}_{E_k^n}$ на множестве всех семейств размера n, при котором (Φ, Ψ) переводит семейство F в семейство F', заданное соотношением $F'(x) = \Phi\big(F\big(\Psi(x)\big)\big)$? Далее мы покажем, что такими Φ и Ψ могут быть только композиции согласованных перестановок и перекодировок семейства.

Заметим, что преобразования перекодировки и перестановки компонент вектора сохраняют расстояние Хэмминга между векторами, т. е. являются изометриями (см. определение 11) пространства E_k^n. Естественным образом возникает обратный вопрос: верно ли, что преобразования, сохраняющие правильность, обязаны быть изометриями пространства E_k^n? Далее мы утвердительно ответим на этот вопрос.

Определение 11. Пусть E_k^n рассматривается как метрическое пространство с метрикой Хэмминга $d(x, y) = |\{i \mid x_i \neq y_i\}|$, $x, y \in E_k^n$. Тогда группой изометрий $\mathrm{Iso}(E_k^n)$ пространства E_k^n будем называть множество отображений

$$\mathrm{Iso}(E_k^n) = \big\{\Phi \in \mathcal{S}_{E_k^n} \mid d\big(\Phi(x), \Phi(y)\big) = d(x, y) \text{ для каждых } x, y \in E_k^n\big\}$$

с операцией композиции отображений.

Нам также понадобится понятие слабой изометрии как отображения, которое сохраняет расстояние между точками, находящимися на строго определённом фиксированном расстоянии.

Определение 12. Будем называть p-изометрией (слабой изометрией) биективное отображение $\Phi\colon E_k^n \to E_k^n$, сохраняющее расстояние между точками, которые находятся на расстоянии p:

$$\big\{\Phi \in \mathcal{S}_{E_k^n} \mid d\big(\Phi(x), \Phi(y)\big) = d(x, y) \text{ для каждых } x, y \in E_k^n,\ d(x, y) = p\big\}.$$

Замечание 5. Легко увидеть, что p-изометрии образуют группу (в частности, обратное к p-изометрии преобразование также является p-изометрией).

Приведём два результата, связывающих множество слабых изометрий и изометрий пространств с метрикой Хэмминга.

Лемма 5 [3, теорема 1; 10, лемма 1]. *Если* Φ *является* 1*-изометрией* E_2^n*, то* Φ *является изометрией* E_2^n*.*

Лемма 6 [6, теорема 4.1]. *Если* Φ *является* 1*-изометрией* E_k^n*,* $k > 2$*,* $n > 2$*, то* Φ *является изометрией* E_k^n*.*

Замечание 6. Из формулировок лемм 5 и 6 видно, что существуют особые случаи, не покрываемые приведёнными выше утверждениями. Рассмотрим каждый из них более подробно.

Случай $k > 2$, $n = 1$ тривиален: любая биекция в указанном вырожденном случае является изометрией.

Случай $k > 2$, $n = 2$: пусть Φ является 1-изометрией и биекцией. Покажем, что Φ также сохраняет расстояние 2. Пусть $\alpha, \beta \in E_k^2$, $d(\alpha, \beta) = 2$. В силу биективности $d\big(\Phi(\alpha), \Phi(\beta)\big) > 0$. Предположим, что $d\big(\Phi(\alpha), \Phi(\beta)\big) = 1$. В таком случае, поскольку Φ^{-1} также является 1-изометрией (см. замечание 5), мы имеем противоречие:

$$1 = d\big(\Phi(\alpha), \Phi(\beta)\big) = d\big(\Phi^{-1}\big(\Phi(\alpha)\big), \Phi^{-1}\big(\Phi(\beta)\big)\big) = d(\alpha, \beta) = 2.$$

Других значений расстояния в случае $n = 2$ не бывает.

Таким образом, мы доказали следующее вспомогательное утверждение.

Лемма 7. *Группа* 1*-изометрий для пространства* E_k^n *с метрикой Хэмминга совпадает с группой всех изометрий.*

Также для пространств Хэмминга верно следующее утверждение, устанавливающее связь между изометриями E_k^n и ранее введёнными преобразованиями векторов (см. определения 6 и 8).

Лемма 8 [9]. *Группа изометрий* $\mathrm{Iso}(E_k^n)$ *состоит из перенумераций и перекодировок векторов.*

Нашей задачей является доказательство того факта, что если Φ и Ψ — биекции и $\Phi\big(F\big(\psi(x)\big)\big)$ — правильное семейство для любого правильного семейства F, то Φ, Ψ являются изометриями пространства $\mathrm{Iso}(E_k^n)$. Для этого мы сначала докажем, что Φ и Ψ должны быть 1-изометриями (леммы 10 и 11). Тогда из леммы 7 будет следовать, что Φ и Ψ являются изометриями E_k^n. Наконец, мы применим лемму 8 совместно с некоторыми дополнительными соображениями и покажем, что биективные преобразования, сохраняющие правильность семейств, исчерпываются композициями перекодировок и согласованных перенумераций семейства (теорема 3).

Замечание 7. Мы рассматриваем только пары биективных преобразований заданного вида. В [13] введён класс преобразований, сохраняющих правильность и сводящихся к замене одной из функций правильного семейства на

другую, т. е. выбирается индекс i, $1 \leqslant i \leqslant n$, затем $f_i(x_1, \ldots, x_n)$ меняется на некоторую $f_i'(x_1, \ldots, x_n)$. С помощью последовательности таких преобразований можно перейти от произвольного правильного семейства размера n к любому другому правильному семейству размера n [13, следствие 3]. Преобразования из [13], вообще говоря, не представимы в виде $\Phi\big(F\big(\Psi(x)\big)\big)$ и поэтому не рассматриваются в нашей работе.

Как уже было отмечено ранее (см. замечание 2), правильное семейство не может принимать противоположные значения. Однако верно следующее утверждение.

Лемма 9. *Пусть $\alpha, \beta \in E_k^n$ — два непротивоположных набора (т. е. $d(\alpha, \beta) < n$). Тогда существует правильное семейство F и точки $x, y \in E_k^n$, такие что $F(x) = \alpha$, $F(y) = \beta$.*

Доказательство. Достаточно рассмотреть правильным образом подобранное треугольное семейство. Без ограничения общности будем предполагать, что первые w координат наборов совпадают $\alpha_1 = \beta_1, \ldots, \alpha_w = \beta_w$, $1 \leqslant w < n$. В таком случае зададим первые w функций треугольного семейства как константы $f_i \equiv \alpha_i$; оставшиеся $n - w$ функций зададим так, чтобы на некотором фиксированном x_0 они принимали значение $\alpha_{w+1}, \ldots, \alpha_n$, а на некотором фиксированном y_0 (отличном от x_0 в первых w координатах) — значение $\beta_{w+1}, \ldots, \beta_n$. Тогда мы получим семейство вида

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_w \\ F_{n-w}(x_1, \ldots, x_w) \end{bmatrix},$$

которое является треугольным и обладает требуемым свойством. □

Лемма 10. *Пусть семейства $G(x)$ вида $G(x) = \Phi\big(F\big(\Psi(x)\big)\big)$ являются правильным для всех правильных семейств F, заданных на E_k^n, Φ и Ψ — биекции множества E_k^n. Тогда Ψ является 1-изометрией пространства Хэмминга E_k^n.*

Доказательство. Докажем от противного. Предположим, что Ψ не является 1-изометрией, Φ и Ψ биективны, и покажем, что существует такое правильное семейство F на E_k^n, что $G(x) = \Phi\big(F\big(\Psi(x)\big)\big)$ не является правильным.

Так как Ψ не 1-изометрия, то найдутся наборы $x_1, x_2 \in E_k^n$, что $d(x_1, x_2) = 1$, но $d\big(\Psi(x_1), \Psi(x_2)\big) > 1$ (заметим, что указанное расстояние не может быть равно 0, так как Ψ биективно). Пусть для определённости x_1 и x_2 различны только в i-й координате и найдутся такие индексы j_1, j_2, что $\Psi(x_1)$ и $\Psi(x_2)$ различны в позициях j_1 и j_2. Подберём такое семейство F, что выполнено неравенство

$$G_i(x_1) = \Phi\big(F\big(\Psi(x_1)\big)\big)[i] \neq \Phi\big(F\big(\Psi(x_2)\big)\big)[i] = G_i(x_2).$$

Рассмотрим множество пар точек (w_1, w_2), $w_1, w_2 \in E_k^n$, таких что $w_1[i] \neq w_2[i]$. Число таких пар точек равно $k^{2n-1}(k-1)$, поскольку есть k^n

способов зафиксировать w_1 и $k^{n-1}(k-1)$ способов зафиксировать w_2. Теперь рассмотрим множество пар точек $(y_1, y_2) = \big(\Phi^{-1}(w_1), \Phi^{-1}(w_2)\big)$. Среди таких пар найдётся пара со свойством $y_1[j_1] = y_2[j_1]$ или $y_1[j_2] = y_2[j_2]$, поскольку число пар, не удовлетворяющих этому свойству, равно $k^{2n-2}(k-1)^2$, что меньше числа $k^{2n-1}(k-1)$. Таким образом, найдутся две точки y_1, y_2 со свойствами

— $\Phi(y_1)[i] \neq \Phi(y_2)[i]$;
— $y_1[j] = y_2[j]$, где $j \in \{j_1, j_2\}$.

Построим по этим точкам семейство F так, чтобы $F\big(\Psi(x_1)\big) = y_1$, $F\big(\Psi(x_2)\big) = y_2$.

Для этого рассмотрим треугольное семейство F, такое что $f_j(\cdot) \equiv y_1[j]$, а остальные функции зависят от j-й переменной таким образом, что если она принимает значение $\Psi(x_1)[j]$, то всё семейство равно y_1, а если она принимает значение $\Psi(x_2)[j]$, то всё семейство равно y_2. Построенное семейство F будет правильным (поскольку оно треугольное). При этом будет выполняться условие

$$\Phi\big(F\big(\Psi(x_1)\big)\big)[i] = \Phi(y_1)[i] \neq \Phi(y_2)[i] = \Phi\big(F(\Psi(x_2))\big)[i],$$

а значит, семейство $G(x)$ не является правильным (нарушено условие правильности на паре наборов x_1, x_2). □

Замечание 8. Из доказанного утверждения и леммы 7 следует, что Ψ является изометрией E_k^n.

Лемма 11. *Пусть семейства $G(x)$ вида $G(x) = \Phi\big(F\big(\Psi(x)\big)\big)$ являются правильным для всех правильных семейств F, заданных на E_k^n, Φ и Ψ — биекции множества E_k^n. Тогда Φ является 1-изометрией пространства Хэмминга E_k^n.*

Доказательство. Случай биективного отображения Ψ, не являющегося изометрией, был разобран ранее, поэтому мы можем предполагать, что Ψ — изометрия.

Предположим, что Φ не 1-изометрия. Это означает, что найдутся наборы $y_1, y_2 \in E_k^n$, такие что $d(y_1, y_2) = 1$, но $d\big(\Phi(y_1), \Phi(y_2)\big) = t > 1$ (указанное расстояние не может быть равно 0, поскольку Φ — биекция). Для определённости обозначим через j индекс, в котором y_1 и y_2 различаются: $y_1[j] \neq y_2[j]$.

Если мы предположим, что $t = n$, то по лемме 9 мы можем найти правильное семейство F, которое принимает оба значения y_1 и y_2 на некоторых x_1, x_2. Но тогда $\Phi\big(F_n\big(\Psi(x)\big)\big)$ не может быть правильным, так как принимает противоположные значения (см. замечание 2). Следовательно, мы имеем $1 < t < n$. Будем считать без ограничения общности, что $\Phi(y_1)$ и $\Phi(y_2)$ различаются в первых t индексах:

$$\Phi(y_1)[i] \neq \Phi(y_2)[i], \quad 1 \leqslant i \leqslant t.$$

Построим два набора $x_1, x_2 \in E_k^n$ и правильное семейство F так, что выполняются условия

$$F_n\big(\Psi(x_1)\big) = y_1, \quad F_n\big(\Psi(x_2)\big) = y_2,$$

при этом потребуем, чтобы

— $x_1[i] \neq x_2[i]$ при $1 \leqslant i \leqslant t$,
— $x_1[i] = x_2[i]$ при $t+1 \leqslant i \leqslant n$.

Поскольку Ψ по предположению является изометрией, то $d\big(\Psi(x_1), \Psi(x_2)\big) = t > 1$, следовательно, найдётся такой индекс $j' \neq j$, что $\Psi(x_1)[j'] \neq \Psi(x_2)[j']$. Зададим j-ю функцию семейства F следующим образом:

— $y_1[j]$, если j'-я переменная принимает значения $\Psi(x_1)[j']$,
— $y_2[j]$, если j'-я переменная принимает значения $\Psi(x_2)[j']$.

Остальные функции f_i положим равными тождественно равными $y_1[i]$, где $1 \leqslant i \leqslant n$, $i \neq j$. Полученное семейство является треугольным, а следовательно, правильным. Для семейства $G(x) = \Phi\big(F\big(\Psi(x)\big)\big)$ условие правильности нарушается на наборах x_1 и x_2. Мы предположили, что Φ не является 1-изометрией, и пришли к противоречию, из которого следует утверждение. □

Замечание 9. Из доказанного утверждения и леммы 7 следует, что Φ является изометрией E_k^n.

Теорема 3. *Пусть семейства $G(x)$ вида $G(x) = \Phi\big(F\big(\Psi(x)\big)\big)$ являются правильным для всех правильных семейств F, заданных на E_k^n, Φ и Ψ — биекции множества E_k^n. Тогда Φ и Ψ имеют вид*

$$\Phi = \sigma \circ A, \quad \Psi = \sigma \circ B,$$

где использованы следующие обозначения:

— $\sigma \in \mathcal{S}_n$ (*перенумерация координат вектора*),
— $A, B \in (\mathcal{S}_{E_k})^n$ (*перекодировки вектора*).

Доказательство. Мы уже показали (см. замечания 8 и 9), что Φ и Ψ обязаны быть изометриями пространства E_k^n. Из леммы 8 следует, что $\Phi = (\sigma_1 \circ A)$, $\Psi = (\sigma_2 \circ B)$, где $\sigma_1, \sigma_2 \in \mathcal{S}_n$, $A, B \in (\mathcal{S}_{E_k})^n$. Покажем, что в таком случае $\sigma_1 = \sigma_2$ (т. е. перенумерация семейства должна быть согласованной).

Применение покомпонентных преобразований A и B не меняет свойства правильности, поэтому можно ограничиться случаем рассмотрения $\Phi = (\sigma_1 \circ I)$, $\Psi = (\sigma_2 \circ I)$, где I — тождественное преобразование $E_k^n \to E_k^n$. Пусть $\sigma_1 \neq \sigma_2$. Тогда существуют i и j со свойством $\sigma_1(i) = \sigma_2(j) = s$, при этом $i \neq j$. В таком случае достаточно рассмотреть треугольное семейство $f_i(x_j) = x_j$, $f_l \equiv \text{const}$, $l \neq i$. Под действием $(\Phi, \Psi) \curvearrowright F$ семейство F перейдёт в семейство, включающее в себя функцию $f_{\sigma_1(i)}\big(x_{\sigma_2(j)}\big) = f_s(x_s) = x_s$, что противоречит правильности. □

5. Заключение

В работе получен критерий правильности семейства функций в терминах неподвижных точек. Показано, что семейство является правильным тогда и

только тогда, когда любая (в том числе тривиальная) перекодировка этого семейства обладает наследственно единственной неподвижной точкой. Установлено, что класс всех перекодировок, обогащённый согласованной перенумерацией переменных и функций, является стабилизатором множества правильных семейств.

Литература

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

[2] Глухов М. М. О применениях квазигрупп в криптографии // Прикладная дискретная математика. — 2008. — № 2. — С. 28—32.

[3] Красин В. Ю. О слабых изометриях булева куба // Дискретный анализ и исследование операций, сер. 1. — 2006. — Т. 13, № 4. — С. 26—32.

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

[5] Царегородцев К. Д. О взаимно однозначном соответствии между правильными семействами булевых функций и рёберными ориентациями булевых кубов // Прикладная дискретная математика. — 2020. — № 48. — С. 16—21.

[6] Bruner R., De Winter S. Weak isometries of Hamming spaces // J. Algebra Combin. Discrete Structures Appl. — 2016. — Vol. 3, no. 3. — P. 209—216.

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

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

[9] Chirivi R. The isometry group for the Hamming distance. — 2015. — `http://annualreport.dmf.unisalento.it/2015/maths/algebra/chirivi1.pdf`.

[10] De Winter S., Korb M. Weak isometries of the Boolean cube // Discrete Math. — 2016. — Vol. 339, no. 2. — P. 877—885.

[11] Galatenko A. V., Nosov V. A., Pankratiev A. E. Latin squares over quasigroups // Lobachevskii J. Math. — 2020. — Vol. 41, no. 2. — P. 194—203.

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

[13] Galatenko A. V., Pankratiev A. E., Staroverov V. M. Generation of proper families of functions // Lobachevskii J. Math. — 2022. — Vol. 43, no. 3. — P. 571—581.

[14] Markovski S., Mileva A. Generating huge quasigroups from small non-linear bijections via extended Feistel function // Quasigroups Related Systems. — 2009. — Vol. 17, no. 1. — P. 91—106.

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

[16] Richard A. Fixed point theorems for Boolean networks expressed in terms of forbidden subnetworks // Theor. Comp. Sci. — 2015. — Vol. 583. — P. 1—26.

[17] Ruet P. Geometric characterization of hereditarily bijective Boolean networks // Cellular Automata. ACRI 2014. — Cham: Springer, 2014. — (Lect. Notes Comp. Sci.; Vol. 8751). — P. 536—545.

[18] Ruet P. Local cycles and dynamical properties of Boolean networks // Math. Struct. Comp. Sci. — 2016. — Vol. 26, no. 4. — P. 702—718.

[19] Sade A. Quasigroups automorphes par le groupe cyclique // Can. J. Math. — 1957. — Vol. 9. — P. 321—335.

[20] Shcherbacov V. A. Quasigroups in cryptology // Comp. Sci. J. Moldova. — 2009. — Vol. 17, no. 2 (50). — P. 193—228.