МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2015 № 1(27)

Свидетельство о регистрации: ПИ №ФС 77-33762
от 16 октября 2008 г.

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Адрес редакции: 634050, г. Томск, пр. Ленина, 36
E-mail: vestnik_pdm@mail.tsu.ru

В журнале публикуются результаты фундаментальных и прикладных научных исследований отечественных и зарубежных ученых, включая студентов и аспирантов, в области дискретной математики и её приложений в криптографии, компьютерной безопасности, кибернетике, информатике, программировании, теории надежности, интеллектуальных системах.

Периодичность выхода журнала: 4 номера в год.

Редактор *Н. И. Шидловская*
Верстка *И. А. Панкратовой*

Подписано к печати 18.03.2015.
Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 13,6. Уч.-изд. л. 15,2. Тираж 300 экз. Заказ № 906.

Отпечатано на оборудовании
Издательского Дома Томского государственного университета
634050, г. Томск, пр. Ленина, 36
Тел.: 8(3822)53-15-28, 52-98-49

СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

ПСЕВДОСЛУЧАЙНЫЕ ГЕНЕРАТОРЫ

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

CONTENTS

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 512.579

ХАРАКТЕРИЗАЦИЯ ПОДПРЯМО НЕРАЗЛОЖИМЫХ ПОЛИГОНОВ

И. Б. Кожухов, А. Р. Халиуллина

Национальный исследовательский университет «МИЭТ», г. Москва, Россия

Исследуются подпрямо неразложимые полигоны (автоматы) над полугруппами. В 1974 г. Е. Н. Ройз было доказано, что у таких полигонов не более двух нулей. Мы характеризуем подпрямо неразложимые полигоны с двумя нулями и сводим характеризацию полигона без нуля или с одним нулём к строению его наименьшего нетривиального подполигона. Исчерпывающим образом охарактеризованы подпрямо неразложимые полигоны над прямоугольными связками. В качестве следствия получается характеризация подпрямо неразложимых полигонов над полугруппами правых нулей и результат Г. Могаддаси 2012 г. о полигонах над полугруппами левых нулей.

Ключевые слова: *полигон над полугруппой, подпрямо неразложимый полигон, прямоугольная связка.*

DOI 10.17223/20710410/27/1

A CHARACTERIZATION OF SUBDIRECTLY IRREDUCIBLE ACTS

I. B. Kozhukhov, A. R. Haliullina

National Research University of Electronic Technology, Moscow, Russia

E-mail: kozhuhov_i_b@mail.ru, haliullinaar@gmail.com

The subdirectly irreducible acts (automata) over semigroups are investigated. In 1974, E. N. Roiz proved that such acts have at most two zeros. Here, we characterize subdirectly irreducible acts with two zeros and reduce the characterization of an act with one zero or without zeros to the structure of its least non-trivial subact. We fully characterize the subdirectly irreducible acts over rectangular bands. As the corollaries we have a characterization of subdirectly irreducible acts over right zero semigroups and the Moghaddassi's result about acts over left zero semigroups.

Keywords: *act over semigroup, subdirectly irreducible act, rectangular band.*

Введение

Решётка конгруэнций $\mathrm{Con}\, A$ универсальной алгебры A — важный производный объект, содержащий существенную информацию о строении алгебры A (если мы знаем все конгруэнции алгебры A, то мы знаем также все её гомоморфные образы). *Полигон* над полугруппой S (или S-полигон) [1] — это множество X, на котором задано действие полугруппы S, т. е. определено отображение $X \times S \to X$, $(x, s) \mapsto xs$, удовлетворяющее

условию $x(st) = (xs)t$ при $x \in X$, $s, t \in S$. Понятие полигона над полугруппой является алгебраическим выражением понятия *автомата*, где X — множество состояний, а S — множество входных сигналов [2]. Кроме того, всякий полигон над полугруппой является *унарной алгеброй*, где операции — это умножение на элементы полугруппы. И наоборот, если A — унарная алгебра, то можно определить произведение унарных операций как произведение отображений, и получим, что A — полигон над полугруппой. Нетрудно видеть, что конгруэнции A как полигона и как унарной алгебры одни и те же. В ряде работ рассматривались решётки конгруэнций полигонов и унарных алгебр. В [3, 4] найдены условия, при которых решётки конгруэнций унаров (т. е. алгебр с одной унарной операцией) являются цепями, дистрибутивными или модулярными решётками.

Универсальная алгебра A называется *подпрямо неразложимой*, если она не разлагается в нетривиальное подпрямое произведение алгебр. Обозначим через Δ_X отношение равенства на множестве X, т. е. $\Delta_X = \{(x, x) : x \in X\}$. Если понятно, о каком множестве идёт речь, будем писать просто Δ. Конгруэнцию ρ будем называть *нетривиальной*, если $\rho \neq \Delta$. Очевидно, алгебра подпрямо неразложима в том и только в том случае, если пересечение любого семейства нетривиальных конгруэнций также является нетривиальной конгруэнцией; алгебра A подпрямо неразложима в том и только в том случае, если она имеет наименьшую нетривиальную конгруэнцию. Будем называть эту конгруэнцию *монолитом* и обозначать $\rho_0(A)$ (или просто ρ_0). Интерес к подпрямо неразложимым алгебрам объясняется теоремой Биркгофа, утверждающей, что всякая алгебра является подпрямым произведением подпрямо неразложимых алгебр [5, теорема II.7.3]. Таким образом, подпрямо неразложимые алгебры являются строительным материалом, из которого строятся все алгебры.

Подпрямо неразложимые коммутативные полигоны описаны в [6]. Условия конечности для подпрямо неразложимых полигонов изучались в [7]. В [8] доказано, что каждый подпрямо неразложимый полигон над полугруппой S состоит не более чем из двух элементов в том и только в том случае, если S — полурешётка (т. е. коммутативная полугруппа идемпотентов). В [9, 10] описаны конгруэнции произвольного полигона над полугруппой правых и полугруппой левых нулей, а в [11] получены необходимые и достаточные условия подпрямой неразложимости правого полигона над полугруппой левых нулей. В данной работе мы получаем характеризацию подпрямо неразложимых полигонов над произвольными полугруппами. В случае полигонов с одним нулём или без нуля вопрос об их подпрямой неразложимости сводится к вопросу о подпрямой неразложимости 0-простых и простых полигонов, а в случае полигонов с двумя нулями решается до конца. Этим исчерпываются все случаи, так как согласно предложению 1 из [12] подпрямо неразложимых полигонов более чем с двумя нулями не существует. Кроме того, используя описание всех полигонов над вполне простой полугруппой $\mathcal{M}(G, I, \Lambda, P)$, полученное в [13], мы обобщаем уже упоминавшийся результат из [12] о наличии не более двух нулей на полигоны над $\mathcal{M}(G, I, \Lambda, P)$, устанавливая, что G-полигон Q (участвующий в описании полигонов над этими полугруппами) имеет не более двух конеразложимых компонент. Наконец, мы описываем подпрямо наразложимые полигоны над прямоугольной связкой. В качестве следствия получаются результат Г. Могаддаси [11] о полигонах над полугруппой левых нулей, а также описание подпрямо неразложимых полигонов над полугруппой правых нулей.

Необходимые сведения из универсальной алгебры можно найти в [5], из теории полугрупп — в [14], из теории полигонов — в [1].

1. Подпрямо неразложимые полигоны над произвольными полугруппами

Заметим, что при $|X| = 2$ полигон X подпрямо неразложим. Поэтому далее будем считать, что $|X| > 2$.

Элемент θ полигона X над полугруппой S называется *нулём*, если $\theta s = \theta$ для всех $s \in S$.

Отметим ряд очевидных свойств полигонов:

1) любая конгруэнция подполигона Y полигона X продолжается до конгруэнции полигона X (продолжением конгруэнции $\rho \in \operatorname{Con} Y$ является $\rho \cup \Delta_X \in \operatorname{Con} X$);
2) отображение $\rho \to \rho \cup \Delta_X$ является решёточным вложением $\operatorname{Con} Y$ в $\operatorname{Con} X$;
3) множество Θ всех нулей полигона X является подполигоном.

Из этих свойств следует отмеченное в [12, предложение 1] утверждение: если X подпрямо неразложим, то $|\Theta| \leqslant 2$ (действительно, так как любое отношение эквивалентности на Θ является конгруэнцией, при $|\Theta| \geqslant 3$ можно найти такие конгруэнции ρ_1, ρ_2, что $\rho_1, \rho_2 \neq \Delta$ и $\rho_1 \cap \rho_2 = \Delta$). В [15, теорема 2.6] этот факт доказан для полигона S_S. Для любых элементов $x \neq y$ полигона X можно определить *главную конгруэнцию* $\rho_{x,y}$ как конгруэнцию, порождённую парой (x, y). Из определений непосредственно следует, что пара $(z, w) \in X \times X$ принадлежит конгруэнции $\rho_{x,y}$ в том и только в том случае, если имеет место цепочка равенств

$$\begin{aligned} z = \ & u_1 s_1, \\ & v_1 s_1 = \ u_2 s_2, \\ & \qquad \dots \\ & \qquad v_{n-1} s_{n-1} = \ u_n s_n, \\ & \qquad\qquad\qquad v_n s_n = w, \end{aligned} \tag{1}$$

где $s_i \in S^1$ и $\{u_i, v_i\} = \{x, y\}$ при $i = 1, 2, \dots, n$. Если X — подпрямо неразложимый полигон над полугруппой S, то его монолит $\rho_0(X)$, очевидно, является главной конгруэнцией. Пусть $\rho_0(X) = \rho_{x,y}$. Тогда из определений следует

Утверждение 1. Полигон X подпрямо неразложим в том и только в том случае, если существуют такие элементы $x, y \in X$, что $x \neq y$ и для любых различных элементов $z, w \in X$ имеет место цепочка равенств (1).

Утверждение 1 даёт необходимые и достаточные условия подпрямой неразложимости произвольного полигона. Однако оно не вполне удобно, так как длины цепей n могут быть сколь угодно большими. В следующих далее теоремах условия включают ограниченное число элементов $s_1, \dots, s_n$ полугруппы S.

Теорема 1. Пусть X — полигон над полугруппой S, имеющий ровно два нуля, скажем θ_1 и θ_2. Тогда X подпрямо неразложим в том и только в том случае, если для любых элементов $a \neq b$ полигона X найдётся такое $s \in S$, что $\{as, bs\} = \{\theta_1, \theta_2\}$.

Доказательство. Достаточность очевидна, так как ясно, что в этом случае $\rho_0 = \rho_{\theta_1,\theta_2} = \{(\theta_1, \theta_2), (\theta_2, \theta_1)\} \cup \Delta_X$.

Необходимость. Пусть X подпрямо неразложим. Так как ρ_{θ_1,θ_2} — минимальная нетривиальная конгруэнция, $\rho_0 = \rho_{\theta_1,\theta_2}$. Докажем, что для любого $a \notin \{\theta_1, \theta_2\}$ выполняется соотношение

$$aS \supseteq \{\theta_1, \theta_2\}. \tag{2}$$

Пусть $a \notin \{\theta_1, \theta_2\}$ и $aS \not\supseteq \{\theta_1, \theta_2\}$. Если $as = a$ для всех $s \in S$, то a — нуль полигона X, отличный от θ_1, θ_2, что противоречит условию. Следовательно, существует элемент $s \in S$, такой, что $as \neq a$. По предположению $\theta_1 \notin aS$ или $\theta_2 \notin aS$. Можно считать,

что $\theta_2 \notin aS$. Тогда $(\theta_1, \theta_2) \notin \rho_{a,as}$, откуда $\rho_0 \not\subseteq \rho_{a,as}$, что также невозможно. Таким образом, условие (2) выполнено. Пусть $a \neq b$. Тогда $\rho_{a,b} \supseteq \rho_0 = \rho_{\theta_1,\theta_2}$. Следовательно, имеет место цепочка равенств

$$\begin{aligned} \theta_1 = \ & c_1 s_1, \\ & d_1 s_1 = \ c_2 s_2, \\ & \dots \\ & d_{n-1} s_{n-1} = \ c_n s_n, \\ & \qquad\qquad d_n s_n = \theta_2, \end{aligned} \tag{3}$$

где $s_i \in S^1$; $\{c_i, d_i\} = \{a, b\}$ при $i = 1, 2, \dots, n$. Пусть эта цепочка самая короткая из возможных. Без ограничения общности можно считать, что $c_1 = a$. Тогда $d_1 = b$. Если $bs_1 = \theta_2$, то $\{as_1, bs_1\} = \{\theta_1, \theta_2\}$, что и требовалось доказать. Если $bs_1 = \theta_1$, то цепочка (3) может быть сокращена на одно звено, что противоречит её выбору. Таким образом, $bs_1 \notin \{\theta_1, \theta_2\}$. Взяв в качестве a элемент bs_1 и применив условие (2), получим, что $bs_1 t = \theta_2$ при некотором $t \in S$. Кроме того, $as_1 t = c_1 s_1 t = \theta_1 t = \theta_1$. Следовательно, $(a, b) \cdot s_1 t = (\theta_1, \theta_2)$, откуда следует требуемое. ■

Полугруппу S назовём *подпрямо неразложимой справа*, если S имеет наименьшую нетривиальную правую конгруэнцию. В [15] отмечено, что подпрямо неразложимая справа полугруппа имеет ядро — наименьший правый идеал. Сформулируем аналогичное утверждение для подпрямо неразложимых полигонов. Полигон X назовём *простым*, если он не имеет подполигонов, отличных от X. Полигон X с нулём θ назовём *0-простым*, если $X \neq \{\theta\}$ и X не имеет подполигонов, отличных от $\{\theta\}$ и X.

Лемма 1. Всякий подпрямо неразложимый полигон X имеет наименьший нетривиальный (т. е. содержащий более одного элемента) подполигон K; при этом K — простой полигон. Если X — подпрямо неразложимый полигон с нулём, то X имеет наименьший ненулевой подполигон K, причём K — 0-простой подполигон.

Доказательство. Для любого нетривиального подполигона A отношение $\rho_A = (A \times A) \cup \Delta_X$, очевидно, является конгруэнцией (*конгруэнцией Риса*). Так как X подпрямо неразложим, $\bigcap\{\rho_A : A \text{ — нетривиальный подполигон}\} \neq \Delta_X$. Это означает, что пересечение K всех нетривиальных подполигонов само является нетривиальным подполигоном. Его простота очевидна. В случае подпрямо неразложимого полигона с нулём аналогично получаем, что пересечение K всех ненулевых подполигонов есть наименьший ненулевой подполигон. Тот факт, что он 0-простой, очевиден. ■

Теорема 2. Пусть X — полигон над полугруппой S, имеющий единственный нуль θ, а также наименьший ненулевой подполигон K, причём $K = \{a, \theta\}$. Тогда X подпрямо неразложим в том и только в том случае, если для любых $x, y \neq \theta$, таких, что $x \neq y$, найдётся $s \in S^1$, при котором $xs = \theta, ys \neq \theta$ или $xs \neq \theta, ys = \theta$.

Доказательство. Необходимость. Очевидно, $\rho_{a,\theta} = \{(a, \theta), (\theta, a)\} \cup \Delta_X$ — конгруэнция полигона X. Следовательно, $\rho_{a,\theta} = \rho_0(X)$. Возьмём любые элементы $x, y \neq \theta$, такие, что $x \neq y$. Если $xs = \theta \Leftrightarrow ys = \theta$, то $\rho_{x,y}$ не содержит пар вида (z, θ) при $z \neq \theta$. Тогда $\rho_{x,y} \cap \rho_{a,\theta} = \Delta_X$, что противоречит подпрямой неразложимости полигона X. Таким образом, $xs = \theta \not\Leftrightarrow ys = \theta$.

Достаточность. Пусть $x, y \in X$ и $x \neq y$. Если $x = \theta$, то так как $ys = a$ при некотором $s \in S^1$, имеем $\rho_{x,y} \supseteq \rho_{a,\theta}$. Аналогично разбирается случай, когда $y = \theta$. Если $x, y \neq \theta$, то по условию найдётся такое $s \in S^1$, что $xs = \theta, ys \neq \theta$ или $xs \neq \theta, ys = \theta$. Оба варианта дают $\rho_{x,y} \supseteq \rho_{a,\theta}$. ■

Теорема 3. Пусть X — полигон над полугруппой S. Предположим, что X имеет единственный нуль θ, а также наименьший ненулевой подполигон K, причём $|K| > 2$. Тогда X является подпрямо неразложимым в том и только в том случае, если выполняются условия:

(a) полигон K подпрямо неразложим;

(b) для любых $x, y \in X \setminus \theta$, таких, что $x \neq y$, выполняется хотя бы одно из следующих условий:

(i) $\exists s \in S\ (xs \neq ys\ \&\ \theta \in \{xs, ys\})$;

(ii) $x, y \notin K$, $\{xs, ys\} \cap K \neq \varnothing$ и $xs \neq ys$ при некотором $s \in S$;

(iii) $x \in K$, $y \notin K$, $ys = yt \notin K$, $xs \neq xt$ при некоторых $s, t \in S^1$;

(iv) $x \notin K$, $y \in K$, $xs = xt \notin K$, $ys \neq yt$ при некоторых $s, t \in S^1$;

(v) $xs \neq ys$ и $xs, ys \in K \setminus \{\theta\}$ при некотором $s \in S^1$.

При этом если существуют такие элементы $x, y \in X \setminus \{\theta\}$, что $x \neq y$ и $xs = \theta \Leftrightarrow ys = \theta$ при всех $s \in S$, то $\rho_0(X) \subseteq ((K \setminus \{\theta\}) \times (K \setminus \{\theta\})) \cup \Delta_X$, а если таких элементов x, y нет, то $\rho_0(X) = \rho_K = (K \times K) \cup \Delta_X$.

Доказательство. Необходимость. Пусть X подпрямо неразложим и $\rho_0(X)$ — наименьшая конгруэнция полигона X. Если $\rho_K = (K \times K) \cup \Delta_X$ — конгруэнция Риса, то $\rho_0(X) \subseteq \rho_K$, поэтому $\rho_0(X) \cap (K \times K)$ — наименьшая конгруэнция на K. Следовательно, K подпрямо неразложим. Таким образом, выполнено условие (a). Пусть $a \in X \setminus \{\theta\}$. По условию K — наименьший ненулевой подполигон, поэтому $aS^1 \supseteq K$. Таким образом, имеем

$$\forall a \in X \setminus \{\theta\}\ \ \exists s \in S^1\ \ (as \in K \setminus \{\theta\}). \tag{4}$$

Заметим, что если $(a, \theta) \in \rho_0(X)$ при некотором $a \neq \theta$, то $\rho_0(X) = \rho_K$, а значит, $\rho_0(X) = \rho_{x_0,y_0}$ при некоторых $x_0, y_0 \in K \setminus \{\theta\}$. Если $(a, \theta) \notin \rho_0(X)$ при всех $a \neq \theta$, то также $\rho_0(X) = \rho_{x_0,y_0}$ при некоторых $x_0, y_0 \in K \setminus \{\theta\}$. Таким образом,

$$\exists x_0, y_0 \in K \setminus \{\theta\}\ \ (\rho_0(X) = \rho_{x_0,y_0}).$$

Пусть $x, y \in X \setminus \{\theta\}$ и $x \neq y$. Предположим, что (i) не выполнено. Докажем, что при $x, y \notin K$ выполнено (ii), при $x \in K, y \notin K$ выполнено (iii), а при $x \notin K$, $y \in K$ выполнено (iv).

Пусть $x, y \notin K$. Рассмотрим цепочки равенств вида

$$\begin{aligned} z = \ & u_1 s_1, \\ & v_1 s_1 = u_2 s_2, \\ & \dots \\ & v_{n-1} s_{n-1} = u_n s_n, \\ & v_n s_n = w, \end{aligned} \tag{5}$$

где $z, w \in K \setminus \{\theta\}$; $z \neq w$; $\{u_i, v_i\} = \{x, y\}$; $s_i \in S^1$ при $i = 1, 2, \dots, n$. Хотя бы одна такая цепочка существует — это следует из включения $\rho_{x_0,y_0} \subseteq \rho_{x,y}$ и равенств (1). Будем считать, что цепочка (5) наиболее короткая из возможных. Если $u_n s_n = z$, то цепочка (5) ввиду несократимости имеет вид $z = u_n s_n$, $v_n s_n = w$, и получим $\{x, y\} \cdot s_n = \{z, w\}$. Если $u_n s_n \in K$, но $u_n s_n \neq z$ ($u_n s_n \neq \theta$, так как $u_n s_n \neq \theta$ и $u_n s = \theta \Leftrightarrow u_n s = \theta$ при всех s), то цепочку (5) можно сократить, удалив последнее звено; это противоречит её несократимости. Если $u_n s_n \notin K$, то имеем $\{x, y\} \cdot s_n = \{w, u_n s_n\}$, поэтому $xs_n \neq ys_n$ и $\{xs_n, ys_n\} \cap K \neq \varnothing$. Таким образом, выполнено (ii).

Пусть теперь $x \in K, y \notin K$. Напомним предположение: $xs = \theta \Leftrightarrow ys = \theta$ при всех $s \in S$. Как и ранее, устанавливаем наличие цепочки равенств (5) и считаем, что эта

цепочка наиболее короткая. Если $u_n s_n \in K$, то $u_n s_n \neq w$ (иначе можно удалить последнюю строчку в (5)). Следовательно, $\{x, y\} \cdot s_n = \{u_n s_n, w\} \subseteq K$, т. е. выполнено (v). Далее считаем, что $u_n s_n \notin K$. Так как $x \in K$, верно $u_n = y$ и $v_{n-1} = y$. Следовательно, $u_n = u_{n-1} = x$. Имеем

$$\begin{aligned} z = \ & xs_{n-1}, \\ & ys_{n-1} = \ ys_n, \\ & \qquad\quad xs_n = w. \end{aligned}$$

Ввиду $x \in K$ выполняется $xs_{n-1} \in K$. Если $xs_{n-1} \neq z$, то цепочка (5) может быть сокращена путём удаления двух последних строчек. Поэтому $xs_{n-1} = z$. Отсюда следует, что $v_{n-2} s_{n-2} = z$, т. е. цепочка (5) имеет вид $z = xs_{n-1}$, $ys_{n-1} = ys_n$, $xs_n = w$. Таким образом, $ys_{n-1} = ys_n$, $xs_{n-1} \neq xs_n$, т. е. выполнено (iii).

При $x \notin K$, $y \in K$ аналогично получаем, что выполнено (iv).

Достаточность. Пусть выполнены условия (a) и (b) и $\rho_0(K)$ — наименьшая нетривиальная конгруэнция полигона K. Ввиду $|K| > 2$ имеет место $\rho_0(K) = \rho_{x_0,y_0}$ при некоторых $x_0, y_0 \in K \setminus \{\theta\}$. Достаточно проверить, что $\rho_{x_0,y_0} \subseteq \rho_{x,y}$ при $x \neq y$. Если $x, y \in K$, то это следует из условия (a). Докажем, что $\rho_{a,\theta} \supseteq \rho_{x_0,y_0}$ при любых $a \neq \theta$. Действительно, так как K — наименьший ненулевой подполигон, выполнено условие (4). Следовательно, $as = x_0$, $at = y_0$ при некоторых $s, t \in S^1$. Отсюда

$$\begin{aligned} x_0 = \ & as, \\ \theta s = \ & \theta t, \\ & at = y_0, \end{aligned}$$

т. е. $\rho_{a,\theta} \supseteq \rho_{x_0,y_0}$. Далее будем считать, что $x, y \neq \theta$.

Пусть выполнено (i). Тогда $\{xs, ys\} = \{a, \theta\}$ для некоторого $a \neq \theta$, откуда $\rho_{x,y} \supseteq$ $\supseteq \rho_{xs,ys} = \rho_{a,\theta} \supseteq \rho_{x_0,y_0}$.

Пусть выполнено (v). Тогда $\rho_{xs,ys} \supseteq \rho_{x_0,y_0}$ ввиду (a). Поэтому $\rho_{x,y} \supseteq \rho_{x_0,y_0}$.

Пусть выполнено (iii). Тогда $\rho_{x,y} \supseteq \rho_{xs,xt}$, а так как $xs \neq xt$ и $xs, xt \in K$, то $\rho_{xs,xt} \supseteq \rho_{x_0,y_0}$. Аналогично случаю (iii) рассматривается случай (iv).

Пусть выполнено (ii). Если $xs = \theta$ или $ys = \theta$, то $\{xs, ys\} = \{a, \theta\}$ при некотором $a \neq \theta$, а значит, $\rho_{x,y} \supseteq \rho_{xs,ys} = \rho_{a,\theta} \supseteq \rho_{x_0,y_0}$. Далее считаем, что $xs, ys \neq \theta$. Если $xs, ys \in K$, то также $\rho_{xs,ys} \supseteq \rho_{x_0,y_0}$. Если $xs \in K$, $ys \notin K$ или $xs \notin K$, $ys \in K$, то выполняются условия (iii), (iv) или (v), разобранные ранее.

Если для некоторых $x, y \in X \setminus \{\theta\}$ имеют место соотношения $x \neq y$ и $xs = \theta \Leftrightarrow$ $\Leftrightarrow ys = \theta$ при всех $s \in S$, то главная конгруэнция $\rho_{x,y}$ не содержит ни одной пары вида (a, θ) при $a \neq \theta$, поэтому $\rho_0(X)$ также не содержит таких пар. Следовательно, $\rho_0(X) \subseteq ((K \setminus \{\theta\}) \times (K \setminus \{\theta\})) \cup \Delta_X$. Если же для любых $x \neq y$ существует такое $s \in S^1$, что $xs = \theta$, $ys \neq \theta$ или $xs \neq \theta$, $ys = \theta$, то ρ_{x_0,y_0} содержит все пары вида (a, θ), где $a \in K$, поэтому $\rho_0(X) = (K \times K) \cup \Delta_X$. ■

Замечание 1. Если $xs = \theta \Leftrightarrow ys = \theta$ при любых $x \neq y$ и $s \in S$, то множество $\{\theta\}$ является классом некоторой нетривиальной конгруэнции, а значит, $\{\theta\}$ — класс конгруэнции $\rho_0(X)$. В работе [12] элементы, образующие одноэлементный класс, названы разделительными. Проверка, является ли нуль θ разделительным, сводится к проверке эквивалентности $xs = \theta \Leftrightarrow ys = \theta$.

Следующая теорема доказана в работе [12]. Она поможет охарактеризовать подпрямо неразложимые полигоны без нуля.

Теорема 4 [12, предложение 3]. Пусть X — подпрямо неразложимый полигон без нуля, а $X \cup \{\theta\}$ — полигон, получающийся из X присоединением к X внешним образом

нуля θ. Тогда X подпрямо неразложим в том и только в том случае, если $X \cup \{\theta\}$ подпрямо неразложим.

Теорема 5. Пусть X — полигон без нуля и K — наименьший подполигон полигона X. Тогда X подпрямо неразложим в том и только в том случае, если K подпрямо неразложим и для любых $x, y \in X$, таких, что $x \neq y$, выполнено одно из следующих условий:

(i) $xs, ys \in K$ и $xs \neq ys$ при некотором $s \in S^1$;
(ii) $xs, xt \in K$, $xs \neq xt$, $ys = yt$ при некоторых $s, t \in S^1$;
(iii) $ys, yt \in K$, $ys \neq yt$, $xs = xt$ при некоторых $s, t \in S^1$.

Доказательство. Теорема следует непосредственно из теорем 3 и 4. ■

2. Подпрямо неразложимые полигоны над прямоугольными связками

Прямоугольной связкой называется прямое произведение $L \times R$, где L — полугруппа левых нулей, а R — полугруппа правых нулей. Прямоугольную связку можно определить также как полугруппу, удовлетворяющую тождествам $x^2 = x$ и $xyz = xz$. Понятно, что сами полугруппы правых и левых нулей являются прямоугольными связками. В свою очередь, прямоугольная связка является частным случаем более общей конструкции — рисовской матричной полугруппы $\mathcal{M}(G, I, \Lambda, P)$, где G — группа; I и Λ — множества; $P = ||p_{\lambda i}||_{\lambda \in \Lambda, i \in I}$ — сэндвич-матрица; $p_{\lambda i} \in G$ [14, § 3.1]. Напомним, что, согласно теореме Риса, рисовская матричная полугруппа — это то же самое, что вполне простая полугруппа [14, теорема 3.5]. В работе [13] описаны все правые полигоны над полугруппой $\mathcal{M}(G, I, \Lambda, P)$. Приведём это описание, так как оно понадобится для дальнейшего изложения.

Очевидно, для любой (необязательно нормальной) подгруппы H группы G множество G/H правых смежных классов Hg является правым G-полигоном относительно действия $Hg \cdot g' = Hgg'$. Через $\coprod\limits_{\alpha \in A} X_\alpha$ обозначим копроизведение (непересекающееся объединение) полигонов X_α над полугруппой. *Ядро* $\ker \varphi$ и *образ* $\operatorname{im} \varphi$ отображения $\varphi : X \to Y$ множеств определим обычным путём, а именно $\ker \varphi = \{(x, x') : x\varphi = x'\varphi\}$, $\operatorname{im} \varphi = X\varphi$.

Теорема 6 [13, теорема 5]. Пусть $S = \mathcal{M}(G, I, \Lambda, P)$ — вполне простая полугруппа, $(H_\alpha)_{\alpha \in A}$ — семейство подгрупп группы G, $Q = \coprod\limits_{\alpha \in \Omega} (G/H_\alpha)$ — копроизведение. Пусть для каждого $i \in I$ задано отображение $\pi_i : X \to Q$, а для каждого $\lambda \in \Lambda$ — отображение $\varkappa_\lambda : Q \to X$, причём

$$\forall q \in Q \ \forall i \in I \ \forall \lambda \in \Lambda \ \ (q\varkappa_\lambda \pi_i = q \cdot p_{\lambda i}). \tag{6}$$

Тогда X становится правым S-полигоном, если определить умножение элементов из X на элементы из S следующим образом: $x \cdot (g)_i \lambda = (x\pi_i \cdot g)\varkappa_\lambda$. Кроме того, всякий правый полигон над полугруппой $S = \mathcal{M}(G, I, \Lambda, P)$ изоморфен полигону, построенному таким образом.

Отметим, что в формулировке этой теоремы в работе [13] содержится дополнительное требование: чтобы для любых $\lambda \in \Lambda$, $i \in I$ каждое множество $\operatorname{im} \varkappa_\lambda$ пересекалось с каждым классом отношения $\ker \pi_i$ ровно по одному элементу. На самом деле это требование является излишним, так как указанное свойство следует из условия (6).

Следующее утверждение показывает, что количество конеразложимых слагаемых в Q не может превышать 2 в случае подпрямо неразложимого полигона.

Утверждение 2. Пусть X — полигон над вполне простой полугруппой $S = \mathcal{M}(G, I, \Lambda, P)$; $Q = \coprod\limits_{\alpha\in\Omega}(G/H_\alpha)$, $\pi_i : X \to Q$, $\varkappa_\lambda : Q \to X$ имеют тот же смысл, что и в теореме 6. Если X подпрямо неразложим, то $|\Omega| \leqslant 2$.

Доказательство. Пусть $|\Omega| \geqslant 3$. Выберем $\alpha, \beta \in \Omega$ такие, что $\alpha \neq \beta$, и положим $\Omega' = \Omega \setminus \{\alpha, \beta\}$. Положим также $Q_\alpha = G/H_\alpha$, $Q_\beta = G/H_\beta$, $Q' = \coprod\limits_{\gamma\neq\alpha,\beta} G/H_\gamma$. Введём отношения

$$\rho_1 = \{(x, y) : x = y \text{ или } \exists\lambda \in \Lambda\,(x, y \in (Q_\alpha \cup Q_\beta)\varkappa_\lambda)\};$$
$$\rho_2 = \{(x, y) : x = y \text{ или } \exists\lambda \in \Lambda\,(x, y \in (Q_\lambda \cup Q')\varkappa_\lambda)\};$$
$$\rho_3 = \{(x, y) : x = y \text{ или } \exists\lambda \in \Lambda\,(x, y \in (Q_\beta \cup Q')\varkappa_\lambda)\}.$$

Проверим, что ρ_1, ρ_2, ρ_3 — конгруэнции. Рефлексивность, симметричность и транзитивность этих отношений очевидна. Пусть $(x, y) \in \rho_1$ и $s = (g)_{i_\nu} \in S$. Тогда либо $x = y$, либо $x = q\varkappa_\lambda$, $y = q'\varkappa_\lambda$ при некоторых $q, q' \in Q_\alpha \cup Q_\beta$, $\lambda \in \Lambda$. Если $x \neq y$, то имеем $xs = x \cdot (g)_{i\nu} = (x\pi_i \cdot g)\varkappa_\nu = (q\varkappa_\lambda\pi_i \cdot g)\varkappa_\nu = (q \cdot p_{\lambda i} \cdot g)\varkappa_\nu \in (Q_\alpha \cup Q_\beta)\varkappa_\nu$, и аналогично $ys \in (Q_\alpha \cup Q_\beta)\varkappa_\nu$. Таким образом, $(xs, ys) \in \rho_1$. Следовательно, ρ_1 — конгруэнция. Аналогично доказывается, что ρ_2 и ρ_3 — также конгруэнции. Далее, так как отображение $\varkappa_\lambda$ инъективно для каждого $\lambda \in \Lambda$, выполняется $|(Q_\alpha \cup Q_\beta)\varkappa_\lambda| \geqslant 2$ и аналогично $|(Q_\alpha \cup Q')\varkappa_\lambda| \geqslant 2$ и $|(Q_\beta \cup Q')\varkappa_\lambda| \geqslant 2$. Это показывает, что $\rho_1, \rho_2, \rho_3 \neq \Delta$. Докажем, что $\rho_1 \cap \rho_2 \cap \rho_3 = \Delta$. Пусть $z \neq z'$ и $(z, z') \in \rho_1 \cap \rho_2 \cap \rho_3$. Тогда $z \in (Q_\alpha \cup Q_\beta)\varkappa_\lambda \cap (Q_\alpha \cup Q')\varkappa_\mu \cap (Q_\beta \cup Q')\varkappa_\nu$ при некоторых $\lambda, \mu, \nu \in \Lambda$. Отсюда получаем $z = q_1\varkappa_\lambda = q_2\varkappa_\mu = q_3\varkappa_\nu$, где $q_1 \in Q_\alpha \cup Q_\beta$; $q_2 \in Q_\alpha \cup Q'$; $q_3 \in Q_\beta \cup Q'$. Возьмём любое $i \in I$. Тогда будем иметь: $z\pi_i = q_1\varkappa_\lambda\pi_i = q_1 \cdot p_{\lambda i} \in Q_\alpha \cup Q_\beta$ и аналогично $z\pi_i \in Q_\alpha \cup Q'$ и $z\pi_i \in Q_\beta \cup Q'$. Но это невозможно, так как $(Q_\alpha \cup Q_\beta) \cap (Q_\alpha \cup Q') \cap (Q_\beta \cup Q') = \varnothing$. Таким образом, $\rho_1 \cap \rho_2 \cap \rho_3 = \Delta$. Это означает, что полигон X не является подпрямо неразложимым. ■

Перейдём теперь к полигонам над прямоугольными связками. Для них теорема 6 существенно упрощается. В этом случае $S = L \times R$ — полугруппа с умножением $(l, r) \cdot (l', r') = (l, r')$ $(l, l' \in L,\ r, r' \in R)$; Q — произвольное множество; $\pi_l : X \to Q$ и $\varkappa_r : Q \to X$ — такие отображения, что $\varkappa_r\pi_l = 1_Q$ (тождественное отображение); операция на полигоне X осуществляется по правилу $x \cdot (l, r) = x\pi_l\varkappa_r$. Заметим, что $\varkappa_r$ — инъективные, а π_l — сюръективные отображения, и множество $\operatorname{im}\varkappa_r$ является множеством представителей классов эквивалентности отношения $\ker\pi_l$ при всех $l \in L$, $r \in R$. В силу утверждения 2 имеем $|Q| \leqslant 2$. Случай $|Q| = 1$ не представляет труда ввиду следующей леммы.

Лемма 2. Если X — полигон над прямоугольной связкой $S = L \times R$ и $|Q| = 1$, то X подпрямо неразложим в том и только в том случае, если $|X| \leqslant 2$.

Доказательство. Так как $|Q| = 1$, имеем $Q = \{q\}$. Положим $q\varkappa_r = a_r$ при $r \in R$. Для любого $x \in X$ и любых $l' \in L$, $r \in R$ имеем $x \cdot (l, r) = x\pi_l\varkappa_r = q\varkappa_r = a_r$. Таким образом, $xs = ys$ при всех $x, y \in X$. Это означает, что на X любое отношение эквивалентности является конгруэнцией. Поэтому если X подпрямо неразложим, то $|X| \leqslant 2$. Обратное утверждение очевидно. ■

Ввиду утверждения 2 и леммы 2 осталось рассмотреть лишь случай, когда $|Q| = 2$. Пусть $Q = \{q_1, q_2\}$. Для $r \in R$ положим $a_r = q_1\varkappa_r$, $b_r = q_2\varkappa_r$, $A = \{a_r : r \in R\}$, $B = \{b_r : r \in R\}$.

Лемма 3. Пусть X — полигон над прямоугольной связкой $S = L \times R$, $Q = \{q_1, q_2\}$, π_l, $\varkappa_r$, a_r, b_r, A, B имеют тот же смысл, что и выше. Если X подпрямо неразложим, то выполняются следующие условия:

(i) $xs = ys$ при любых $s \in S$ и $x, y \in X$ таких, что $x, y \in A$ или $x, y \in B$;
(ii) $|A|, |B| \leqslant 2$;
(iii) $|A| + |B| \leqslant 3$.

Доказательство.

(i) Пусть $x, y \in A$, $s = (l, r) \in S$. Тогда $x = q_1\varkappa_{r_1}$, $y = q_1\varkappa_{r_2}$ при некоторых $r_1, r_2 \in R$. Имеем $xs = x\pi_l\varkappa_r = q_1\varkappa_{r_1}\pi_l\varkappa_r = q_1 \cdot 1 \cdot \varkappa_r = a_r$ и аналогично $ys = a_r$. Следовательно, $xs = ys$.

(ii) Пусть $|A| \geqslant 3$. Из п. (i) видно, что любое отношение эквивалентности на множестве A продолжается до конгруэнции полигона X. Точнее, если ρ — отношение эквивалентности на A, то $\rho \cup \Delta_X \in \operatorname{Con} X$. Так как $|A| \geqslant 3$, существуют отношения эквивалентности ρ_1, ρ_2 на A, такие, что $\rho_1, \rho_2 \neq \Delta_A$, а $\rho_1 \cap \rho_2 = \Delta_A$. Положим ${\rho_1}' = \rho_1 \cup \Delta_X$, ${\rho_2}' = \rho_2 \cup \Delta_X$. Тогда $\rho_1', \rho_2' \in \operatorname{Con} X$, $\rho_1', \rho_2' \neq \Delta_X$ и $\rho_1' \cap \rho_2' = \Delta_X$. Это противоречит предположению о том, что X подпрямо неразложим.

(iii) Пусть $|A| = |B| = 2$. Положим $\rho_1 = (A \times A) \cup \Delta_X$, $\rho_2 = (B \times B) \cup \Delta_X$. Тогда $\rho_1, \rho_2 \in \operatorname{Con} X$, $\rho_1, \rho_2 \neq \Delta_X$, а $\rho_1 \cap \rho_2 = \Delta_X$, что противоречит подпрямой неразложимости полигона X. ■

Теорема 7. Пусть X — полигон над прямоугольной связкой $S = L \times R$ и $|X| > 2$. Пусть Q и $\varkappa_r$ ($r \in R$) имеют тот же смысл, что в теореме 6. Тогда X подпрямо неразложим в том и только в том случае, если $Q = \{q_1, q_2\}$ — двухэлементное множество, а множества $A = \{q_1\varkappa_r : r \in R\}$, $B = \{q_2\varkappa_r : r \in R\}$ удовлетворяют одному из следующих условий:

(i) $|A| = |B| = 1$, скажем, $A = \{a\}$, $B = \{b\}$, и для любых $x \neq y$ существует такое $s \in S$, что $\{xs, ys\} = \{a, b\}$;
(ii) $|A| = 2$, $|B| = 1$, скажем $A = \{a_1, a_2\}$, $B = \{b\}$; $xS \cap A \neq \varnothing$ при $x \neq b$ и для любых $x, y \neq b$ если $x \neq y$ и $\{x, y\} \neq A$, то $xs \neq ys$ при некотором $s \in S$;
(iii) $|A| = 1$, $|B| = 2$ — условие, двойственное условию (ii).

Доказательство. Необходимость. Пусть X — подпрямо неразложимый полигон и $|X| \geqslant 3$. Ввиду утверждения 2 и леммы 2 $|Q| = 2$. Пусть $Q = \{q_1, q_2\}$. Ввиду леммы 3 возможны лишь следующие варианты: a) $|A| = |B| = 1$; b) $|A| = 2$, $|B| = 1$; c) $|A| = 1$, $|B| = 2$.

a) Пусть $|A| = |B| = 1$, $A = \{a\}$, $B = \{b\}$. Ясно, что a и b — нули полигона X. Из теоремы 2 следует, что выполняется условие (i).

b) Пусть $|A| = 2$, $|B| = 1$, $A = \{a_1, a_2\}$, $B = \{b\}$. Очевидно, что b является нулём полигона X. Далее, отношение $\rho = \{(a_1, a_2), (a_2, a_1)\} \cup \Delta_X$ является конгруэнцией. Так как это минимальное отличное от Δ отношение эквивалентности, $\rho = \rho_0(X)$. Пусть $x \neq b$. Если $x \in A$, то $xS \subseteq A$, а значит, $xS \cap A \neq \varnothing$. Пусть $x \notin A$. Так как $XS = A \cup B$ и $x \neq a_1, a_2, b$, выполняется $x \notin XS$, поэтому $|xS^1| \geqslant 2$. Следовательно, $(xS^1 \times xS^1) \cup \Delta_X$ — нетривиальная конгруэнция, а значит, $a_1, a_2 \in xS^1$. Так как $x \notin A$, верно $a_1, a_2 \in xS$. Пусть $x, y \neq b$ и $x \neq y$. Если $xs = ys$ при всех $s \in S$, то главная конгруэнция $\rho_{x,y} = \{(x, y), (y, x)\} \cup \Delta_X$. Следовательно, $\rho_{x,y} = \rho_0$, а значит, $\{x, y\} = \{a_1, a_2\}$.

c) В случае, когда $|A| = 1, |B| = 2$, рассуждаем аналогично предыдущему.

Достаточность. Пусть $|X| \geqslant 3$ и выполнено (i). Тогда $\rho_{x,y} \supseteq \rho_{a,b}$ при любых $x \neq y$. Это означает, что X подпрямо неразложим и $\rho_0(X) = \rho_{a,b}$. Предположим, что выполнено (ii). Пусть $x, y \in X$ и $x \neq y$. Далее разберём два случая.

С л у ч а й 1: $b \in \{x, y\}$. Можно считать, что $x \neq b, y = b$. Тогда $xS \cap A \neq \varnothing$, поэтому $xs = a_i$ при некотором $s \in S$. Пусть $xs = a_1$. Из определения множества A следует, что $a_1S = a_2S = A$. Поэтому $a_1t = a_2$ при некотором $t \in S$. Получаем $(x, y) \cdot s = (a_1, b)$, $(x, y) \cdot st = (a_2, b)$. Следовательно, $(a_1, b), (a_2, b) \in \rho_{x,y}$, поэтому $(a_1, a_2) \in \rho_{x,y}$, а значит, $\rho_{a_1,a_2} \in \rho_{x,y}$.

С л у ч а й 2: $x, y \neq b$. Если $\{x, y\} = \{a_1, a_2\}$, то $\rho_{x,y} = \rho_{a_1,a_2}$. Пусть $\{x, y\} \neq \neq \{a_1, a_2\}$. Тогда по условию $xs \neq ys$ при некотором $s \in S$. Но $XS = A \cup B$, поэтому $\{xs, ys\} \subseteq \{a_1, a_2, b\}$. Если $\{xs, ys\} \subseteq \{a_1, a_2\}$, то $\rho_{x,y} \supseteq \rho_{a_1,a_2}$, что и требовалось. Если $\{xs, ys\} \subseteq \{a_1, b\}$, то $\rho_{x,y} \supseteq \rho_{a_1,b}$, а так как $a_2 \in a_1S$, верно $\rho_{x,y} \supseteq \rho_{a_2,b}$. Следовательно, $\rho_{x,y} \supseteq \rho_{a_1,a_2}$.

Если выполнено (iii), рассуждаем так же, как при рассмотрении случая (ii). ■

Следствие 1 [11, теорема 3.2]. Пусть X — полигон над полугруппой левых нулей L и $|X| > 2$. Тогда X подпрямо неразложим в том и только в том случае, если X имеет ровно два нуля и для любых $x \neq y$ существует такое $s \in L$, что $xs \neq ys$.

Доказательство. Если $|L| = 1$, то полугруппа состоит из одного элемента. В этом случае, как нетрудно видеть, подпрямо неразложимые полигоны X — это в точности такие, что $|X| \leqslant 2$. Поэтому далее будем считать, что $|L| > 1$. По теореме 7 $|Q| = 2$, а так как $|R| = 1$, верно $|A| = |B| = 1$. Таким образом, случаи (ii) и (iii) теоремы 7 здесь невозможны, а из (i) получаем, что X подпрямо неразложим тогда и только тогда, когда для любых $x \neq y$ при некотором $s \in L$ имеем $xs \neq ys$. При этом $s \neq 1$, так как $|L| > 1$. ■

Следствие 2. Пусть X — полигон над полугруппой правых нулей R. Тогда X подпрямо неразложим в том и только в том случае, если $|X| \leqslant 2$ или X изоморфен полигону $Y = \{a_1, a_2, b\}$, такому, что $a_1R = a_2R = \{a_1, a_2\}$, $bR = \{b\}$.

Доказательство. Пусть X — полигон над полугруппой правых нулей R и $|X| \geqslant 3$. По теореме 7 $Q = \{q_1, q_2\}$ и либо $|A| = |B| = 1$, либо $|A| = 2$, $|B| = 1$, либо $|A| = 1$, $|B| = 2$. Второй и третий случаи аналогичны друг другу, поэтому будем рассматривать лишь один из них. Так как $|L| = 1$, то имеем только одно отображение π_l, будем обозначать его π. Умножение элементов из X на элементы из R осуществляется по правилу $xr = x\pi\varkappa_r$. Положим $X_1 = q_1\pi^{-1}$, $X_2 = q_2\pi^{-1}$. Очевидно, что $X_1 \cup X_2 = X$ и $X_1 \cap X_2 = \varnothing$. Заметим, что $xR \subseteq A$ при $x \in X_1$ и $xR \subseteq B$ при $x \in X_2$.

Пусть $|A| = |B| = 1$. Имеем $A = \{a\}$, $B = \{b\}$. Отсюда получаем $X_1R = \{a\}$, $X_2R = \{b\}$. Возьмём произвольный элемент x из X. Если $x \notin \{a, b\}$ и, скажем, $x \in X_1$, то $xr = x\pi\varkappa_r = q_1\varkappa_r$ и $ar = a\pi\varkappa_r = q_1\varkappa_r$, т. е. $xr = ar$. По условию (i) теоремы 7 X не является подпрямо неразложимым. Следовательно, такого x нет, а значит, $X = \{a, b\}$.

Пусть $|A| = 2$, $|B| = 1$. Имеем $A = \{a_1, a_2\}$, $B = \{b\}$. Предположим, что X подпрямо неразложим. Тогда выполняется условие (ii) теоремы 7. Следовательно, $xR \cap A \neq \varnothing$ при $x \neq b$. Если $x \in X_2 \setminus \{b\}$, то $xR = \{b\}$ и $xR \cap A = \varnothing$. Значит, $X_2 = \{b\}$. Пусть $x \in X_1 \setminus \{a_1, a_2\}$. Тогда $\{x, a_1\} \neq \{a_1, a_2\}$. Поэтому по теореме 7 $xr \neq a_1r$ при некотором $r \in R$. Но $xr = x\pi\varkappa_r = q_1\varkappa_r$ и $a_1r = a_1\pi\varkappa_r = q_1\varkappa_r$. Получили противоречие, следовательно, $X_1 = \{a_1, a_2\}$. Таким образом, $X = \{a_1, a_2, b\}$. Из определения элементов a_1, a_2, b следует, что $a_1R = a_2R = \{a_1, a_2\}$, $bR = \{b\}$. Тот факт, что полигон X подпрямо неразложим, очевиден, его наименьшая нетривиальная конгруэнция есть $\{(a_1, a_2), (a_2, a_1)\} \cup \Delta_X$. ■

ЛИТЕРАТУРА

1. *Kilp M., Knauer U., and Mikhalev A. V.* Monoids, Acts and Categories. Berlin, N.Y.: W. de Gruyter, 2000.
2. *Плоткин Б. И., Гринглаз Л. Я., Гварамия А. А.* Элементы алгебраической теории автоматов. М.: Высш. шк., 1994. 191 с.
3. *Егорова Д. П., Скорняков Л. А.* О структуре конгруэнций унарной алгебры // Межвуз. науч. сб. «Упорядоченные множества и решётки». Саратов, 1977. Вып. 4. С. 28–40.
4. *Егорова Д. П.* Структура конгруэнций унарной алгебры // Межвуз. науч. сб. «Упорядоченные множества и решётки». Саратов, 1978. Вып. 5. С. 11–44.
5. *Кон П.* Универсальная алгебра. М.: Мир, 1968. 286 с.
6. *Ésik Z. and Imreh B.* Subdirectly irreducible commutative automata // Acta Cybernetica. 1981. V. 5. No. 1. P. 251–260.
7. *Кожухов И. Б.* Условия конечности для подпрямо неразложимых полигонов и модулей // Фунд. и прикл. матем. 1998. Т. 4. № 2. С. 1–5.
8. *Kozhukhov I. B.* One characteristical property of semilattices // Commun. Algebra. 1997. V. 25. No. 8. P. 2569–2577.
9. *Халиуллина А. Р.* Конгруэнции полигонов над полугруппами правых нулей // Чебышевский сборник. 2013. Т. 14. № 3. С. 142–146.
10. *Халиуллина А. Р.* Конгруэнции правых полигонов над полугруппами правых и левых нулей // Материалы 12-й Междунар. конф. «Алгебра и теория чисел». Тула, 2014. С. 139–142.
11. *Moghaddasi Gh.* On injective and subdirectly irreducible S-acts over left zero semigroups // Turk. J. Math. 2012. V. 36. P. 359–365.
12. *Ройз Е. Н.* О подпрямо неразложимых монарах // Межвуз. науч. сб. «Упорядоченные множества и решётки». Саратов, 1974. Вып. 2. С. 80–84.
13. *Avdeyev A. Yu. and Kozhukhov I. B.* Acts over completely 0-simple semigroups // Acta Cybernetica. 2000. V. 14. No. 4. P. 523–531.
14. *Клиффорд А., Престон Г.* Алгебраическая теория полугрупп. Т. 1. М.: Мир, 1972. 286 с.
15. *Rankin S. A., Reis C. M., and Thierrin G.* Right subdirectly irreducible semigroups // Pacif. J. Math. 1979. V. 85. No. 2. P. 403–412.

REFERENCES

1. *Kilp M., Knauer U., and Mikhalev A. V.* Monoids, Acts and Categories. Berlin, N.Y., W. de Gruyter, 2000.
2. *Plotkin B. I., Gringlaz L. Ja., Gvaramija A. A.* Jelementy algebraicheskoj teorii avtomatov. Moscow, Vyssh. Shk. Publ., 1994. 191 p. (in Russian)
3. *Egorova D. P., Skornjakov L. A.* O strukture kongrujencij unarnoj algebry. Mezhvuz. nauch. sb. «Uporjadochennye mnozhestva i reshjotki». Saratov, 1977, no. 4, pp. 28–40. (in Russian)
4. *Egorova D. P.* Struktura kongrujencij unarnoj algebry. Mezhvuz. nauch. sb. «Uporjadochennye mnozhestva i reshjotki». Saratov, 1978, no. 5, pp. 11–44. (in Russian)
5. *Kon P.* Universal'naja algebra. Moscow, Mir Publ., 1968. 286 p. (in Russian)
6. *Ésik Z. and Imreh B.* Subdirectly irreducible commutative automata. Acta Cybernetica, 1981, vol. 5, no. 1, pp. 251–260.
7. *Kozhukhov I. B.* Uslovija konechnosti dlja podprjamo nerazlozhimyh poligonov i modulej. Fund. i prikl. matem., 1998, vol. 4, no. 2, pp. 1–5. (in Russian)
8. *Kozhukhov I. B.* One characteristical property of semilattices. Commun. Algebra, 1997, vol. 25, no. 8, pp. 2569–2577.

9. *Haliullina A. R.* Kongrujencii poligonov nad polugruppami pravyh nulej. Chebyshevskij sbornik, 2013, vol. 14, no. 3, pp. 142–146. (in Russian)
10. *Haliullina A. R.* Kongrujencii pravyh poligonov nad polugruppami pravyh i levyh nulej. Materialy 12 Mezhdunar. konf. «Algebra i teorija chisel», Tula, 2014, pp. 139–142. (in Russian)
11. *Moghaddasi Gh.* On injective and subdirectly irreducible S-acts over left zero semigroups. Turk. J. Math., 2012, vol. 36, pp. 359–365.
12. *Rojz E. N.* O podprjamo nerazlozhimyh monarah. Mezhvuz. nauch. sb. «Uporjadochennye mnozhestva i reshjotki». Saratov, 1974, no. 2, pp. 80–84. (in Russian)
13. *Avdeyev A. Yu. and Kozhukhov I. B.* Acts over completely 0-simple semigroups. Acta Cybernetica, 2000, vol. 14, no. 4, pp. 523–531.
14. *Klifford A., Preston G.* Algebraicheskaja teorija polugrupp. V. 1. Moscow, Mir Publ., 1972. 286 p. (in Russian)
15. *Rankin S. A., Reis C. M., and Thierrin G.* Right subdirectly irreducible semigroups. Pacif. J. Math., 1979, vol. 85, no. 2, pp. 403–412.

УДК 519.716

О КЛАССАХ ФУНКЦИЙ ТРЁХЗНАЧНОЙ ЛОГИКИ, ПОРОЖДЁННЫХ СИММЕТРИЧЕСКИМИ ФУНКЦИЯМИ С ОГРАНИЧЕННЫМ ЧИСЛОМ СЛОЁВ[1]

А. В. Михайлович

Национальный исследовательский университет Высшая школа экономики, г. Москва, Россия

Изучаются замкнутые классы функций трёхзначной логики, порождённые симметрическими функциями, принимающими значение 1 на ограниченном числе слоёв и нулевое значение — на остальных наборах. Для этих классов получены критерии базируемости и конечной порождённости. Установлена зависимость наличия базиса (конечного базиса) в рассматриваемом классе от существования базиса (конечного базиса соответственно) в подклассах, порождённых монотонными и немонотонными функциями порождающей системы по отдельности.

Ключевые слова: *функции многозначной логики, замкнутый класс, порождающая система.*

DOI 10.17223/20710410/27/2

CLOSED CLASSES OF THREE-VALUED LOGIC FUNCTIONS GENERATED BY SYMMETRIC FUNCTIONS WITH A BOUNDED NUMBER OF LAYERS

A. V. Mikhailovich

National Research University Higher School of Economics, Moscow, Russia

E-mail: avmikhailovich@gmail.com

Closed classes of three-valued logic functions of which a generating system consists of symmetric functions with values in the set $\{0, 1\}$ and with value 1 at a bounded subset of layers from $\{1, 2\}^n$ are considered. Some criteria for existence of a basis and of a finite basis are obtained for these classes. It is shown how the existence of a basis or of a finite basis depends on the existence of a basis or of a finite basis in subclasses generated by monotonous or non-monotonous functions.

Keywords: *multi-valued logic functions, closed classes, generating systems.*

Введение

Рассматривается задача о конечной порождённости и существовании базисов для некоторых семейств замкнутых классов функций трёхзначной логики. Э. Л. Пост [1, 2] описал все замкнутые классы булевых функций и показал, что каждый такой класс имеет конечный базис. На случай функций k-значной логики (P_k) при $k \geqslant 3$ эти результаты не распространяются. В работе [3] показано, что при всех $k \geqslant 3$ в P_k существуют

[1]Работа выполнена при поддержке программы «Научный фонд НИУ ВШЭ» в 2014/2015 г., проект № 14-01-0144.

как замкнутые классы со счётным базисом, так и классы, не имеющие базиса. Следует отметить, что порождающие системы классов из этих примеров состоят из симметрических функций, принимающих значения только из множества $\{0,1\}$ и равных нулю на единичном наборе и наборах, содержащих хотя бы одну нулевую компоненту. В работах [4 – 7] рассматривались некоторые семейства классов, порождённых симметрическими функциями такого вида. В частности, в [7] получены критерии базируемости и конечной порождённости для классов, порождённых немонотонными симметрическими функциями с ограниченным числом слоёв. В данной работе рассматриваются классы, порождённые произвольными симметрическими функциями с ограниченным числом слоёв такого вида. Для этих классов получены критерии базируемости и конечной порождённости в терминах свойств подклассов, порождённых немонотонными и монотонными функциями порождающей системы по отдельности. Отметим, что задача о возможности алгоритмической проверки базируемости и конечной порождённости является сложной самостоятельной задачей. Все недостающие определения можно найти в работах [6 – 8].

1. Определения и вспомогательные утверждения

Функции f и g из P_k называются *конгруэнтными*, если одна из них получается из другой переименованием переменных без отождествления (обозначение $f \cong g$). Функция $f(x_1, \ldots, x_n)$ называется *симметрической*, если она не меняется при любой перестановке своих аргументов. Пусть $\mathfrak{A} \subset P_k$. Множество всех функций, которые могут быть реализованы простыми формулами (простой называется формула, у которой собственными подформулами являются только символы переменных) над $\mathfrak{A}$ и применением операции введения фиктивной переменной, будем обозначать через $\langle \mathfrak{A} \rangle$. Пусть $A_1 \subset E_3^{n_1}$, …, $A_p \subset E_3^{n_p}$, $p \geqslant 1$, $n = n_1 + \ldots + n_p$. Обозначим через $A_1 \times \ldots \times A_p$ множество всех наборов из E_3^n вида $(\widetilde{\alpha^1}, \ldots, \widetilde{\alpha^p})$, где $\widetilde{\alpha^i} \in A_i$, $i = 1, \ldots, p$. Пусть $\widetilde{\alpha} \in E_3^n$. Число единиц в наборе $\widetilde{\alpha}$ обозначим через $|\widetilde{\alpha}|$. Набор из E_3^n, все компоненты которого равны α, будем обозначать α^n.

Обозначим через R множество всех функций трёхзначной логики, принимающих значения только из множества $\{0,1\}$ и равных нулю на единичном наборе и на всех наборах, содержащих хотя бы одну нулевую компоненту. Пусть $f(x_1, \ldots, x_n) \in R$; N_f — множество всех наборов из E_3^n, на которых функция f принимает значение 1; e_f и d_f — соответственно число единиц и двоек в наборе из N_f с максимальным числом единиц. Пусть $F \subset R$, $k \in \mathbb{Z}^+$ (через $\mathbb{Z}^+$ обозначается множество всех неотрицательных целых чисел). Если для любой фукнции f из множества F выполняется неравенство $e_f \leqslant k$, то множество F будем называть *k-ограниченным*. Если при этом существует функция g из множества F, такая, что $e_g = k$, то множество F будем называть *точно k-ограниченным*.

Множество $\mathcal{L}$ всех наборов из E_3^n, которые получаются друг из друга перестановкой компонент, называется *слоем*. Слой из $\{1,2\}^n$, содержащий e единиц и d двоек, $e + d = n$, будем обозначать $\mathcal{L}(e,d)$. Множество всех симметрических функций из R обозначим S. В данной работе рассматриваются только функции из множества R, поэтому в дальнейшем симметрическими функциями будем называть функции множества S, не оговаривая это отдельно. Функцию $f(x_1, \ldots, x_n)$ из R будем называть *m-слойной симметрической функцией*, если существует m различных слоёв $\mathcal{L}_1, \ldots, \mathcal{L}_m$, $m \geqslant 1$, из множества $\{1,2\}^n$, таких, что $N_f = \mathcal{L}_1 \cup \ldots \cup \mathcal{L}_m$. Семейство всех m-слойных симметрических функций обозначим S^m. Положим $\mathrm{S}^{(m)} = \cup \mathrm{S}^i$, где объединение берётся по всем i, $1 \leqslant i \leqslant m$. Функцию из R будем называть *монотонной*, если она монотонна

относительно порядка $0 < 1 < 2$ на множестве E_3. Множество всех монотонных (немонотонных) симметрических функций из R будем обозначать MS (соответственно NS). Положим $\mathrm{MS}^m = \mathrm{S}^m \cap \mathrm{MS}$, $\mathrm{MS}^{(m)} = \mathrm{S}^{(m)} \cap \mathrm{MS}$, $\mathrm{NS}^m = \mathrm{S}^m \cap \mathrm{NS}$, $\mathrm{NS}^{(m)} = \mathrm{S}^{(m)} \cap \mathrm{NS}$. Пусть $F \subset \mathrm{S}$ (соответственно $F \subset \mathrm{MS}$, $F \subset \mathrm{NS}$). Если существует такое число $m \in \mathbb{N}$, что $F \subset \mathrm{S}^{(m)}$ (соответственно $F \subset \mathrm{MS}^{(m)}$, $F \subset \mathrm{NS}^{(m)}$), то будем называть F множеством симметрических функций (соответственно монотонных симметрических, немонотонных симметрических) с ограниченным числом слоёв.

Сформулируем и при необходимости докажем вспомогательные утверждения.

Лемма 1 [6]. Если формула над R обращается на некотором наборе в единицу, то и любая её подформула обращается на этом наборе в единицу.

Лемма 2 [6]. Пусть $f(x_1, \ldots, x_n) \in \mathrm{NS}^l$, $l \geqslant 1$, Φ — формула над S, реализующая функцию f, Φ_1 — подформула формулы Φ, имеющая вид $g(\mathcal{B}_1, \ldots, \mathcal{B}_m)$, где $\mathcal{B}_1, \ldots, \mathcal{B}_m$ — формулы над S, $g \in \mathrm{S}^{(l)}$. Тогда среди формул $\mathcal{B}_1, \ldots, \mathcal{B}_m$ есть символы переменных из множества $\{x_1, \ldots, x_n\}$, причем символы всех переменных встречаются одинаковое число раз.

Лемма 3. Пусть $f(x_1, \ldots, x_n) \in \mathrm{S}$, Φ — некоторая формула над R, реализующая функцию f, Φ_1 — подформула формулы Φ, имеющая вид $g(\mathcal{B}_1, \ldots, \mathcal{B}_m)$, где $g(x_1, \ldots, x_m) \in \mathrm{S}$, а $\mathcal{B}_1, \ldots, \mathcal{B}_m$ — формулы над R. Тогда справедливы неравенства $e_f \leqslant e_g$ и $e_f/d_f \leqslant e_g/d_g$. При этом если Φ_1 не является простой формулой, то имеют место строгие неравенства $e_f < e_g$ и $e_f/d_f < e_g/d_g$.

Доказательство леммы 3 проводится аналогично доказательству утверждения 1.2.6 из работы [6].

Лемма 4. Пусть $f, g \in \mathrm{S}$, $H \subset \mathrm{S}$, $f, g \notin [H]$. Тогда $[\{f\} \cup H] = [\{g\} \cup H]$ в том и только в том случае, когда $f \cong g$.

Доказательство. Нетрудно видеть, что для любых конгруэнтных функций f и g из S, для любого подмножества H множества S выполняется равенство $[\{f\} \cup H] = [\{g\} \cup H]$.

Пусть $H \subset \mathrm{S}$, $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_m) \in \mathrm{S} \backslash [H]$ и выполняется равенство $[\{f\} \cup H] = [\{g\} \cup H]$. Тогда $f \in [\{g\} \cup H]$ и $g \in [\{f\} \cup H]$. Пусть Φ — формула над $\{g\} \cup H$, реализующая функцию f. Поскольку $f \notin [H]$, то существует подформула Φ_1 формулы Φ, имеющая вид $g(\mathcal{B}_1, \ldots, \mathcal{B}_m)$, где $\mathcal{B}_1, \ldots, \mathcal{B}_m$ — формулы над $\{g\} \cup H$. Из леммы 3 следует, что выполняются неравенства $e_f \leqslant e_g$, $e_f/d_f \leqslant e_g/d_g$. Аналогично можно показать, что $e_g \leqslant e_f$, $e_g/d_g \leqslant e_f/d_f$. Следовательно, $e_f = e_g$, $e_f/d_f = e_g/d_g$. Значит, выполняются равенства $m = n$ и $d_g = d_f$ и формула Φ_1 является простой. Нетрудно показать, что среди тривиальных формул $\mathcal{B}_1, \ldots, \mathcal{B}_m$ символ каждой переменной из $\{x_1, \ldots, x_n\}$ встречается ровно по одному разу. Следовательно, в силу леммы 1 выполняется включение $N_f \subset N_g$. Аналогично можно показать, что $N_g \subset N_f$. Следовательно, $N_f = N_g$, а значит, $f \cong g$. ■

Пусть $f, g \in \mathrm{NS}^m$, $m \geqslant 1$, $A \subset R$. Будем писать $f \preceq_A g$, если $f \in [\{g\} \cup A]$. Из леммы 4 следует, что соотношения $f \preceq_A g$ и $g \preceq_A f$ одновременно выполняются в том и только в том случае, когда функции f и g конгруэнтны. Следовательно, отношение $\preceq_A$ является порядком на любом множестве попарно неконгруэнтных функций из NS^m. Поскольку в дальнейшем данное отношение рассматривается только на таких множествах, будем называть его порядком $\preceq_A$. Множество H попарно неконгруэнтных функций из $\mathrm{NS}^m \backslash [A]$ называется *цепью относительно порядка* $\preceq_A$, если любые два элемента множества H сравнимы относительно порядка $\preceq_A$. Пусть G — множество

попарно неконгруэнтных функций из $\mathrm{NS}^m\backslash[A]$. Цепь $H \subset G$ называется *максимальной цепью* множества G относительно порядка $\preceq_A$, если для любой цепи $H_1 \subset \mathrm{NS}^m\backslash[A]$, такой, что $H \subset H_1$, $H \neq H_1$, цепь H_1 не является подмножеством множества G. Функция $f \in H$ называется *верхней гранью* цепи H относительно порядка $\preceq_A$, если для любой функции $g \in H$ выполняется неравенство $g \preceq_A f$. Цепь называется *ограниченной относительно порядка* $\preceq_A$, если она имеет верхнюю грань относительно порядка $\preceq_A$.

Докажем вспомогательное утверждение, анонсированное в [10].

Лемма 5. Пусть подмножество F множества функций R содержит счётное число попарно неконгруэнтных немонотонных симметрических функций. Тогда класс $G = [F]$ не имеет конечного базиса.

Доказательство. Предположим, что класс G имеет конечный базис $\mathfrak{A} = \{g_1(x_1, \ldots, x_{n_1}), \ldots, g_r(x_1, \ldots, x_{n_r})\}$. Положим $n = \max(n_1, \ldots, n_r)$.

Пусть $f(x_1, \ldots, x_m)$ — некоторая немонотонная симметрическая функция из множества F, такая, что $m > 2n$. Поскольку множество F содержит счётное число попарно неконгруэнтных немонотонных симметрических функций, такая функция существует. Пусть Φ — формула над $\mathfrak{A}$, реализующая функцию f.

Предположим сначала, что $e_f \geqslant n$. Пусть $g_s(x_{i_1}, \ldots, x_{i_{n_s}})$ — простая подформула формулы Φ, $1 \leqslant s \leqslant r$. Рассмотрим набор $\widetilde{\alpha} \in \mathcal{L}(e_f, m-e_f)$, такой, что $\alpha_{i_1} = \ldots = \alpha_{i_{n_s}} = 1$. Поскольку $e_f \geqslant n \geqslant n_s$, такой набор существует. В силу включения $\mathcal{L}(e_f, m-e_f) \subset N_f$ выполняется равенство $f(\widetilde{\alpha}) = 1$. Применяя лемму 1, получаем, что $g_s(1^{n_s}) = g_s(\alpha_{i_1}, \ldots, \alpha_{i_{n_s}}) = 1$. Но по определению множества R выполняется $g_s(1^{n_s}) = 0$. Получили противоречие.

Пусть теперь $e_f < n$. Покажем, что для любого набора $\widetilde{\alpha}$ из $\{1,2\}^m$, такого, что $|\widetilde{\alpha}| \leqslant e_f$, и для любой подформулы Φ_1 формулы Φ выполняется равенство $\Phi_1(\widetilde{\alpha}) = 1$. Доказательство будем проводить индукцией по глубине подформулы Φ_1.

Пусть Φ_1 — простая формула, имеющая вид $g_s(x_{i_1}, \ldots, x_{i_{n_s}})$, $1 \leqslant s \leqslant r$. Без ограничения общности будем считать, что среди переменных $x_{i_1}, \ldots, x_{i_{n_s}}$ встречаются символы $x_1, \ldots, x_t$, и только они. Положим $a = |(\alpha_1, \ldots, \alpha_t)|$, $b = e_f - a$. Определим набор $\widetilde{\beta}$ из $\mathcal{L}(e_f, m-e_f)$ так: $\widetilde{\beta} = (\alpha_1, \ldots, \alpha_t, 1^b, 2^{m-t-b})$. Поскольку $\mathcal{L}(e_f, m-e_f) \subset N_f$, то в силу леммы 1 выполняется равенство $\Phi_1(\widetilde{\beta}) = 1$. Кроме того, из определения набора $\widetilde{\beta}$ следует равенство $\Phi_1(\widetilde{\beta}) = \Phi_1(\widetilde{\alpha})$. Значит, $\Phi_1(\widetilde{\alpha}) = 1$.

Пусть теперь Φ_1 — формула глубины d и Φ_1 имеет вид $g_s(\mathcal{B}_1, \ldots, \mathcal{B}_{n_s})$, где глубина каждой из формул $\mathcal{B}_1, \ldots, \mathcal{B}_{n_s}$ не превосходит $d-1$. Без огранечения общности будем считать, что подформулы $\mathcal{B}_1, \ldots, \mathcal{B}_q$ являются символами переменных, а подформулы $\mathcal{B}_{q+1}, \ldots, \mathcal{B}_{n_s}$ — нетривиальными формулами. По предположению индукции для любой нетривиальной подформулы $\mathcal{B}_t$, $1 \leqslant t \leqslant n_s$, для любого набора $\widetilde{\gamma}$ из $\{1,2\}^m$, такого, что $|\widetilde{\gamma}| \leqslant e_f$, выполняется равенство $\mathcal{B}_t(\widetilde{\gamma}) = 1$. Пусть среди $\mathcal{B}_1, \ldots, \mathcal{B}_q$ встречаются символы переменных $x_1, \ldots, x_t$, и только они. Положим $a = |(\alpha_1, \ldots, \alpha_t)|$, $b = e_f - a$. Определим набор $\widetilde{\beta}$ из $\mathcal{L}(e_f, m-e_f)$ так: $\widetilde{\beta} = (\alpha_1, \ldots, \alpha_t, 1^b, 2^{m-t-b})$. Поскольку $\mathcal{L}(e_f, m-e_f) \subset N_f$, то в силу леммы 1 выполняется равенство $\Phi_1(\widetilde{\beta}) = 1$. Значит, $g_s(\alpha_{i_1}, \ldots, \alpha_{i_q}, 1^{n_s-q}) = 1$. Поскольку наборы $\widetilde{\alpha}$ и $\widetilde{\beta}$ совпадают на первых t компонентах и для любой подформулы $\mathcal{B}_t$, $q < t \leqslant n_s$, для любого набора $\widetilde{\gamma}$ из $\{1,2\}^m$, такого, что $|\widetilde{\gamma}| \leqslant e_f$, выполняется равенство $\mathcal{B}_t(\widetilde{\gamma}) = 1$, то справедливо равенство $\Phi_1(\widetilde{\alpha}) = 1$.

Таким образом, получаем, что для любого набора $\widetilde{\alpha}$, такого, что $|\widetilde{\alpha}| \leqslant e_f$, выполняется равенство $f(\widetilde{\alpha}) = 1$. Поскольку e_f — число единиц в наборе с максимальным числом единиц из N_f, то функция f является монотонной симметрической. Получили противоречие. Следовательно, класс G не имеет конечного базиса. ■

Для доказательства основного результата потребуются также следующие утверждения.

Лемма 6 [9]. Пусть $F \subset \mathrm{S}$, $H \subset R$, $G = [F \cup H]$ и существует такое $n \in \mathbb{Z}^+$, что число существенных переменных у каждой функции из множества H не превосходит n. Тогда если класс G имеет базис, то и класс $[\{f \in F : e_f \geqslant n\}]$ имеет базис.

Лемма 7 [9]. Пусть $F \subset \mathrm{S}$ и существует функция f из F, такая, что $e_f > 0$; $H \subset R$, $G = [F \cup H]$. Пусть существует такое $n \in \mathbb{Z}^+$, что число существенных переменных у каждой функции из множества H не превосходит n. Тогда если класс $[\{f \in F : e_f \geqslant n\}]$ имеет базис, то и класс G имеет базис.

Лемма 8. Пусть $F \subset \mathrm{S}$ и существует функция f из F, такая, что $e_f > 0$; $k \in \mathbb{Z}^+$, H — k-ограниченное множество симметрических функций, $G = [H \cup F]$, $G' = [F]$. Тогда класс G имеет базис в том и только в том случае, когда класс G' имеет базис.

Доказательство. Обозначим через F^+ множество функций f из F, таких, что $e_f > k$. Пусть класс G' (соответственно G) имеет базис. Применяя лемму 6, получаем, что класс $[F^+]$ имеет базис. Далее, применяя лемму 7, получаем, что класс G (соответственно G') имеет базис. ■

Лемма 9 [6]. Пусть $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_m)$ — функции из MS, $n \geqslant m \geqslant 1$. Пусть $e_f < e_g$. Тогда $f \in [\{g\}]$.

Лемма 10. Пусть $k \in \mathbb{N}$, G — некоторое точно k-ограниченное множество попарно неконгруэнтных монотонных симметрических функций, $F = [G]$. Тогда класс F имеет базис, причём базис класса F конечный в том и только в том случае, когда множество $G \cap \mathrm{MS}^k$ конечно.

Доказательство. Положим $G^k = G \cap \mathrm{MS}^k$. Обозначим через n_0 минимальное число существенных переменных у функций из G^k, через f_0 — произвольную функцию из G^k, у которой n_0 существенных переменных, через G^0 — множество функций из G, число существенных переменных у которых не превосходит n_0.

Покажем сначала, что $G \subset [G^k \cup G^0]$. Пусть $f(x_1, \ldots, x_n) \in G$. Если $e_f = k$, то $f \in G^k$. Если $e_f < k$, $n \leqslant n_0$, то $f \in G^0$. Если $e_f < k$ и $n > n_0 > 1$, то в силу леммы 9 выполняется включение $f \in [\{f_0\}]$. Следовательно, $G \subset [G^k \cup G^0]$.

Покажем, что для любой функции $f(x_1, \ldots, x_n)$ из G^k выполняется соотношение $f \notin [(G^k \cup G^0) \backslash \{f\}]$. Предположим, что это не так. Пусть Φ — формула над $(G^k \cup G^0) \backslash \{f\}$, реализующая функцию f. Поскольку для любой функции g из $G^k \cup G^0$ верно неравенство $e_g \leqslant e_f$, то из леммы 3 следует, что формула Φ простая. Следовательно, существует функция $g(x_1, \ldots, x_m)$ из $G^k \cup G^0$, такая, что $f \in [\{g\}]$. Из леммы 3 следует, что $e_g = e_f$ и $e_f/d_f \leqslant e_g/d_g$. Следовательно, $d_g \leqslant d_f$. Поскольку формула Φ простая, то $n \leqslant m$. Кроме того, выполняются равенства $n = e_f + d_f$, $m = e_g + d_g$. Значит, $d_f \leqslant d_g$. Следовательно, $d_f = d_g$. Получаем, что $f \cong g$, что противоречит условию леммы. Поэтому для любой функции f из G^k выполняется соотношение $f \notin [(G^k \cup G^0) \backslash \{f\}]$. Поскольку множество G^0 конечно, существует подмножество H множества G^0, такое, что $[G^0 \cup G^k] = [H \cup G^k]$ и для любой функции g из H выполняется соотношение $g \notin [(H \cup G^k) \backslash \{g\}]$. Значит, класс F имеет базис $H \cup G^k$. Поскольку множество H конечно, класс F имеет конечный базис в том и только в том случае, когда множество G^k конечно. ■

Основные результаты данной работы — критерии базируемости и конечной порождённости для классов, порождённых множествами симметрических функций с ограниченным числом слоёв, — существенно опираются на критерии базируемости и конечной

порождённости для классов, порождённых множествами монотонных симметрических функций и немонотонных симметрических функций с ограниченным числом слоёв по отдельности. Критерий конечной порождённости для классов, порождённых k-ограниченным множеством монотонных симметрических функций, приведён выше (поскольку функции монотонные, то множество функций с ограниченным числом слоёв является k-ограниченным множеством для некоторого k из $\mathbb{Z}^+$). Кроме того, показано, что при $k \geqslant 1$ такие классы всегда имеют базис. Следующая теорема устанавливает, в каких случаях класс, порождённый множеством немонотонных симметрических функций с ограниченным числом слоёв, имеет базис и в каком случае этот базис конечный.

Теорема 1 [7]. Пусть $k \in \mathbb{N}$, G — некоторое множество попарно неконгруэнтных функций из $\mathrm{NS}^{(k)}$, $G^l = G \cap \mathrm{NS}^l$, $H^l = G \cap (\mathrm{NS}^{(k)} \backslash \mathrm{NS}^{(l)})$, $1 \leqslant l \leqslant k$, $F = [G]$. Тогда справедливы следующие утверждения:

1. Класс F имеет конечный базис, если и только если множество G конечно.
2. Класс F имеет счётный базис тогда и только тогда, когда для любого l каждая функция множества $G^l \backslash [H^l]$ содержится в ограниченной максимальной цепи множества $G^l \backslash [H^l]$ относительно порядка $\preceq_{H^l}$.
3. Класс F не имеет базиса тогда и только тогда, когда существует m, $1 \leqslant m \leqslant l$, и существует функция $h \in G^m \backslash [H^m]$, которая не содержится ни в какой ограниченной максимальной цепи множества $G^l \backslash [H^l]$ относительно порядка $\preceq_{H^l}$.

2. Основные результаты

Теорема 2. Пусть $k \in \mathbb{N}$, G — некоторое множество попарно неконгруэнтных функций из $S^{(k)}$, $F = [G]$, множество $G \cap \mathrm{MS}$ является точно l-ограниченным для некоторого $l \in \mathbb{Z}^+$, $l \leqslant k$. Тогда справедливы следующие утверждения.

1. Класс F имеет конечный базис тогда и только тогда, когда множество $G \cap \mathrm{NS}$ конечно и выполняется по крайней мере одно из следующих условий:
   а) класс $[G \cap \mathrm{MS}]$ имеет конечный базис;
   б) существует функция $f \in \langle G \cap (\mathrm{NS}^{(k)} \backslash \mathrm{NS}^{(l-1)}) \rangle$, такая, что для некоторых $e, d \in \mathbb{N}$ выполняется включение $\bigcup\limits_{i=0}^{l} \mathcal{L}(i, d-i) \times (1^e) \subset N_f$.
2. Класс F имеет счётный базис тогда и только тогда, когда класс $[G \cap \mathrm{NS}]$ имеет базис и выполняется по крайней мере одно из следующих условий:
   а) класс $[G \cap \mathrm{NS}]$ имеет счётный базис;
   б) класс $[G \cap \mathrm{MS}]$ имеет счётный базис и не существует функции f из $\langle G \cap (\mathrm{NS}^{(k)} \backslash \mathrm{NS}^{(l-1)}) \rangle$, такой, что для некоторых $e, d \in \mathbb{N}$ выполняется включение $\bigcup\limits_{i=0}^{l} \mathcal{L}(i, d-i) \times (1^e) \subset N_f$.
3. Класс F не имеет базиса тогда и только тогда, когда класс $[G \cap \mathrm{NS}]$ не имеет базиса или G является 0-ограниченным множеством, содержащим счётное число попарно неконгруэнтных функций.

Доказательство. Докажем утверждение 1. Пусть класс F имеет конечный базис $\mathfrak{A}$. В силу леммы 5 множество $G \cap \mathrm{NS}$ конечно. Если класс $[G \cap \mathrm{MS}]$ имеет конечный базис, то первое условие утверждения выполнено. Пусть класс $[G \cap \mathrm{MS}]$ не имеет конечного базиса. Положим $A = G \cap \mathrm{MS}^l$. В силу леммы 10 множество A счётно. Кроме того, из леммы 3 следует, что для любой функции f из A выполняется соотношение $f \notin [A \backslash \{f\}]$. Поскольку базис $\mathfrak{A}$ является конечным, существует конечное

множество $B \subset G$, такое, что $\mathfrak{A} \subset [B]$. Пусть функция f из $\mathfrak{A}$ реализуется формулой Υ_f над B. Обозначим через n_0 максимальное число существенных переменных в функциях из множества B. Поскольку множество A счётно, то существует функция $f(x_1, \ldots, x_n)$ из A, такая, что $n > n_0$. Рассмотрим формулу Φ над $\mathfrak{A}$, реализующую функцию f, и формулу $\pi(\Phi)$ над B, полученную заменой в формуле Φ каждой функции f из базиса $\mathfrak{A}$ на соответствующую подформулу Υ_f. Поскольку $n > n_0$, формула $\pi(\Phi)$ не является простой.

Пусть Φ_1 — подформула формулы $\pi(\Phi)$, имеющая вид $g(\mathcal{B}_1, \ldots, \mathcal{B}_m)$, где g — функция из B, а $\mathcal{B}_1, \ldots, \mathcal{B}_m$ — простые формулы над B или символы переменных из множества $\{x_1, \ldots, x_n\}$. Без ограничения общности будем считать, что $\mathcal{B}_1, \ldots, \mathcal{B}_s$ — символы переменных из множества $\{x_1, \ldots, x_t\}$, $t \leqslant n$, а $\mathcal{B}_{s+1}, \ldots, \mathcal{B}_m$ — простые формулы. Обозначим через $g_1(x_1, \ldots, x_r)$ функцию, которую реализует формула $g(\mathcal{B}_1, \ldots, \mathcal{B}_s, x_{t+1}, \ldots, x_r)$. Очевидно, что $g_1 \in \langle\{g\}\rangle$. Из леммы 1 следует, что множество N_{g_1} содержит все наборы, имеющие вид $(\widetilde{\alpha}, 1^{r-t})$, где $\widetilde{\alpha} \in \mathcal{L}(e, t-e)$, $0 \leqslant e \leqslant l$.

Покажем теперь, что если выполняются условия утверждения 1, то класс F имеет конечный базис. По условию множество $G \cap \mathrm{NS}$ конечно. Если класс $[G \cap \mathrm{MS}]$ имеет конечный базис, то очевидно, что множество F имеет конечный базис. Пусть класс $[G \cap \mathrm{MS}]$ не имеет конечного базиса и существует функция $f \in \langle G \cap (\mathrm{NS}^{(k)} \backslash \mathrm{NS}^{(l-1)})\rangle$, такая, что для некоторых $e, d \in \mathbb{N}$ выполняется включение $\bigcup\limits_{i=0}^{l} \mathcal{L}(i, d-i) \times (1^e) \subset N_f$. Пусть d_0 — максимальное число, такое, что выполняется включение $\bigcup\limits_{i=0}^{d_0} \mathcal{L}(i, d-i) \times (1^e) \subset N_f$. В силу определения множества NS выполняется неравенство $d > d_0$.

Построим сначала функцию $f_1(x_1, \ldots, x_{n_1}) \in [\{f\}]$, такую, что для некоторого $d_1 \leqslant d$, $d_1 \in \mathbb{N}$, выполняется включение $\bigcup\limits_{i=0}^{l} \mathcal{L}(i, d_1 - i) \times (1) \subset N_f$ и существует набор $\widetilde{\alpha} \in \mathcal{L}(l+1, d_1 - l - 1) \times 1$, такой, что $\widetilde{\alpha} \notin N_{f_1}$. Если $d_0 = l$, то функции f и f_1 совпадают. Пусть теперь $d_0 > l$. Без ограничения общности будем считать, что набор $(1^{d_0+1}, 2^{d-d_0-1}, 1^e)$ не содержится в N_f. Тогда

$$f_1(x_1, \ldots, x_{n_1}) = f(\underbrace{x_1, \ldots, x_1}_{d_0-l+1}, x_2, \ldots, x_l, \underbrace{x_{l+1}, \ldots, x_{l+1}}_{e}).$$

Очевидно, что набор $(1^{l+1}, 2^{d_1-l-1}, 1)$ не содержится в N_{f_1}, а все наборы из множества $\bigcup\limits_{i=0}^{l} \mathcal{L}(i, d_1 - i) \times (1)$ содержатся в N_{f_1}.

Построим функцию $f_2(x_1, \ldots, x_{n_1})$, такую, что $\bigcup\limits_{i=0}^{l} \mathcal{L}(i, d_1 - i) \times (1) \subset N_{f_2}$ и для любого набора $\widetilde{\alpha}$ из $\mathcal{L}(l+1, d_1 - l - 1) \times (1)$ набор $\widetilde{\alpha}$ не содержится в N_{f_2}.

Положим $s = C_{d_1}^{l+1}$, $X = \{x_1, \ldots, x_{d_1}\}$. Обозначим через (Y^1, Z^1), (Y^2, Z^2), $\ldots$, (Y^s, Z^s) всевозможные разбиения множества X на помножества, содержащие $l+1$ и $d_1 - l - 1$ элементов соответственно. Пусть $\widetilde{y}^i$ — некоторая фиксированная перестановка переменных из множества Y^i, а $\widetilde{z}^i$ — некоторая фиксированная перестановка переменных из множества Z^i, $i = 1, \ldots, s$. Покажем, что

$$f_2(x_1, \ldots, x_{n_2}) = \underbrace{f_1(\widetilde{y}^1, \widetilde{z}^1, f_1(\widetilde{y}^2, \widetilde{z}^2, f_1(\ldots(f_1}_{s \text{ символов } f_1}(\widetilde{y}^s, \widetilde{z}^s, x_{n_1}\underbrace{)\ldots))}_{s}).$$

Для каждого t, $1 \leqslant t \leqslant s$ определим формулу Φ_t. Положим $\Phi_t = f_1(\widetilde{y}^t, \widetilde{z}^t, u)$. Рассмотрим набор $\widetilde{\alpha}$ из $\{1, 2\}^{n_1 - 1}$. Пусть $a = |\widetilde{\alpha}| \leqslant l$. Поскольку выполняется включение

$\mathcal{L}(a, d_1 - a) \times (1) \subset N_{f_1}$, то для любого i, $1 \leqslant i \leqslant s$, верно равенство $\Phi_i(\widetilde{\alpha}, 1) = 1$. Индукцией по глубине подформулы формулы, реализующей функцию f_2, нетрудно показать, что любая её подформула принимает значение 1 на наборе $(\widetilde{\alpha}, 1)$. Значит, $f_2(\widetilde{\alpha}, 1) = 1$.

Пусть теперь $a = l + 1$. Тогда существует разбиение (Y^p, Z^p), $i \leqslant p \leqslant s$, такое, что все компоненты набора $\widetilde{\alpha}$, соответствующие переменным из множества Y^p, принимают значение 1. Поскольку $f_1(1^{l+1}, 2^{d_1 - l}, 1) = 0$, подформула

$$\underbrace{f_1(\widetilde{y}^p, \widetilde{z}^p, f_1(\widetilde{y}^{p+1}, \widetilde{z}^{p+1}, f_1(\ldots(f_1}_{s-p+1 \text{ символов } f_1}(\widetilde{y}^s, \widetilde{z}^s, x_{n_1})\underbrace{)\ldots))}_{s-p+1}$$

принимает значение 0 на наборе $(\widetilde{\alpha}, 1)$. В силу леммы 1 выполняется равенство $f_2(\widetilde{\alpha}, 1) = 0$.

Пусть $g(x_1, \ldots, x_m)$ — функция из $G \cap \mathrm{MS}^l$, такая, что $m \geqslant d_1$, а $g_1, \ldots, g_r$ — все функции из $G \cap \mathrm{MS}^l$, зависящие от меньшего чем m числа переменных. Покажем, что $G \cap \mathrm{MS}^l \subset [\{g_1, \ldots, g_r, g, f\}]$. Для этого достаточно показать, что для любой функции $h(x_1, \ldots, x_p)$ из M^l, такой, что $p > m$, выполняется соотношение $h \in [\{f_2\} \cup \{g\}]$. Положим $s = C_p^{d_1}$, $X = \{x_1, \ldots, x_p\}$. Обозначим через (Y^1, Z^1), (Y^2, Z^2), $\ldots$, (Y^s, Z^s) всевозможные разбиения множества X на помножества, содержащие d_1 и $p - d_1$ элементов соответственно. Пусть $\widetilde{y}^i$ — некоторая фиксированная перестановка переменных из множества Y^i, а $\widetilde{z}^i$ — некоторая фиксированная перестановка переменных из множества Z^i, $i = 1, \ldots, s$. Покажем, что

$$h(x_1, \ldots, x_p) = \underbrace{f_2(\widetilde{y}^1, \widetilde{z}^1, f_2(\widetilde{y}^2, \widetilde{z}^2, f_2(\ldots(f_2}_{s \text{ символов } f_2}(\widetilde{y}^s, \widetilde{z}^s, g(x_1, \ldots, x_m))\underbrace{)\ldots))}_{s}.$$

Рассмотрим произвольный набор $\widetilde{\alpha}$ из $\{1, 2\}^p$. Пусть $a = |\widetilde{\alpha}| \leqslant l$. Покажем, что для любой подформулы Φ формулы, реализующей функцию h, выполняется равенство $\Phi(\widetilde{\alpha}) = 1$.

Обозначим через Φ_t формулу, имеющую вид

$$\underbrace{f_2(\widetilde{y}^t, \widetilde{z}^t, f_2(\widetilde{y}^{t+1}, \widetilde{z}^{t+1}, f_2(\ldots(f_2}_{s-t+1 \text{ символов } f_2}(\widetilde{y}^s, \widetilde{z}^s, g(x_1, \ldots, x_m))\underbrace{)\ldots))}_{s-t+1}, \quad 1 \leqslant t \leqslant s,$$

а через Φ_{s+1} — формулу $g(x_1, \ldots, x_m)$. Индукцией по t от $s+1$ до 1 нетрудно показать, что для любого набора $\widetilde{\alpha}$ из $\{1, 2\}^p$, такого, что $|\widetilde{\alpha}| \leqslant l$, выполняется $\Phi_t(\widetilde{\alpha}) = 1$.

Пусть теперь $l < a < p - (d_1 - l) - 1$. Без ограничения общности будем считать, что $\widetilde{\alpha} = (1^a, 2^{p-a})$. Рассмотрим разбиение множества X следующего вида: $Y^r = \{x_1, \ldots, x_{l+1},\ x_{p-(d_1-l)+2}, \ldots, x_p\}$, $Z^r = \{x_{l+2}, \ldots, x_{p-(d_1-l)+1}\}$. Рассмотрим подформулу Φ_r. Значение формулы Φ_r на наборе $\widetilde{\alpha}$ совпадает со значением функции f_2 на наборе $(\widetilde{\beta}, 1)$, где $\widetilde{\beta}$ — набор из $\mathcal{L}(l+1, d_1 - l - 1)$. Следовательно, $\Phi_r(\widetilde{\alpha}) = 0$. В силу леммы 1 выполняется равенство $\Phi_1(\widetilde{\alpha}) = 0$.

Пусть теперь $a \geqslant p - (d_1 - l + 1)$. Тогда $|(\alpha_1, \ldots, \alpha_m)| \geqslant m - (d_1 - l + 1)$. Поэтому $g(\alpha_1, \ldots, \alpha_m) = 0$. В силу леммы 1 $\Phi_1(\widetilde{\alpha}) = 0$. Следовательно, формула Φ_1 реализует функцию h.

Таким образом, класс F имеет конечный базис.

Докажем утверждение 2. Пусть класс F имеет счётный базис. Очевидно, что в этом случае множество G счётно. Поскольку $G \subset \mathrm{S}^{(k)}$, существует число $l \leqslant k$, такое, что множество $G \cap \mathrm{MS}$ является l-ограниченным. Из леммы 8 следует, что класс $[G \cap \mathrm{NS}]$ имеет базис. Если множество $G \cap \mathrm{NS}$ счётно, то в силу леммы 5 класс $[G \cap \mathrm{NS}]$ не

имеет конечного базиса, а значит, он имеет счётный базис, и в этом случае утверждение доказано. Пусть множество $G \cap \mathrm{NS}$ конечно. Тогда класс $G \cap \mathrm{MS}$ имеет счётный базис. Если существует функция f, такая, что для некоторых $e, d \in \mathbb{N}$ выполняется включение $\bigcup\limits_{i=0}^{l} \mathcal{L}(i, d-i) \times (1^e) \subset N_f$, то, как показано выше, класс F имеет конечный базис. Следовательно, такой функции не существует.

Пусть выполняется одно из условий утверждения 2. Пусть класс $[G \cap \mathrm{NS}]$ имеет счётный базис. В силу теоремы 1 множество $G \cap \mathrm{NS}$ счётно и в силу леммы 5 класс F не имеет конечного базиса. Поскольку для некоторого $l \leqslant k$ множество $G \cap \mathrm{MS}$ является l-ограниченным, в силу леммы 8 класс F имеет базис. Следовательно, класс F имеет счётный базис.

Пусть теперь множество $G \cap \mathrm{NS}$ конечно. Тогда класс $[G \cap \mathrm{MS}]$ имеет счётный базис. Поскольку для некоторого $l \leqslant k$ множество $G \cap \mathrm{MS}$ является l-ограниченным, применяя лемму 8, получаем, что класс F имеет базис. Предположим, что класс F имеет конечный базис. Выше показано, что в этом случае существует функция f, такая, что для некоторых $e, d \in \mathbb{N}$ выполняется включение $\bigcup\limits_{i=0}^{l} \mathcal{L}(i, d-i) \times (1^e) \subset N_f$. По условию такой функции не существует. Следовательно, класс F имеет счётный базис.

Утверждение 3 следует из справедливости утверждений 1 и 2. ■

ЛИТЕРАТУРА

1. *Post E. L.* Introduction to a general theory of elementary propositions // Am. J. Math. 1921. V. 43. No. 3. P. 163–185.
2. *Post E. L.* The Two-Valued Iterative Systems of Mathematical Logic. Ann. Math. Studies. Princeton Univ. Press, 1941. 122 p.
3. *Янов Ю. И., Мучник А. А.* О существовании k-значных замкнутых классов, не имеющих конечного базиса // ДАН СССР. 1959. Т. 127. № 1. С. 44–46.
4. *Михайлович А. В.* О замкнутых классах трехзначной логики, порожденных симметрическими функциями // Вестн. Моск. ун-та. Матем. Механ. 2008. № 4. С. 54–57.
5. *Михайлович А. В.* О классах функций трехзначной логики, порожденных монотонными симметрическими функциями // Вестн. Моск. ун-та. Матем. Механ. 2009. № 1. С. 33–37.
6. *Михайлович А. В.* О замкнутых классах функций многозначной логики, порожденных симметрическими функциями // Математические вопросы кибернетики. М.: Физматлит, 2013. Вып. 18. С. 123–212.
7. *Михайлович А. В.* О базируемости замкнутых классов функций трехзначной логики, порожденных симметрическими функциями с ограниченным числом слоев // Материалы IX молодежной науч. школы по дискретной математике и её приложениям (Москва, 16–21 сентября 2013 г.). М.: Изд-во ИПМ РАН, 2013. С. 80–85.
8. *Яблонский С. В.* Введение в дискретную математику. М.: Высшая школа, 2001. 384 с.
9. *Михайлович А. В.* О замкнутых классах трехзначной логики, порожденных системами, содержащими симметрические функции // Вестн. Моск. ун-та. Матем. Механ. 2012. № 1. С. 58–62.
10. *Михайлович А. В.* О свойствах замкнутых классов функций трехзначной логики, порожденных симметрическими функциями // Материалы X Междунар. семинара «Дискретная математика и ее приложения» (Москва, 1–6 февраля 2010 г.). М.: Изд-во механико-математического факультета МГУ, 2010. С. 193–196.

REFERENCES

1. *Post E. L.* Introduction to a general theory of elementary propositions. Am. J. Math., 1921, vol. 43, no. 3, pp. 163–185.
2. *Post E. L.* The Two-Valued Iterative Systems of Mathematical Logic. Ann. Math. Studies. Princeton Univ. Press, 1941. 122 p.
3. *Janov Ju. I., Muchnik A. A.* O sushhestvovanii k-znachnyh zamknutyh klassov, ne imejushhih konechnogo bazisa. DAN SSSR, 1959, vol. 127, no. 1, pp. 44–46. (in Russian)
4. *Mikhailovich A. V.* O zamknutyh klassah trehznachnoj logiki, porozhdennyh simmetricheskimi funkcijami. Vestn. Mosk. un-ta. Matem. Mehan., 2008, no. 4, pp. 54–57. (in Russian)
5. *Mikhailovich A. V.* O klassah funkcij trehznachnoj logiki, porozhdennyh monotonnymi simmetricheskimi funkcijami. Vestn. Mosk. un-ta. Matem. Mehan., 2009, no. 1, pp. 33–37. (in Russian)
6. *Mikhailovich A. V.* O zamknutyh klassah funkcij mnogoznachnoj logiki, porozhdennyh simmetricheskimi funkcijami. Matematicheskie voprosy kibernetiki. Moscow, Fizmatlit Publ., 2013, no. 18, pp. 123–212. (in Russian)
7. *Mikhailovich A. V.* O baziruemosti zamknutyh klassov funkcij trehznachnoj logiki, porozhdennyh simmetricheskimi funkcijami s ogranichennym chislom sloev. Materialy IX molodezhnoj nauch. shkoly po diskretnoj matematike i ejo prilozhenijam (Moscow, 16–21 september, 2013). Moscow, IPM RAN Publ., 2013, pp. 80–85. (in Russian)
8. *Jablonskij S. V.* Vvedenie v diskretnuju matematiku. Moscow, Vysshaja Shkola Publ., 2001. 384 p. (in Russian)
9. *Mikhailovich A. V.* O zamknutyh klassah trehznachnoj logiki, porozhdennyh sistemami, soderzhashhimi simmetricheskie funkcii. Vestn. Mosk. un-ta. Matem. Mehan., 2012, no. 1, pp. 58–62. (in Russian)
10. *Mikhailovich A. V.* O svojstvah zamknutyh klassov funkcij trehznachnoj logiki, porozhdennyh simmetricheskimi funkcijami. Materialy X Mezhdunar. seminara «Diskretnaja matematika i ee prilozhenija» (Moscow, 1–6 february, 2010). Moscow, DMM MSU Publ., 2010, pp. 193–196. (in Russian)

УДК 512.625.5

ЭРГОДИЧЕСКИЕ ДИНАМИЧЕСКИЕ СИСТЕМЫ В ДЕКАРТОВОЙ СТЕПЕНИ КОЛЬЦА ЦЕЛЫХ 2-АДИЧЕСКИХ ЧИСЕЛ

В. В. Сопин

Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

Доказывается, что для любого 1-липшицева эргодического отображения $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, где $k > 1$ и $k \in \mathbb{N}$, существуют 1-липшицево эргодическое отображение $G : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$ и два биективных отображения H_k, $T_{k,P}$, что $G = H_k \circ T_{k,P} \circ F \circ H_k^{-1}$ и $F = H_k^{-1} \circ T_{k,P^{-1}} \circ G \circ H_k$.

Ключевые слова: *эргодическая теория, 1-липшицевы сохраняющие меру преобразования, декартово произведение, T-функции.*

DOI 10.17223/20710410/27/3

ERGODIC DYNAMICAL SYSTEMS OVER THE CARTESIAN POWER OF THE RING OF 2-ADIC INTEGERS

V. V. Sopin

Lomonosov Moscow State University, Moscow, Russia

E-mail: VvS@myself.com

It is proved that, for any 1-lipschitz ergodic map $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, where $k > 1$ and $k \in \mathbb{N}$, there are 1-lipschitz ergodic map $G : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$ and two bijections H_k, $T_{k,P}$ such that $G = H_k \circ T_{k,P} \circ F \circ H_k^{-1}$ and $F = H_k^{-1} \circ T_{k,P^{-1}} \circ G \circ H_k$.

Keywords: *ergodic, 1-lipschitz measure-preserving p-adic functions, p-adic analysis, cartesian product, T-functions.*

Введение

T-функция — это такое преобразование двоичных слов в двоичные слова, что каждый i-й бит выходного слова не зависит от бит с номерами $i + 1$, $i + 2$, ... входных слов. Все логические и большинство арифметических операций по модулю 2^n, $n \in \mathbb{N}$, а также их композиции являются T-функциями.

Транзитивные T-функции (последнее означает, что последовательность n-битных слов $w, f(w), f(f(w)), \ldots$ имеет максимально длинный период, т. е. период длины 2^n) являются криптографическими примитивами, так как на их основе можно строить псевдослучайные генераторы с многими важными криптографическими свойствами: высокой линейной сложностью, равномерным распределением подслов и другими, а главное — с хорошим быстродействием, так как T-функции легко программируются.

А. Климов и А. Шамир привлекли внимание мирового криптографического сообщества к T-функциям в своей работе [1], хотя и сами T-функции, и важность их для криптографии были известны значительно ранее (см., например, [2 – 5], где получены критерии транзитивности T-функций). Отметим также, что, как указано в [2, 6], исторически первый критерий транзитивности T-функций (булевых отображений треугольного вида) был известен ещё с 1970-х годов.

Задача описания транзитивных T-функций одной переменной была решена во многом благодаря p-адическому анализу, так как T-функция — это 1-липшицево отображение в 2-адической метрике, а её транзитивность эквивалентна эргодичности [6, 7].

Более формально: рассмотрим $\mathbb{Z}_2^k$, $k \in \mathbb{N}$, — декартову степень кольца целых 2-адических чисел с мерой Хаара μ, нормализованной так, что $\mu(\mathbb{Z}_2^k) = 1$. Везде далее будем рассматривать эргодичность только в классе сохраняющих нормированную меру Хаара отображений.

Отображение $f : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$ называется сохраняющим меру, если $\mu(f^{-1}(S)) = \mu(S)$ для любого измеримого множества $S \subseteq \mathbb{Z}_2^k$.

Сохраняющее меру отображение $g : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$ называется эргодическим, если для любого измеримого множества S из $g^{-1}(S) = S$ следует, что $\mu(S) = 0$ или $\mu(S) = 1$.

В главе 4.6.2 работы [6] описывается способ построения эргодического 1-липшицева отображения на $\mathbb{Z}_2^k$, $k \in \mathbb{N}$, из эргодического 1-липшицева отображения на $\mathbb{Z}_2$. Такой способ часто используется в вычислительной технике, но, очевидно, описывает не весь класс эргодических 1-липшицевых отображений на $\mathbb{Z}_2^k$ (пояснения можно найти в п. 3 данной работы) ввиду их более сложной структуры.

В работе доказано, что любое эргодическое 1-липшицево отображение F на $\mathbb{Z}_2^k$, $k \in \mathbb{N}$, может быть представлено определённым образом через k сохраняющих меру 1-липшицевых отображений на $\mathbb{Z}_2$ и k отображений на $\mathbb{F}_2^k$ (векторном пространстве размерности k над полем из двух элементов), возможно, с помощью некоторого дополнительного преобразования, определяющегося через перестановку степени 2^k. Данный результат представлен в п. 2.

Кроме того, для отображения F существует 1-липшицево эргодическое отображение G на $\mathbb{Z}_2$, что F может быть получено из G двумя преобразованиями, одному из которых также можно поставить в соответствие некоторую перестановку степени 2^k, а второе отвечает за представление вектора длины k из целых 2-адических чисел через целое 2-адическое число. Важно, что верно обратное утверждение для F и G при использовании обратных преобразований к описанным двум. Последний результат содержится в п. 3.

Краткое напоминание о 2-адических числах дано в п. 1.

1. 2-адические числа

Для произвольного ненулевого целого числа a определим $\operatorname{ord}_2 a$ равным кратности вхождения 2 в разложение a на простые сомножители. Для произвольного рационального числа $x = a/b$ положим $\operatorname{ord}_2 x = \operatorname{ord}_2 a - \operatorname{ord}_2 b$.

Определим на $\mathbb{Q}$ норму $\|\cdot\|_2$:

$$\|x\|_2 = \begin{cases} 2^{-\operatorname{ord}_2 x}, \text{ если } x \neq 0, \\ 0, \text{ если } x = 0. \end{cases}$$

Определим расстояние между двумя числами a и b

$$d(a, b) = \|a - b\|_2$$

и тем самым зададим на кольце рациональных чисел метрику. Пополнение метрического пространства $(\mathbb{Q}, d)$ будем называть полем 2-адических чисел и обозначать $\mathbb{Q}_2$.

Множество $\mathbb{Z}_2 = \{x \in \mathbb{Q} : \|x\|_2 \leqslant 1\}$ называется множеством целых 2-адических чисел. Элементы кольца $\mathbb{Z}_2$ называются целыми 2-адическими числами.

Каждому целому 2-адическому числу x можно сопоставить бесконечную последовательность $x_1, x_2, \ldots$ вычетов x_n по модулю 2^n, $0 \leqslant x_n < 2^n$, удовлетворяющих условию $x_{n+1} \equiv x_n \pmod{2^n}$, и это сопоставление взаимно-однозначное. Сложение и умножение целых 2-адических чисел определяется как почленное сложение и умножение таких последовательностей.

Кроме того, каждому целому 2-адическому числу x можно поставить во взаимно-однозначное соответствие ряд

$$\sum_{j=0}^{\infty} \alpha_j 2^j \quad \left(x_n = \sum_{j=0}^{n-1} \alpha_j 2^j \right), \text{ где } \alpha_i \in \{0,1\},\ i \in \mathbb{N}.$$

Будем рассматривать на декартовой степени $\mathbb{Z}_2^k$, $k > 1$, следующую метрику:

$$\|(\sigma_1, \ldots, \sigma_k) - (\delta_1, \ldots, \delta_k)\|_2 = \max\{\|\sigma_i - \delta_i\|_2 : i = 1, \ldots, k\}$$

для любых $\sigma = (\sigma_1, \ldots, \sigma_k), \delta = (\delta_1, \ldots, \delta_k) \in \mathbb{Z}_2^k$.

Определим отображение mod 2^n, $n \in \mathbb{N}$, для любого $x = (x^1, \ldots, x^k) \in \mathbb{Z}_2^k$, $k \in \mathbb{N}$:

$$(x^1, \ldots, x^k) \bmod 2^n = (x_n^1, \ldots, x_n^k) = \left(\sum_{i=0}^{2^{n-1}} \alpha_i^1 2^i, \ldots, \sum_{i=0}^{2^{n-1}} \alpha_i^k 2^i \right).$$

2. Описание через k отображений от одной переменной

Определение 1 [6, 7]. 1-липшицевость $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, $k \in \mathbb{N}$, означает, что

$$\forall x, y \in \mathbb{Z}_2^k \ (\|F(x) - F(y)\|_2 \leqslant \|x - y\|_2),$$

то есть $F(x) \equiv F(x \bmod 2^n) \bmod 2^n$.

Определение 2. Графом 1-липшицева сохраняющего меру отображения $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, $k \in \mathbb{N}$, по модулю 2^n назовём ориентированный граф, вершинами которого являются векторы $(i_1, \ldots, i_k)$, где $i_j \in \{0, \ldots, 2^n - 1\}$, $j = 1, \ldots, k$. Из вершины y идёт дуга в вершину z, если $F(y) \equiv z \bmod 2^n$.

Определение 3. 1-липшицево сохраняющее меру отображение $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, где $k \in \mathbb{N}$, называется транзитивным по модулю 2^n, если граф F по модулю 2^n представляет собой цикл.

Из работ [6, 7] известно, что 1-липшицево сохраняющее меру отображение F на $\mathbb{Z}_2^k$, $k \in \mathbb{N}$, является эргодическим тогда и только тогда, когда оно транзитивно по всем модулям 2^n, $n \in \mathbb{N}$.

Для 1-липшицевых отображений из транзитивности по всем модулям 2^n, $n \in \mathbb{N}$, следует сохранение меры. Кроме того, для сохранения меры 1-липшицевому отображению необходимо и достаточно быть биективным по всем модулям натуральной степени двойки [6, 7].

В работе [6] описывается способ построения 1-липшицева эргодического отображения на $\mathbb{Z}_2^k$, $k > 1$, из 1-липшицева эргодического отображения на $\mathbb{Z}_2$. Однако такой способ описывает не всевозможные такие отображения на $\mathbb{Z}_2^k$ хотя бы из тех соображений, что транзитивность по модулю два 1-липшицева сохраняющего меру отображения $f : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$ предполагает

$$f(0) \bmod 2 = 1 \text{ и } f(1) \bmod 2 = 0,$$

то есть «чётные значения» переводятся отображением f в «нечётные» и наоборот. Предлагаемый в [6] способ разбиения на k координат сохранит данное свойство отображения f в какой-то координате (возможно, в другом разряде, а не нулевом), что, вообще говоря, не предполагает общий случай.

Определим класс отображений $\mathfrak{F}_k$, $k > 1$, как множество всех эргодических 1-липшицевых отображений $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, которые по модулю 2 любой вектор из $\mathbb{F}_2^k$ с $1 \leqslant j \leqslant k$ нулевых координат НЕ переводят в вектор, у которого все эти j координат также нулевые, и выполняется сравнение $F((1,\ldots,1)) \equiv (0,\ldots,0) \pmod 2$.

Класс отображений $\mathfrak{F}_k$ не является пустым для любого $k > 1$, так как содержит по крайней мере те 1-липшицевы эргодические отображения, граф которых по модулю 2 представляет собой следующий цикл: $0, 1, 2, \ldots, 2^k - 1$, где значения разрядов, начиная от нулевого и заканчивая $(k-1)$-м, в двоичном представлении данных чисел рассматриваются как значения соответствующих координат двоичных векторов размерности k.

Принадлежность таких отображений классу $\mathfrak{F}_k$ становится очевидной, если увидеть, что последовательность $0, 1, 2, \ldots, 2^k - 1$ генерируется отображением $x + 1$, и прибавление единицы как раз и означает, что какой-то нулевой разряд станет ненулевым.

Формальное доказательство существования таких отображений будет следовать из теоремы 2 или теоремы 3. В дальнейшем мы увидим, что на самом деле графы 1-липшицевых эргодических отображений по модулю 2 имеют всевозможные циклы.

Теорема 1. Для любых $F \in \mathfrak{F}_k$ и $\sigma = (\sigma_1, \ldots, \sigma_k) \in \mathbb{Z}_2^k$ выполняется

$$F(\sigma) = \sum_{i=1}^{k} f_i(\sigma_i) p_i(\sigma \bmod 2),\ \ f_i : \mathbb{Z}_2 \mapsto \mathbb{Z}_2,\ \ p_i : \mathbb{F}_2^k \mapsto \mathbb{F}_2^k,$$

где f_i — 1-липшицевы сохраняющие меру отображения, у которых граф по модулю 2 есть цикл длины 2, а значения $p_i(\sigma \bmod 2)$, $i = 1, \ldots, k$, такие, что i-я координата равна единице, причём определитель матрицы, составленной из $p_i(\sigma \bmod 2)$, не равен нулю.

Доказательство. Покажем, как можно построить p_i; при этом необходимо помнить, что $f_i(0) \bmod 2 = 1$ и $f_i(1) \bmod 2 = 0$, $i = 1, \ldots, k$, ввиду условия транзитивности по модулю 2.

Пусть вектор $\sigma \bmod 2$ имеет $1 \leqslant j \leqslant k$ каких-то нулевых координат, а отображение $F \bmod 2$ переводит его в другой вектор $\delta = (\delta_1, \ldots, \delta_k)$, у которого не все эти j координат нулевые (такие условия гарантирует принадлежность отображения классу $\mathfrak{F}_k$). Тогда p_i построим следующим образом:

— в случае $\sigma \bmod 2 = (1, \ldots, 1)$ каждому p_i ставим в соответствие вектор с одной единичной координатой на i-м месте;
— иначе
  1) всем $p_i(\sigma \bmod 2)$, кроме одного произвольного $p_l(\sigma \bmod 2)$: $\delta_l = 1$, $\sigma_l = 0$ (такой существует по условию), поставим в соответствие вектор с одной единичной координатой на i-м месте;
  2) $p_l(\sigma \bmod 2)$ поставим в соответствие вектор, у которого единичная координата стоит на l-м месте и на всех тех местах, где δ_m и $\sigma_m \bmod 2$ одновременно равны нулю или единице, $m = 1, \ldots, k$, $m \neq l$.

Очевидно, что построенные $p_i(\sigma \bmod 2)$ удовлетворяют заявленным условиям.

Тем самым доказано равенство

$$F(\sigma) \bmod 2 = \sum_{i=1}^{k} f_i(\sigma_i) p_i(\sigma \bmod 2) \bmod 2$$

для любых 1-липшицевых сохраняющих меру f_i, у которых граф по модулю 2 представляет собой цикл длины 2 ($f_i(0) \bmod 2 = 1$ и $f_i(1) \bmod 2 = 0$, $i = 1, \ldots, k$).

Например, рассмотрим цикл $(0,0); (1,0); (0,1); (1,1)$, тогда

$$\begin{gathered} p_1(0,0) = (1,1);\ p_2(0,0) = (0,1); \\ p_1(1,0) = (1,0);\ p_2(1,0) = (0,1); \\ p_1(0,1) = (1,1);\ p_2(0,1) = (0,1); \\ p_1(1,1) = (1,0);\ p_2(1,1) = (0,1). \end{gathered}$$

Цикл $(0,0); (1,0); (1,1); (0,1)$ представить с линейно независимыми p_1 и p_2 в $\mathbb{F}_2^2$ уже нельзя.

Далее будем строить f_i индукционно по разрядам 2-адических чисел. Опишем переход $n \mapsto n+1$. Рассмотрим два таких произвольных вектора $\sigma = (\sigma_1, \ldots, \sigma_k)$ и $\delta = (\delta_1, \ldots, \delta_k)$, что $F(\sigma) \equiv \delta \pmod{2^{n+1}}$, причём по предположению

$$F(\sigma \bmod 2^n) \equiv \sum_{i=1}^{k} f_i(\sigma_i \bmod 2^n) p_i(\sigma \bmod 2) \equiv \delta \bmod 2^n.$$

Далее

$$\begin{gathered} F(\sigma) - (F(\sigma \bmod 2^n) \bmod 2^n) \equiv \sum_{i=1}^{k} [f_i(\sigma_i) - (f_i(\sigma_i \bmod 2^n) \bmod 2^n)] p_i(\sigma \bmod 2) \equiv \\ \equiv \delta - (\delta \bmod 2^n) \bmod 2^{n+1}. \end{gathered}$$

Матрица из $p_i(\sigma \bmod 2)$ имеет ненулевой определитель, значит, $p_i(\sigma \bmod 2)$ являются базисом в $\mathbb{F}_2^k$. Тогда по вектору $\triangle^n(\delta)$, координаты которого равны соответствующим n-м разрядам координат δ, можно найти единственный вектор $(e_1, \ldots, e_k)$, $e_j \in \{0,1\}$, что

$$(e_1 p_1(\sigma \bmod 2) \oplus \ldots \oplus e_k p_k(\sigma \bmod 2)) = \triangle^n(\delta).$$

Определим

$$f_i(\sigma_i) \bmod 2^{n+1} = f_i(\sigma_i \bmod 2^n) \bmod 2^n + e_i 2^n, \quad i = 1, \ldots, k,$$

и перейдём к пределу по n, который существует ввиду определения 2-адических чисел через вычеты (см. п. 1).

Для полученных f_i выполняется равенство

$$F(\sigma) = \sum_{i=1}^{k} f_i(\sigma_i) p_i(\sigma \bmod 2)$$

для любого $\sigma = (\sigma_1, \ldots, \sigma_k)$ из $\mathbb{Z}_2^k$, так как оно выполняется по любому модулю, равному натуральной степени двойки.

Действительно, если предположить противное, то существует $\xi \in \mathbb{Z}_2^k$, для которого

$$F(\xi) \neq \sum_{i=1}^{k} f_i(\xi_i) p_i(\xi \bmod 2),$$

значит, существует какая-то координата и разряд в этой координате, в котором значения $F(\xi)$ и $\sum\limits_{i=1}^{k} f_i(\xi_i)p_i(\xi \bmod 2)$ отличаются, что приводит к противоречию с их равенством по всем модулям натуральной степени двойки.

По построению полученные f_i, $i = 1, \ldots, k$, 1-липшицевы. Действительно, возьмём произвольные $x, y \in \mathbb{Z}_2$, тогда для $\mathbf{x} = (0, \ldots, 0, x, 0, \ldots, 0)$, $\mathbf{y} = (0, \ldots, 0, y, 0, \ldots, 0) \in \in \mathbb{Z}_2^k$ выполняется

$$\|f_j(x)p_j(\mathbf{x}) - f_j(y)p_j(\mathbf{y}) + \sum_{i=1, i\neq j}^{k} f_i(0)(p_i(\mathbf{x}) - p_i(\mathbf{y}))\|_2 =$$
$$= \|F((0, \ldots, 0, x, 0, \ldots, 0)) - F((0, \ldots, 0, y, 0, \ldots, 0))\|_2 \leqslant \|x - y\|_2.$$

Если $x \equiv y \bmod 2$, то $p_i(\mathbf{x}) = p_i(\mathbf{y})$, $i = 1, \ldots, k$ (см. определение p_i), иначе справедливо $\|x-y\|_2 = 1$; 1 является максимальным возможным значением (см. п. 1), и неравенство превращается в тривиальное.

Отображение f_i сохраняет меру (ввиду 1-липшицевости для этого необходима и достаточна биективность по всем модулям 2^n, $n \in \mathbb{N}$ [6]), так как, предполагая противное, мы не получим транзитивность F по какому-то модулю ввиду того, что если

$$f_i(\sigma_i \bmod 2^n) \equiv f_i(\sigma_i \bmod 2^n + 2^n) \bmod 2^{n+1},$$

то мы не получим всевозможные значения F по модулю 2^{n+1}.

Более того, если при данных p_i, $i = 1, \ldots, k$, i-я координата отображения F выражается только через f_i, то отображение f_i является эргодическим, так как иначе оно не транзитивно по какому-то модулю 2^m. Следовательно, мы также не получим все значения i-й координаты отображения F по этому модулю ввиду того, что тогда граф f_i по модулю 2^m имеет не один цикл и i-я координата $F \bmod 2^m$ принимает только значения вершин какого-то цикла графа f_i по модулю 2^m, в котором не представлены всевозможные значения. ■

Все 1-липшицевы эргодические отображения сопряжены друг с другом [8]. Более подробно об этом можно найти в работах В. Сущанского и его соавторов [9, 10]. Но для описания всего класса 1-липшицевых эргодических отображений из какого-то одного требуется счётное число соответствующих преобразований, вид которых может быть очень сложным [10].

Возьмём произвольное сохраняющее меру 1-липшицево отображение $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, где $k > 1$, и представим всё множество $\mathbb{Z}_2^k$ в виде разбиения на подмножества мощности 2^k следующего вида:

$$\mathcal{F}_k(x_0) = \{x_0, F(x_0), \ldots, F^{2^k-1}(x_0)\}, \quad x_0 \in \mathbb{Z}_2^k \;\; x_0 \equiv (0, \ldots, 0) \bmod 2.$$

Подмножества $\mathcal{F}_k(x_0)$ при различных x_0 не пересекаются ввиду сохранения меры отображением F, так как сохранение меры означает биекцию отображения [6]. А за счёт 1-липшицевости F выполняется

$$F^{2^k}(x_0) = x, \text{ где } x \equiv (0, \ldots, 0) \bmod 2.$$

Преобразование $T_{k,P}$, которому можно поставить в соответствие перестановку P степени 2^k, определяется для любого $x \in \mathbb{Z}_2^k$, где x принадлежит некоторому $\mathcal{F}_k(x_0)$, причём $F^j(x_0) = x$, $j = 0, \ldots, 2^k - 1$, следующим образом:

$$T_{k,P} \circ F(x) = F^{P(j+1)}(x_0).$$

Теорема 2. Для любого эргодического 1-липшицева отображения $F \notin \mathfrak{F}_k$ существуют такие перестановка P степени 2^k и отображение $G \in \mathfrak{F}_k$, что

$$G = T_{k,P} \circ F \text{ и } F = T_{k,P^{-1}} \circ G.$$

Доказательство. Выберем перестановку P вершин на графе F по модулю 2 (данный граф представляет собой цикл ввиду эргодичности F [6, 7]) так, чтобы её цикл принадлежал множеству циклов, полученных рассмотрением графов всех отображений класса $\mathfrak{F}_k$ по модулю 2. Такая перестановка существует, но не единственна.

Рассмотрим отображение $G = T_{k,P} \circ F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$; оно сохраняет меру, так как произвольная перестановка не влияет на свойство сохранения меры; 1-липшицевость отображения G следует из 1-липшицевости F. Напомним, что 1-липшицевость означает $F(x) \equiv F(x \bmod 2^n) \bmod 2^n$ для любых $x \in \mathbb{Z}_2^k$, $n \in \mathbb{N}$.

Так как эргодичность в случае 1-липшицева сохраняющего меру отображения эквивалента транзитивности по любому модулю натуральной степени двойки [6, 7], а произвольная перестановка элементов на графе 1-липшицева сохраняющего меру отображения не влияет на транзитивность этого отображения (цикл останется циклом), то G является эргодическим отображением. Значит, $G \in \mathfrak{F}_k$.

Равенство $F = T_{k,P^{-1}} \circ G$ следует из определения отображения $T_{k,P}$. ■

3. Описание через одно отображение от одной переменной

Определим отображение $H_k : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2$ для любого натурального $k > 1$ следующим образом:

$$H_k\left(\sum_{i=0}^{\infty} \alpha_i^0 2^i, \sum_{i=0}^{\infty} \alpha_i^1 2^i, \ldots, \sum_{i=0}^{\infty} \alpha_i^{k-1} 2^i\right) = \sum_{i=0}^{\infty} \sum_{j=0}^{k-1} \alpha_i^j 2^{ik+j}, \text{ где } \alpha_i^j \in \{0, 1\}.$$

Так как элементы $\mathbb{Z}/2^n\mathbb{Z}$ — кольца вычетов по модулю 2^n, $n \in \mathbb{N}$, — можно рассматривать как элементы $\mathbb{Z}_2$, то для любого 1-липшицева сохраняющего меру отображения $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$ определим также следующие отображения из $(\mathbb{Z}/2^n\mathbb{Z})^k$ в $\mathbb{Z}/2^{kn}\mathbb{Z}$:

$$H_{k,n} = H_k(x_1 \bmod 2^n, \ldots, x_k \bmod 2^n) \text{ и } T_{k,n,P} \circ F(x) = H_{k,n} \circ T_{k,P} \circ F(x).$$

Отметим, что $T_{k,n,P}$ и $H_{k,n}$, $T_{k,P}$ и H_k, очевидно, имеют обратные при любых натуральных k, n и любой перестановки степени 2^k, так как они являются биективными отображениями.

Для любого 1-липшицева сохраняющего меру отображения $G : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$ рассмотрим разбиение $\mathbb{Z}_2$ на непересекающиеся подмножества мощности 2^k следующего вида:

$$\mathcal{G}_k(y_0) = \{y_0, G(y_0), \ldots, G^{2^k-1}(y_0)\},$$

где $y_0 \in \mathbb{Z}_2$, $y_0 \equiv 0 \bmod 2$, k — некоторое натуральное. Тот факт, что это именно разбиение, следует из свойств отображения G и доказывается теми же рассуждениями, что и для $\mathcal{F}_k$. Таким образом, можно определить отображения $T_{k,P}$ и $T_{k,n,P}$ в случае $G : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$.

Теорема 3. Для любого 1-липшицева сохраняющего меру транзитивного по модулю 2 отображения $F : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$, $k > 1$, существуют такие 1-липшицево сохраняющее меру транзитивное по модулю 2^k отображение $G : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$ и перестановка P степени 2^k, что справедливо

$$G = H_k \circ T_{k,P} \circ F \circ H_k^{-1} \quad \text{и} \quad F = H_k^{-1} \circ T_{k,P^{-1}} \circ G \circ H_k,$$

причём F — эргодическое отображение тогда и только тогда, когда G эргодическое.

Доказательство. Возьмём произвольное 1-липшицево сохраняющее меру транзитивное по модулю 2^k отображение на $\mathbb{Z}_2$ и вычислим его цикл C по модулю 2^k.

Выберем такую перестановку P элементов цикла отображения $H_{k,1} \circ F \circ H_{k,1}^{-1}$, чтобы получившийся цикл был равен C.

Для любого натурального n рассмотрим $G_n = T_{k,n,P} \circ F \circ H_{k,n}^{-1}$. Очевидно, G_n можно описать через некоторый граф.

При переходе $n \mapsto n+1$, $n > 1$, каждый цикл графа 1-липшицева сохраняющего меру отображения на $\mathbb{Z}_2^k$ или увеличивает в 2^k раз число своих элементов, или превращается в 2, 4, ..., либо 2^k цикла с одинаковым числом элементов (см. определение 1-липшицевости в п. 2). Каждый цикл графа 1-липшицевых сохраняющих меру отображений на $\mathbb{Z}_2$ при переходе $n \mapsto n+1$, $n > 1$, или увеличивает число своих элементов в 2 раза, или превращается в два цикла с одинаковым числом элементов. Таким образом, существует 1-липшицево сохраняющее меру отображение на $\mathbb{Z}_2$, что его граф по модулю $2^{k(n+1)}$ имеет такое же количество циклов соответствующей длины, что и граф G_{n+1}.

Благодаря преобразованию $T_{k,P}$, которое мы применяем к F, можно утверждать, что граф отображения G_n может быть построен с помощью некоторого 1-липшицева сохраняющего меру отображения $\hat{G}_n$ от одной переменной ввиду $F(x) \equiv \equiv F(x \bmod 2^n) \bmod 2^n$, а значит, $G_{n+1}(y) \equiv G_n(y \bmod 2^{kn}) \bmod 2^{kn}$ (см. определение H_k), так как можно описать таким образом граф G_1 (см. начало доказательства) и соответственно — для всех последующих G_n ввиду того, что при переходе $kn \mapsto k(n+1)$, $n > 1$, старшие k разрядов у вершин графов по модулю 2^{kn+k} всех 1-липшицевых сохраняющих меру отображений от одной переменной принимают всевозможные значения, поэтому можем выбрать подходящее.

Отображение G определяется как предел по n отображений $\hat{G}_n \bmod 2^n$. Предел существует ввиду определения 2-адических чисел через вычеты (см. п. 1).

Свойства 1-липшицевости и сохранения меры G следуют из 1-липшицевости и сохранения меры отображений $\hat{G}_n$, так как 1-липшицевость очевидна (по построению, см. определение 1-липшицевости), для сохранения меры необходима и достаточна биективность по любому модулю натуральной степени двойки в случае 1-липшицевости отображения [6], и биективность по большему модулю означает биективность по меньшему ввиду 1-липшицевости.

Рассмотрим $F_n = T_{k,n,P}^{-1} \circ G \circ H_{k,n}$ и теми же рассуждениями получим некоторое сохраняющее меру 1-липшицево отображение $\tilde{F} : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^k$. Переходя к пределу, построим последовательность векторов с координатами, представляющими собой вычеты по модулю 2^n, а каждая координата ввиду определения 2-адических чисел из п. 1 через вычеты сходится к 2-адическому числу. Значит, предел существует.

Предположим, что $F \neq \tilde{F}$, тогда существует $x \in \mathbb{Z}_2^k$, что $F(x) \neq \tilde{F}(x)$. Отсюда у векторов $F(x)$, $\tilde{F}(x)$ должна существовать координата, в которой они отличаются. Значит, существует разряд $m \in \mathbb{N}$ в этой координате, по которому $F(x)$, $\tilde{F}(x)$ отличаются, что, в свою очередь, приводит к противоречию с равенством $F \bmod 2^n$ и F_n для любого натурального n, так как

$$F_n = T_{k,n,P}^{-1} \circ G \circ H_{k,n}, \quad G \bmod p^{kn} = T_{k,n,P} \circ F \circ H_{k,n}^{-1}.$$

Теми же рассуждениями доказывается, что $F = H_k^{-1} \circ T_{k,P^{-1}} \circ G \circ H_k$ и соответственно $G = H_k \circ T_{k,P} \circ F \circ H_k^{-1}$. Очевидно, что $T_{k,P}^{-1} = T_{k,P^{-1}}$.

Рассмотрим вопрос эргодичности.

Необходимость следует из того, что если F транзитивно по каждому модулю натуральной степени двойки (граф представляет собой один единственный цикл), то транзитивным по этим модулям будет и G по построению (на самом деле по построению следует для 2^{kn} при любом натуральном n, но транзитивность по большему модулю означает транзитивность по всем меньшим ввиду 1-липшицевости), а это и означает эргодичность для 1-липшицевых сохраняющих меру отображений [6].

Действительно, воспользуемся равенством $F \bmod 2^n = T_{k,n,P}^{-1} \circ G \circ H_{k,n}$. Так как произвольная перестановка элементов на графе по некоторому модулю не влияет на свойство транзитивности по этому модулю, то $T_{k,n,P} \circ F \circ H_{k,n}^{-1}$ определяет некоторый цикл. Следовательно, $G \bmod 2^{kn}$ определит тот же цикл.

Достаточность следует из того, что все рассуждения можно повторить в обратную сторону, воспользовавшись равенством $G \bmod 2^{kn} = T_{k,n,P} \circ F \circ H_{k,n}^{-1}$. ■

ЛИТЕРАТУРА

1. *Klimov A. and Shamir A.* Cryptographic applications of T-functions, Selected areas in cryptography // LNCS. 2004. No. 3006. P. 248–261.
2. *Anashin V. S.* Uniformly distributed sequences of p-adic integers // Math. Notes. 1994. V. 55. No. 1–2. P. 109–133.
3. *Anashin V. S.* Uniformly distributed sequences over p-adic integers // Proc. Intern. Conf. “Number Theoretic and Algebraic Methods in Computer Science”, Moscow, Juny–July 1993. World Scientific, 1995. P. 1–18.
4. *Anashin V. S.* Uniformly distributed sequences in computer algebra or how to construct program generators of random numbers // J. Math. Sci. 1998. V. 89. No. 4. P. 1355–1390.
5. *Anashin V. S.* Uniformly distributed sequences of p-adic integers // Discr. Math. Appl. 2002. V. 12. No. 6. P. 527–590.
6. *Anashin V. S. and Khrennikov A. U.* Applied Algebraic Dynamics. Berlin: de Gruyter Expositions in Mathematics, 2009. 558 p.
7. *Anashin V. S., Khrennikov A. U., and Yurova E.* T-functions revisited: new criteria for bijectivity/transitivity // Designs, Codes, and Cryptography. 2014. V. 71. No. 3. P. 383–407.
8. *Durand F. and Paccaut F.* Minimal polynomial dynamics on the set of 3-adic integers // Designs, Codes, and Cryptography. 2009. V. 41. No. 2. P. 302–314.
9. *Slupik A. and Sushchansky V.* Minimal generating sets and Cayley graphs of Sylow p-subgroups of finite symmetric groups // Algebra Discr. Math. 2009. No. 4. P. 167–184.
10. *Lavrenyuk Y. and Sushchansky V.* Automorphisms of homogeneous symmetric groups and hierarchomorphisms of rooted trees // Algebra Discr. Math. 2003. No. 4. P. 33–49.

REFERENCES

1. *Klimov A. and Shamir A.* Cryptographic applications of T-functions, Selected areas in cryptography. LNCS, 2004, no. 3006, pp. 248–261.
2. *Anashin V. S.* Uniformly distributed sequences of p-adic integers. Math. Notes, 1994, vol. 55, no. 1–2, pp. 109–133.
3. *Anashin V. S.* Uniformly distributed sequences over p-adic integers. Proc. Intern. Conf. “Number Theoretic and Algebraic Methods in Computer Science”, Moscow, Juny–July 1993. World Scientific, 1995, pp. 1–18.
4. *Anashin V. S.* Uniformly distributed sequences in computer algebra or how to construct program generators of random numbers. J. Math. Sci., 1998, vol. 89, no. 4, pp. 1355–1390.
5. *Anashin V. S.* Uniformly distributed sequences of p-adic integers. Discr. Math. Appl., 2002, vol. 12, no. 6, pp. 527–590.

6. *Anashin V. S. and Khrennikov A. U.* Applied Algebraic Dynamics. Berlin, de Gruyter Expositions in Mathematics, 2009. 558 p.
7. *Anashin V. S., Khrennikov A. U., and Yurova E.* T-functions revisited: new criteria for bijectivity/transitivity. Designs, Codes, and Cryptography, 2014, vol. 71, no. 3, pp. 383–407.
8. *Durand F. and Paccaut F.* Minimal polynomial dynamics on the set of 3-adic integers. Designs, Codes, and Cryptography, 2009, vol. 41, no. 2, pp. 302–314.
9. *Slupik A. and Sushchansky V.* Minimal generating sets and Cayley graphs of Sylow p-subgroups of finite symmetric groups. Algebra Discr. Math., 2009, no. 4, pp. 167–184.
10. *Lavrenyuk Y. and Sushchansky V.* Automorphisms of homogeneous symmetric groups and hierarchomorphisms of rooted trees. Algebra Discr. Math., 2003, no. 4, pp. 33–49.

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7

ОБ ОЦЕНКЕ ЧИСЛА РАУНДОВ С НЕВОЗМОЖНЫМИ РАЗНОСТЯМИ В ОБОБЩЁННЫХ АЛГОРИТМАХ ШИФРОВАНИЯ ФЕЙСТЕЛЯ

М. А. Пудовкина, А. В. Токтарев

Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия

Исследуется семейство обобщённых алгоритмов шифрования Фейстеля. С использованием методов теории графов и теории чисел получены верхняя и нижняя оценки максимального числа раундов, для которого существуют невозможные разности для любого алгоритма блочного шифрования из семейства.

Ключевые слова: *обобщённый алгоритм шифрования Фейстеля, невозможная разность, число Фробениуса.*

DOI 10.17223/20710410/27/4

BOUNDS FOR THE NUMBER OF ROUNDS WITH IMPOSSIBLE DIFFERENCES IN GENERALIZED FEISTEL SCHEMES

M. A. Pudovkina, A. V. Toktarev

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia

E-mail: maricap@rambler.ru, toktarev@gmail.com

The class of ciphers described by a generalized Feistel scheme is considered. Some upper and lower bounds for the maximum number of rounds with impossible differences are provided. They do not depend on the type of Feistel scheme and on the number of nonlinear functions or blocks in the register.

Keywords: *block cipher, generalized Feistel scheme, impossible differential, differential probability.*

Введение

Обобщённые алгоритмы шифрования Фейстеля представляют естественное обобщение алгоритма шифрования Фейстеля [1, 2]. Они лежат в основе таких шифрсистем, как CAST-256, MARS, SMS4, CLEFIA, Piccolo, HIGHT и др. В основном обобщение осуществляется посредством увеличения числа ячеек регистра сдвига и выбором ячеек, содержимое которых меняется нелинейными функциями усложнения, зависящими от раундового ключа. При этом для обратимости раундовой функции не требуется обратимость нелинейных функций усложнения. Часто для построения функции усложнения используется SP-сеть. В последние годы стали предлагаться модификации

обобщённых алгоритмов шифрования Фейстеля, улучшающие их свойства рассеивания [3 – 5].

Пусть K — ключевое множество; V_n — n-мерное векторное пространство над $\mathrm{GF}(2)$; $g_k^{(r)}$ — раундовая функция зашифрования на ключе $k \in K$; $\oplus$ — бинарная операция покоординатного сложения в V_n. При атаке на l-раундовый n-битный алгоритм блочного шифрования один из этапов разностного метода и его обобщений состоит в нахождении для некоторого числа раундов r, $r \leqslant l$, элементов матрицы $\mathbf{p}^{(r)} = \left(p_{\lambda\lambda'}^{(r)}\right)$ вероятностей переходов ненулевых разностей n-битных блоков текста r-раундовой функции зашифрования, т. е.

$$p_{\lambda\lambda'}^{(r)} = 2^{-n}|K|^{-1}\left|\left\{(x,k) \in V_n \times K : g_k^{(r)}(x) \oplus g_k^{(r)}(x \oplus \lambda) = \lambda'\right\}\right|.$$

Матрица $\mathbf{p}^r$ также называется r-раундовой матрицей вероятностей переходов разностей. Как правило, в разностном методе ищется наибольшее r, при котором существуют $\lambda^{(0)}$, $\lambda^{(r)}$, такие, что $p_{\lambda^{(0)}\lambda^{(r)}}^{(r)} > 2^{-n}$, и при этом r находятся такие $\lambda^{(0)}, \lambda^{(r)}$, для которых $p_{\lambda^{(0)}\lambda^{(r)}}^{(r)}$ принимает максимальное значение. Так как найти точное значение элемента $p_{\lambda^{(0)}\lambda^{(r)}}^{(r)}$ часто не удаётся, приводится нижняя оценка $\widetilde{p}_{\lambda^{(0)}\lambda^{(r)}}^{(r)}$ для $p_{\lambda^{(0)}\lambda^{(r)}}^{(r)} > 2^{-n}$. Для марковских алгоритмов блочного шифрования [6], у которых раундовые функции реализуют одно и то же отображение на декартовом произведении множества n-битных блоков текста и множества раундовых ключей, величина $\widetilde{p}_{\lambda^{(0)}\lambda^{(r)}}^{(r)}$ находится с помощью разностной характеристики последовательности $\bar{\lambda} = \lambda^{(0)}, \lambda^{(1)}, \ldots, \lambda^{(r)}$ n-битных разностей промежуточных блоков текстов, у которой $p_{\lambda^{(i)}\lambda^{(i+1)}}^{(1)} > 0$ для каждого $i \in \{0, \ldots, r-1\}$, при этом полагают $\widetilde{p}_{(\lambda^{(0)}\lambda^{(r)})}^{(r)} = \prod_{i=0}^{(r-1)} p_{\lambda^{(i)}\lambda^{(i+1)}}^{(1)}$.

Для многих алгоритмов блочного шифрования существует такое число раундов $\widetilde{r}$, что матрица $\mathbf{p}^{(r)}$ не является положительной для каждого $r \in \{1, \ldots, \widetilde{r}\}$, т. е. среди элементов матрицы $\mathbf{p}^{(r)}$ есть нулевые. Например, при $r = 1$ такой матрицей является матрица $\mathbf{p}^{(1)}$ алгоритма шифрования Фейстеля.

Равенство $p_{\lambda\lambda'}^{(r)} = 0$ для некоторых ненулевых разностей $\lambda, \lambda' \in V_n$ означает, что ни при каком ключе шифрования $k \in K$ и блоке открытого текста $x \in V_n$ не выполняется равенство $g_k^{(r)}(x) \oplus g_k^{(r)}(x \oplus \lambda) = \lambda'$.

В этом случае пара λ, λ' называется r-раундовой невозможной разностью. Существование невозможной разности может позволить применить атаки различения, а также найти некоторые биты ключа шифрования или весь ключ с помощью метода невозможных разностей, первоначально предложенного в работе [7], а затем модифицированного в [8]. Часто рассматривается такая пара (Λ, Λ') r-раундовых невозможных множеств разностей, что каждая пара $(\lambda, \lambda') \in \Lambda \times \Lambda'$ является r-раундовой невозможной разностью.

При поиске невозможных разностей нередко применяется аналог разностной характеристики. В этом случае рассматривается такая последовательность множеств разностей $\bar{\Lambda} = \Lambda_0, \ldots, \Lambda_r$, что $\Lambda_0 \subset V_n$,

$$\Lambda_i = \{g_{k^{(i)}}(x) \oplus g_{k^{(i)}}(x \oplus \lambda) : (\lambda, x, k^{(i)}) \in \Lambda_{i-1} \times V_n \times K_i\}, i = 1, \ldots, r,$$

где K_i — множество раундовых ключей i-го раунда; $g_{k^{(i)}} : V_n \to V_n$ — раундовая функция на раундовом ключе $k^{(i)} \in K_i$. Если $\Lambda_r \neq V_n \setminus \{\bar{0}_n\}$, то пара $\Lambda_0, V_n \setminus (\Lambda_r \cup \{\bar{0}_n\})$ является r-раундовым невозможным множеством разностей, где $\bar{0}_n$ — нулевой n-мерный вектор.

В данной работе рассматривается семейство обобщённых алгоритмов шифрования Фейстеля. В частности, это семейство включает в себя сбалансированные алгоритмы шифрования, предложенные в работах [1, 2, 5, 9, 10]. Приведены оценки сверху и снизу максимального числа раундов, для которого вероятность любой r-раундовой разности равна нулю для любого алгоритма шифрования из семейства. Предложен подход получения оценок для обобщённого алгоритма шифрования Фейстеля.

В п. 1 приводятся описания рассматриваемых семейств обобщённых алгоритмов шифрования Фейстеля. В п. 2 описаны свойства невозможных разностей и их применения к обобщённым алгоритмам шифрования Фейстеля. Пункт 3 посвящён теоретико-графовым свойствам обобщённых алгоритмов шифрования Фестеля. В п. 4 приведены верхние и нижние оценки максимального числа раундов, для которых существует l-раундовая невозможная разность. Доказательство оценок основано на теории числовых полугрупп.

1. Основные обозначения и определения

1.1. Обозначения

Пусть $\mathbb{N}$ — множество натуральных чисел; $\mathbb{N}_0 = \mathbb{N}\bigcup\{0\}$; $m, d, c \in \mathbb{N}$, $n = dm$; $c \in \{1, \ldots, m\}$; $B^\times = B\backslash\{0\}$ при $B \subseteq V_n$; $W = (A, A')$ — разбиение множества $\{1, \ldots, m\}$ на два подмножества A, A'; $W^{(m)}$ — множество всех упорядоченных разбиений множества $\{1, \ldots, m\}$ на два подмножества; $P(B)$ — множество всех подмножеств множества B; $S(B)$ — множество всех подстановок на B; $k = (k_1, \ldots, k_c) \in V_d^c$; $f_i : V_d^2 \to V_d$, $f_{i,k_i}(\alpha) = f_i(\alpha, k_i)$ для всех $\alpha \in V_d$, $i = 1, \ldots, c$;

$$F_d^{(c)} = \left\{(f_1, \ldots, f_c) : f_i : V_d^2 \to V_d, i = 1, \ldots, c\right\}.$$

Здесь d — число бит в ячейке регистра; m — длина регистра; n — длина блока шифрования; c — количество функций усложнения $f_1, \ldots, f_c$ на одном раунде; $k_1, \ldots, k_c$ — ключи, используемые в этих функциях шифрования.

1.2. Описание обобщённых алгоритмов шифрования Фейстеля

Кроме классического алгоритма шифрования Фейстеля (например, используемого в DES), существуют различные его модификации. Говоря об обобщённых алгоритмах шифрования Фейстеля, будем иметь в виду объединение большинства из них. Некоторые обобщения, например алгоритмы шифрования Фейстеля 1-го, 2-го и 3-го типов, представлены в работе [11]. Блочными шифрсистемами, построенными на основе обобщённых алгоритмов шифрования Фейстеля, являются Skipjack, BEAR/LION, BlowFish, Camelia, DEAL, DES, MARS, Twofish. Обобщённые алгоритмы шифрования Фейстеля с длиной регистра 4 отражены в работе [9]. На рис. 1 изображено 19 обобщённых алгоритмов шифрования Фейстеля с длиной регистра 4.

Приведём описание математической модели, включающей эти обобщения. Рассмотрим семейство алгоритмов шифрования Фейстеля, заданных следующими параметрами: натуральным числом c; разбиением $W = (A, A') \in W^{(m)}$; отображением $\chi : A' \to P(A)$; $f \in F_d^{(c)}$; биективными отображениями $\rho \in S(\{1, \ldots, m\})$, $\varphi : X(A') \to \{1, \ldots, c\}$, где $X(A') = \bigcup\limits_{i \in A', j \in \chi(i)} (i, j)$. Отметим, что для любого A' верно тождество $|X(A')| = c$.

Рассмотрим отображения $v_\rho, h_k \in S(V_d^m)$, определённые как

$$v_\rho : (\alpha_1, \ldots, \alpha_m) \mapsto \left(\alpha_{\rho^{-1}(1)}, \ldots, \alpha_{\rho^{-1}(m)}\right), \quad h_k : (\alpha_1, \ldots, \alpha_m) \mapsto (\alpha'_1, \ldots, \alpha'_m),$$

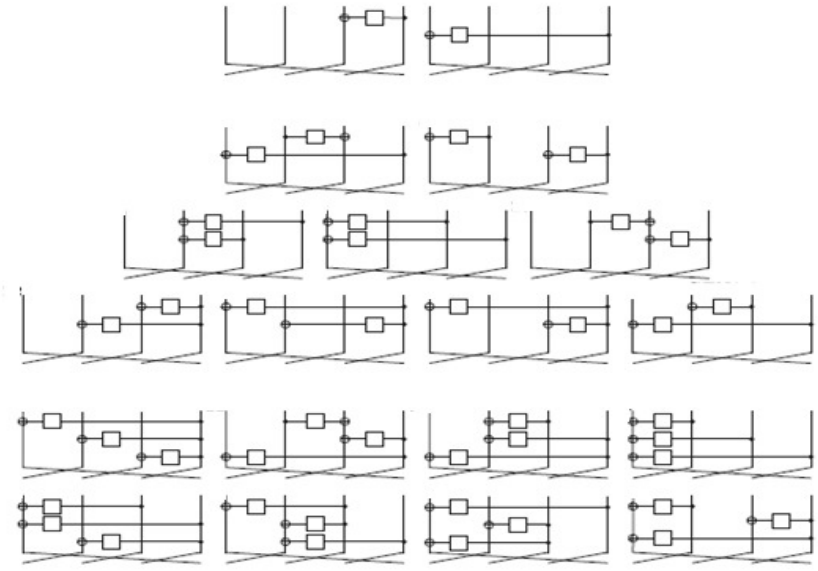


Рис. 1. Раундовые функции обобщённых алгоритмов шифрования Фейстеля с длиной регистра 4

где

$$\alpha'_i = \begin{cases} \alpha_i, & \text{если } i \in A, \\ \alpha_i \bigoplus\limits_{j \in \chi(i)} f_{\varphi(i,j),k_{\varphi(i,j)}}(\alpha_j), & \text{если } i \in A'. \end{cases}$$

Обобщённый алгоритм шифрования Фейстеля задаётся раундовой функцией $g_k \in S(V_d^m)$, где $g_k = v_\rho h_k$. Пусть $g_{k^{(r)}} \dots g_{k^{(1)}}$ — r-раундовая функция шифрования на ключе $k = (k^{(1)}, \dots, k^{(r)}) \in (V_d^c)^r$.

Семейство обобщённых алгоритмов шифрования Фейстеля с фиксированными параметрами $(W, \chi, \varphi, \rho)_c$ будем называть $(W, \chi, \varphi, \rho)_c$-семейством. Каждый алгоритм блочного шифрования из $(W, \chi, \varphi, \rho)_c$-семейства задан фиксированным набором функций $f \in F_d^{(c)}$ и называется $(W, \chi, \varphi, \rho, f)_c$-алгоритмом шифрования. Обозначим через $G_c(W, \chi, \varphi, \rho)$ множество всех $(W, \chi, \varphi, \rho, f)_c$-алгоритмов шифрования.

Будем писать $g \in G_c(W, \chi, \varphi, \rho)$, если g является раундовой функцией $(W, \chi, \varphi, \rho, f)_c$-алгоритма шифрования. Обозначение $g_{k^{(i)}}$ показывает зависимость g от конкретного раундового ключа $k^{(i)}$.

Для нижнего крайнего справа семейства, изображённого на рис. 1, параметры $(W, \chi, \varphi, \rho)_c$-семейства следующие:

$$g_k : (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \mapsto (\alpha_2, \alpha_3 \oplus f_{1,k_1}(\alpha_4), \alpha_4, \alpha_1 \oplus f_{2,k_2}(\alpha_2) \oplus f_{3,k_3}(\alpha_4)),$$

$W = (A, A')$, $A = \{2, 4\}$, $A' = \{1, 3\}$, $\chi(1) = \{2, 4\}$, $\chi(3) = \{4\}$, $\varphi(1, 2) = 1$, $\varphi(1, 4) = 2$, $\varphi(3, 4) = 3$, $\rho = (1, 4, 3, 2)$.

Заметим, что многие обобщённые алгоритмы шифрования Фейстеля основаны на описанной конструкции и ρ^{-1} часто совпадает с циклом $(1, 2, \dots, m)$. Для обобщённых алгоритмов шифрования Фейстеля 1-го типа [12, 13] получаем

$$g_k : (\alpha_1, \dots, \alpha_m) \mapsto (\alpha_2 \oplus f_{1,k_1}(\alpha_1), \alpha_3, \dots, \alpha_m, \alpha_1),$$

где $c = 1$; $A' = \{2\}$; $A = \{1, \ldots, m\} \backslash \{2\}$; $\chi(2) = \{1\}$; $\varphi(2, 1) = 1$ и $\rho^{-1} = (1, 2, \ldots, m)$. Для обобщённых алгоритмов шифрования Фейстеля 2-го типа [11] и чётного числа m получаем

$$g_k : (\alpha_1, \ldots, \alpha_m) \mapsto (\alpha_2 \oplus f_{1,k_1}(\alpha_1), \alpha_3, \alpha_4 \oplus f_{2,k_2}(\alpha_3), \alpha_5, \ldots, \alpha_m, \alpha_1),$$

где $c = m/2$; $A' = \{2i : i \in \{1, \ldots, m/2\}\}$; $A = \{1, \ldots, m\} \backslash A'$; $\chi(2i) = \varphi(2i, i-1) = \{i\}$, $i \in \{1, \ldots, m/2\}$, и $\rho^{-1} = (1, 2, \ldots, m)$. В работе [9] приведены различные классификации обобщённых алгоритмов шифрования Фейстеля для параметров $m = 4$ и $\rho^{-1} = (1, 2, 3, 4)$.

Отметим, что перестановка ρ^{-1} может не совпадать с циклом $(1, 2, \ldots, m)$. Такие перестановки рассмотрены в работах [4, 5]. Например, $\rho^{-1} = (1, 3, 5, 7)(2, 8, 6, 4)$ используется в блочной шифрсистеме Piccolo [4].

2. Невозможные усечённые разности

Существование невозможной разности для r раундов обобщённого алгоритма шифрования Фейстеля означает возможность применения метода невозможных разностей. Для анализа стойкости алгоритма важно оценивать максимальное число раундов, для которого существуют невозможные разности.

Рассмотрим произвольное $(W, \chi, \varphi, \rho)_c$-семейство. Пусть $\alpha^{(0)}$ — n-битный открытый текст, δ — ненулевая n-битная разность. Для $\delta \in V_n^\times$ оценим верхнюю и нижнюю границы числа раундов $r = r_{W,\chi,\varphi,\rho}(\delta)$, удовлетворяющего следующим условиям:

1) для любых $g \in G_c(W, \chi, \varphi, \rho)$, $(k^{(1)}, \ldots, k^{(r)}) \in (V_d^c)^r$, $\alpha^{(0)} \in V_n$ и некоторого $\delta' \in V_n^\times$ выполняется неравенство $g_{k^{(r)}} \ldots g_{k^{(1)}}(\alpha^{(0)}) \oplus g_{k^{(r)}} \ldots g_{k^{(1)}}(\delta \oplus \alpha^{(0)}) \neq \delta'$;
2) для любого $\delta' \in V_n^\times$ существуют $\alpha^{(0)} \in V_n$, $g \in G_c(W, \chi, \varphi, \rho)$, $(k^{(1)}, \ldots, k^{(r+1)}) \in \in (V_d^c)^{r+1}$, удовлетворяющие равенству

$$g_{k^{(r+1)}} \ldots g_{k^{(1)}}(\alpha^{(0)}) \oplus g_{k^{(r+1)}} \ldots g_{k^{(1)}}(\delta \oplus \alpha^{(0)}) = \delta'.$$

Пусть $r_{W,\chi,\varphi,\rho} = \max\{r_{W,\chi,\varphi,\rho}(\delta) : \delta \in V_n^\times\}$ и l — такое произвольное натуральное число, что $l > r_{W,\chi,\varphi,\rho}$. Тогда $r_{W,\chi,\varphi,\rho}$ — максимальное число раундов, для которого не существует невозможной разности для любого l-раундового $(W, \chi, \varphi, \rho, f)_c$-алгоритма шифрования. Другими словами, все элементы его разностной матрицы ненулевые.

Отметим, что если алгоритм шифрования Фейстеля не имеет невозможных разностей на раунде с номером r, то он не имеет невозможных разностей на любом раунде больше r. Действительно, пусть алгоритм шифрования не имеет невозможных разностей на r раундах, а на $(r+1)$-м раунде разность $\alpha \in V_n^\times$ имеет парную невозможную $\beta \in V_n^\times$. Зашифруем два открытых текста с разностью α на ключе $k \in V_d^c$; пусть при этом выходной разностью первого раунда будет $\beta' \in V_n^\times$. Тогда в силу того, что на r раундах невозможных разностей нет, существуют ключи на r раундах шифрования, переводящие блоки с разностью β' в блоки с разностью β. Значит, существуют ключи на $r+1$ раундах шифрования, переводящие блоки с разностью α в блоки с разностью β. Получено противоречие — значит, на $(r+1)$-м раунде также отсутствуют невозможные разности.

Некоторые $(W, \chi, \varphi, \rho)_c$-семейства имеют невозможные разности для любого числа раундов $l \in \mathbb{N}$. Это означает, что для каждого $l \in \mathbb{N}$ существует такая пара $(\delta, \delta') \in \in \left(V_d^\times\right)^2$, что $g_{k^{(l)}} \ldots g_{k^{(1)}}(\alpha^{(0)}) \oplus g_{k^{(l)}} \ldots g_{k^{(1)}}(\delta \oplus \alpha^{(0)}) \neq \delta'$ для любых $g \in G_c(W, \chi, \varphi, \rho)$, $(k^{(1)}, \ldots, k^{(l)}) \in (V_d^c)^l$, $\alpha^{(0)} \in V_n$. В этом случае положим, что $r_{W,\chi,\varphi,\rho} = \infty$. Если $r_{W,\chi,\varphi,\rho}$

конечно, то после некоторого (конечного) числа раундов $(W, \chi, \varphi, \rho)_c$-семейство не имеет невозможных разностей.

Для специального типа обобщённых алгоритмов шифрования Фейстеля в работах [14, 15] для параметра $r_{W,\chi,\varphi,\rho}$ получены различные оценки.

Для получения верхней и нижней оценок параметра $r_{W,\chi,\varphi,\rho}$ используется аддитивная коммутативная полугруппа $(D, \oplus)$, заданная на множестве $D = \{\gamma, \Delta, \tilde{0}\}$. Похожее множество, состоящее из пяти элементов, использовано в [5] для классификации разностей в ячейках регистра обобщённого алгоритма шифрования Фейстеля. Полугруппа $(D, \oplus)$ определена следующим образом:

$\oplus$	γ	Δ	$\tilde{0}$
γ	Δ	Δ	γ
Δ	Δ	Δ	Δ
$\tilde{0}$	γ	Δ	$\tilde{0}$

Для произвольных векторов $\alpha_1 = \left(\alpha_1^{(1)}, \ldots, \alpha_1^{(m)}\right)$, $\alpha_2 = \left(\alpha_2^{(1)}, \ldots, \alpha_2^{(m)}\right)$ из V_d^m обозначим $\alpha_1 \to \alpha_2$, если существуют такие раундовый ключ $k \in V_d^c$ и открытые тексты $x_1, x_2 \in V_d^m$, что $\alpha_1 = x_1 \oplus x_2$, $\alpha_2 = g_k(x_1) \oplus g_k(x_2)$.

Приведём пример, иллюстрирующий построение невозможных усеченных разностей на основе введёной полугруппы. Рассмотрим обобщённый алгоритм шифрования Фейстеля, заданный как $g_k : (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \mapsto (\alpha_2, \alpha_3 \oplus f_{1,k}(\alpha_4), \alpha_4, \alpha_1)$.

Приведём 14-раундовую усеченную разность:

$$(\tilde{0}, \tilde{0}, \gamma, \tilde{0}) \to (\tilde{0}, \gamma, \tilde{0}, \tilde{0}) \to (\gamma, \tilde{0}, \tilde{0}, \tilde{0}) \to (\tilde{0}, \tilde{0}, \tilde{0}, \gamma) \to (\tilde{0}, \Delta, \gamma, \tilde{0}) \to$$
$$\to (\Delta, \gamma, \tilde{0}, \tilde{0}) \to (\gamma, \tilde{0}, \tilde{0}, \ \Delta) \to (\tilde{0}, \Delta, \Delta, \gamma) \to (\Delta, \Delta, \gamma, \tilde{0}) \to (\Delta, \gamma, \tilde{0}, \Delta) \to$$
$$\to (\Delta, \gamma, \Delta, \Delta) \to (\gamma, \Delta, \Delta, \Delta) \to (\Delta, \Delta, \Delta, \gamma) \to (\Delta, \Delta, \gamma, \Delta) \to (\Delta, \Delta, \Delta, \Delta).$$

Очевидно, что максимальное число раундов, для которого существует невозможная разность, зависит от входной разности. Покажем, что максимальное число раундов достигается, если у входной разности существует ненулевая координата.

Рассмотрим $(W, \chi, \varphi, \rho)_c$-семейство, s — номер раунда, x_1, x_2 — md-битные открытые тексты, $x_i = \left(x_i^{(1)}, \ldots, x_i^{(m)}\right) \in V_d^m$, где $i \in \{1, 2\}$. Обозначим

$$x_i^{(s)} = \left(x_i^{(1,s)}, \ldots, x_i^{(m,s)}\right) = g_{k^{(s)}} g_{k^{(s-1)}} \ldots g_{k^{(1)}} \left(x_i^{(1)}, \ldots, x_i^{(m)}\right),$$

где $x_i^{(s)}$ — шифртекст после s раундов шифрования; $k^{(1)}, \ldots, k^{(s)}$ — раундовые ключи из V_d^c. Пусть E — множество всех отображений из V_d^2 в V_d.

Определим отображение $\lambda : V_d^m \times V_d^m \times \mathbb{N} \to D^m$, где $\lambda(x_1, x_2, s) = \left(l^{(1,s)}, \ldots, l^{(m,s)}\right)$;

$$l^{(i,s)} = \begin{cases} \tilde{0}, & \text{если } \forall k^{(1)}, \ldots, k^{(s)} \in V_d^c, \varepsilon_1, \ldots, \varepsilon_c \in E \left(x_1^{(i,s)} = x_2^{(i,s)}\right), \\ \gamma, & \text{если } \forall k^{(1)}, \ldots, k^{(s)} \in V_d^c, \varepsilon_1, \ldots, \varepsilon_c \in E \left(x_1^{(i,s)} \neq x_2^{(i,s)}\right), \\ \Delta, & \text{если } \forall z \in V_d^c \, \exists k^{(1)}, \ldots, k^{(s)} \in V_d^c, \varepsilon_1, \ldots, \varepsilon_c \in E \left(x_1^{(i,s)} \oplus x_2^{(i,s)} = z\right). \end{cases}$$

Отметим, что $\lambda(x_1, x_2, s)$ определяет усечённую разность s-го раунда. Пусть

$$\Theta_{x_1,x_2,s} = \left\{i \in \{1, \ldots, m\} : l^{(i,s)} \in \left\{\tilde{0}, \gamma\right\}\right\},$$
$$\Psi_{x_1,x_2,s} = \left\{i \in \{1, \ldots, m\} : l^{(i,s)} = \Delta\right\},$$
$$\Upsilon_{x_1,x_2,s} = \left\{i \in \{1, \ldots, m\} : l^{(i,s)} \neq \tilde{0}\right\}.$$

Следующая лемма отражает важный факт об упомянутых выше множествах.

Зафиксируем произвольные числа $i \in \{1, \ldots, m\}$, $s \in \mathbb{N}$ и ненулевой вектор $\alpha \in V_d$.

Лемма 1. Пусть x_1, x_2, y_1, y_2 — такие md-битные тесты, что

$$x_1 \oplus x_2 = \left(0, \ldots, 0, \underbrace{\alpha}_{i}, 0, \ldots, 0\right) \in V_d^m, \quad y_1 \oplus y_2 = (\beta_1, \beta_2, \ldots, \beta_m) \in V_d^m,$$

где β_{j_1}, β_{j_2} — ненулевые d-битные векторы для некоторых $j_1, j_2 \in \{1, \ldots, m\}$, $j_1 \neq j_2$. Тогда имеют место включения $\Upsilon_{x_1,x_2,s} \subseteq \Upsilon_{y_1,y_2,s}$, $\Theta_{y_1,y_2,s} \subseteq \Theta_{x_1,x_2,s}$, $\Psi_{x_1,x_2,s} \subseteq \Psi_{y_1,y_2,s}$.

Доказательство. Проводится по индукции относительно числа s и числа ненулевых элементов среди $\beta_1, \ldots, \beta_m$ и представляет собой перебор всевозможных вариантов и проверку условия включения. ■

Утверждение 1. Пусть $i \in \{1, \ldots, m\}$ и векторы

$$\delta = (\bar{0}_d, \ldots, \bar{0}_d, \delta_i, \bar{0}_d, \ldots, \bar{0}_d), \quad \delta' = (\delta'_1, \delta'_2, \ldots, \delta'_{m-1}, \delta'_m)$$

таковы, что $\delta_i \neq \bar{0}_d$, $\delta'_{j_1} \neq \bar{0}_d$, $\delta'_{j_2} \neq \bar{0}_d$ для некоторых $j_1, j_2 \in \{1, \ldots, m\}$, $j_1 \neq j_2$. Тогда $r_{W,\chi,\varphi,\rho}(\delta') \leqslant r_{W,\chi,\varphi,\rho}(\delta)$ для любого $(W, \chi, \varphi, \rho)_c$-семейства.

Доказательство. Пусть $r_1 = r_{W,\chi,\varphi,\rho}(\delta) + 1$, $r_2 = r_{W,\chi,\varphi,\rho}(\delta')$, $x_2 = x_1 \oplus \delta'$. Из леммы 1 следует, что $|\Theta_{x_1,x_2,r_1}| = 0$, но $|\Theta_{x_1,x_2,r_2}| > 0$. Таким образом, $r_{W,\chi,\varphi,\rho}(\delta) + 1 > r_{W,\chi,\varphi,\rho}(\delta')$. Отсюда $r_{W,\chi,\varphi,\rho}(\delta) \geqslant r_{W,\chi,\varphi,\rho}(\delta')$. ■

Утверждение 2. Пусть $i \in \{1, \ldots, m\}$, $\alpha \in V_d^\times$ и $\delta = \left(0, \ldots, 0, \underbrace{\alpha}_{i}, 0, \ldots, 0\right) \in V_d^m$.

Тогда для любого $(W, \chi, \varphi, \rho)_c$-семейства справедливо равенство $r_{W,\chi,\varphi,\rho} = r_{W,\chi,\varphi,\rho}(\delta)$.

Таким образом, для нахождения нижней границы параметра $r_{W,\chi,\varphi,\rho}$ следует рассматривать только разности с ровно одной ненулевой координатой.

3. Представление обобщённого алгоритма шифрования Фейстеля в виде орграфа

Для заданного $(W, \chi, \varphi, \rho)_c$-семейства рассмотрим ориентированный помеченный граф $\Gamma_{W,\chi,\varphi,\rho} = (X, Y)$ с множествами вершин X и дуг Y. Между вершинами орграфа $\Gamma_{W,\chi,\varphi,\rho}$ и ячейками регистров обобщённого алгоритма шифрования Фейстеля существует взаимно однозначное соответствие. Каждая вершина имеет такой же номер, как соответствующая ячейка регистра. Вершины с номерами i и j соединены дугой, если значение регистровой ячейки с номером j зависит от значения в регистровой ячейке с номером i после одного раунда зашифрования, другими словами, если верно одно из следующих условий:

1) $\rho(i) = j$;
2) $i \in A$ и существует $l \in A'$, такое, что $i \in \chi(l)$, $\rho(l) = j$.

Если выполнено первое условие, то дуга не имеет метки; иначе дуга помечена меткой Ф.

Приведём пример орграфа, соответствующего некоторому обобщённому алгоритму шифрования Фейстеля. Рассмотрим обобщённый алгоритма шифрования Фейстеля вида $g_k : (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \mapsto (\alpha_2, \alpha_3 \oplus f_{1,k}(\alpha_4), \alpha_4, \alpha_1)$. Он принадлежит $(W, \chi, \varphi, \rho)_c$-семейству с параметрами

$$W = (A, A'), A = \{1, 2, 4\}, A' = \{3\}, \chi(3) = \{4\}, \varphi(3, 4) = 1, \rho = (1, 4, 3, 2).$$

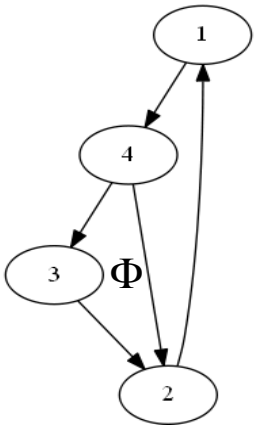


Рис. 2. Орграф обобщённого алгоритма шифрования Фейстеля

Соответствующий орграф представлен на рис. 2.

Напомним некоторые определения из теории графов. Маршрут в графе (орграфе) из вершины i в вершину j — это последовательность вершин и рёбер (дуг), инцидентных двум соседним вершинам; путь — это ориентированный маршрут; длина пути — количество дуг в нём; замкнутый путь — это путь, у которого первая и последняя вершины совпадают; простой путь — это путь без повторяющихся вершин; орцепь — путь без повторяющихся дуг; простая орцепь — орцепь без повторяющихся вершин; контур — замкнутая орцепь; простой контур — контур без повторяющихся вершин. Максимальный кратчайший путь между вершинами орграфа Γ называется диаметром и обозначается $\mathrm{d}(\Gamma)$. Примитивным орграфом называется такой сильносвязный орграф, что наибольший общий делитель длин всех его простых контуров равен 1. Для произвольного замкнутого пути w через $\mathrm{len}(w)$ обозначим его длину.

4. Числовые полугруппы с порождающими элементами и оценки

Пусть M — полугруппа с элементами из $\mathbb{N}_0$, замкнутая относительно операции сложения. Числовую полугруппу, порождённую элементами $d_1, \ldots, d_v \in \mathbb{N}$, определим как $M = \langle d_1, \ldots, d_v \rangle = \left\{ \sum\limits_{i=1}^{v} n_i d_i : n_i \in \mathbb{N}_0 \right\}$. Наибольшее целое число, которое не принадлежит числовой полугруппе M, называется числом Фробениуса полугруппы M.

Пусть U — множество всех числовых полугрупп, $g(S)$ — число Фробениуса полугруппы $S \in U$.

4.1. Построение множества порождающих элементов числовой полугруппы для каждой вершины примитивного орграфа $\Gamma_{W,\chi,\varphi,\rho}$

Оценки максимального числа раундов $r_{W,\chi,\varphi,\rho}$, для которого существуют невозможные разности для любого алгоритма шифрования Фейстеля из $(W, \chi, \varphi, \rho)_c$-семейства, получены с использованием максимального числа Фробениуса числовых полугрупп, соответствующих вершинам орграфа $\Gamma_{W,\chi,\varphi,\rho}$ обобщённого алгоритма шифрования Фейстеля.

Алгоритм состоит из двух шагов. На первом шаге для каждой вершины орграфа $\Gamma_{W,\chi,\varphi,\rho}$ находятся порождающие элементы соответствующей ей полугруппы. На втором шаге определяются числа Фробениуса для найденных числовых полугрупп. Затем выбирается максимальное из полученных чисел Фробениуса.

Пусть V — множество номеров вершин орграфа $\Gamma_{W,\chi,\varphi,\rho}$; C_i — множество его простых контуров, содержащих вершину с номером $i \in V$.

Для любой вершины с номером $i \in \{1, \ldots, m\}$ и простого контура $w \in C_i$ через $C_{i,w}$ обозначим множество простых контуров, принадлежащих целиком какому-либо маршруту с началом в вершине i и второй вершиной, принадлежащей контуру w.

Алгоритм 1. Алгоритм нахождения максимального числа Фробениуса

Вход: орграф $\Gamma_{W,\chi,\varphi,\rho}$

Выход: $g_{\max}$; множества $G(i,w)$, $G(i,w,d)$ для всех вершин $i \in \{1,\ldots,m\}$ и контуров $w \in C_i$, $d \in C_{i,w}$

1: **Для** каждой вершины $i \in V$

2: Найти все простые контуры из C_i.

3: **Для** каждого простого контура $w \in C_i$

4: $s := w$, $C_{i,w} := \{w\}$, $G(i,w,w) := \{\mathrm{len}(w)\}$.

5: **Для** каждой вершины j, принадлежащей контуру s (за исключением вершины i)

6: Найти все простые контуры (исключая s), которые содержат вершину j, но не содержат вершину i, и поместить их в множество C'_j.

7: Если $C'_j \neq \varnothing$, то добавить все элементы множества C'_j в $C_{i,w}$.
Вычислить множество

$$G(i,w,s') = \bigcup_{d \in G_{i,w,s}} \left\{ d + \sum_{s \in C'_j} m_i \cdot \mathrm{len}(s) : 0 \leqslant m_i < d \right\}.$$

8: **Для** каждого простого контура $s' \in C'_j$ положить $s := s'$ и повторить шаги 5–7.

9: Вычислить множество $G(i,w) = \bigcup\limits_{d \in C_{i,w}} G(i,w,d)$.

10: **Для** каждой вершины с номером $i \in V$ вычислить число Фробениуса полугруппы $\left\langle \bigcup\limits_{w \in C_i} G(i,w) \right\rangle$.

11: Найти максимальное из чисел Фробениуса, вычисленных на шаге 10, и обозначить его $g_{\max}$.

Приведём пример нахождения $g_{\max}$ для обобщённого алгоритма шифрования Фейстеля с раундовой функцией $g_k : (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \mapsto (\alpha_2, \alpha_3, \alpha_4, \alpha_1 \oplus f_{1,k}(\alpha_4))$, которая принадлежит $(W, \chi, \varphi, \rho)_c$-семейству с параметрами $W = (A, A')$, $A = \{2,3,4\}$, $A' = \{1\}$), $\chi(1) = \{4\}$, $\varphi(1,4) = 1$, $\rho = (1,4,3,2)$. Соответствующий орграф представлен на рис. 3.

Прокомментируем работу алгоритма. Заметим, что орграф на рис. 3 содержит два простых контура. Первый из них (w_1) содержит все вершины из множества $\{1,2,3,4\}$; второй (w_2) — одну вершину 4. Приведём шаги работы алгоритма.

1–2. $C_1 = C_2 = C_3 = \{w_1\}$, $C_4 = \{w_1, w_2\}$.

3. Для каждой вершины $i \in \{1,2,3\}$ и контура w_1 применим шаги 4–9 и получим $C_{1,w_1} = C_{2,w_1} = C_{3,w_1} = \{w_2\}$, $G(1,w_1) = G(2,w_1) = G(3,w_1) = \{4,5,6,7\}$.
Для вершины 4 и циклов w_1, w_2 применим шаги 4–9 и получим $C_{4,w_1} = \varnothing$, $C_{4,w_2} = \varnothing$, $G(4,w_1) = \{4\}$, $G(4,w_2) = \{1\}$.

10. Получим

$$\left\langle \bigcup_{d \in C_1} G(1,d) \right\rangle = \left\langle \bigcup_{d \in C_2} G(2,d) \right\rangle = \left\langle \bigcup_{d \in C_3} G(3,d) \right\rangle = \langle 4,5,6,7 \rangle, \left\langle \bigcup_{d \in C_4} G(4,d) \right\rangle = \langle 1,4 \rangle.$$

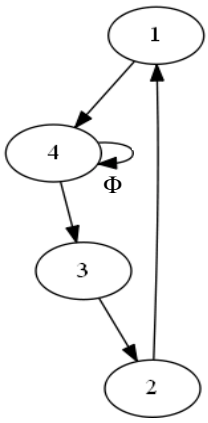


Рис. 3. Орграф обобщённого алгоритма шифрования Фейстеля

Числа Фробениуса полученных числовых полугрупп:

$$g(\langle 4,5,6,7\rangle)=3,\quad g(\langle 1,4\rangle)=0.$$

11. $g_{\max}=3$.

4.2. Оценки максимального числа раундов $r_{W,\chi,\varphi,\rho}$

Приведём необходимое и достаточное условие конечности параметра $r_{W,\chi,\varphi,\rho}$. Для этого сформулируем и докажем ряд лемм и утверждение. Для формулировок нам потребуются следующие обозначения.

Пусть r — номер раунда и $\alpha=\left(\alpha^{(1)},\ldots,\alpha^{(m)}\right)\in V_d^m$. Зададим такое отображение $\theta: V_d\to D$, что для любой d-битной разности δ имеет место

$$\theta(\delta)=\begin{cases}\gamma, & \text{если } \delta\neq\bar{0}_d,\\ \tilde{0}, & \text{если } \delta=\bar{0}_d.\end{cases}$$

Для входной разности $\alpha=\left(\alpha^{(1)},\ldots,\alpha^{(m)}\right)\in V_d^m$ зададим отображение $\xi: V_d^m\times\mathbb{N}\to$ $\to D^m$ как

$$\xi(\alpha,r)=(t_1,\ldots,t_m)=\begin{cases}\lambda(\alpha,\bar{0}_{md},r), & \text{если } r>0,\\ \left(\theta\left(\alpha^{(1)}\right),\ldots,\theta\left(\alpha^{(m)}\right)\right), & \text{если } r=0.\end{cases}$$

Рассмотрим ориентированный помеченный орграф $\Gamma_{W,\chi,\varphi,\rho,\alpha,r}=(V,R,\upsilon)$, соответствующий $(W,\chi,\varphi,\rho)_c$-семейству, где $V=\{v_1,\ldots,v_m\}$ — упорядоченное и пронумерованное множество вершин; R — множество дуг. Отображение $\upsilon: V\to D$ задаёт соответствие множеств вершин и меток и действует на V как $\upsilon(v_i)=t_i$. Заметим, что любой орграф $\Gamma_{W,\chi,\varphi,\rho,\alpha,r}$ имеет те же множества вершин и дуг, что и орграф $\Gamma_{W,\chi,\varphi,\rho}$, но метки его вершин зависят от параметров α и r.

Лемма 2. Для любых таких чисел $s,v\in\mathbb{N}$, $d_1,\ldots,d_v\in\mathbb{N}$, что $(s,d_1,\ldots,d_v)=1$, и числовой полугруппы $M=\langle d_1,\ldots,d_v\rangle$ положим

$$G(s,d_1,\ldots,d_v)=\left\{s+\sum_{i=1}^{v}m_id_i:0\leqslant m_i<s\right\},\quad I(M,s)=\left\{s+\sum_{i=1}^{v}n_id_i:n_i\in\mathbb{N}\right\}\bigcup\{0\}.$$

Тогда $I(M,s)=\langle G(s,d_1,\ldots,d_v)\rangle$.

Доказательство. Любой элемент из $I(M,s)$ может быть представлен как

$$s + d_1u_1 + \ldots + d_vu_v,$$

где $u_1, \ldots, u_v \in \mathbb{N}_0$. Рассмотрим два случая:

1) $u_1 = \ldots = u_v = 0$;

2) существует такое натуральное число j, что $1 \leqslant j \leqslant v$ и $u_j \neq 0$.

Пусть $u_1 = \ldots = u_v = 0$. Тогда $I(M,s) = \{s, 0\}$ и имеет место включение $I(M,s) \subseteq$ $\subseteq G(s, d_1, \ldots, d_v)$.

Пусть существует такое число $j \in \{1, \ldots, v\}$, что $u_j \neq 0$. Положим $\{m_1, \ldots, m_r\} =$ $= \{u_j : 0 < u_j < s, j \in \{1, \ldots, v\}\}$, а соответствующие коэффициенты из $\{d_1, \ldots, d_v\}$ обозначим как $d_m^{(1)}, \ldots, d_m^{(r)}$. Аналогично положим

$$\{h_1, \ldots, h_w\} = \{u_j : u_j \geqslant s, j \in \{1, \ldots, v\}\},$$

а соответствующие коэффициенты из $\{d_1, \ldots, d_v\}$ обозначим $d_h^{(1)}, \ldots, d_h^{(r)}$. Ясно, что каждое число из $\{h_1, \ldots, h_w\}$ представимо как $h_i = k_i s + m_h^{(i)}$, где $k_i > 0$; $0 \leqslant m_h^{(i)} < s$ для любого $i \in \{1, \ldots, w\}$. Таким образом,

$$\begin{aligned} s + d_1u_1 + \ldots + d_vu_v &= s + \sum_{i=1}^{r} d_m^{(i)} m_i + \sum_{i=1}^{w} d_h^{(i)} h_i = \\ &= s + \sum_{i=1}^{r} d_m^{(i)} m_i + \sum_{i=1}^{w} \left(s + d_h^{(i)} m_h^{(i)} \right) + \sum_{i=1}^{w} (k_i - 1)s. \end{aligned}$$

Значит, $I(M,s) \subseteq \langle G(s, d_1, \ldots, d_v) \rangle$. Доказательство включения $\langle G(s, d_1, \ldots, d_v) \rangle \subseteq$ $\subseteq I(M,s)$ очевидно. ■

Имеет место следующая

Лемма 3. Длина замкнутого пути w представима в виде суммы длин простых контуров (не обязательно различных), все дуги и вершины которых принадлежат этому пути.

Лемма 4. Для любых $i \in \{1, \ldots, m\}$, простого контура w, проходящего через вершину с номером i, простого контура $d \in C_{i,w}$ и $g \in G(i, w, d)$ существует замкнутый путь длины g с началом и концом в вершине с номером i, где множества $C_{i,w}$ и $G(i, w, d)$ — результаты работы алгоритма 1.

Доказательство. Для любых простых контуров w, d и вершины i, принадлежащей контуру w, множество $G(i, w, d)$ образовано путём последовательного обхода простых контуров, начиная с вершины i. Значит, для любого $g \in G(i, w, d)$ существует такая последовательность простых контуров w,s_1, …, s_k, d, что существует замкнутый маршрут с началом в вершине i, содержащий только эти контуры (возможно, многократно). ■

Лемма 5. Пусть орграф $\Gamma_{W,\chi,\varphi,\rho}$ примитивен и $\alpha = \left(0, \ldots, 0, \underbrace{\alpha^{(i)}}_{i}, 0, \ldots, 0\right) \in V_d^m$. Тогда в орграфе $\Gamma_{W,\chi,\rho,\alpha,r}$ метка вершины i не равна $\tilde{0}$ тогда и только тогда, когда $r \in \left\langle \bigcup\limits_{d \in C_i} G(i,d) \right\rangle$, где множество $G(i,d)$ — выход алгоритма 1.

Доказательство. Опишем процесс образования орграфа $\Gamma_{W,\chi,\rho,\alpha,r+1}$ из орграфа $\Gamma_{W,\chi,\rho,\alpha,r}$.

Зафиксируем вершину с номером j. Рассмотрим все дуги (пусть их число равно $t \in \{1,\dots,m\}$) с концом в вершине j. Пусть номера вершин, являющихся началом этих дуг, образуют множество $U = \{u_1,\dots,u_t\}$ и в графе $\Gamma_{W,\chi,\rho,\alpha,r}$ каждая вершина из множества U с номером u_k, $1 \leqslant k \leqslant t$, помечена меткой $v_k \in D$. Тогда метка вершины j в графе $\Gamma_{W,\chi,\rho,\alpha,r+1}$ равна $\bigoplus\limits_{i=1}^{t} v_i$. Значит, в орграфе $\Gamma_{W,\chi,\rho,\alpha,r}$ метка вершины i не равна $\tilde{0}$ тогда и только тогда, когда r — длина замкнутого пути, проходящего через вершину i. Рассмотрим такой произвольный замкнутый путь w, что вершина i находится только в начале и конце этого пути.

Из лемм 2 и 3 следует, что длина любого замкнутого пути, проходящего через вершину i, принадлежит множеству $P = \left\langle \bigcup\limits_{d \in C_i} G(i,d) \right\rangle$.

Рассмотрим произвольный элемент p множества P. Пусть он образован генераторами $g_1, \dots, g_k$. Докажем, что существует замкнутый путь длины p с началом и концом в вершине i. Доказательство проведём индукцией по числу k.

Пусть $k = 1$. Ясно, что $g_1 \in G(i,w)$ для некоторого простого контура w, проходящего через вершину i. Из алгоритма 1 следует, что $g_1 \in G(i,w,d)$ для некоторого простого контура $d \in C_{i,w}$. Из леммы 4 следует, что существует замкнутый путь длины g_1 с началом и концом в вершине i.

Пусть утверждение верно для k генераторов $g_1, \dots, g_k$. Докажем для $k+1$.

В силу леммы 4 существует замкнутый путь с началом и концом в вершине i длины g_{k+1}. Отсюда, учитывая предположение индукции и примитивность графа $\Gamma_{W,\chi,\rho,\alpha,r}$, получаем справедливость индуктивного перехода для $k+1$.

Утверждение леммы 5 напрямую следует из доказанного факта и леммы 4. ■

Утверждение 3. Для любого $(W,\chi,\varphi,\rho)_c$-семейства число $r_{W,\chi,\varphi,\rho}$ конечно тогда и только тогда, когда орграф $\Gamma_{W,\chi,\varphi,\rho}$ примитивен.

Доказательство. Пусть орграф $\Gamma_{W,\chi,\rho,\alpha,r}$ импримитивен. Рассмотрим входную разность

$$\alpha = \left(0,\dots,0,\ \underbrace{\alpha^{(i)}}_{i},0,\dots,0\right) \in V_d^m.$$

Если орграф $\Gamma_{W,\chi,\rho,\alpha,r}$ не является сильносвязным, то существуют по крайне мере два таких несвязных подграфа Γ_1 и Γ_2, что вершина i принадлежит множеству вершин подграфа Γ_1.

Метки всех вершин графа Γ_2 равны $\tilde{0}$. Очевидно, что невозможные разности существуют для любого r. Отсюда $r_{W,\chi,\varphi,\rho}$ бесконечно.

Если орграф $\Gamma_{W,\chi,\rho,\alpha,r}$ сильно связен, но наибольший общий делитель длин всех простых контуров равен $t > 1$, то все графы $\Gamma_{W,\chi,\rho,\alpha,tq+1}$, $q \in \mathbb{N}$, имеют метку $\tilde{0}$ у вершины i. Число таких графов бесконечно. Таким образом, $r_{W,\chi,\varphi,\rho}$ бесконечно.

Если орграф $\Gamma_{W,\chi,\rho,\alpha,r}$ примитивен, то из леммы 5 следует, что $r_{W,\chi,\varphi,\rho}$ конечно. ■

Отметим, что если параметр $r_{W,\chi,\varphi,\rho}$ бесконечен, то все алгоритмы шифрования Фейстеля из $(W,\chi,\varphi,\rho)_c$-семейства не являются стойкими к методу невозможных разностей.

Пусть $p_{\max}$ — длина максимального простого контура в орграфе $\Gamma_{W,\chi,\varphi,\rho}$. В следующем утверждении приведены нижняя и верхняя оценки конечного числа $r_{W,\chi,\varphi,\rho}$. Это основной результат работы.

Утверждение 4. Для любого $(W,\chi,\varphi,\rho)_c$-семейства с примитивным орграфом $\Gamma_{W,\chi,\varphi,\rho}$ справедливы неравенства

$$\max\left(g_{\max},\mathrm{d}\left(\Gamma_{W,\chi,\varphi,\rho}\right)\right)\leqslant r_{W,\chi,\varphi,\rho}\leqslant g_{\max}+\mathrm{d}\left(\Gamma_{W,\chi,\varphi,\rho}\right)+p_{\max}.$$

Доказательство. Используем утверждение 1 и рассмотрим входную разность

$$\alpha=\left(0,\ldots,0,\underbrace{\alpha^{(i)}}_{i},0,\ldots,0\right)\in V_d^m.$$

Пусть $r=\max\left(g_{\max},\mathrm{d}\left(\Gamma_{W,\chi,\varphi,\rho}\right)\right)$. Из определения диаметра орграфа, числа Фробениуса и леммы 4 получаем, что орграф $\Gamma_{W,\chi,\rho,\alpha,r}$ содержит по крайней мере одну вершину с меткой не равной Δ. Отсюда $\max\left(g_{\max},\mathrm{d}\left(\Gamma_{W,\chi,\varphi,\rho}\right)\right)\leqslant r_{W,\chi,\varphi,\rho}$.

Пусть $r=g_{\max}+\mathrm{d}\left(\Gamma_{W,\chi,\varphi,\rho}\right)$. Очевидно, что все метки орграфа $\Gamma_{W,\chi,\rho,\alpha,r}$ принадлежат множеству $\{\Delta,\gamma\}$.

Пусть $l=r+p_{\max}$. Из равенств $\gamma\oplus\gamma=\Delta$, $\gamma\oplus\Delta=\Delta$, $\Delta\oplus\Delta=\Delta$ следует, что метки всех вершин в орграфе $\Gamma_{W,\chi,\rho,\alpha,l}$ равны Δ. Таким образом, $r_{W,\chi,\varphi,\rho}\leqslant g_{\max}+\mathrm{d}\left(\Gamma_{W,\chi,\varphi,\rho}\right)+$ $+\,p_{\max}$. ■

Используя результаты утверждения 4, приведём пример нахождения оценок сверху и снизу величины $r_{W,\chi,\varphi,\rho}$ для обобщённых алгоритмов шифрования Фейстеля 1-го типа. Рассмотрим такое $(W,\chi,\varphi,\rho)_c$-семейство, что $|A|=\{1,\ldots,m\}\setminus\{j\}$, $|A'|=\{j\}$ для некоторых $i,j\in\{1,\ldots,m\}$, $\chi\left(j\right)=i$. Ясно, что орграф $\Gamma_{W,\chi,\varphi,\rho}$, соответствующий семейству, есть объединение двух простых контуров и состоит из m вершин; он показан на рис. 4.

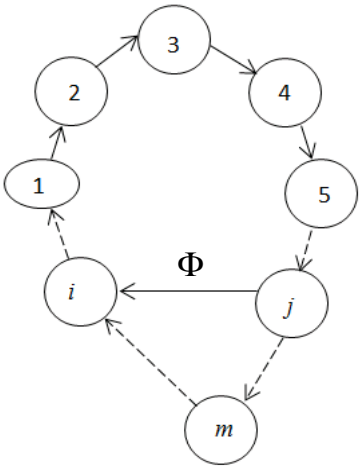


Рис. 4. Орграф обобщённого алгоритма шифрования Фейстеля 1-го типа

Из рис. 4 видно, что $\mathrm{d}(\Gamma_{W,\chi,\varphi,\rho})=m-1$. По теореме Сильвестра [16] имеем

$$g\left(\langle m+o\left(i,j\right),m\rangle\right)=\left(m+o\left(i,j\right)\right)m-o\left(i,j\right)-2m.$$

Здесь $o(i,j)$ — длина простого контура с началом в вершине i, проходящего через вершину j и содержащего дугу с меткой Ф.

Длина максимального простого контура равна m. Очевидно, что $g\left(\langle m + o\left(i,j\right), m\rangle\right)$ максимально, если $o\left(i,j\right) = m - 1$. В этом случае получаем

$$g_{\max} = g\left(\langle 2m-1, m\rangle\right) = 2m^2 - 4m + 1,$$
$$2m^2 - 4m + 1 \leqslant r_{W,\chi,\varphi,\rho} \leqslant 2m^2 - 4m + 1 + m - 1 + m = 2m\left(m-1\right).$$

В таблице приведены сравнительные характеристики оценок числа раундов для конкретных шифров и заявленного разработчиками числа раундов.

Алгоритм шифрования	Оценка снизу	Оценка сверху	Заявленное число раундов
CAST-256	3	10	48
RC-6	2	10	20
MARS	9	13	32

ЛИТЕРАТУРА

1. *Nyberg K.* Generlized Feistel networks // ASIACRYPT'1996. LNCS. 1996. V. 1163. P. 91–104.
2. *Schneier B. and Kelsey J.* Unbalanced Feistel networks and block cipher design // FSE'2005. LNCS. 2005. V. 3557. P. 121–144.
3. *Zhang L., Wu W., and Zhang L.* Proposition of two cipher structures // Inscrypt'2009. LNCS. 2010. V. 6151. P. 215–229.
4. *Shibutani K., Isobe T., Hiwatari H., et al.* Piccolo: an ultra-lightweight blockcipher // CHES'2011. LNCS. 2011. V. 6917. P. 342–357.
5. *Suzaki T. and Minematsu K.* Improving the generalized Feistel // FSE'2010. LNCS. 2010. V. 6147. P. 19–39.
6. *Lai X., Massey J. L., and Murphy S.* Markov ciphers and differential cryptanalysis // EuroCrypt'91. LNCS. 1991. V. 547. P. 17–38.
7. *Knudsen L. R.* DEAL — a 128-bit block cipher. Technical report 151. Department of Informatics, University of Bergen, Norway, February 1998.
8. *Biham E., Biryukov A., and Shamir A.* Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials // EUROCRYPT'99. LNCS. 1999. V. 1592. P. 12–23.
9. *Bogdanov A. and Shibutani K.* Generalized Feistel networks revisited // Designs, Codes and Cryptography. 2012. V. 66. P. 75–79.
10. *Li R., Sun B., Li C., and Qu L.* Cryptanalysis of a generalized unbalanced Feistel network structure // ACISP'2010. LNCS. 2010. V. 6168. P. 1–18.
11. *Zheng Y., Matsumoto T., and Imai H.* On the construction of block ciphers provably secure and not relying on any unproved hypotheses // CRYPTO'1989. LNCS. 1989. V. 435. P. 461–480.
12. *Schnorr C. P.* On the construction of random number generators and random function generators // EUROCRYPT'88. LNCS. 1988. V. 330. P. 225–232.
13. *Feistel H., Notz W., and Smith J. L.* Some cryptographic techniques for machine-to-machine data communications // Proc. IEEE. 1975. V. 63. No. 11. P. 1545–1554.
14. *Luo Y., Wu Z., Lai X., and Gong G.* A unified method for finding impossible differentials of block cipher structures // Inform. Sci. 2014. V. 263. P. 211–220.
15. *Kim J., Hong S., and Lim J.* Impossible differential cryptanalysis using matrix method // Discr. Math. 2010. V. 310. P. 988–1002.
16. *Sylvester J. J.* Problem 7382 // Math. Quest. From Educat. Times. 1884. V. 37. P. 26.

REFERENCES

1. *Nyberg K.* Generlized Feistel networks. ASIACRYPT'1996, LNCS, 1996, vol. 1163, pp. 91–104.
2. *Schneier B. and Kelsey J.* Unbalanced Feistel networks and block cipher design. FSE'2005, LNCS, 2005, vol. 3557, pp. 121–144.
3. *Zhang L., Wu W., and Zhang L.* Proposition of two cipher structures. Inscrypt'2009, LNCS, 2010, vol. 6151, pp. 215–229.
4. *Shibutani K., Isobe T., Hiwatari H., et al.* Piccolo: an ultra-lightweight blockcipher. CHES'2011, LNCS, 2011, vol. 6917, pp. 342–357.
5. *Suzaki T. and Minematsu K.* Improving the generalized Feistel. FSE'2010, LNCS, 2010, vol. 6147, pp. 19–39.
6. *Lai X., Massey J. L., and Murphy S.* Markov ciphers and differential cryptanalysis. EuroCrypt'91, LNCS, 1991, vol. 547, pp. 17–38.
7. *Knudsen L. R.* DEAL — a 128-bit block cipher. Technical report 151. Department of Informatics, University of Bergen, Norway, February 1998.
8. *Biham E., Biryukov A., and Shamir A.* Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. EUROCRYPT'99, LNCS, 1999, vol. 1592, pp. 12–23.
9. *Bogdanov A. and Shibutani K.* Generalized Feistel networks revisited. Designs, Codes and Cryptography, 2012, vol. 66, pp. 75–79.
10. *Li R., Sun B., Li C., and Qu L.* Cryptanalysis of a generalized unbalanced Feistel network structure. ACISP'2010, LNCS, 2010, vol. 6168, pp. 1–18.
11. *Zheng Y., Matsumoto T., and Imai H.* On the construction of block ciphers provably secure and not relying on any unproved hypotheses. CRYPTO'1989, LNCS, 1989, vol. 435, pp. 461–480.
12. *Schnorr C. P.* On the construction of random number generators and random function generators. EUROCRYPT'88, LNCS, 1988, vol. 330, pp. 225–232.
13. *Feistel H., Notz W., and Smith J. L.* Some cryptographic techniques for machine-to-machine data communications. Proc. IEEE, 1975, vol. 63, no. 11, pp. 1545–1554.
14. *Luo Y., Wu Z., Lai X., and Gong G.* A unified method for finding impossible differentials of block cipher structures. Inform. Sci., 2014, vol. 263, pp. 211–220.
15. *Kim J., Hong S., and Lim J.* Impossible differential cryptanalysis using matrix method. Discr. Math., 2010, vol. 310, pp. 988–1002.
16. *Sylvester J. J.* Problem 7382 // Math. Quest. From Educat. Times, 1884, vol. 37, p. 26.

ПСЕВДОСЛУЧАЙНЫЕ ГЕНЕРАТОРЫ

УДК 519.7

СВОЙСТВА ПОЛИНОМИАЛЬНЫХ ГЕНЕРАТОРОВ С ВЫХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТЬЮ НАИБОЛЬШЕГО ПЕРИОДА НАД КОЛЬЦОМ ГАЛУА

Д. М. Ермилов

Лаборатория ТВП, г. Москва, Россия

Пусть $R = \mathrm{GR}(q^n, p^n)$ — кольцо Галуа мощности q^n и характеристики p^n, где $q = p^m$, и $G_{f,R}$ — граф биективного преобразования кольца R, задаваемого полиномом $f(x) \in R[x]$. Если $n > 1$ или $q \neq p$, то граф $G_{f,R}$ не может быть циклом. Максимальная длина цикла в таком графе не превосходит $q(q-1)p^{n-2}$. Полиномы, для которых граф $G_{f,R}$ содержит цикл указанной длины, назовём полиномами с максимальной длиной цикла. Для таких полиномов предложен алгоритм проверки, лежит ли заданный элемент кольца на каком-либо цикле длины $q(q-1)p^{n-2}$ графа $G_{f,R}$. Алгоритм требует выполнения порядка dq операций умножения и порядка dq операций сложения в кольце R, $d = \deg f(x)$, $d < |R|$. Предложен также алгоритм построения системы представителей различных циклов графа $G_{f,R}$, имеющих длину $q(q-1)p^{n-2}$. Алгоритм построения представителей всех циклов длины $q(q-1)p^{n-2}$ требует выполнения порядка $d(q-1)q^{n-1}$ операций умножения и порядка $d(q-1)q^{n-1}$ операций сложения в кольце R. Алгоритм построения представителей M различных циклов длины $q(q-1)p^{n-2}$ требует выполнения порядка $d(q-1)q^{k-1}$ операций умножения и порядка $d(q-1)q^{k-1}$ операций сложения в кольце R, где $k = \lceil \log_{q/p} M \rceil + 1$.

Ключевые слова: *кольца Галуа, нелинейные генераторы, псевдослучайные последовательности, полиномиальный конгруэнтный генератор.*

DOI 10.17223/20710410/27/5

FEATURES OF MAXIMAL PERIOD POLYNOMIAL GENERATORS OVER THE GALOIS RING

D. M. Ermilov

Laboratory TVP, Moscow, Russia

E-mail: wwwermilov@gmail.com

For a polynomial mapping over the Galois ring $R = \mathrm{GR}(q^n, p^n)$ with the cardinality q^n and characteristic p^n, the maximal length of a cycle equals $q(q-1)p^{n-2}$. In this paper, we present an algorithm for constructing the system of representatives of all maximal length cycles and an algorithm for constructing an element in a cycle of maximal length for a polynomial substitution $f \in R[x]$. The complexity of the first algorithm equals $d(q-1)q^{n-1}$ multiplication operations and $d(q-1)q^{n-1}$ addition operations in R, the complexity of the second algorithm equals dq multiplication operations and

dq addition operations in R where $d = \deg(f)$.

Keywords: *nonlinear recurrent sequences, Galois ring.*

Введение

При синтезе поточных шифрсистем актуальной задачей является построение генераторов псевдослучайных последовательностей с хорошими криптографическими свойствами. К генераторам псевдослучайных последовательностей предъявляются такие требования, как быстродействие, простота реализации, возможность гарантирования криптографических параметров. Для выработки псевдослучайных последовательностей широко применяются *полиномиальные конгруэнтные генераторы*, которые являются обобщением хорошо известных линейных конгруэнтных генераторов. Полиномиальный конгруэнтный генератор над кольцом R — это автомат с выходной последовательностью $x_0, x_1, \ldots$, которая определяется соотношением

$$x_{i+1} = f(x_i), \tag{1}$$

где $x_0 \in R$; $f(x) \in R[x]$.

Изучение полиномиальных генераторов началось со случая, когда R — кольцо вычетов. Общие свойства функций и полиномиальных преобразований примарных колец вычетов можно найти в работе [1].

Интересен случай, когда последовательность (1) имеет наибольший период. Над кольцом вычетов $\mathbb{Z}_m$ наибольший период последовательности (1) равен m. Из работы [2] следует, что указанный период достижим. Полиномы, задающие последовательность (1) периода m, называют *полноцикловыми* или *транзитивными*. Описание полноцикловых линейных и квадратичных полиномов над кольцами вычетов дано Д. Кнутом в работе [3], а общий случай рассмотрен М. В. Лариным в [4]. В. С. Анашин [5] указал классы полноцикловых полиномиальных преобразований колец вычетов.

В работе [6] изучается орграф полиномиального преобразования над коммутативным локальным кольцом, предложена классификация вершин орграфа, найдено число его циклических точек.

А. А. Нечаевым в [7] описаны биективные полиномиальные преобразования конечных коммутативных колец главных идеалов, а также найдено их количество. Изучение периодических свойств последовательности (1) в случае, когда R — кольцо Галуа, начато в [8].

В настоящей работе на основе результатов [8] исследуются свойства графов полиномиальных преобразований колец Галуа, содержащих циклы максимальной длины.

1. Обозначения

Рассмотрим кольцо Галуа $R = \mathrm{GR}(q^n, p^n)$ мощности q^n и характеристики p^n, где $q = p^m$, $m > 1$, $n > 1$. Пусть $f(x) \in R[x]$ — полином над кольцом R, задающий биективное преобразование этого кольца [7]. Граф указанного преобразования над кольцом R обозначим через $G_{f,R}$. Напомним, что цикловая структура графа — это таблица $[l_1^{k_1}, \ldots, l_t^{k_t}]$, указывающая, что граф состоит из k_1 циклов длины l_1, $\ldots$, k_t циклов длины l_t. В работе [8] показано, что граф полиномиального преобразования кольца R не содержит циклов, длина которых больше $q(q-1)p^{n-2}$.

Биективные полиномы над кольцом R, такие, что граф $G_{f,R}$ содержит цикл длины $q(q-1)p^{n-2}$, назовём *полиномами с максимальной длиной цикла* (*МДЦ-полиномами*). Вычисления на ЭВМ показывают, что указанные полиномы существуют.

Пример 1. Рассмотрим кольцо Галуа $R = \mathrm{GR}(15625, 125)$. Кольцо R изоморфно кольцу $R' = \mathbb{Z}_{125}[y]/(y^2 + y + 1)$. Элементы кольца R' суть классы вида

$$[a_1 y + a_0]_{y^2+y+1},$$

которые будем обозначать векторами $(a_1, a_0) \in \mathbb{Z}_{125}^2$. Например, элемент $[2y+1]_{y^2+y+1} \in$ $\in R'$ будем обозначать вектором $(2, 1)$. Отождествим кольцо R с кольцом R'. Рассмотрим следующий полином $f(x) \in R[x]$:

$$\begin{gathered} f(x) = (1,4)x^{24} + (1,3)x^{23} + (4,2)x^{21} + (4,2)x^{20} + (0,1)x^{19} + (3,1)x^{18} + \\ +(2,2)x^{17} + (3,4)x^{15} + (0,1)x^{14} + (3,3)x^{13} + (3,0)x^{12} + (1,1)x^{11} + (2,2)x^{10} + \\ +(3,3)x^9 + (4,3)x^8 + (2,4)x^7 + (0,24)x^6 + (0,3)x^5 + \\ +(3,0)x^4 + (4,1)x^3 + (3,4)x^2 + (4,3)x + (0,1). \end{gathered}$$

Цикловая структура графа $G_{f,R}$ равна $[3000^5, 600^1, 25^1]$, и $f(x)$ является МДЦ-полином над R.

Критерий того, что полином над кольцом R является МДЦ-полиномом, приведён в работе [8].

Пусть далее $f(x) \in R[x]$ — МДЦ-полином. При использовании $f(x)$ в качестве криптографического примитива представляются актуальными следующие задачи:

1) проверка того, что заданный элемент $a \in R$ лежит на каком-то цикле максимальной длины графа $G_{f,R}$;
2) эффективное построение системы представителей M различных циклов длины $q(q-1)p^{n-2}$ графа $G_{f,R}$.

Параметр M не может превышать значения $(q/p)^{n-2}$, так как в графе $G_{f,R}$ содержится ровно $(q/p)^{n-2}$ циклов длины $(q-1)qp^{n-2}$ [9]. Введём необходимые обозначения.

Обозначим через $f^{[0]}$ тождественное преобразование, а через $f^{[m]}$, $m \in \mathbb{N}$, — преобразование $f \circ f \circ \cdots \circ f$ (m раз), где $\circ$ — операция композиции; $f(x) \in R[x]$.

Положим $J = pR$ и $R_i = R/J^i$, $i \in \{1, \ldots, n\}$. *Координатным множеством* $\Gamma(R)$ кольца R называют множество элементов $\{x \in R : x^q = x\}$. Согласно [10], всякий элемент $a \in R$ однозначно представляется в виде

$$a = \gamma_0(a) + p\gamma_1(a) + p^2\gamma_2(a) + \cdots + p^{n-1}\gamma_{n-1}(a),$$

где $\gamma_i(a) \in \Gamma(R)$, $i = 0, 1, \ldots, n-1$. Это представление называют *разложением Тейхмюллера* элемента $a \in R$. Кольцо R_i состоит из непересекающихся классов $a + J^i$, $a \in R$. Элемент a называют представителем класса $a + J^i$ в кольце R. Там, где это не будет приводить к недоразумению, элементы кольца R_i будем отождествлять с их представителями в кольце R и вместо координатного множества $\Gamma(R_i)$ писать $\Gamma(R)$, $i \in \{1, \ldots, n\}$. Рассмотрим естественные эпиморфизмы колец

$$\varphi_i : R \to R_i$$

для $i \in \{1, \ldots, n\}$, которые естественным образом продолжаются до эпиморфизмов колец многочленов

$$\widehat{\varphi}_i : R[x] \to R_i[x].$$

Положим $f_i(x) = \widehat{\varphi}_i(f(x))$, $i = 1, \ldots, n$. Производную многочлена $f(x)$ кольца $R[x]$ будем обозначать $f'(x)$ [11].

В дальнейшем понадобится следующее утверждение.

Утверждение 1 [8]. Пусть $f(x) \in R[x]$. Для любых $s \in \mathbb{N}$ и $x, y \in R$ верно соотношение

$$f(x + p^s y) \equiv f(x) + p^s y f'(x) \,(\mathrm{mod}\ J^{s+1}).$$

2. Определение принадлежности элемента циклу максимальной длины

Для решения первой задачи докажем

Утверждение 2. Пусть $f(x) \in R[x]$ — МДЦ-полином, $F(x) = f^{[q]}(x)$. Элемент $a \in R$ лежит на цикле длины $q(q-1)p^{n-2}$ графа $G_{f,R}$ в том и только в том случае, если $\gamma_1(a)$ не является решением сравнения

$$F(\gamma_0(a)) - \gamma_0(a) \equiv p(e - F'(\gamma_0(a)))x \pmod{J^2}. \tag{2}$$

Доказательство. Так как $f(x)$ — МДЦ-полином, из результатов работы [8] следует, что цикловая структура графа G_{f_2,R_2} имеет вид $[q(q-1)^1, q^1]$. При этом для того чтобы элемент $a \in R$ лежал на каком-либо цикле длины $q(q-1)p^{n-2}$, необходимо и достаточно, чтобы элемент $\varphi_2(a)$ лежал на цикле длины $q(q-1)$ графа G_{f_2,R_2}. Найдём необходимое и достаточное условие, при котором элемент $\varphi_2(a)$ лежит на цикле длины q графа G_{f_2,R_2}.

Из условия, что $\varphi_2(a)$ лежит на цикле длины q графа G_{f_2,R_2} и утверждения 1, имеем

$$F(\gamma_0(a) + p\gamma_1(a)) \equiv F(\gamma_0(a)) + p\gamma_1(a)F'(\gamma_0(a)) \equiv \gamma_0(a) + p\gamma_1(a) \pmod{J^2}.$$

Последнему сравнению равносильно сравнение

$$F(\gamma_0(a)) - \gamma_0(a) \equiv p(e - F'(\gamma_0(a)))\gamma_1(a) \pmod{J^2},$$

из которого следует доказываемое утверждение. ■

Замечание 1. Выполнению сравнения (2) равносильно выполнение некоторого сравнения по модулю J. Действительно, так как $F(\gamma_0(a)) \equiv \gamma_0(a) \pmod{J}$, найдётся элемент $a' \in \Gamma(R)$, такой, что $F(\gamma_0(a)) \equiv \gamma_0(a) + pa' \pmod{J^2}$. В таком случае сравнение (2) запишется в виде $pa' \equiv p(e - F'(\gamma_0(a)))x \pmod{J^2}$. Последнему сравнению равносильно сравнение по модулю J:

$$a' \equiv (e - F'(\gamma_0(a)))x \pmod{J}. \tag{3}$$

Сформулируем алгоритм, определяющий, лежит ли заданный элемент на каком-либо цикле длины $q(q-1)p^{n-2}$ графа $G_{f,R}$.

Замечание 2. Пусть $f(x) = a_0 + a_1x + a_2x^2 + \ldots = a_0 + x(a_1 + x(a_2 + \ldots)\ldots)$; отсюда видно, что для нахождения значения многочлена в точке требуется d умножений и d сложений элементов кольца, где $d = \deg f(x)$.

Оценим сложность алгоритма 1. Пусть $d = \deg f(x)$. На шаге 1 алгоритма необходимо последовательно вычислить значения $f(\gamma_0(a))$, $f^{[2]}(\gamma_0(a))$, $\ldots$, $f^{[q]}(\gamma_0(a))$. При этом параллельно с шагом 1 можно выполнять шаг 2, вычисляя произведение элементов указанной цепочки, и по формуле (4) найти $F'(\gamma_0(a)) \pmod{J^2}$. Таким образом, для выполнения шагов 1 и 2 потребуется $dq + q = (d+1)q$ операций умножения и столько же операций сложения в кольце R.

Шаг 3 алгоритма осуществляется за одну операцию умножения и одну операцию сложения в кольце R. Общая сложность алгоритма равна $(d+1)q + 1$ операций умножения и $(d+1)q + 1$ операций сложения в кольце R.

В итоге верна

Алгоритм 1. Определение принадлежности элемента кольца R циклу максимальной длины графа $G_{f,R}$

Вход: $f(x) \in R[x]$ — МДЦ-полином, элемент $a \in R$

Выход: ДА, если элемент a лежит на цикле длины $q(q-1)p^{n-2}$ графа $G_{f,R}$; НЕТ — иначе

1: Найти значение $F(\gamma_0(a)) \pmod{J^2}$.

2: Найти значение $F'(\gamma_0(a)) \pmod{J^2}$, используя формулу

$$F'(\gamma_0(a)) \equiv (f^{[q]}(x))'_{x=\gamma_0(a)} \equiv \prod_{i=0}^{q-1} f(f^{[i]}(\gamma_0(a))) \pmod{J^2}. \tag{4}$$

3: Проверить, является ли $\gamma_1(a)$ решением сравнения

$$a' \equiv (e - F'(\gamma_0(a)))x \pmod{J},$$

где a' находится из сравнения $F(\gamma_0(a)) \equiv \gamma_0(a) + pa' \pmod{J^2}$.

4: **Если** является, **то**

5: выдать ответ НЕТ,

6: **иначе**

7: выдать ответ ДА.

Теорема 1. Пусть $f(x) \in R[x]$ — МДЦ-полином. Существует алгоритм, проверяющий, лежит ли заданный элемент $a \in R$ на каком-либо цикле длины $q(q-1)p^{n-2}$ графа $G_{f,R}$, требующий порядка dq операций умножения и порядка dq операций сложения в кольце R.

3. Построение системы представителей циклов максимальной длины

Сначала решим задачу для $M = (q/p)^{n-2}$. Обозначим систему представителей всех различных циклов графа $G_{f,R}$ длины $q(q-1)p^{n-2}$ через $W_{f,R}$. Строить набор $W_{f,R}$ будем итеративно, последовательно строя цепочку множеств

$$W_{f_1,R_1}, W_{f_2,R_2}, \ldots, W_{f_n,R_n}, \tag{5}$$

где $f_i(x) = \widehat{\varphi}_i(f(x))$, $i = 1, \ldots, n$. Тогда $W_{f,R} = W_{f_n,R_n}$.

Из результатов работы [8] следует, что цикловые структуры графов G_{f_1,R_1} и G_{f_2,R_2} равны $[q^1]$ и $[q(q-1)^1, q^1]$ соответственно, а для $k \geqslant 3$ в графе G_{f_k,R_k} содержится $(q/p)^{k-2}$ циклов длины $q(q-1)p^{k-2}$.

Множество W_{f_1,R_1} состоит из одного элемента, так как граф G_{f_1,R_1} является циклом. Поэтому в качестве W_{f_1,R_1} можно выбрать любое одноэлементное множество $\{a\}$, $a \in R_1$. Цикловая структура графа G_{f_2,R_2} имеет вид $[q(q-1)^1, q^1]$. Тогда $W_{f_2,R_2} = \{a'\}$, где $\gamma_0(a') = a$, а координату $\gamma_1(a')$ необходимо взять отличной от решения сравнения (3).

Далее покажем, как по известному множеству W_{f_k,R_k} построить $W_{f_{k+1},R_{k+1}}$, $k \geqslant 2$. Рассмотрим естественные эпиморфизмы $\varphi_i : R_{i+1} \to R_i$ для $i = 1, \ldots, n-1$. Для каждого $a \in W_{f_k,R_k}$ обозначим через C_a цикл графа G_{f_k,R_k}, на котором лежит элемент a.

Элементы прообраза $\varphi_k^{-1}(C_a)$ лежат на q/p циклах длины $q(q-1)p^{k-1}$ графа $G_{f_{k+1},R_{k+1}}$ [8, теорема 30]. Пусть $A_a = \{a_1, a_2, \ldots, a_{q/p}\}$ — множество представителей этих циклов. Для разных элементов $a_1, a_2 \in W_{f_k,R_k}$ прообразы $\varphi_k^{-1}(C_{a_1})$ и $\varphi_k^{-1}(C_{a_2})$ не пересекаются, значит, множества A_{a_1} и A_{a_2} также не пересекаются. Из равен-

ства $\frac{q}{p}|W_{f_k,R_k}| = |W_{f_{k+1},R_{k+1}}|$ следует, что $\bigcup\limits_{a\in W_{f_k,R_k}} A_a = W_{f_{k+1},R_{k+1}}$. Это означает, что для построения системы представителей $W_{f_{k+1},R_{k+1}}$ достаточно для каждого элемента $a \in W_{f_k,R_k}$ построить множество A_a.

Пусть a принадлежит множеству W_{f_k,R_k}. Установим связь между элементами α кольца R_{k+1}, которые лежат на одном цикле максимальной длины и обладают свойством $\varphi_k(\alpha) = a$.

Утверждение 3. Пусть элемент $a \in W_{f_k,R_k}$ является представителем цикла C максимальной длины графа G_{f_k,R_k}. Тогда на любом цикле $C^{'}$ максимальной длины графа $G_{f_{k+1},R_{k+1}}$, таком, что $\varphi_k(C^{'}) = C$, лежат ровно p элементов, образ которых под действием эпиморфизма φ_k совпадает с a.

Доказательство. Пусть $F(x) = f^{[q(q-1)p^{k-2}]}(x)$ есть $q(q-1)p^{k-2}$-я композиционная степень полинома $f(x)$ и $a^{'}-$ элемент на цикле $C^{'}$ максимальной длины графа $G_{f_{k+1},R_{k+1}}$ со свойством $\varphi_i(a^{'}) = a$. Тогда для каждого $k \in \{1,\dots,p\}$ выполняется равенство $\varphi_i(F^{[k]}(a^{'})) = a$. ■

Лемма 1. Пусть $f(x)$ — МДЦ-полином над кольцом R. Тогда существует элемент $c \in R$, такой, что для любого элемента $a \in R$, лежащего на цикле длины t графа $G_{f,R}$, верно равенство

$$\left(f^{[t]}(x)\right)^{'}_{x=a} = c.$$

Доказательство. Обозначим через $F(x) = f^{[t]}(x)$. Достаточно доказать, что $F'(x) = F^{'}(f(x))$ для всех $x \in R$, лежащих на цикле длины t графа $G_{f,R}$.

По формуле производной сложной функции для указанных $x \in R$ имеем

$$F^{'}(x) = \left(f^{[t]}(x)\right)^{'} = f^{'}\left(f^{[t-1]}(x)\right)\left(f^{[t-1]}(x)\right)^{'} = \prod_{i=0}^{t-1} f^{'}\left(f^{[i]}(x)\right).$$

С другой стороны,

$$F^{'}(f(x)) = \prod_{i=0}^{t-1} f^{'}\left(f^{[i]}(f(x))\right) = \prod_{i=1}^{t} f^{'}\left(f^{[i]}(x)\right) = f^{'}(x)\prod_{i=1}^{t-1} f^{'}\left(f^{[i]}(f(x))\right) = \prod_{i=0}^{t-1} f^{'}\left(f^{[i]}(x)\right).$$

Лемма доказана. ■

Теорема 2. Пусть $a_1 = a + p^k a_1^{'}$, $\dots$, $a_p = a + p^k a_p^{'}$ — элементы на некотором цикле максимальной длины $q(q-1)p^{k-1}$ графа $G_{f_{k+1},R_{k+1}}$, образ которых под действием эпиморфизма φ_k совпадает с $a \in W_{f_k,R_k}$. Тогда для некоторого $r \in \Gamma(R)$ выполняется соотношение $a_{i+1}^{'} = a_i^{'} + r$, $i = 1, 2, \dots, p-1$.

Доказательство. Пусть $G(x) = f^{[q(q-1)p^{k-2}]}(x)$ есть $q(q-1)p^{k-2}$-я композиционная степень полинома $f(x)$. Тогда выполняются сравнения $G(a_i) \equiv a_{i+1} \pmod{J^{k+1}}$ для $i = 1,\dots,p-1$. Кроме того, так как $G(a) \equiv a \pmod{J^k}$ и $G(a) \not\equiv a \pmod{J^{k+1}}$, то $G(a) \equiv a + p^k r \pmod{J^{k+1}}$ для некоторого $r \in R$. Воспользуемся результатом утверждения 1 и запишем последовательность сравнений

$$a_{i+1} \equiv G(a_i) \equiv G(a + p^k a_i^{'}) \equiv G(a) + p^k a_i^{'} G^{'}(a) \equiv a + p^k(a_i^{'} G^{'}(a) + r) \pmod{J^{k+1}}.$$

Для завершения доказательства осталось показать, что $G^{'}(a) \equiv e \pmod{J}$. Положив $F(x) = f^{[q]}(x)$, получим

$$G^{'}(x) = (F^{[(q-1)p^{k-2}]}(x))^{'} = \prod_{i=0}^{(q-1)p^{k-2}-1} F^{'}(F^{[(q-1)p^{k-2}]}(x)).$$

По лемме 1 существует элемент $c \in R$, такой, что для всех элементов $a \in R$ выполняется равенство $F^{'}(a) \equiv c \pmod J$. Тогда для любого элемента $y \in R$ верны сравнения

$$G^{'}(y) \equiv \prod_{i=0}^{(q-1)p^{k-2}-1} F^{'}(F^{[(q-1)p^{k-2}]}(y)) \equiv c^{(q-1)p^{k-2}} \equiv e^{p^{k-2}} \equiv e \pmod J.$$

Теорема доказана. ■

Определим на $\Gamma(R)$ операции $\oplus$ и $\otimes$: если $\alpha, \beta \in \Gamma(R)$, то

$$\alpha \oplus \beta = \gamma_0(\alpha + \beta), \quad \alpha \otimes \beta = \gamma_0(\alpha\beta) = \alpha\beta.$$

Алгебра $(\Gamma(R), \oplus, \otimes)$ изоморфна полю $\mathrm{GF}(q)$. Далее вместо поля $(\Gamma(R), \oplus, \otimes)$ будем писать просто $\Gamma(R)$.

Следствие 1. Пусть $a \in W_{f_k,R_k}$. Два элемента $a + p^k a^{'}$ и $a + p^k a^{''}$ кольца R_{k+1} лежат на одном и том же цикле максимальной длины графа $G_{f_{k+1},R_{k+1}}$ в том и только в том случае, если элементы $a^{'}, a^{''} \in \Gamma(R)$ лежат на одном цикле графа $G_{x+r,\Gamma(R)}$ полиномиального преобразования $x + r$, где элемент $r \in \Gamma(R)$ находится из сравнения

$$G(a) \equiv a + p^k r \pmod{J^{k+1}},$$

а $G(x) = f^{[q(q-1)p^{k-2}]}(x)$ есть $q(q-1)p^{k-2}$-я композиционная степень полинома $f(x)$.

Граф $G_{x+r,\Gamma(R)}$ состоит из q/p циклов длины p. Элементы каждого цикла графа $G_{x+r,\Gamma(R)}$ образуют смежный класс аддитивной группы поля $\Gamma(R)$ по подгруппе $\langle r \rangle$. Это означает, что для нахождения q/p элементов поля $\Gamma(R)$, которые лежат на разных циклах графа $G_{x+r,\Gamma(R)}$, достаточно найти представителей смежных классов группы $(\Gamma(R), \oplus)$ по подгруппе $\langle r \rangle$.

Обозначим через $\Gamma_0(R)$ простое подполе [11] поля $\Gamma(R)$. Если на группе $(\Gamma(R), \oplus)$ ввести внешнюю операцию умножения на элементы $\Gamma_0(R)$, то получим векторное пространство размерности m. Дополнив до базиса пространства элемент r, получим базис $r, r_2, \ldots, r_m$. Рассмотрим представление пространства в виде прямой суммы подпространств

$$\Gamma(R) = \langle r \rangle \oplus \langle r_2 \rangle \oplus \cdots \oplus \langle r_m \rangle.$$

Тогда множество

$$\{\langle r_2 \rangle \oplus \cdots \oplus \langle r_m \rangle\}$$

совпадает с множеством представителей смежных классов группы $(\Gamma(R), \oplus)$ по подгруппе $(\langle r \rangle, \oplus)$.

Изложим алгоритм построения системы $W_{f,R}$ представителей циклов максимальной длины графа $G_{f,R}$.

Как отмечалось выше, в качестве W_{f_1,R_1} можно взять любое одноэлементное множество $\{a\}$, $a \in R_1$, а в качестве W_{f_2,R_2} — одноэлементное множество $\{a^{'}\}$, где $a^{'}$ — элемент на цикле длины $q(q-1)$ графа G_{f_2,R_2}.

Покажем, как по имеющемуся элементу $a \in W_{f_k,R_k}$ построить множество из q/p элементов $A_a \subset W_{f_{k+1},R_{k+1}}$, $k \geqslant 3$.

Оценим сложность алгоритма 2.

Пусть $d = \deg f(x)$. Тогда значение многочлена $f(x)$ в точке $a \in R$ можно найти за d операций умножения и d операций сложения в кольце R. Для выполнения шага 1 алгоритма необходимо $q(q-1)p^{k-2}$ раз вычислить значение многочлена $f(x)$ степени d. На шаге 2 не требуется выполнения элементарных операций.

Алгоритм 2. Построение множества A_a

Вход: $f(x) \in R[x]$, $a \in W_{f_k,R_k}$
Выход: множество $A_a \subset W_{f_{k+1},R_{k+1}}$
1: Находим элемент $r \in \Gamma(R)$, такой, что

$$f^{[q(q-1)p^{k-2}]}(a) \equiv a + p^k r \pmod{J^{k+1}}.$$

2: Дополняем до базиса пространства $\Gamma(R)$ элемент r, получим базис $r, r_2, \ldots, r_m$. Тогда множество A_a совпадает с множеством

$$\{c_2 r_2 + \cdots + c_m r_m : c_i \in \Gamma(R), i = 2, \ldots, m\}.$$

Для построения множества $W_{f_{k+1},R_{k+1}}$ необходимо применить алгоритм 2 для каждого элемента $a \in W_{f_k,R_k}$. Следовательно, для построения множества $W_{f_{k+1},R_{k+1}}$ по имеющемуся множеству W_{f_k,R_k} требуется

$$|W_{f_k,R_k}| dq(q-1)p^{k-2} = \left(\frac{q}{p}\right)^{k-2} dq(q-1)p^{k-2} = d(q-1)q^{k-1}$$

операций умножения и столько же операций сложения в кольце R.

Для построения системы представителей циклов максимальной длины $W_{f,R}$ графа $G_{f,R}$ необходимо построить цепочку множеств (5), которая требует

$$\sum_{i=3}^{n} d(q-1)q^{k-1} = d(q-1)\sum_{i=1}^{n-2}\left(\frac{q}{p}\right)^{k-2} = d(q-1)q^{n-1}$$

операций умножения и столько же операций сложения в кольце R.

В итоге верна

Теорема 3. Пусть $f(x) \in R[x]$ — МДЦ-полином. Существует алгоритм построения системы $W_{f,R}$ представителей всех различных циклов длины $(q-1)qp^{n-2}$ графа $G_{f,R}$, требующий порядка $d(q-1)q^{n-1}$ операций умножения и порядка $d(q-1)q^{n-1}$ операций сложения в кольце R, где $d = \deg f$.

В работе [9] показано, что в графе $G_{f,R}$ ровно q^{n-1} точек не лежат на циклах максимальной длины. Отсюда следует, что алгоритм тотального опробования построения системы представителей циклов максимальной длины графа $G_{f,R}$ требует не менее $d(q-1)q^{n-1}$ и не более dq^n операций умножения и столько же операций сложения в кольце R и требует объём памяти, необходимый для хранения элементов кольца R. Предложенный алгоритм требует порядка $d(q-1)q^{n-1}$ операций умножения и порядка $d(q-1)q^{n-1}$ операций сложения в кольце R и не требует хранить в памяти все элементы кольца R.

Пусть далее $1 \leqslant M < (q/p)^{n-2}$. Необходимо построить множество W_M представителей M различных циклов длины $q(q-1)p^{n-2}$. Для этого построим множество W_{f_k,R_k} указанным выше способом, где k — минимальное натуральное число, удовлетворяющее условию $|M| < (q/p)^k$. Старшие $n-k-1$ разрядов элементов множества W_{f_k,R_k} зададим произвольно, например нулями. Обозначим полученное множество через W'_{f_k,R_k}. Имеет место включение $W_M \subseteq W'_{f_k,R_k}$. Таким образом, для построения множества W_M

требуется порядка $d(q-1)q^{k-1}$ операций умножения и порядка $d(q-1)q^{k-1}$ операций сложения, где $k = \lceil \log_{q/p} M \rceil + 1$. Хранить в памяти все элементы кольца R не требуется.

Теорема 4. Пусть $f(x) \in R[x]$ — МДЦ-полином. Существует алгоритм построения системы W_M представителей M различных циклов длины $(q-1)qp^{n-2}$ графа $G_{f,R}$, требующий порядка $d(q-1)q^{k-1}$ операций умножения и порядка $d(q-1)q^{k-1}$ операций сложения в кольце R, где $k = \lceil \log_{q/p} M \rceil + 1$.

Алгоритм тотального опробования построения множества W_M требует не менее $dMq(q-1)p^{n-2}$ и не более $dq^{n-1} + dMq(q-1)p^{n-2}$ операций умножения и столько же операций сложения в кольце R и требует хранить в памяти все элементы кольца R.

Заключение

В работе исследуется граф преобразования, задаваемого МДЦ-полиномом. Предложены алгоритмы построения системы представителей циклов максимальной длины графа преобразования, задаваемого МДЦ-полиномом. Построен алгоритм проверки, лежит ли заданный элемент кольца на каком-либо цикле максимальной длины графа преобразования.

Изучение полиномиальных конгруэнтных генераторов над кольцами Галуа далеко от завершения. По мнению автора, перспективными задачами являются вычисление ранга и изучение статистических свойств выходной последовательности полиномиального конгруэнтного генератора над кольцом Галуа.

ЛИТЕРАТУРА

1. *Carlitz L.* Functions and polynomials (mod p^n) // Acta Arithm. 1964. No. 9. P. 66–78.
2. *Анашин В. С.* О группах и кольцах, обладающих транзитивными полиномами // XVI Всес. алгебраическая конф. Тезисы. Ч. II. Л., 1981. С. 4–5.
3. *Кнут Д.* Искусство программирования. Т. 2. М.: Вильямс, 2000.
4. *Ларин М. В.* Транзитивные полиномиальные преобразования колец вычетов // Дискретная математика. 2002. Т. 14. Вып. 2. С. 20–32.
5. *Анашин В. С.* Равномерно распределенные последовательности целых p-адических чисел // Дискретная математика. 2002. Т. 14. Вып. 4. С. 1–63.
6. *Викторенков В. Е.* Орграф полиномиального преобразования над коммутативным локальным кольцом // Обозрение прикл. и промышл. матем. 2000. Т. 7. Вып. 2. С. 327.
7. *Нечаев А. А.* Полиномиальные преобразования конечных коммутативных колец главных идеалов // Матем. заметки. 1980. Т. 27. Вып. 6. С. 885–899.
8. *Ермилов Д. М., Козлитин О. А.* Цикловая структура полиномиального генератора над кольцом Галуа // Матем. вопросы криптографии. 2013. Т. 4. Вып. 1. С. 27–57.
9. *Ермилов Д. М.* О цикловой структуре биективных полиномиальных преобразований колец Галуа максимального периода // Обозрение прикл. и промышл. матем. 2013. Т. 20. Вып. 3.
10. *Елизаров В. П.* Конечные кольца. М.: Гелиос АРВ, 2006. 304 с.
11. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. М.: Гелиос АРВ, 2003. 749 с.

REFERENCES

1. *Carlitz L.* Functions and polynomials (mod p^n). Acta Arithm., 1964, no. 9, pp. 66–78.
2. *Anashin V. S.* O gruppah i kol'cah, obladajushhih tranzitivnymi polinomami. XVI Vsesojuznaja algebraicheskaja konferencija. Tezisy. P. II. Leningrad, 1981, pp. 4–5. (in Russian)

3. *Knuth D.* The Art of Computer Programming. V. 2. Reading, Massachusetts, Addison-Wesley, 1997.
4. *Larin M. V.* Tranzitivnye polinomial'nye preobrazovanija kolec vychetov. Diskretnaya matematika, 2002, vol. 14, no. 2, pp. 20–32. (in Russian)
5. *Anashin V. S.* Ravnomerno raspredelennye posledovatel'nosti celyh p-adicheskih chisel. Diskretnaya matematika, 2002, vol. 14, no. 4, pp. 1–63. (in Russian)
6. *Viktorenkov V. E.* Orgraf polinomial'nogo preobrazovanija nad kommutativnym lokal'nym kol'com. Obozrenie prikl. i promyshl. matem., 2000, vol. 7, no. 2, pp. 327. (in Russian)
7. *Nechaev A. A.* Polinomial'nye preobrazovanija konechnyh kommutativnyh kolec glavnyh idealov. Matem. Zametki, 1980, vol. 27, no. 6, pp. 885–899. (in Russian)
8. *Ermilov D. M., Kozlitin O. A.* Ciklovaja struktura polinomial'nogo generatora nad kol'com Galua. Matem. Voprosy Kriptografii, 2013, vol. 4, no. 1, pp. 27–57. (in Russian)
9. *Ermilov D. M.* O ciklovoj strukture biektivnyh polinomial'nyh preobrazovanij kolec Galua maksimal'nogo perioda. Obozrenie prikl. i promyshl. matem., 2013, vol. 20, no. 3. (in Russian)
10. *Elizarov V. P.* Konechnye kol'ca. Moscow, Gelios ARV Publ., 2006. 304 p. (in Russian)
11. *Gluhov M. M., Elizarov V. P., Nechaev A. A.* Algebra. Moscow, Gelios ARV Publ., 2003. 749 p. (in Russian)

УДК 512.624.5

ПЕРИОДЫ РАЗРЯДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЛИНЕЙНЫХ РЕКУРРЕНТ МАКСИМАЛЬНОГО ПЕРИОДА НАД КОНЕЧНЫМИ ПРОСТЫМИ ПОЛЯМИ

С. А. Кузьмин

г. Москва, Россия

Найдены периоды разрядных последовательностей, полученных из r-ичного разложения знаков линейной рекуррентной последовательности максимального периода над конечным простым полем для произвольного натурального $r \geqslant 3$.

Ключевые слова: *линейные рекурренты максимального периода, разрядные последовательности, конечные поля, простые поля, период последовательности.*

DOI 10.17223/20710410/27/6

PERIODS OF DIGIT-POSITION SEQUENCES RECEIVED FROM LINEAR RECURRENT SEQUENCES OF MAXIMAL PERIOD OVER FINITE PRIME FIELDS

S. A. Kuzmin

Moscow, Russia

E-mail: kzmn_sr@mail.ru

In the paper, for any integer $r \geqslant 3$, the periods of digit-position sequences obtained from r-ary representation of elements in a linear recurrent sequence of the maximal period over prime field are computed.

Keywords: *linear recurrent sequences of maximal period, digit-position sequences, finite fields, prime fields, periods of linear recurrent sequences.*

Введение

Пусть дано поле вычетов $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, где p — простое число, $p \geqslant 3$. Пусть также u — линейная рекуррентная последовательность (ЛРП) максимального периода (МП) над полем $\mathbb{Z}_p$ с характеристическим многочленом $g(x)$ степени m. Известно, что период линейной рекурренты u равен $T(u) = p^m - 1$ [1, с. 330].

Пусть целое число r удовлетворяет условиям $1 < r < p$. В этом случае знаки $u(i)$, $i \geqslant 0$, ЛРП u однозначно представляются в виде

$$u(i) = \sum_{t=0}^{k} u_t(i) r^t, \tag{1}$$

где $0 \leqslant u_t(i) < r$; $k = [\log_r p]$.

Для каждого $s \in \{1, \ldots, k\}$ из элементов $u_s(i)$ r-ичного разложения знаков ЛРП u образуем разрядные последовательности $u_s = (u_s(0), u_s(1), \ldots)$. Будем рассматривать их как усложнения ЛРП u.

Отметим, что в настоящее время наблюдается большой интерес к изучению p-ичных разрядных последовательностей над кольцами вычетов по модулю p^n. Это связано с тем, что данные последовательности обладают высокой линейной сложностью и могут рассматриваться как псевдослучайные последовательности для датчиков случайных чисел. С большим количеством работ по этой тематике можно ознакомиться в [2, 3]. Следует также отметить работы зарубежных авторов [4, 5], в которых проводится анализ частотных и алгебраических свойств приведённых по модулю 2 ЛРП МП над кольцами вычетов вида $\mathbb{Z}_{p^n}$ и $\mathbb{Z}_{pq}$, где q и p — различные простые числа.

Нетрудно заметить, что так как $T(u)$ является одним из периодов ЛРП u_s, то, согласно [1, с. 320], $T(u_s)$ делит период ЛРП u.

Для $r = 2$ и для некоторых $r \geqslant 3$ А. С. Кузьминым в [6] найдены периоды ЛРП u_s, $s \in \{1, \ldots, k\}$. В настоящей работе этот результат обобщён для случая $r \geqslant 3$. Доказано, что $T(u_s) = T(u)$ для всех $r \geqslant 3$ и любого $s \in \{1, \ldots, k\}$.

1. Общие сведения

Для натурального числа r, удовлетворяющего условию $2 \leqslant r < p$, рассмотрим r-ичное разложение числа p:

$$p = a_k r^k + a_{k-1} r^{k-1} + \cdots + a_1 r + a_0,$$

где $k = [\log_r p]$; $a_i \in \{0, \ldots, r-1\}$. Выделим s-й разряд полученного разложения:

$$p = \theta + a_s r^s + a(s) r^{s+1}, \tag{2}$$

где

$$\theta = \begin{cases} \sum\limits_{t=0}^{s-1} a_t r^t, & \text{если } s \neq 0, \\ 0, & \text{если } s = 0, \end{cases} \qquad a(s) = \sum_{t=s+1}^{k} a_t r^{t-s-1},$$

рассмотрение $a(s)$ при $k = 0$ лишено смысла.

Нетрудно заметить, что для элементов θ и $a(s)$ справедливы следующие свойства.

Лемма 1. Во введённых обозначениях при $s \neq 0$ имеют место следующие соотношения:

1) $\theta \equiv p \pmod{r^s}$;
2) $0 < \theta < r^s$;
3) $\theta \not\equiv -1 \pmod{p}$;
4) $a(s) + 1 < p$.

Отметим, что, согласно работе [6], справедливы неравества $\dfrac{T(u)}{d} \leqslant T(u_s) \leqslant T(u)$, где d — наибольший общий делитель чисел появлений элементов $\omega \in \{0, \ldots, r-1\}$ в последовательности u_s на отрезке длины $T(u)$.

Воспользуемся результатом, который даёт следующая теорема.

Теорема 1 [6]. Если $a_s \geqslant 2$ и $r \geqslant 3$, то наибольший общий делитель количеств появлений элементов $\omega \in \{0, \ldots, r-1\}$ на отрезке длины $T(u)$ последовательности u_s равен единице. При этих условиях $T(u_s) = T(u)$.

Получаем, что для всех возможных значений a_s, за исключением $a_s = 0$ и $a_s = 1$, период $T(u_s)$ заведомо равен периоду исходной рекурренты.

Для нахождения периодов в двух оставшихся случаях применим следующий подход. Рассмотрим функции $\delta_s : \mathbb{Z}_p \to \mathbb{Z}_p$, $s \in \{0, \ldots, k\}$, $k = [\log_r p]$, задаваемые по

правилу: $\delta_s(y) = y_s$ для всех $y \in \mathbb{Z}_p$, где y_s — s-я координата r-ичного разложения числа $y = y_0 + y_1 r + \cdots + y_k r^k$.

Тогда, согласно [7, с. 179], получаем, что для всех $s \in \{0, \ldots, k\}$ функции δ_s однозначно представимы над $\mathbb{Z}_p$ полиномами вида $C^{(s)}(x) = \sum\limits_{t=0}^{p-1} c_t^{(s)} x^t$.

Таким образом, для всех $y \in \mathbb{Z}_p$ справедливо $\delta_s(y) = C^{(s)}(y)$. Многочлены $C^{(s)}(x)$ могут быть найдены при помощи интерполяционной формулы Лагранжа, представленной, согласно [6], в виде

$$C^{(s)}(x) = \delta_s(0) - \sum_{j=0}^{p-1} \delta_s(j) x^{p-1} - \sum_{k=1}^{p-2} x^k \sum_{j=1}^{p-1} \delta_s(j) j^{p-k-1}. \tag{3}$$

Кроме того, в работе [6] доказана следующая лемма.

Лемма 2 [6]. Пусть u — ЛРП МП над полем $\mathbb{Z}_p$, $T(u) = p^m - 1$ и многочлен $h(x) = \sum\limits_{j=0}^{p-1} h_j x^j$, заданный над полем $\mathbb{Z}_p$, отличен от константы. Тогда период $T(v)$ последовательности v, знаки которой определяются равенством $v(i) = h(u(i))$, $i \geqslant 0$, равен $\sigma(p^m - 1)/(p-1)$, где $(p-1)/\sigma$ — наибольший общий делитель $p-1$ и чисел $j \in \{1, 2, \ldots, p-2\}$, для которых коэффициент h_j при x^j отличен от нуля.

Используем лемму 2 для оценки $T(u_s)$ при $a_s < 2$. Для этого установим, когда коэффициент $c_{p-2}^{(s)}$ многочлена $C^{(s)}$ отличен от 0. Вычисление коэффициента $c_{p-2}^{(s)}$ производится по той причине, что если он не сравним с нулём по модулю p, то, согласно лемме 2, период $T(u_s)$ последовательности u_s будет заведомо равен периоду $T(u)$ последовательности u при любом выборе $s \in \{0, \ldots, k\}$, независимо от других коэффициентов в выражении (3).

2. Основные результаты

Из формулы (3) непосредственно вытекает, что коэффициент при x^{p-2} в многочлене $C^{(s)}(x)$ имеет вид

$$c_{p-2}^{(s)} = -\sum_{j=0}^{p-1} j \delta_s(j). \tag{4}$$

Представим число p в виде (2), тогда суммирование в формуле (4) можно разбить на три суммы: по старшим разрядам, s-му и младшим соответственно. При этом индекс суммирования также представляется посредством r-ичного разложения с выделенным s-м разрядом.

Формула (4) для подсчёта значений $-c_{p-2}^{(s)}$ в случае $a_s = 0$ имеет вид

$$-c_{p-2}^{(s)} = \sum_{k=0}^{a(s)-1} \sum_{t=0}^{r-1} \sum_{j=0}^{r^s-1} t(kr^{s+1} + tr^s + j) + \sum_{k=a(s)}^{a(s)} \sum_{t=0}^{0} \sum_{j=0}^{\theta-1} t(kr^{s+1} + tr^s + j), \tag{5}$$

а для случая $a_s = 1$ формула (5) принимает вид

$$\begin{aligned} -c_{p-2}^{(s)} = \sum_{k=0}^{a(s)-1} \sum_{t=0}^{r-1} \sum_{j=0}^{r^s-1} t(kr^{s+1} + tr^s + j) + \sum_{k=a(s)}^{a(s)} \sum_{t=0}^{0} \sum_{j=0}^{r^s-1} t(kr^{s+1} + tr^s + j) + \\ + \sum_{k=a(s)}^{a(s)} \sum_{t=1}^{1} \sum_{j=0}^{\theta-1} t(kr^{s+1} + tr^s + j). \end{aligned} \tag{6}$$

Так как получаемые в ходе анализа формулы (6) громоздкие выражения не дают возможности определить, верно условие $-c_{p-2}^{(s)} \neq 0$ или нет, применим следующий подход: введём вспомогательные функции δ'_s, определив их для любого $j \in \{0, \dots, p-1\}$ по правилу

$$\delta'_s(j) = \begin{cases} 1, \text{ если } \delta_s(j) \neq 0, \\ 0, \text{ если } \delta_s(j) = 0. \end{cases}$$

Таким образом произведено отождествление всех ненулевых значений функций δ_s. Функции $\delta'_s(x)$ также представимы многочленами $C'^{(s)}(x)$ над полем $\mathbb{Z}_p$, которые находятся при помощи формулы (3) с заменой $\delta_s(j)$ на $\delta'_s(j)$. При этом если $u'_s = (\delta'_s(u(0), \delta'_s(u(1)\dots)$ и $T(u'_s) = p^m - 1$, то очевидно, что $T(u_s) = p^m - 1$, так как справедливы неравенства $T(u) \geqslant T(u_s) \geqslant T(u'_s)$.

Формула (4) для случая $a_s = 0$ принимает вид

$$-c_{p-2}^{\prime(s)} = \sum_{k=0}^{a(s)-1} \sum_{t=1}^{r-1} \sum_{j=0}^{r^s-1} (kr^{s+1} + tr^s + j), \tag{7}$$

а для случая $a_s = 1$

$$-c_{p-2}^{\prime(s)} = \sum_{k=0}^{a(s)-1} \sum_{t=1}^{r-1} \sum_{j=0}^{r^s-1} (kr^{s+1} + tr^s + j) + \sum_{k=a(s)}^{a(s)} \sum_{t=1}^{1} \sum_{j=0}^{\theta-1} (kr^{s+1} + tr^s + j). \tag{8}$$

Лемма 3. Пусть для числа p выполнены условия (2). Тогда для любого $a_s \in \{0, 1\}$ коэффициент при x^{p-2} в многочлене $C'^{(s)}(x)$ отличен от нуля, за исключением случая $a_s = 0$, $\theta = r^s - 1$.

Доказательство. Рассмотрим сначала случай $a_s = 0$, то есть $p = a(s)r^{s+1} + \theta$. Вычислим $-c_{p-2}^{\prime(s)}$ по формуле (7):

$$-c_{p-2}^{\prime(s)} = \sum_{k=0}^{a(s)-1} \sum_{t=1}^{r-1} \sum_{j=0}^{r^s-1} (kr^{s+1} + tr^s + j) = a(s) \sum_{t=1}^{r-1} \sum_{j=0}^{r^s-1} \left(\frac{a(s)-1}{2} r^{s+1} + tr^s + j \right) =$$

$$= a(s)(r-1) \sum_{j=0}^{r^s-1} \left(\frac{a(s)-1}{2} r^{s+1} + \frac{r^{s+1}}{2} + j \right) =$$

$$= \frac{a(s)(r-1)r^s}{2} ((a(s)-1)r^{s+1} + r^{s+1} + r^s - 1) = \frac{a(s)(r-1)r^s}{2} (a(s)r^{s+1} + r^s - 1).$$

Выясним, когда выполняется соотношение $c_{p-2}^{\prime(s)}(x) \equiv 0 \pmod p$.

Заметим, что ни один из элементов, входящих в произведение $a(s)(r-1)r^s/2$, не сравним с нулем по модулю p, а следовательно, и $a(s)(r-1)r^s/2 \not\equiv 0 \pmod p$. Значит, $c_{p-2}^{\prime(s)}(x) \equiv 0 \pmod p$ тогда и только тогда, когда $a(s)r^{s+1} + r^s - 1 \equiv 0 \pmod p$, что возможно только при $\theta = r^s - 1$.

Теперь рассмотрим случай $a_s = 1$, то есть $p = a(s)r^{s+1} + r^s + \theta$. Из (7) и (8) следует, что к вычисленной выше сумме будет добавлено слагаемое

$$\sum_{k=a}^{a(s)} \sum_{t=1}^{1} \sum_{j=0}^{\theta-1} (kr^{s+1} + tr^s + j) = \sum_{j=0}^{\theta-1} (a(s)r^{s+1} + r^s + j) = \theta \left(a(s)r^{s+1} + r^s + (\theta-1)/2 \right).$$

Надо выяснить, верно ли сравнение

$$\frac{a(s)(r-1)r^s}{2} (a(s)r^{s+1} + r^s - 1) + \theta(a(s)r^{s+1} + r^s + (\theta-1)/2) \equiv 0 \pmod p. \tag{9}$$

Так как $p = a(s)r^{s+1} + r^s + \theta$, то $-\theta \equiv r^{s+1} + r^s \pmod p$.

Из (9) получаем $a(s)(r-1)r^s(-\theta-1) + \theta(-1-\theta) \equiv 0 \pmod p$. Так как, согласно лемме 1, $-1-\theta \not\equiv 0 \pmod p$, то элемент $(-1-\theta)$ является обратимым в $\mathbb{Z}_p$. Последнее сравнение равносильно сравнению

$$a(s)(r-1)r^s + \theta \equiv -r^s - \theta - a(s)r^s + \theta = -a(s)r^s - r^s \equiv 0 \pmod p,$$

что выполняется тогда и только тогда, когда $1 + a(s) \equiv 0 \pmod p$. В итоге получаем противоречие с видом числа p, так как, согласно лемме 1, справедливо неравенство $a(s) + 1 < p$, а значит, $-c'^{(s)}_{p-2} \neq 0$, что и требовалось доказать. ■

Теорема 2. Пусть $p = \theta + a_s r^s + a(s)r^{s+1}$, u — ЛРП МП над полем $\mathbb{Z}_p$, последовательности u'_t для любого $t \in \{0, \ldots, k\}$, $k = [\log_r p]$, образованы из последовательностей u_t путём замены в формуле (3) всех значений $y_t = \delta_t(j)$ на

$$\delta'_t(j) = \begin{cases} 1, & \text{если } \delta_t(j) \neq 0, \\ 0, & \text{если } \delta_t(j) = 0. \end{cases}$$

Тогда $T(u'_s) = T(u)$ всегда, за исключением случая $a_s = 0$, $\theta = r^s - 1$.

Доказательство. Заметим, что лемма 2 справедлива и для многочленов $C'^{(s)}(x)$. Тогда сокращение периода ЛРП u'_s возможно, если наибольший общий делитель $p-1$ и чисел $j \in \{1, 2, \ldots, p-2\}$, для которых $c'^{(s)}_j \neq 0$, больше единицы. По лемме 3 коэффициент при x^{p-2} в многочлене $C'^{(s)}(x)$ отличен от нуля, и так как $(p-2, p-1) = 1$, то и наибольший общий делитель всех $j \in \{1, 2, \ldots, p-2\}$, таких, что $c'^{(s)}_j \neq 0$, равен единице. Значит, выполняется равенство $T(u'_s) = p^m - 1 = T(u)$. ■

Следствие 1. В условиях теоремы 2 верно равенство $T(u_t) = T(u)$.

Доказательство следствия вытекает из двойного неравенства $T(u) \geqslant T(u_t) \geqslant T(u'_t)$ для любого $t \in \{0, \ldots, k\}$, $k = [\log_r p]$.

Таким образом, остался не исследованным вопрос о равенстве нулю коэффициента при x^{p-2} в случае $\theta = r^s - 1, a_s = 0$, то есть в случае $p = a(s)r^{s+1} + r^s - 1$.

Лемма 4. Пусть $p = a(s)r^{s+1} + r^s - 1$. Тогда коэффициент при x^{p-2} в многочлене $C^{(s)}(x)$ отличен от нуля при $r \geqslant 3$.

Доказательство. Заметим, что $a(s) \neq 0$, так как иначе получим противоречие с леммой 1. Вычислим сумму (5), учитывая, что $p > r \geqslant 3$:

$$-c^{(s)}_{p-2} = \sum_{k=0}^{a(s)-1} \sum_{t=0}^{r-1} \sum_{j=0}^{r^s-1} t(kr^{s+1} + tr^s + j) + \sum_{k=a(s)}^{a(s)} \sum_{t=0}^{0} \sum_{j=0}^{\theta-1} t(kr^{s+1} + tr^s + j) =$$

$$= \sum_{t=0}^{r-1} \sum_{j=0}^{r^s-1} t\left(\frac{a(s)(a(s)-1)}{2} r^{s+1} + ta(s)r^s + a(s)j\right) =$$

$$= \sum_{j=0}^{r^s-1} \left(\frac{a(s)r(r-1)(a(s)-1)}{4} r^{s+1} + \frac{a(s)r^{s+1}(r-1)(2r-1)}{6} + \frac{a(s)r(r-1)j}{2}\right) =$$

$$= \frac{a(s)r(r-1)(a(s)-1)}{4} r^{2s+1} + \frac{a(s)(r-1)(2r-1)}{6} r^{2s+1} + \frac{a(s)(r^s-1)(r-1)r^{s+1}}{4} =$$

$$= \frac{a(s)r^{s+1}(r-1)}{12}(3r^{s+1}(a(s)-1) + 2r^s(2r-1) + 3(r^s-1)).$$

Так как $\dfrac{a(s)r^{s+1}(r-1)}{12} \not\equiv 0 \pmod p$, сравнение (9) эквивалентно сравнению

$$3r^{s+1}(a(s)-1)+2r^s(2r-1)+3(r^s-1)\equiv 0 \pmod p. \tag{10}$$

Раскроем в полученном выражении скобки. Учитывая сравнение

$$a(s)r^{s+1}\equiv 1-r^s \pmod p,$$

получаем, что выполнение сравнения (10) эквивалентно выполнению сравнения

$$3(1-r^s)+r^{s+1}+r^s-3\equiv 0 \pmod p.$$

Следовательно, $r^{s+1}-2r^s\equiv 0 \pmod p$. Поэтому $r^s(r-2)\equiv 0 \pmod p$, что равносильно сравнению $r-2\equiv 0 \pmod p$. Последнее не выполняется, так как $3\leqslant r<p$.

Таким образом, коэффициент при x^{p-2} в многочлене $C^{(s)}(x)$ отличен от нуля. ■

Теорема 3. Пусть $p=a(s)r^{s+1}+r^s-1$, $r\geqslant 3$, u — ЛРП МП над полем $\mathbb{Z}_p$, последовательности u_s образованы из последовательности u по правилу (1). Тогда $T(u_s)=T(u)$.

Доказательство. Согласно лемме 2, сокращение периода ЛРП u_t возможно, если наибольший общий делитель $p-1$ и чисел $j\in\{1,2,\ldots,p-2\}$, для которых $c_j^{(s)}\neq 0$, больше единицы. Согласно лемме 4, коэффициент при x^{p-2} в многочлене $C^{(s)}(x)$ отличен от нуля, и так как $(p-2,p-1)=1$, то и наибольший общий делитель всех j, таких, что $c_j^{(s)}\neq 0$, равен единице. Значит, $T(u_t)=T(u)=p^m-1$. ■

Замечание 1. Пусть $r=2$. Тогда для каждого нечётного простого числа p, не являющегося числом Мерсенна, найдётся такое s, что $p=2^s-1+a(s)2^{s+1}$. Для так выбранного s в работе [6] доказано, что $T(u_s)=T(u)/2$, и $T(u_t)=T(u)$ для всех $t\neq s$.

Заключение

Из следствия к теореме 2 и теоремы 3 следует, что периоды всех разрядных последовательностей u_s равны периоду последовательности u во всех случаях, за исключением $r=2$, $\theta=r^s-1$ и $a(s)\neq 0$.

ЛИТЕРАТУРА

1. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. Т. 2. М.: Гелиос АРВ, 2003. 416 с.
2. Труды по дискретной математике. Т. 1. / сост. В. Н. Сачков, Ю. Н. Горчинский, А. Н. Зубков, С. В. Яблонский. М.: ТВП, 1997. 280 с.
3. Труды по дискретной математике. Т. 2. / сост. В. Н. Сачков, Ю. Н. Горчинский, А. Н. Зубков, С. В. Яблонский. М.: ТВП, 1998. 314 с.
4. *Zhu X. Y. and Qi W.-F.* On the distinctness of modular reductions of maximal length sequences modulo odd prime powers // Math. Comput. 2008. V. 77. No. 263. P. 1623–1637.
5. *Zheng Q.-X. and Qi W.-F.* A new result on the distinctness of primitive sequences over $\mathbb{Z}/(pq)$ modulo 2 // Finite Fields Their Appl. 2011. V. 17. No. 3. P. 254–274.
6. *Кузьмин А. С.* О периодах разрядов в r-ичной системе счисления знаков линейных рекуррентных последовательностей над конечными простыми полями // Безопасность информационных технологий. 1995. Вып. 4. С. 71–75.
7. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. Т. 1. М.: Гелиос АРВ, 2003. 336 с.

REFERENCES

1. *Gluhov M. M., Elizarov V. P., Nechaev A. A.* Algebra. V. 2. Moscow, Gelios ARV Publ., 2003. 416 p. (in Russian)
2. Sachkov V. N., Gorchinskij Ju. N., Zubkov A. N., Jablonskij S. V., eds. Trudy po Diskretnoi Matematike. V. 1. Moscow, TVP Publ., 1997. 280 p. (in Russian)
3. Sachkov V. N., Gorchinskij Ju. N., Zubkov A. N., Jablonskij S. V., eds. Trudy po Diskretnoi Matematike. V. 2. Moscow, TVP Publ., 1998. 314 p. (in Russian)
4. *Zhu X. Y. and Qi W.-F.* On the distinctness of modular reductions of maximal length sequences modulo odd prime powers. Math. Comput., 2008, vol. 77, no. 263, pp. 1623–1637.
5. *Zheng Q.-X. and Qi W.-F.* A new result on the distinctness of primitive sequences over $\mathbb{Z}/(pq)$ modulo 2. Finite Fields Their Appl., 2011, vol. 17, no. 3, pp. 254–274.
6. *Kuz'min A. S.* O periodah razrjadov v r-ichnoj sisteme schislenija znakov linejnyh rekurrentnyh posledovatel'nostej nad konechnymi prostymi poljami. Bezopasnost' Informacionnyh Tehnologij, 1995, no. 4, pp. 71–75. (in Russian)
7. *Gluhov M. M., Elizarov V. P., Nechaev A. A.* Algebra. V. 1. Moscow, Gelios ARV Publ., 2003. 336 p. (in Russian)

УДК 519.214.5

О РАСПРЕДЕЛЕНИИ ЧИСЛА ЕДИНИЦ В ДВОИЧНОЙ МУЛЬТИЦИКЛИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНОСТИ[1]

Н. М. Меженная

Московский государственный технический университет им. Н. Э. Баумана, г. Москва, Россия

Работа посвящена исследованию устойчивости теоретико-вероятностной модели, описывающей генератор Пола. Для этого изучено распределение случайной величины, равной числу единиц в выходной последовательности мультициклического генератора над полем GF(2) в случае, когда двоичные случайные величины, заполняющие регистры, независимы, а вероятности появления единиц в регистрах отличны от 1/2 и могут меняться с ростом длин регистров. Получены точные выражения математического ожидания и дисперсии для этой случайной величины. В случае когда число регистров фиксировано, получены условия, при которых распределение нормированного числа единиц сходится к распределению произведения независимых случайных величин, каждая из которых распределена по стандартному нормальному закону. Доказана нормальная предельная теорема для нормированного числа единиц в случае, когда число регистров стремится к бесконечности. Результаты показывают, что нарушение свойства равновероятности распределения знаков в регистрах приводит к существенным изменениям свойств указанных предельных распределений по сравнению с равновероятным случаем.

Ключевые слова: *мультициклическая последовательность, генератор Пола, центральная предельная теорема.*

DOI 10.17223/20710410/27/7

ON DISTRIBUTION OF NUMBER OF ONES IN BINARY MULTICYCLE SEQUENCE

N. M. Mezhennaya

Bauman Moscow State Technical University, Moscow, Russia

E-mail: natalia.mezhennaya@gmail.com

The work is devoted to studying the stability of probability-theoretical model which describes Pohl generator. For the purpose, we investigate the distribution of random variable equalled to the number of ones in the outcome sequence of a multicycle generator over the field GF(2) in the case when binary random variables filling the registers are independent and the probabilities of one's occurrences in registers differ from 1/2 and can change with growing the registers lengths. The exact expressions for expectation and variance of the random variable are given. For the case when the number of registers is finite, we derive the conditions under which the distribution of normalized number of ones converges to the distribution of the product of independent

[1]Работа выполнена при финансовой поддержке Министерства образования и науки РФ (тема № 1.2640.2014).

random variables each of which is distributed by standard normal law. We prove the central limit theorem for normalized number of ones when the number of registers tends to infinity. It is shown that breaking the property of equiprobable distribution for binary characters in registers results in significant differences of properties of the limit distributions compared to equiprobable case.

Keywords: *multicycle sequence, Pohl generator, central limit theorem.*

Введение

Пусть $X^{(i)} = \left(X_0^{(i)}, \ldots, X_{n_i-1}^{(i)}\right)$, $i = 1, \ldots, r$;

$$\mathbf{P}\{X_j^{(i)} = 1\} = 1 - \mathbf{P}\{X_j^{(i)} = 0\} = p_i, \quad j = 0, \ldots; n_i - 1, \tag{1}$$

случайные величины, образующие наборы $X^{(1)}, \ldots, X^{(r)}$, независимы в совокупности. При этом знаки $X_j^{(i)}$, $j = 0, \ldots, n_i - 1$, представляют собой заполнения i-го регистра $X^{(i)}$, $i = 1, \ldots, r$. Обычно считается, что числа $n_1, \ldots, n_r$ попарно взаимно просты.

Пусть последовательность Z_t, $t = 0, \ldots, n_1, \ldots n_r - 1$, образована по правилу

$$Z_t = \bigoplus_{i=1}^{r} X_{t(n_i)}^{(i)}, \tag{2}$$

где $t(n) = t \bmod n$. Последовательность Z_t, построенную по формуле (2), принято называть мультициклической [1, 2].

Если случайные величины, представляющие заполнения регистров, независимы в совокупности и распределены равновероятно, то последовательность представляет собой естественную теоретико-вероятностную модель выходной последовательности мультициклического генератора с r регистрами (генератора Пола).

Свойства мультициклической последовательности Z_t при равновероятном распределении знаков в наборах $X^{(1)}, \ldots, X^{(r)}$ изучены в работах [2–5]. В [2] отмечено, что если выходная последовательность Z_t имеет длину порядка $\sqrt{n_1 \ldots n_r}$ и менее, то она обладает свойствами, аналогичными свойствам последовательности из независимых равновероятно распределённых двоичных случайных величин. Это позволяет использовать генератор Пола в качестве генератора псевдослучайных чисел с большой длиной цикла (примеры других генераторов с большой длиной цикла можно найти в [6, 7]).

В работах [3–5] изучен случай, когда длина выходной последовательности равна длине полного цикла $n_1 \cdot \ldots \cdot n_r$. В [3] в предположении, что регистры заполнены равновероятными независимыми случайными величинами, получены оценки точности аппроксимации распределения числа единиц в мультициклической случайной последовательности логнормальным распределением и распределением произведения r независимых нормальных случайных величин.

Интересным представляется вопрос, как изменится предельное распределение числа единиц в выходной последовательности при нарушении условий модели, связанных с независимостью случайных величин, представляющих заполнения регистров. В [5] показано, что замена условия независимости знаков, образующих заполнения регистров, на условие их конечной зависимости не меняет вид предельных распределений.

В настоящей работе проведено исследование устойчивости данной модели для случая, когда двоичные знаки, образующие наборы $X^{(1)}, \ldots, X^{(r)}$, независимы, а их вероятности могут меняться с ростом длин регистров. Оказывается, что в этом случае предельные распределения числа единиц в выходной последовательности могут существенно отличаться от предельных распределений, приведённых в работах [3, 5].

1. Основные результаты

Обозначим

$$S_i = \sum_{j=0}^{n_i-1} X_j^{(i)}, i = 1, \ldots, r, \quad \xi_r = \sum_{j=0}^{n_1 \ldots n_r - 1} Z_j.$$

Известно [3], что

$$n_1 \ldots n_r - 2\xi_r = (n_1 - 2S_1) \ldots (n_r - 2S_r). \tag{3}$$

Теорема 1. Пусть случайные величины в наборах $X^{(1)}, \ldots, X^{(r)}$ независимы в совокупности и имеют распределения (1). Тогда

$$\mathbf{E}\xi_r = \frac{1}{2} n_1 \ldots n_r \left(1 - \prod_{i=1}^{r} (1 - 2p_i)\right); \tag{4}$$

$$\mathbf{D}\xi_r = \frac{1}{4}\left(\prod_{i=1}^{r} \left(n_i^2 (1-2p_i)^2 + 4n_i p_i (1-p_i)\right) - \left(n_1 \ldots n_r \prod_{i=1}^{r} (1-2p_i)\right)^2\right). \tag{5}$$

Доказательство. Вычислим математическое ожидание случайной величины ξ_r. Из (3) следует, что

$$\mathbf{E}\xi_r = \frac{1}{2}\left(n_1 \ldots n_r - \mathbf{E}(n_1 - 2S_1) \ldots (n_r - 2S_r)\right) =$$
$$= \frac{1}{2}\left(n_1 \ldots n_r - (n_1 - 2\mathbf{E}S_1) \ldots (n_r - 2\mathbf{E}S_r)\right) =$$
$$= \frac{1}{2}\left(n_1 \ldots n_r - (n_1 - 2n_1p_1) \ldots (n_r - 2n_rp_r)\right) = \frac{1}{2} n_1 \ldots n_r \left(1 - \prod_{i=1}^{r} (1-2p_i)\right).$$

Теперь вычислим дисперсию. Из (3) получим

$$\mathbf{D}\xi_r = \frac{1}{4}\mathbf{D}\left((n_1 - 2S_1) \ldots (n_r - 2S_r)\right) =$$
$$= \frac{1}{4}\left(\mathbf{E}\left((n_1 - 2S_1)^2 \ldots (n_r - 2S_r)^2\right) - \left(\mathbf{E}(n_1 - 2S_1) \ldots (n_r - 2S_r)\right)^2\right) =$$
$$= \frac{1}{4}\left(\mathbf{E}(n_1 - 2S_1)^2 \ldots \mathbf{E}(n_r - 2S_r)^2 - \left((n_1 - 2n_1p_1) \ldots (n_r - 2n_rp_r)\right)^2\right).$$

Так как

$$\mathbf{E}(n_i - 2S_i)^2 = \mathbf{E}(n_i - 2n_ip_i + 2n_ip_i - 2S_i)^2 = (n_i - 2n_ip_i)^2 + 4\mathbf{E}(n_ip_i - S_i)^2 =$$
$$= n_i^2(1-2p_i)^2 + 4\mathbf{D}S_i = n_i^2(1-2p_i)^2 + 4n_ip_i(1-p_i),$$

то

$$\mathbf{D}\xi_r = \frac{1}{4}\left(\prod_{i=1}^{r} \left(n_i^2 (1-2p_i)^2 + 4n_i p_i (1-p_i)\right) - \left(n_1 \ldots n_r \prod_{i=1}^{r} (1-2p_i)\right)^2\right).$$

Теорема доказана. ■

Замечание 1. При $p_1 = \ldots = p_r = 1/2$ формулы (4) и (5) совпадают с формулами (4) работы [3].

Пусть $S_i^* = \dfrac{S_i - n_ip_i}{\sqrt{n_ip_i(1-p_i)}}$, $i = 1, \ldots, r$. Тогда

$$n_i - 2S_i = n_i(1-2p_i) - 2\sqrt{n_ip_i(1-p_i)}S_i^* = 2\sqrt{n_ip_i(1-p_i)}\left(\frac{n_i(1-2p_i)}{2\sqrt{n_ip_i(1-p_i)}} - S_i^*\right).$$

Обозначим $a_i = \dfrac{n_i(1-2p_i)}{2\sqrt{n_i p_i(1-p_i)}}$, $\tilde{\xi}_r = \dfrac{n_1 \dots n_r - 2\xi_r}{2^r \left(\prod\limits_{i=1}^{r} n_i p_i (1-p_i) \right)^{1/2}}$. Из (3) следует, что

$$\tilde{\xi}_r = \prod_{i=1}^{r} (a_i - S_i^*). \tag{6}$$

Перенумеруем векторы $X^{(1)}, \dots, X^{(r)}$ так, что $|a_1| \leqslant |a_2| \leqslant \dots \leqslant |a_r|$.

Теорема 2. Пусть случайные величины в наборах $X^{(1)}, \dots, X^{(r)}$ независимы в совокупности и имеют распределения (1). Пусть $n_1, \dots, n_r \to \infty$ и вероятности $p_i = p_i(n_i)$, $i = 1, \dots, r$, меняются так, что $n_i p_i(1-p_i) \to \infty$, $i = 1, \dots, k$. Тогда если

$$a_i \to c_i \in \mathbb{R}, \quad i = 1, \dots, k, \quad |a_i| \to +\infty, \quad i = k+1, \dots, r, \quad 1 \leqslant k \leqslant r-1,$$

то $\dfrac{\tilde{\xi}_r}{a_{k+1} \dots a_r} \xrightarrow{\mathbf{d}} \prod\limits_{i=1}^{k} \eta_i$, где случайные величины $\eta_1, \dots, \eta_r$ независимы и имеют нормальный закон распределения со средними $c_1, \dots, c_r$ соответственно и единичными дисперсиями.

Доказательство. Заметим, что при указанных условиях выполнены условия теоремы Муавра — Лапласа для случайных величин S_i^*, $i = 1, \dots, k$ [8, гл. I, § 6], значит, при $k = r$ утверждение теоремы очевидно. Пусть $k \leqslant r-1$. Из (6) следует, что

$$\begin{gathered} \frac{\tilde{\xi}_r}{a_{k+1} \dots a_r} = \frac{1}{a_{k+1} \dots a_r} \prod_{i=1}^{r} (a_i - S_i^*) = \\ = (a_1 - S_1^*) \dots (a_k - S_k^*) \left(1 - \frac{1}{a_{k+1}} S_{k+1}^*\right) \dots \left(1 - \frac{1}{a_r} S_r^*\right). \end{gathered} \tag{7}$$

При $i = k+1, \dots, r$ из неравенства Чебышева имеем

$$\mathbf{P}\left\{ \left| 1 - \frac{1}{a_i} S_i^* - 1 \right| > x \right\} = \mathbf{P}\left\{ |S_i^*| > |a_i| x \right\} \leqslant \frac{1}{(a_i x)^2} \mathbf{D} S_i^* = \frac{1}{(a_i x)^2}. \tag{8}$$

Так как правая часть в неравенстве (8) стремится к нулю в условиях теоремы, то из (7) и (8) следует, что

$$\begin{gathered} a_i - S_i^* \xrightarrow{\mathbf{d}} \eta_i, \ \ a_i \to c_i, \ \ i = 1, \dots, k, \\ 1 - \frac{1}{a_i} S_i^* \xrightarrow{\mathbf{P}} 1, \ \ |a_i| \to +\infty, \ \ i = k+1, \dots, r. \end{gathered}$$

Тогда из (7) и независимости случайных величин $S_1^*, \dots, S_r^*$ получаем утверждение теоремы. ■

Замечание 2. Условия теоремы 2 выполнены, если, например,

$$p_i = \frac{1}{2} - \frac{c_i}{\sqrt{n_i}}, \ i = 1, \dots, k, \quad p_i = \frac{1}{2} - \frac{A_i}{\sqrt{n_i}}, \ i = k+1, \dots, r,$$

где $c_1, \dots, c_k$ — постоянные, а $A_{k+1}, \dots, A_r$ — бесконечно большие величины, такие, что $A_i / \sqrt{n_i} \to 0$ при $n_1, \dots, n_r \to \infty$. В этом случае главный член дисперсии случайной величины ξ_r (см. (5)) равен

$$4^r \sum_{i=k+1}^{r} \sqrt{n_i} A_i \prod_{\substack{j=k+1,\dots,r; \\ j \neq i}} n_j A_j^2 \prod_{l=1}^{k} n_l c_l^2.$$

Следствие 1. Пусть выполнены условия теоремы 2 и $a_i \to 0 \in \mathbb{R}$, $i = 1, \ldots, r$. Тогда $\tilde{\xi}_r \xrightarrow{\mathrm{d}} \prod\limits_{i=1}^{r} \eta_i$, где случайные величины $\eta_1, \ldots, \eta_r$ независимы и имеют стандартный нормальный закон распределения.

Замечание 3. Следствие 1 указывает условия на характер изменения вероятностей $p_1, \ldots, p_r$, при выполнении которых сохраняет свой вид предельное распределение следствия 2 работы [3].

Теорема 3. Пусть случайные величины в наборах $X^{(1)}, \ldots, X^{(r)}$ независимы в совокупности и имеют распределения (1). Пусть при $n_1, \ldots, n_r \to +\infty$ вероятности $p_i = p_i(n_i)$, $i = 1, \ldots, r$, меняются так, что $n_i p_i (1 - p_i) \to \infty$. Если $|a_i| \to +\infty$, $i = 1, \ldots, r$, то закон распределения случайной величины $\dfrac{\tilde{\xi}_r - a_1 \ldots a_r}{a_1 \ldots a_r \sqrt{\frac{1}{a_1^2} + \frac{1}{a_2^2} + \ldots + \frac{1}{a_r^2}}}$ сходится к стандартному нормальному закону.

Доказательство. Из (6) имеем

$$\begin{aligned}
\frac{\tilde{\xi}_r}{a_2 \ldots a_r} &= \frac{1}{a_2 \ldots a_r} \prod_{i=1}^{r} (a_i - S_i^*) = (a_1 - S_1^*) \left(1 - \frac{1}{a_2} S_2^*\right) \ldots \left(1 - \frac{1}{a_r} S_r^*\right) = \\
&= a_1 \left(1 - \sum_{i=1}^{r} \frac{S_i^*}{a_i} + \sum_{i=2}^{r} \sum_{1 \leqslant j_1 < \ldots < j_i \leqslant r} (-1)^i \frac{S_{j_1}^* \ldots S_{j_i}^*}{a_{j_1} \ldots a_{j_i}}\right) = \qquad (9) \\
&= a_1 - \sum_{i=1}^{r} \frac{a_1 S_i^*}{a_i} + \sum_{i=2}^{r} \sum_{1 \leqslant j_1 < \ldots < j_i \leqslant r} (-1)^i \frac{a_1 S_{j_1}^* \ldots S_{j_i}^*}{a_{j_1} \ldots a_{j_i}}.
\end{aligned}$$

Заметим, что при $x > 0$ в силу неравенства Чебышева

$$\begin{aligned}
&\mathbf{P}\left\{\left|\sum_{i=2}^{r} \sum_{1 \leqslant j_1 < \ldots < j_i \leqslant r} (-1)^i \frac{a_1 S_{j_1}^* \ldots S_{j_i}^*}{a_{j_1} \ldots a_{j_i}}\right| > x\right\} \leqslant \frac{1}{x^2} \mathbf{D}\left(\sum_{i=2}^{r} \sum_{1 \leqslant j_1 < \ldots < j_i \leqslant r} (-1)^i \frac{a_1 S_{j_1}^* \ldots S_{j_i}^*}{a_{j_1} \ldots a_{j_i}}\right) \leqslant \\
&\leqslant \frac{1}{x^2} \sum_{i=2}^{r} \sum_{1 \leqslant j_1 < \ldots < j_i \leqslant r} \sum_{i'=2}^{r} \sum_{1 \leqslant k_1 < \ldots < k_{i'} \leqslant r} (-1)^{i+i'} \operatorname{cov}\left(\frac{a_1 S_{j_1}^* \ldots S_{j_i}^*}{a_{j_1} \ldots a_{j_i}}, \frac{a_1 S_{k_1}^* \ldots S_{k_{i'}}^*}{a_{k_1} \ldots a_{k_{i'}}}\right) \leqslant \qquad (10) \\
&\leqslant \frac{1}{x^2} \sum_{i=2}^{r} \sum_{1 \leqslant j_1 < \ldots < j_i \leqslant r} \sum_{i'=2}^{r} \sum_{1 \leqslant k_1 < \ldots < k_{i'} \leqslant r} \left|\frac{a_1}{a_{j_1} \ldots a_{j_i}}\right| \left|\frac{a_1}{a_{k_1} \ldots a_{k_{i'}}}\right| \left|\operatorname{cov}\left(S_{j_1}^* \ldots S_{j_i}^*, S_{k_1}^* \ldots S_{k_{i'}}^*\right)\right|.
\end{aligned}$$

Заметим, что

$$\mathbf{D}\left(S_{j_1}^* \ldots S_{j_i}^*\right) = \mathbf{E}\left(S_{j_1}^* \ldots S_{j_i}^*\right)^2 = \mathbf{E}\left(S_{j_1}^*\right)^2 \ldots \mathbf{E}\left(S_{j_i}^*\right)^2 = \mathbf{D}S_{j_1}^* \ldots \mathbf{D}S_{j_i}^* = 1.$$

Если существует l, для которого $j_l \notin \{k_1, \ldots, k_{i'}\}$, то

$$\begin{aligned}
\operatorname{cov}\left(S_{j_1}^* \ldots S_{j_i}^*, S_{k_1}^* \ldots S_{k_{i'}}^*\right) &= \mathbf{E}\left(S_{j_1}^* \ldots S_{j_i}^* S_{k_1}^* \ldots S_{k_{i'}}^*\right) = \\
&= \mathbf{E}S_{j_l}^* \mathbf{E}\left(S_{j_1}^* \ldots S_{j_l-1}^* S_{j_l+1}^* \ldots S_{j_i}^* S_{k_1}^* \ldots S_{k_{i'}}^*\right) = 0.
\end{aligned}$$

Значит, $\operatorname{cov}\left(S_{j_1}^* \ldots S_{j_i}^*, S_{k_1}^* \ldots S_{k_{i'}}^*\right) \neq 0$ только при $i = i', j_1 = k_1, \ldots, j_i = k_{i'}$ и

$$\operatorname{cov}\left(S_{j_1}^* \ldots S_{j_i}^*, S_{j_1}^* \ldots S_{j_i}^*\right) = \mathbf{D}\left(S_{j_1}^* \ldots S_{j_i}^*\right) = 1.$$

Подставляя последнюю оценку в (10), получаем

$$\mathbf{P}\left\{\left|\sum_{i=2}^{r} \sum_{1 \leqslant j_1 < \ldots < j_i \leqslant r} (-1)^i \frac{a_1 S_{j_1}^* \ldots S_{j_i}^*}{a_{j_1} \ldots a_{j_i}}\right| > x\right\} \leqslant \frac{1}{x^2} \sum_{i=2}^{r} \sum_{1 \leqslant j_1 < \ldots < j_i \leqslant r} \left(\frac{a_1}{a_{j_1} \ldots a_{j_i}}\right)^2. \qquad (11)$$

Так как $\dfrac{a_1}{a_{j_1}\dots a_{j_i}} \to 0$ при любом $i \geqslant 2$, правая часть формулы (11) стремится к нулю. Значит,

$$\frac{\tilde{\xi}_r - a_1\dots a_r}{a_1\dots a_r\sqrt{\frac{1}{a_1^2}+\dots+\frac{1}{a_r^2}}} = -\left(\sum_{i=1}^{r}\frac{S_i^*}{a_i\sqrt{\frac{1}{a_1^2}+\dots+\frac{1}{a_r^2}}} + \frac{1}{a_1\sqrt{\frac{1}{a_1^2}+\dots+\frac{1}{a_r^2}}}\eta\right), \tag{12}$$

где

$$\eta = \sum_{i=2}^{r}\sum_{1\leqslant j_1<\dots<j_i\leqslant r}(-1)^i\frac{a_1 S_{j_1}^*\dots S_{j_i}^*}{a_{j_1}\dots a_{j_i}} \xrightarrow{\mathbf{P}} 0. \tag{13}$$

Далее из свойств нормального распределения, ограниченности коэффициентов $\dfrac{1}{a_i\sqrt{\frac{1}{a_1^2}+\dots+\frac{1}{a_r^2}}}$ при всех $i = 1,\dots,r$ выражения $\sum\limits_{i=1}^{r}\dfrac{S_i^*}{a_i\sqrt{\frac{1}{a_1^2}+\dots+\frac{1}{a_r^2}}}$, независимости случайных величин $S_1^*,\dots,S_r^*$ и сходимости их распределений к стандартному нормальному закону получаем, что случайная величина $\sum\limits_{i=1}^{r}\dfrac{S_i^*}{a_i\sqrt{\frac{1}{a_1^2}+\dots+\frac{1}{a_r^2}}}$ имеет в пределе стандартный нормальный закон распределения. Значит, из формул (12), (13) и симметричности плотности распределения стандартного нормального закона следует утверждение теоремы. ■

Замечание 4. Условия теоремы 3 выполнены, если, например, случайные величины в наборах $X^{(1)},\dots,X^{(r)}$ независимы в совокупности, $n_i \to +\infty$ при всех $i = 1,\dots,r$, а вероятности p_i остаются постоянными.

Теперь обратимся к случаю, когда число регистров r при переходе к пределу стремится к бесконечности.

Теорема 4. Пусть случайные величины в наборах $X^{(1)},\dots,X^{(r)}$ независимы в совокупности и имеют распределения (1), $p_i = p_i(n_i)$, $i = 1,\dots,r$. Пусть при $r \to +\infty$ величины $n_1,\dots,n_r$ и $p_1,\dots,p_r$ меняются так, что

$$\sum_{i=2}^{r}\sum_{1\leqslant j_1<\dots<j_i\leqslant r}\left(\frac{a_1}{a_{j_1}\dots a_{j_i}}\right)^2 \to 0 \quad \text{и} \quad \frac{\sum\limits_{i=1}^{r}|a_i|^{-3}(p_i(1-p_i))^{-3/4}}{\left(\sum\limits_{i=1}^{r}\dfrac{1}{a_i^2}\right)^{3/2}} \to 0. \tag{14}$$

Тогда закон распределения случайной величины $\dfrac{\tilde{\xi}_r - a_1\dots a_r}{a_1\dots a_r\sqrt{\frac{1}{a_1^2}+\dots+\frac{1}{a_r^2}}}$ сходится к стандартному нормальному закону.

Доказательство. Воспользуемся представлением (9). Из оценки (11) и первого из условий (14) следует соотношение (13). Значит, остаётся показать, что при $r \to \infty$ случайная величина $\nu = \sum\limits_{i=1}^{r}\dfrac{S_i^*}{a_i\sqrt{\frac{1}{a_1^2}+\dots+\frac{1}{a_r^2}}}$ сходится по распределению к стандартному нормальному закону.

Для этого воспользуемся неравенством Берри — Эссеена [8, с. 356], согласно которому при любом $x \in \mathbb{R}$

$$|F_\nu(x) - \Phi(x)| \leqslant C \frac{\sum\limits_{i=1}^{r} \mathbf{E}\left|\dfrac{a_1 S_i^*}{a_i}\right|^3}{\left(1 + \left(\dfrac{a_1}{a_2}\right)^2 + \ldots + \left(\dfrac{a_1}{a_r}\right)^2\right)^{3/2}} = C \frac{\sum\limits_{i=1}^{r} \mathbf{E}\left|\dfrac{S_i^*}{a_i}\right|^3}{\left(\dfrac{1}{a_1^2} + \ldots + \dfrac{1}{a_r^2}\right)^{3/2}}. \qquad (15)$$

Оценим отдельно каждое слагаемое в числителе правой части последней оценки. В силу неравенства Ляпунова [9, с. 48] имеем

$$\mathbf{E}\left|\frac{S_i^*}{a_i}\right|^3 = \frac{1}{|a_i|^3}\mathbf{E}|S_i^*|^3 \leqslant \frac{1}{|a_i|^3}\left(\mathbf{E}(S_i^*)^4\right)^{3/4}.$$

Для вычисления $\mathbf{E}(S_i^*)^4$ воспользуемся производящей функцией моментов для биномиальной случайной величины S_i. Обозначим через $g_X(t) = \mathbf{E}e^{tX}$ производящую функцию моментов случайной величины X. Имеем

$$g_{S_i - n_i p_i}(t) = \mathbf{E}e^{t(S_i - n_i p_i)} = e^{-tn_i p_i}\mathbf{E}e^{tS_i} = e^{-tn_i p_i} g_{S_i}(t) = e^{-tn_i p_i}\left(1 - p_i + p_i e^t\right)^n.$$

Тогда

$$\begin{aligned}
\mathbf{E}(S_i^*)^4 &= \frac{1}{\left(n_i p_i (1-p_i)\right)^2} \frac{d^4}{dt^4} g_{S_i - n_i p_i}(t)\Big|_{t=0} = \\
&= \frac{1}{\left(n_i p_i (1-p_i)\right)^2} \frac{n_i p_i (1-p_i)}{24} \left(1 + 3(n_i - 2)p_i(1-p_i)\right) = \\
&= \frac{1}{24 n_i p_i (1-p_i)} \left(1 + 3(n_i - 2)p_i(1-p_i)\right) \leqslant \\
&\leqslant \frac{1}{24 n_i p_i (1-p_i)} \left(1 + \frac{3}{4}(n_i - 2)\right) \leqslant \frac{1}{24 n_i p_i (1-p_i)} \frac{3}{4} n_i = \frac{1}{32 p_i (1-p_i)}.
\end{aligned}$$

Поэтому в правой части неравенства (15) получим

$$|F_\nu(x) - \Phi(x)| \leqslant \frac{C}{(32)^{3/4}} \frac{\sum\limits_{i=1}^{r} |a_i|^{-3} \left(p_i(1-p_i)\right)^{-3/4}}{\left(\dfrac{1}{a_1^2} + \ldots + \dfrac{1}{a_r^2}\right)^{3/2}}.$$

В условиях теоремы правая часть последней оценки стремится к нулю при $r \to \infty$. ■

Замечание 5. Условия теоремы 4 выполнены, если, например, случайные величины в наборах $X^{(1)}, \ldots, X^{(r)}$ независимы в совокупности, $r \to +\infty$, $n_i \to +\infty$, а вероятности p_i остаются постоянными, $\sum\limits_{i=2}^{r} \sum\limits_{1 \leqslant j_1 < \ldots < j_i \leqslant r} \dfrac{n_1}{n_{j_1} \ldots n_{j_i}} \to 0$ и $\dfrac{\sum\limits_{i=1}^{r} n_i^{-3/2}}{\left(\sum\limits_{i=1}^{r} \dfrac{1}{n_i}\right)^{3/2}} \to 0.$

Замечание 6. Вместо условий (14) теоремы 4 можно написать более простые, но несколько более грубые условия:

$$\frac{r}{a_2} \to 0, \quad \max\left\{\left(p_i(1-p_i)\right)^{-3/4}\right\} \frac{a_r^3}{a_1^2 \sqrt{r}} \to 0.$$

Действительно,

$$\sum_{i=2}^{r}\sum_{1\leqslant j_1<\ldots<j_i\leqslant r}\left(\frac{a_1}{a_{j_1}\ldots a_{j_i}}\right)^2\leqslant\sum_{i=2}^{r}\sum_{1\leqslant j_1<\ldots<j_i\leqslant r}\left(\frac{a_1}{a_1a_{j_2}\ldots a_{j_i}}\right)^2<$$

$$<\sum_{i=2}^{r}C_r^i a_2^{-2(i-1)}=a_2^2\sum_{i=2}^{r}C_r^i a_2^{-2i}=$$

$$=a_2^2\left((1+a_2^{-2})^r-1-\frac{r}{a_2^2}\right)\leqslant a_2^2\left(e^{r/a_2^2}-1-\frac{r}{a_2^2}\right)\leqslant a_2^2\frac{r^2}{2a_2^4}e^{r/a_2^2}=\frac{r^2}{2a_2^2}e^{r/a_2^2}.$$

Значит, если $r/a_2\to 0$, то выполнено первое из условий (14).

Аналогично

$$\frac{\sum\limits_{i=1}^{r}|a_i|^{-3}(p_i(1-p_i))^{-3/4}}{\left(\sum\limits_{i=1}^{r}\dfrac{1}{a_i^2}\right)^{3/2}}\leqslant\max\left\{(p_i(1-p_i))^{-3/4}\right\}\frac{\sum\limits_{i=1}^{r}|a_i|^{-3}}{\left(\sum\limits_{i=1}^{r}\dfrac{1}{a_i^2}\right)^{3/2}}\leqslant$$

$$\leqslant\max\left\{(p_i(1-p_i))^{-3/4}\right\}\frac{r}{|a_1|^3(ra_r^{-2})^{3/2}}=\max\left\{(p_i(1-p_i))^{-3/4}\right\}\frac{|a_r|^3}{|a_1|^3\sqrt{r}}.$$

Значит, если правая часть последней формулы стремится к нулю, то выполнено второе условие в (14).

Заключение

Проведено исследование устойчивости модели, описывающей генератор Пола. Для этого изучены вероятностные свойства числа единиц в выходной последовательности мультициклического генератора над полем GF(2) в случае, когда двоичные случайные знаки, заполняющие регистры, независимы, а вероятности появления единиц в регистрах отличны от $1/2$ и могут меняться с ростом длин регистров. Для случая фиксированного числа регистров доказана предельная теорема о сходимости распределения нормированного числа единиц к распределению произведения независимых случайных величин, каждая из которых распределена по стандартному нормальному закону. Доказана также нормальная предельная теорема для нормированного числа единиц в случае, когда число регистров стремится к бесконечности. Результаты показывают, что нарушение свойства равновероятности распределения знаков в регистрах приводит к существенным изменениям свойств указанных предельных распределений по сравнению с равновероятным случаем.

Автор выражает признательность В. Г. Михайлову за ценные замечания и постоянное внимание к работе.

ЛИТЕРАТУРА

1. *Pohl P.* The multicyclic vector method of generating pseudo-random numbers. I. Theoretical background, description of the method and algebraic analysis. Report TRITA-NA-7307. Stockholm, Sweden: Royal Inst. of Technology, 1973. 36 p.
2. *Pohl P.* Description of MCV, a pseudo-random number generator // Scand. Actuarial J. 1976. No. 1. P. 1–14.
3. *Меженная Н. М., Михайлов В. Г.* О распределении числа единиц в выходной последовательности генератора Пола над полем GF(2) // Математические вопросы криптографии. 2013. Т. 4. № 4. С. 95–107.

4. *Меженная Н. М.* Предельные теоремы для числа плотных серий с заданными параметрами в выходной последовательности генератора Пола // Инженерный журнал: наука и инновации. 2013. № 4(16). С. 1–8.
5. *Mezhennaya N. M.* Convergence rate estimators for the number of ones in outcome sequence of MCV generator with m-dependent registers items // Siber. Electr. Math. Rep. 2014. V. 11. P. 18–25.
6. *Douglas W. M.* A nonlinear random number generator with known, long cycle length // Cryptologia. 1993. V. 17(1). P. 55–62.
7. *Deng L.-Y. and Xu H.* A system of high-dimensional, efficient, long-cycle and portable uniform random number generators // ACM Trans. Modeling Comp. Simul. 2003. V. 13(4). P. 299–309.
8. *Ширяев А. Н.* Вероятность. М.: Наука, 1989. 581 с.
9. *Севастьянов Б. А.* Курс теории вероятностей и математической статистики. М.: Наука, 1982. 256 с.

REFERENCES

1. *Pohl P.* The multicyclic vector method of generating pseudo-random numbers. I. Theoretical background, description of the method and algebraic analysis. Report TRITA-NA-7307. The Royal Institute of Technology, Department of Information Processing and Computer Science, Stockholm, Sweden, 1973. 36 p.
2. *Pohl P.* Description of MCV, a pseudo-random number generator. Scand. Actuarial J., 1976, no. 1, pp. 1–14.
3. *Mezhennaja N. M., Mihajlov V. G.* O raspredelenii chisla edinic v vyhodnoj posledovatel'nosti generatora Pola nad polem GF(2). Matematicheskie Voprosy Kriptografii, 2013, vol. 4, no. 4, pp. 95–107. (in Russian)
4. *Mezhennaja N. M.* Predel'nye teoremy dlja chisla plotnyh serij s zadannymi parametrami v vyhodnoj posledovatel'nosti generatora Pola. Inzhenernyj Zhurnal: Nauka i Innovacii, 2013, no. 4(16), pp. 1–8. (in Russian)
5. *Mezhennaya N. M.* Convergence rate estimators for the number of ones in outcome sequence of MCV generator with m-dependent registers items. Siber. Electr. Math. Rep., 2014, vol. 11, pp. 18–25.
6. *Douglas W. M.* A nonlinear random number generator with known, long cycle length. Cryptologia, 1993, vol. 17(1), pp. 55–62.
7. *Deng L.-Y. and Xu H.* A system of high-dimensional, efficient, long-cycle and portable uniform random number generators. ACM Trans. Modeling Comp. Simul., 2003, vol. 13(4), pp. 299–309.
8. *Shirjaev A. N.* Verojatnost'. Moscow, Nauka Publ., 1989. 581 p. (in Russian)
9. *Sevast'janov B. A.* Kurs teorii verojatnostej i matematicheskoj statistiki. Moscow, Nauka Publ., 1982. 256 p. (in Russian)

УДК 519.4

О НЕКОТОРЫХ КЛАССАХ РАЗЛОЖИМЫХ ЦЕПЕЙ МАРКОВА НА КОНЕЧНОЙ АБЕЛЕВОЙ ГРУППЕ

М. И. Рожков

Московский институт электроники и математики Национального исследовательского университета Высшая Школа Экономики, г. Москва, Россия

Рассматривается задача разложения простой однородной цепи Маркова Γ в сумму $s \geqslant 2$ взаимно независимых составляющих цепей Маркова $\Gamma^{(i)}$, заданных на конечной абелевой группе G. Данная задача связана с известной процедурой укрупнения состояний цепи Маркова. Описывается широкий класс цепей, допускающих такое разложение в сумму двух цепей бесконечным числом способов. Результаты данной работы могут быть полезны при оценке возможностей восстановления параметров исходных цепей Маркова, поступающих в узел суммирования, по результирующей последовательности. Такого сорта задачи возникают при построении и исследовании свойств генераторов случайных последовательностей.

Ключевые слова: *разложение цепи Маркова, сумма цепей Маркова, укрупнение состояний цепи Маркова.*

DOI 10.17223/20710410/27/8

ON SOME CLASSES OF DECOMPOSABLE MARKOV CHAINS ON FINITE ABELIAN GROUP

M. I. Rozhkov

National Research University Higher School of Economics, Moscow, Russia

E-mail: rozhkov.m.i@yandex.ru

The problem for the decomposition of a given simple homogeneous Markov chain into the sum of the components of the chain is considered. The class of chains allowing this decomposition in the infinite number of ways is described.

Keywords: *decomposition of a Markov chain, the summation of Markov chains.*

1. Постановка задачи

Пусть $\Gamma^{(i)} = \gamma_1(i), \gamma_2(i), \ldots$, $i = 1, \ldots, s$ — независимые реализации простых однородных цепей Маркова на конечной абелевой группе $G = (G, +)$ с соответствующими матрицами переходных вероятностей

$$\pi^{(i)} = ||p^{(i)}(g, h)||, \quad g, h \in G, \quad i = 1, 2, \ldots, s.$$

Положим $\Gamma = \gamma_1, \gamma_2, \ldots$, где

$$\gamma_j = \sum_{i=1}^{s} \gamma_j(i), \quad j = 1, 2, \ldots$$

В работах [1, 2] исследовались условия, при которых элементы результирующей последовательности Γ также связаны простой однородной цепью Маркова с некоторой матрицей переходных вероятностей

$$\pi = ||p(g,h)||, \quad g,h \in G,$$

которая не зависит от начального распределения исходных цепей (т. е. от распределения величин $\gamma_1(i)$, $i = 1, 2, \ldots, s$). В этом случае будем говорить, что цепь Γ разложима в сумму цепей Маркова. Отметим, что рассматриваемая задача разложения цепи Маркова в сумму цепей тесным образом связана с известной процедурой укрупнения состояний цепи Маркова [3].

С каждой строкой матрицы $\pi^{(i)} = ||p^{(i)}(g,h)||$, $g,h \in G$, свяжем элемент группового кольца DG (определение группового кольца см. в [4])

$$p^{(i)}(g) = \sum_{h \in G} p^{(i)}(g,h) \cdot h,$$

где D — поле действительных (рациональных) чисел. Элемент $p^{(i)}(g)$ будем называть характеристической функцией соответствующей строки матрицы $\pi^{(i)}$. В [1, теорема 1 и лемма 3] найдено следующее строение матрицы переходных вероятностей $\pi = ||p(g,h)||$ цепи Γ, являющейся суммой исходных цепей $\Gamma^{(i)}$.

Теорема 1. Пусть сумма $s \geqslant 2$ цепей Маркова с матрицами переходных вероятностей $\pi^{(i)} = ||p^{(i)}(g,h)||$, $g,h \in G$, $i = 1, 2, \ldots, s$, является цепью Маркова с матрицей переходных вероятностей $\pi = ||p(g,h)||$, $g,h \in G$. Тогда для характеристических функций $p(g)$ строк матрицы π в групповом кольце DG выполняются соотношения

$$p(0) = p^{(1)}(0) \cdot p^{(2)}(0) \cdot \ldots \cdot p^{(s)}(0), \quad p(g) = p(0)f(g), \quad g \in G, \tag{1}$$

где f — гомоморфизм группы G в группу мультипликативно обратимых элементов кольца DG; 0 — нулевой элемент группы G.

Вопрос о том, всегда ли цепь с матрицей $\pi = ||p(g,h)||$, характеристические функции строк которой удовлетворяют соотношениям (1), разлагается в сумму s цепей, является открытым. При этом известно следующее достаточное условие марковости для суммы цепей.

Теорема 2 [2, теорема 3]. Пусть на конечной абелевой группе G заданы $s \geqslant 2$ цепей Маркова $\Gamma^{(i)}$ с матрицами переходных вероятностей

$$\pi^{(i)} = ||p^{(i)}(g,h)||, \quad g,h \in G, \quad i = 1, 2, \ldots, s.$$

Сумма цепей Маркова $\Gamma^{(i)}$ также является цепью Маркова, если характеристические функции строк матриц $\pi^{(i)}$ удовлетворяют соотношениям

$$p^{(i)}(g) = p^{(i)}(0)f(g), \quad g \in G, \quad i = 1, 2, \ldots, s,$$

где f — гомоморфизм группы G в группу мультипликативно обратимых элементов кольца DG.

В дальнейшем потребуются два вспомогательных утверждения. Элемент

$$p = \sum_{h \in G} p(h) \cdot h$$

группового кольца DG будем называть вероятностным, если $\sum\limits_{h \in G} p(h) = 1$, $p(h) \geqslant 0$.

Лемма 1. Пусть G — конечная абелева группа, D — поле действительных (рациональных) чисел, $f(g) = \sum\limits_{h\in G} f(g,h)\cdot h$ — произвольный гомоморфизм группы G в группу мультипликативно обратимых элементов кольца DG, такой, что $\sum\limits_{h\in G} f(g,h) = 1$ для любого элемента $g \in G$, M — максимальное значение абсолютных величин коэффициентов $f(g,h)$, $g,h \in G$.

Тогда для любого вероятностного элемента вида

$$p = \frac{1}{|G|}\sum_{h\in G} h + \sum_{h\in G}\varepsilon(h)h, \quad |\varepsilon(h)| < \frac{1}{|G|^2 M}, \quad \sum_{h\in G}\varepsilon(h) = 0$$

произведение $p\cdot f(g)$ также является вероятностным элементом при любом $g \in G$.

Доказательство. Заметим, что

$$p\cdot f(g) = \frac{1}{|G|}\sum_{h\in G} h + \sum_{h\in G}\sum_{r\in G}(\varepsilon(r)f(g,h-r))h.$$

Кроме того, справедливо неравенство

$$|\sum_{r\in G}\varepsilon(r)f(g,h-r)| < \frac{1}{|G|^2 M}M\cdot|G| = 1/|G|.$$

Отсюда следует, что все коэффициенты элемента $p\cdot f(g)$ положительны, и утверждение леммы 1 доказано. ■

Лемма 2. Пусть $p = \frac{1}{|G|}\sum\limits_{h\in G} h + \sum\limits_{h\in G}\varepsilon(h)h$, $\sum\limits_{h\in G}\varepsilon(h) = 0$, — произвольный вероятностный элемент. Тогда справедливо разложение

$$p = L\cdot R,$$

$$L = \frac{1}{|G|}\sum_{h\in G} h + \sum_{h\in G}\varepsilon\cdot h + \delta\cdot 0, \quad \varepsilon\neq 0, \quad \delta\neq 0, \quad \varepsilon|G| + \delta = 0,$$

$$R = \frac{1}{|G|}\sum_{h\in G} h + \sum_{h\in G} r(h)h, \quad r(h) = \varepsilon(h)/\delta.$$

Справедливость леммы 2 проверяется непосредственными расчётами.

2. Основные результаты

Основным результатом настоящей работы является следующее утверждение.

Теорема 3. Пусть цепь Маркова Γ имеет матрицу переходных вероятностей $\pi = ||p(g,h)||$, для характеристических функций строк которой выполнены следующие условия:

1) $p(0) = \frac{1}{|G|}\sum\limits_{h\in G} h + \sum\limits_{h\in G}\varepsilon(h)h$, $|\varepsilon(h)| < (1/|G|)^4(1/M)^2$, $\sum\limits_{h\in G}\varepsilon(h) = 0$;
2) $p(g) = p(0)f(g)$, $g\in G$,

где $f(g) = \sum\limits_{h\in G} f(g,h)h$ — заданный гомоморфизм группы G в группу мультипликативно обратимых элементов кольца DG; M — максимальное значение абсолютных величин коэффициентов $f(g,h)$, $g,h\in G$.

Тогда существует разложение $p(0) = p^{(1)}(0)p^{(2)}(0)$, при котором цепь Γ представляется суммой цепей $\Gamma = \Gamma^{(1)} + \Gamma^{(2)}$ с матрицами переходных вероятностей $\pi^{(i)} = ||p^{(i)}(g,h)||$, $g,h\in G$, $i = 1,2$, характеристические функции строк которых имеют вид

$$p^{(i)}(g) = p^{(i)}(0)f(g), \quad g\in G, \quad i = 1,2.$$

Доказательство. В соответствии с леммой 2 для характеристической функции $p(0)$ справедливо разложение

$$p(0) = p^{(1)}(0)p^{(2)}(0) = L \cdot R,$$
$$L = \frac{1}{|G|}\sum_{h\in G} h + \sum_{h\in G} \varepsilon \cdot h + \delta \cdot 0, \quad \varepsilon \neq 0, \quad \delta \neq 0, \quad \varepsilon|G| + \delta = 0,$$
$$R = \frac{1}{|G|}\sum_{h\in G} h + \sum_{h\in G} r(h)h, \quad r(h) = \varepsilon(h)/\delta.$$

Положим в данном разложении

$$|\varepsilon| = (1/|G|)^3(1/M). \tag{2}$$

Тогда

$$|\delta| = |\varepsilon| \cdot |G| = (1/|G|)^2(1/M), \quad |\varepsilon + \delta| = |\varepsilon|(|G| - 1) < (1/|G|)^2(1/M); \tag{3}$$
$$|r(h)| = |\varepsilon(h)/\delta| < (1/|G|)^4(1/M)^2\delta^{-1} = (1/|G|)^2(1/M). \tag{4}$$

Из соотношений (2)–(4) следует, что при указанном выборе параметра ε каждая из функций $p^{(j)}(0)$, $j = 1, 2$, удовлетворяет условиям леммы 1. Тем самым при любом $g \in G$ элемент $p^{(j)}(0)f(g)$ является вероятностным. Теперь справедливость теоремы вытекает из теоремы 2. ■

Следующее утверждение показывает, что разложение $\Gamma = \Gamma^{(1)} + \Gamma^{(2)}$ в условиях теоремы 3 является неоднозначным.

Теорема 4. Пусть выполнены условия теоремы 3. Тогда существует бесконечное множество разложений $p(0) = p^{(1)}(0)p^{(2)}(0)$, при каждом из которых цепь Γ представляется суммой цепей $\Gamma = \Gamma^{(1)} + \Gamma^{(2)}$ с матрицами переходных вероятностей

$$\pi^{(i)} = ||p^{(i)}(g, h)||, \quad g, h \in G, \quad i = 1, 2,$$

характеристические функции строк которых имеют вид

$$p^{(i)}(g) = p^{(i)}(0)f(g), \quad g \in G, \quad i = 1, 2.$$

Доказательство. Пусть в представлении

$$p(0) = \frac{1}{|G|}\sum_{h\in G} h + \sum_{h\in G} \varepsilon(h)h, \quad |\varepsilon(h)| < (1/|G|)^4(1/M)^2, \quad \sum_{h\in G} \varepsilon(h) = 0$$

имеет место $0 < \beta < \max\limits_{h\in G}\{|\varepsilon(h)|\}/((1/|G|)^4(1/M)^2) < 1$. Пусть α — произвольное фиксированное число, $\beta < \alpha < 1$. В соответствии с леммой 2 для характеристической функции $p(0)$ справедливо разложение

$$p(0) = p^{(1)}(0)p^{(2)}(0) = L \cdot R, \tag{5}$$
$$L = \frac{1}{|G|}\sum_{h\in G} h + \sum_{h\in G} \varepsilon \cdot h + \delta \cdot 0, \quad \varepsilon \neq 0, \quad \delta \neq 0, \quad \varepsilon|G| + \delta = 0,$$
$$R = \frac{1}{|G|}\sum_{h\in G} h + \sum_{h\in G} r(h)h, \quad r(h) = \varepsilon(h)/\delta.$$

Положим в разложении (5)

$$|\varepsilon| = (1/|G|)^3(1/M)\alpha. \tag{6}$$

Тогда

$$|\delta| = |\varepsilon| \cdot |G| = (1/|G|)^2(1/M)\alpha, \quad |\varepsilon + \delta| = |\varepsilon|(|G| - 1) < (1/|G|)^2(1/M)\alpha; \tag{7}$$

$$|r(h)| = |\varepsilon(h)/\delta| < \beta(1/|G|)^4(1/M)^2\delta^{-1} = (\beta/\alpha)(1/|G|)^2(1/M). \tag{8}$$

Из соотношений (6)–(8) следует, что при указанном выборе параметра ε каждая из функций $p^{(j)}(0)$, $j = 1, 2$, удовлетворяет условиям леммы 1. Тем самым при любом $g \in G$ элемент $p^{(j)}(0)f(g)$ является вероятностным. Следовательно, учитывая теорему 2, исходная цепь Γ является суммой цепей $\Gamma = \Gamma^{(1)} + \Gamma^{(2)}$ с матрицами переходных вероятностей

$$\pi^{(i)} = ||p^{(i)}(g, h)||, \quad g, h \in G, \quad i = 1, 2,$$

характеристические функции строк которых имеют вид

$$p^{(i)}(g) = p^{(i)}(0)f(g), \quad g \in G, \quad i = 1, 2.$$

При этом различные параметры α ($\beta < \alpha < 1$) отвечают разным матрицам $\pi^{(i)}$ переходных вероятностей. ■

3. Заключительные замечания

Отметим, что из разложения $p(0) = p^{(1)}(0)p^{(2)}(0)$ и вероятностности многочленов $p(0)f(g)$, $g \in G$, не всегда «автоматически» следует вероятностность всех многочленов $p^{(j)}(0)f(g)$, $j = 1, 2$. Об этом свидетельствует следующий пример. Рассмотрим группу $G = \mathbb{Z}_m = \{0, 1, 2, 3\}$ вычетов по модулю $m = 4$. В этом случае кольцо DG есть кольцо многочленов $D[x]/(x^4 - 1)$ по модулю многочлена $x^4 - 1$. И соответственно вероятностные элементы кольца DG принимают вид многочленов

$$p = \sum_{h \in G} p(h)h = \sum_{j \in Z_m} p(j)x^j = p(0) + p(1)x + p(2)x^2 + p(3)x^3.$$

Рассмотрим вероятностные многочлены

$$p = p(x) = p^{(1)}(x)p^{(2)}(x),$$

$$p^{(1)}(x) = p^{(2)}(x) = (1/2 + \varepsilon) + (1/2 - \varepsilon)x, \quad 0 < \varepsilon < 1/2(\sqrt{2} - 1),$$

а также гомоморфизм f группы $\mathbb{Z}_m$ в группу мультипликативно обратимых элементов кольца $D[x]/(x^4 - 1)$:

$$f(m) = \theta^m, \quad \theta = 1/2(1 + x + x^2 + x^3) - 1, \quad m \in \{0, 1, 2, 3\}.$$

Так как $p^{(1)}(x)\theta = -\varepsilon + \varepsilon x + 1/2 \cdot x^2 + 1/2 \cdot x^3$, многочлен $p^{(1)}(x)f(1)$ не является вероятностным. В то же время любой многочлен $p(x)f(m)$ является вероятностным в силу того, что

1) $\theta^2 = 1$;
2) все коэффициенты многочлена $p(x) = (1/2 + \varepsilon)^2 + (1/2 - 2\varepsilon^2)x + (1/2 - \varepsilon)^2x^2$ меньше $1/2$;
3) $p(x)\theta = 1/2(1 + x + x^2 + x^3) - p(x)$.

Результаты данной работы являются развитием аналогичного сорта результатов относительно разложимых законов распределения на конечной абелевой группе (см., например, [5]) и могут быть полезны при оценке возможностей восстановления параметров исходных цепей Маркова, поступающих в узел суммирования, по результирующей последовательности. Такого сорта задачи возникают при построении и исследовании свойств генераторов случайных последовательностей.

ЛИТЕРАТУРА

1. *Рожков М. И.* О суммировании цепей Маркова на конечной группе // Труды по дискретной математике. 2000. Т. 3. С. 195–214.
2. *Рожков М. И.* Суммирование марковских последовательностей на конечной абелевой группе // Дискретная математика. 2010. Т. 22. № 3. С. 44–62.
3. *Кемени Дж., Снелл Дж.* Конечные цепи Маркова. М.: Наука, 1970.
4. *Кэртис Ч., Райнер И.* Теория представлений конечных групп и ассоциативных алгебр. М.: Наука, 1969. 688 с.
5. *Воробьев Н. Н.* Сложение независимых случайных величин на конечных абелевых группах // Математический сб. 1954. Т. 34(76). № 1. С. 89–126.

REFERENCES

1. *Rozhkov M. I.* O summirovanii cepej Markova na konechnoj gruppe. Trudy po Diskretnoi Matematike, 2000, vol. 3, pp. 195–214. (in Russian)
2. *Rozhkov M. I.* Summirovanie markovskih posledovatel'nostej na konechnoj abelevoj gruppe. Diskretnaya Matematika, 2010, vol. 22, no. 3, pp. 44–62. (in Russian)
3. *Kemeni Dzh., Snell Dzh.* Konechnye cepi Markova. Moscow, Nauka Publ., 1970. (in Russian)
4. *Kjertis Ch., Rajner I.* Teorija predstavlenij konechnyh grupp i associativnyh algebr. Moscow, Nauka Publ., 1969. 688 p. (in Russian)
5. *Vorob'ev N. N.* Slozhenie nezavisimyh sluchajnyh velichin na konechnyh abelevyh gruppah. Matematicheskii Sb., 1954, vol. 34(76), no. 1, pp. 89–126. (in Russian)

ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ

УДК 519.17

ЭКСПОНЕНЦИАЛЬНЫЕ ПРОИЗВОДЯЩИЕ ФУНКЦИИ ПОСЛЕДОВАТЕЛЬНОСТИ ЧИСЕЛ k-ДОЛЬНЫХ ГРАФОВ

Р. М. Ганопольский

Тюменский государственный университет, г. Тюмень, Россия

Рассматривается специальный вид экспоненциальных производящих функций последовательности чисел k-дольных графов. Эти функции учитывают количество вершин в каждой доле. Выводится соотношение, являющееся вариацией экспоненциальной теоремы для этих производящих функций. Делается вывод о возможности обобщения полученного соотношения для гиперграфов и мультиграфов. Анализируются полученные выражения и их упрощённые частные случаи. Рассматриваются варианты практического применения соотношений и частных случаев в физике и математике.

Ключевые слова: *k-дольный граф, гиперграф, мультиграф, связные графы, покрытие, производящие функции, экспоненциальная теорема.*

DOI 10.17223/20710410/27/9

THE EXPONENTIAL GENERATING FUNCTIONS FOR SEQUENCE OF THE NUMBERS OF k-PARTITE GRAPHS

R. M. Ganopolsky

Tyumen State University, Tyumen, Russia

E-mail: rodion@utmn.ru

A specific kind of exponential generating functions for the sequence of the numbers of k-partite graphs is considered. These functions take into account the numbers of vertices in each part. A relation is obtained for such generating functions. This relation is a variant of the exponential theorem for these generating functions. It is concluded that it is possible to generalize the obtained relation for hypergraphs and multigraphs. The obtained expression and its simplified special cases are analyzed. The applications of the relations and special cases in physics and mathematics are considered.

Keywords: *k-partite graph, hypergraph, multigraph, connected graph, cover, generating functions, exponential theorem.*

Введение

Граф G с множеством вершин V ($|V| = n$) называется k-дольным графом, если вершины графа разбиты на k непересекающихся непустых подмножества V_i так, что

$$\bigcup_{i=1}^{k} V_i = V; \quad V_i \neq \varnothing; \quad |V_i| = n_i > 0; \quad V_i \cap V_j = \varnothing, \quad i, j = 1, \ldots, k, \quad i \neq j,$$

и нет рёбер, соединяющих вершины одного и того же подмножества [1 – 3]. При этом 1-дольный граф — это множество вершин без рёбер, а 0-дольным графом является только пустой граф. Очевидно, что любой k-дольный граф при $k < n$ можно преобразовать в $(k+1)$-дольный, разбив вершины на большее количество подмножеств. В общем случае k-дольный граф $(k > 0)$ состоит из $s \geqslant 1$ компонент связности, каждая из которых является связным l_i-дольным графом $(i = 1, \ldots, s,\ l_i = 1, \ldots, k)$.

Определим множество X как множество номеров долей графа:

$$X = \{1, 2, \ldots, k\}. \tag{1}$$

Множество номеров долей любой из компонент связности графа является подмножеством X. Мощность этого подмножества равна количеству долей компоненты связности. Так как несколько различных компонент связности графа могут иметь совпадающие множества номеров долей, семейство всех множеств номеров долей всех компонент связности k-дольного графа может содержать повторяющиеся подмножества и в общем случае является повторяющимся покрытием множества X. Для того чтобы избавиться от повторяющихся подмножеств, введём следующее понятие.

Пусть набор связных l-дольных графов $(0 < l \leqslant k)$ — это все компоненты связности исходного графа, множества (мощности l) номеров долей которых тождественны. Любой несвязный k-дольный граф можно разбить на наборы связных l_i-дольных графов. Каждый набор определяется уникальным множеством номеров долей. У двух любых наборов множества номеров их долей отличаются. Тогда семейство множеств номеров долей наборов связных l_i-дольных графов является неповторяющимся покрытием множества X.

В работе [4] введены комбинаторные числа неупорядоченных покрытий конечного множества мощности n подмножествами с фиксированными мощностями

$$ {}_nN(k_1, k_2, \ldots, k_n), \tag{2}$$

где k_i — количество подмножеств мощности i в покрытии. В случае, когда часть коэффициентов $k_i = 0$, используется альтернативное обозначение

$$ {}_nN^{k_1 k_2 \cdots k_m}_{l_1\, l_2 \cdots l_m},$$

где k_i — количество подмножеств мощности l_i в покрытии. Если все подмножества в покрытии имеют мощность l, то коэффициент имеет вид ${}_nN^k_l$.

В работах [5, 6] рассматриваются производящие функции последовательности чисел (2):
обычная

$$F(x; A_1, A_2, A_3, \ldots) = \sum_{j \geqslant 0} x^j \sum_{k=0}^{j} C_j^k (-1)^k \prod_{i=1}^{j-k} (1 + A_i)^{C_{j-k}^i} = \sum_{j \geqslant 0} \frac{x^j \prod\limits_{i=1}^{j} (1 + A_i)^{C_j^i}}{(1+x)^{j+1}} \tag{3}$$

и экспоненциальная

$$E(x; A_1, A_2, A_3, \ldots) = \sum_{j \geqslant 0} \frac{x^j}{j!} \sum_{k=0}^{j} C_j^k (-1)^k \prod_{i=1}^{j-k} (1 + A_i)^{C_{j-k}^i} = e^{-x} \sum_{j \geqslant 0} \frac{x^j}{j!} \prod_{i=1}^{j} (1 + A_i)^{C_j^i}. \tag{4}$$

Числа (2) в этих функциях являются коэффициентами перед мономами $x^n \prod\limits_i A_i^{k_i}$ в случае обычной производящей функции и перед выражением $\dfrac{x^n}{n!} \prod\limits_i A_i^{k_i}$ — в случае экспоненциальной. В разложении функции E по степеням x выражения перед $\dfrac{x^n}{n!}$ (для

функции F — перед x^n) являются производящими функциями последовательности чисел (2) с фиксированным n:

$$\sum_{k=0}^{n} C_n^k (-1)^k \prod_{i=1}^{n-k} (1+A_i)^{C_{n-k}^i}.$$

Для введённых комбинаторных чисел в работе [4] получена формула

$${}_nN_{l_1\,l_2\cdots l_m}^{k_1k_2\cdots k_m} = \prod_{i=1}^{m} C_{C_n^{l_i}}^{k_i} + \sum_{i\geqslant 1}(-1)^i C_n^i \prod_{j=1}^{m} C_{C_{n-i}^{l_j}}^{k_j},$$

где $C_j^i = \dfrac{j!}{i!(j-i)!}$ — биномиальный коэффициент. Там же получено значение суммы чисел покрытий, состоящих из множеств одной мощности

$$\sum_{n\geqslant 1} \frac{(-1)^n}{n}\, {}_nN_l^k = \frac{(-1)^{k+l-1}}{kl}, \tag{5}$$

и значение суммы для случая, когда в покрытии подмножества разной мощности (m>1)

$$\sum_{n\geqslant 1} \frac{(-1)^n}{n}\, {}_nN_{l_1\,l_2\cdots l_m}^{k_1k_2\cdots k_m} = 0. \tag{6}$$

1. Экспоненциальные производящие функции

Экспоненциальную производящую функцию последовательности чисел наборов связных k-дольных графов по переменным $x_1, x_2, \ldots, x_k$ (индексы переменных определяют номера долей) определим как

$$A_k(1,2,\ldots,k) = \sum_{n_i>0} \frac{x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}}{n_1!n_2!\cdots n_k!} a_k(n_1,n_2,\ldots,n_k), \tag{7}$$

а экспоненциальную производящую функцию последовательности чисел связных k-дольных графов как

$$D_k(1,2,\ldots,k) = \sum_{n_i>0} \frac{x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}}{n_1!n_2!\cdots n_k!} d_k(n_1,n_2,\ldots,n_k), \tag{8}$$

где a_k и d_k — соответственно числа наборов связных k-дольных графов и числа связных k-дольных графов, имеющих в каждой доле с номером i определённое количество n_i вершин. Сумма выполняется по $n_1 > 0$, $n_2 > 0$, …, $n_k > 0$, таким, что $n_1 + n_2 + \ldots + n_k = n$. Параметрами функций являются номера долей графов. Если связные l-дольные графы являются компонентами k-дольного графа и $l < k$, то экспоненциальные производящие функции записываются следующим образом:

$$A_l(i_1,i_2,\ldots,i_l) \text{ и } D_l(i_1,i_2,\ldots,i_l), \text{ где } 1 \leqslant i_1 < i_2 < \ldots < i_l \leqslant k,$$

то есть множество номеров долей связных l-дольных графов и множество номеров долей набора связных l-дольных графов являются подмножествами множества X (1). Переменными функций A_l и D_l являются x_{i_1}, x_{i_2}, …, x_{i_l}.

Рассмотрим набор, состоящий из $m \geqslant 1$ связных k-дольных графов. Каждая доля исходного графа разбита на m непустых подмножеств. Каждое подмножество является

долей связного k-дольного графа. Пусть n_{ij} — мощность доли с номером i связного k-дольного графа с номером j. Очевидно,

$$\forall i, j\ (n_{ij} > 0); \tag{9}$$

$$\sum_{j=1}^{m} n_{ij} = n_i. \tag{10}$$

Количество разбиений множества мощности n_i на m непустых подмножеств равно

$$\frac{1}{m!} \sum_{\sum n_{ij} = n_i} \frac{n_i!}{\prod\limits_{j=1}^{m} n_{ij}!},$$

где суммирование идёт по всем возможным значениям n_{ij}, удовлетворяющим соотношениям (9), (10); множитель $1/m!$ необходим, так как связные графы, образующие набор, неразличимы. Тогда числа a_k и d_k связаны формулой

$$a_k(n_1, n_2, \ldots, n_k) = \sum_{m>0} \frac{\prod\limits_{i=1}^{k} n_i!}{m!} \sum_{\sum n_{ij} = n_i} \prod_{j=1}^{m} \frac{1}{n_{1j}! n_{2j}! \ldots n_{kj}!} d_k(n_{1j}, n_{2j}, \ldots, n_{kj}),$$

где сумма идёт по всем возможным m-разбиениям k долей исходного графа.

Просуммировав по всем возможным n_i и поменяв порядок суммирования, с учётом (7) и (8) получим формулу для производящей функции последовательности чисел наборов k-дольных графов:

$$A_k = \sum_{m>0} \frac{1}{m!} \sum_{n_i>0} \sum_{\sum n_{ij} = n_i} \prod_{j=1}^{m} \frac{x_1^{n_{1j}} x_2^{n_{2j}} \ldots x_k^{n_{kj}}}{n_{1j}! n_{2j}! \ldots n_{kj}!} d_k(n_{1j}, n_{2j}, \ldots, n_{kj}) = e^{D_k} - 1. \tag{11}$$

Вывод соотношения (11), как и сама формула, аналогичен выводу экспоненциальной формулы [1].

Экспоненциальную производящую функцию последовательности чисел k-дольных графов определим аналогично функциям (7) и (8):

$$F_k(1, 2, \ldots, k) = \sum_{n_i>0} \frac{x_1^{n_1} x_2^{n_2} \ldots x_k^{n_k}}{n_1! n_2! \ldots n_k!} f_k(n_1, n_2, \ldots, n_k), \tag{12}$$

где f_k — число k-дольных графов, имеющих в каждой доле (с номером i) определённое количество (n_i) вершин. Сумма выполняется по $n_1 > 0$, $n_2 > 0$, …, $n_k > 0$, таким, что $n_1 + n_2 + \ldots + n_k = n$.

Проведём преобразования, аналогичные выводу формулы (11). Учтём, что:

1) множество номеров долей набора связных k-дольных графов является подмножеством множества X (1), а семейство всех таких множеств номеров долей является покрытием множества X;
2) так как множества номеров долей двух любых наборов связных k-дольных графов не равны друг другу, все наборы связных графов различимы. Значит, множитель $1/m!$ не нужен.

Таким образом, получаем

$$F_k = \sum_{S=\{U_\alpha\}} \prod_{U_\alpha} A_{|U_\alpha|}(U_\alpha), \tag{13}$$

где сумма идёт по всем покрытиям S множества X, а произведение — по всем подмножествам U_α, входящим в покрытие S. Применив соотношение (11), в итоге получаем

$$F_k = \sum_{S=\{U_\alpha\}} \prod_{U_\alpha} (\exp D_{|U_\alpha|} - 1). \tag{14}$$

Частные случаи:

$$F_0 = 1,$$
$$F_1 = A_1 = e^{x_1} - 1,$$
$$F_2 = A_2(1,2)(1 + A_1(1) + A_1(2)) + A_1(1)A_1(2) = e^{D_2(1,2)+x_1+x_2} - e^{x_1} - e^{x_2} + 1.$$

Изначально на k-дольные графы G не было введено никаких ограничений. Из проведённых преобразований видно, что полученные соотношения являются верными для всех классов графов, удовлетворяющих следующим критериям:

1) если в класс входит k-дольный граф G, то в этот класс должны входить и все k-дольные графы, получаемые из G перестановками вершин в любой из k долей;
2) если в класс входит k-дольный граф, имеющий несколько компонент связности, то должны входить и все эти компоненты связности.

Обобщениями графов являются мультиграфы и гиперграфы. В гиперграфах одно ребро может соединять более двух вершин, а в мультиграфах между двумя вершинами может быть больше одного ребра (кратные рёбра) [1, 2]. Обобщением k-дольного графа является k-дольный гиперграф — вершины гиперграфа V разбиты на k непересекающихся непустых подмножеств V_i так, что нет рёбер, соединяющих вершины одного и того же подмножества. Аналогичные определения можно дать для k-дольного мультиграфа и k-дольного мультиграфа-гиперграфа (кратные рёбра соединяют более двух вершин). Вывод соотношений (11) и (14) для мультиграфов, гиперграфов и мультиграфов-гиперграфов эквивалентен выводу соотношений для экспоненциальной производящей функции последовательности чисел k-дольных графов.

2. Анализ функций

Приравняв в соотношении (14) все переменные x_i одной переменной x, получим

$$F_k = \sum_{i \geqslant 0} {}_kN(i_1, i_2, \ldots, i_k) \prod_j A_j^{i_j} = \sum_{i \geqslant 0} {}_kN(i_1, i_2, \ldots, i_k) \prod_j (e^{D_j} - 1)^{i_j}, \tag{15}$$

где ${}_kN(i_1, i_2, \ldots, i_k)$ — комбинаторные числа (2), а суммирование идёт по всем $i_j \geqslant 0$; A_j и D_j являются функциями только от переменной x.

Используем (4) и (11):

$$F_k = \sum_{j=0}^{k} C_k^j (-1)^j \prod_{i=1}^{k-j} (1 + A_i)^{C_{k-j}^i} = \sum_{j=0}^{k} C_k^j (-1)^j \exp\Big(\sum_{i=1}^{k-j} D_i C_{k-j}^i\Big). \tag{16}$$

Просуммируем все функции F_k, домножив в одном случае на y^k, а в другом на $y^k/k!$, и воспользуемся соотношениями (3) и (4):

$$\sum_{k \geqslant 0} y^k F_k = \sum_{k \geqslant 0} \frac{y^k \prod_{i=1}^{k} (1 + A_i)^{C_k^i}}{(1+y)^{k+1}} = \sum_{k \geqslant 0} \frac{y^k \exp\left(\sum_{i=1}^{k} D_i C_k^i\right)}{(1+y)^{k+1}},$$

$$\sum_{k \geqslant 0} \frac{y^k F_k}{k!} = e^{-y} \sum_{k \geqslant 0} \frac{y^k}{k!} \prod_{j=0}^{k} (1 + A_j)^{C_k^j} = e^{-y} \sum_{k \geqslant 0} \frac{y^k}{k!} \exp\left(\sum_{j=0}^{k} C_k^j D_j\right).$$

Частные случаи формулы (16):

$$F_0 = 1,$$
$$F_1 = A_1 = e^x - 1,$$
$$F_2 = A_2(1 + 2A_1) + A_1^2 = (A_2 + 1)(A_1 + 1)^2 - 2(A_1 + 1) + 1 = e^{D_2+2x} - 2e^x + 1,$$
$$F_3 = (A_3 + 1)(A_2 + 1)^3(A_1 + 1)^3 - 3(A_2 + 1)(A_1 + 1)^2 + 3(A_1 + 1) - 1 =$$
$$= e^{D_3+3D_2+3x} - 3e^{D_2+2x} + 3e^x - 1.$$

Пусть есть функция $f(G)$, ставящая в соответствие каждому графу какое-то число. Для функции выполняются следующие условия:

1) значение функции от пустого графа равно 1;
2) значение функции от графа, имеющего несколько компонент связности, равно произведению значений функции от компонент связности;
3) значение функции не зависит от нумерации вершин, а значит, и от перестановок строк или столбцов в матрице смежности.

Примером такой функции является хроматическая функция [3].

Пусть необходимо найти сумму значений этой функции от всех дольных графов

$$S = \sum_k b_k \sum_{G_k} \frac{1}{|V_1|! \dots |V_k|!} f(G_k(V_1, \dots, V_k)) F_k(1, 2, \dots, k),$$

где суммирование идёт по всем k-дольным графам G_k, разбитым на k непустых долей V_i, а коэффициенты b_k — параметры суммы. Тогда из (12), (13), (15) и (16) следует

$$S = \sum_k b_k \sum_{i \geqslant 0_k} N(i_1, i_2, \dots, i_k) \prod_j \tilde{A}_j^{i_j} = \sum_k b_k \sum_{j=0}^{k} C_k^j (-1)^j \prod_{i=1}^{k-j} (1 + \tilde{A}_i)^{C_{k-j}^i},$$

где $\tilde{A}_j$ — сумма значений функции от всех наборов связных j-дольных графов: $\tilde{A}_j = e^{\tilde{D}_j} - 1$; $\tilde{D}_j$ — сумма значений функции от всех связных j-дольных графов.

Для $b_k = (-1)^k/k$ (без пустого графа) при учёте (5) и (6) сумма S примет вид

$$S = \sum_{k>0} \sum_{l>0} \frac{(-1)^{k+l-1}}{kl} \tilde{A}_l^k = \sum_{l>0} \frac{(-1)^l}{l} \ln(1 + \tilde{A}_l) = \sum_{l>0} \frac{(-1)^l}{l} \tilde{D}_l, \tag{17}$$

где мы воспользовались разложением в ряд натурального логарифма

$$\ln(1 + x) = \sum_{n>0} \frac{(-1)^{n-1} x^n}{n}.$$

Таким образом, сумма значений функций от всех дольных графов с коэффициентом $(-1)^k/k$ (k — количество долей графа) равна сумме значений этой функции от всех связных дольных графов с этим же коэффициентом.

Заключение

В работе введён специальный вид экспоненциальной производящей функции последовательности чисел k-дольных графов. Выводится соотношение, являющееся обобщением экспоненциальной теоремы для данного вида экспоненциальных производящих функций. Анализируется полученное выражение. Определена связь между компонентами связности k-дольных графов и покрытиями множеств. Аналогично понятию

k-дольных графов вводится понятие k-дольных гиперграфов и мультиграфов. Делается вывод о возможности обобщения выражения для экспоненциальной производящей функции последовательности чисел k-дольных графов для случая k-дольных гиперграфов и мультиграфов.

Полученные результаты, в частности (16) и (17), могут быть использованы для упрощения оперирования с диаграммами Фейнмана в квантовой теории, диаграммами теории возмущений в теории струн [7] и статистической физике [8 – 10]. Диаграммы Феймана и их аналоги являются по сути k-дольными графами и мультиграфами, что позволяет применять методы теории графов для упрощения выражений и вычисления бесконечных рядов таких диаграмм. Полученные соотношения можно также использовать для анализа схем в схемотехнике, блок-схем в теории информационных систем, структур баз данных с сетевой моделью, криптостойкости алгоритмов в криптологии [11] и т. п.

ЛИТЕРАТУРА

1. *Стенли Р.* Перечислительная комбинаторика. Деревья, производящие функции и симметрические функции. М.: Мир, 2005.
2. *Харари Ф.* Теория графов. М.: УРСС, 2003.
3. *Уилсон Р.* Введение в теорию графов. М.: Мир, 1977.
4. *Ганопольский Р. М.* Число неупорядоченных покрытий конечного множества подмножествами фиксированного размера // Прикладная дискретная математика. 2010. № 4(10). С. 5–17.
5. *Ганопольский Р. М.* Производящие функции последовательности чисел покрытий конечного множества // Прикладная дискретная математика. 2011. № 1(11). С. 5–13.
6. *Ганопольский Р. М.* Производящие функции последовательности чисел связных покрытий // Прикладная дискретная математика. 2013. № 3(21). С. 5–10.
7. *Каку М.* Введение в теорию суперструн. М.: Мир, 1999.
8. *Фейнман Р.* Статистическая механика. Курс лекций. М.: Мир, 1975.
9. *Абрикосов А. А., Горьков Л. П., Дзялошинский И. Е.* Методы квантовой теории поля в статистической физике. М.: Физматгиз, 1962.
10. *Лифшиц Е. М., Питаевский Л. П.* Статистическая физика. Ч. 2. М.: Наука, 1978.
11. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.

REFERENCES

1. *Stenli R.* Perechislitel'naja kombinatorika. Derev'ja, proizvodjashhie funkcii i simmetricheskie funkcii. Moscow, Mir Publ., 2005. (in Russian)
2. *Harary F.* Graph Theory. Addison-Wesley, Reading, 1994.
3. *Uilson R.* Vvedenie v teoriju grafov. Moscow, Mir Publ., 1977. (in Russian)
4. *Ganopolsky R. M.* Chislo neuporjadochennyh pokrytij konechnogo mnozhestva podmnozhestvami fiksirovannogo razmera. Prikladnaya Diskretnaya Matematika, 2010, no. 4(10), pp. 5–17. (in Russian)
5. *Ganopolsky R. M.* Proizvodjashhie funkcii posledovatel'nosti chisel pokrytij konechnogo mnozhestva. Prikladnaya Diskretnaya Matematika, 2011, no. 1(11), pp. 5–13. (in Russian)
6. *Ganopolsky R. M.* Proizvodjashhie funkcii posledovatel'nosti chisel svjaznyh pokrytij. Prikladnaya Diskretnaya Matematika, 2013, no. 3(21), pp. 5–10. (in Russian)
7. *Kaku M.* Vvedenie v teoriju superstrun. Moscow, Mir Publ., 1999. (in Russian)
8. *Fejnman R.* Statisticheskaja mehanika. Kurs lekcij. Moscow, Mir Publ., 1975. (in Russian)

9. *Abrikosov A. A., Gor'kov L. P., Dzjaloshinskij I. E.* Metody kvantovoj teorii polja v statisticheskoj fizike. Moscow, Fizmatgiz Publ., 1962. (in Russian)
10. *Lifshic E. M., Pitaevskij L. P.* Statisticheskaja fizika. P. 2. Moscow, Nauka Publ., 1978. (in Russian)
11. *Fomichev V. M.* Metody diskretnoj matematiki v kriptologii. Moscow, Dialog-MIFI Publ., 2010. (in Russian)

УДК 519.628

РЁБЕРНО-ВЕРШИННЫЕ ИНЦИДЕНТНЫЕ ПАРОСОЧЕТАНИЯ В ЗАДАЧАХ РАСПИСАНИЙ[1]

А. М. Магомедов, Т. А. Магомедов

Дагестанский государственный университет, г. Махачкала, Россия

С использованием рёберно-вершинных инцидентных паросочетаний решена задача оптимизации расписания, исходные данные для которого представлены графом со степенями вершин не выше трёх.

Ключевые слова: *граф, паросочетание, расписание, оптимизация.*

DOI 10.17223/20710410/27/10

EDGE-VERTEX INCIDENT MATCHINGS IN SCHEDULING

A. M. Magomedov, T. A. Magomedov

Dagestan State University, Makhachkala, Russia

E-mail: magomedtagir1@yandex.ru

The optimization problem for schedules represented by means of graphs with maximal vertex degree 3 is solved by using the edge-vertex incident matchings.

Keywords: *graph matching, scheduling, optimization.*

Введение

Все использованные в данной работе, но не определенные в ней обозначения и понятия соответствуют принятым в [1]. Множества вершин и рёбер графа G будем обозначать $V(G)$ и $E(G)$ соответственно, степень вершины v и максимальную степень вершины графа — $d_G v$ и $\Delta(G)$. Для цикломатического числа $|E(G)| - |V(G)| + 1$ связного графа G примем обозначение $\gamma(G)$.

Разные содержательные аспекты проблемы оптимизации расписания не раз освещались в литературе, начиная с известной NP-полной задачи «Составление учебного расписания» [2, с. 311]. Задача построения безоконных расписаний в общем виде относится к числу NP-полных задач. Принято считать, что существующих в настоящее время методов недостаточно, чтобы выяснить разрешимость NP-полных задач за полиномиальное время; более точно — проверить гипотезу $\mathrm{P} \neq \mathrm{NP}$. Поэтому выделение нетривиальных частных случаев NP-полных задач, разрешимых за полиномиальное время, заслуживает внимания, особенно когда они имеют практические приложения, как в нашем случае.

Укажем на сравнительно недавние результаты в данном направлении.

Для случая, когда количество занятий в каждом классе равно пяти, а количество занятий каждого учителя — двум, условия существования расписания длины 5

[1]Работа поддержана проектом № 2014/33 на выполнение государственных работ в сфере научной деятельности в рамках базовой части госзадания Минобрнауки России, а также ОМИ ДНЦ РАН.

без окон для учителей получены в [3]. Здесь и далее под *длиной расписания* понимается продолжительность времени (в академических часах) от начала первого занятия до завершения последнего занятия расписания (считается, что продолжительность занятия равна одному академическому часу).

Связный граф G будем называть *примитивом*, если $\gamma(G) \leqslant 1$ и $\Delta(G) = 3$. Пусть G — связный граф, такой, что $\Delta(G) = 2p + 1$, $p \in \mathbb{Z}^+$. Разбиение графа G на p рёберно-непересекающихся примитивов G_i $(i = 1, \ldots, p)$ будем называть *сбалансированным разбиением на примитивы*, если для каждой вершины v графа G и для каждого $i = 1, \ldots, p$ в примитив G_i включены $\lceil d_G v/p \rceil$ либо $\lfloor d_G v/p \rfloor$ рёбер, инцидентных вершине v. Сбалансированные разбиения на примитивы востребованы в задачах оптимизации расписаний и интервальных раскрасок графов.

Теорема 1 [4]. Пусть G — связный граф, $\Delta(G) = 2p + 1$ $(p \in \mathbb{Z}^+)$. Граф G допускает сбалансированное разбиение на примитивы тогда и только тогда, когда для каждого подграфа G' графа G справедливо неравенство

$$|E(G')| \leqslant p|V(G')|. \tag{1}$$

Теорема 2 [5]. Проверка условий (1) для всех подграфов графа G может быть выполнена за время $\mathrm{O}(|V(G)|^3 \log |V(G)|)$.

Из теоремы 1 видна актуальность рассмотрения случая, когда граф G является примитивом. Этому случаю и посвящена настоящая работа. Найдены эффективно проверяемые необходимые и достаточные условия существования безоконного расписания длины 3. Показано применение рёберно-вершинных инцидентных паросочетаний к решению задачи оптимизации расписания.

1. Рёберно-вершинные инцидентные паросочетания и безоконные расписания

Пусть исходные данные к школьному расписанию учебных занятий заданы связным графом G, $\Delta(G) = 3$; каждое ребро e соответствует учителю $t = t(e)$, а концевые вершины ребра e — классам $c_1(t)$ и $c_2(t)$, в каждом из которых учитель t должен провести по одному занятию. Требуется выяснить существование расписания длины 3, в котором учителя и классы не имеют окон.

Инъективное отображение $E(G) \to V(G)$ множества рёбер графа в множество вершин, такое, что каждое ребро отображается в одну из своих инцидентных вершин, называется *рёберно-вершинным инцидентным паросочетанием* (*р-вип*) графа G. Понятно, что для существования у графа G *р-вип* необходимо выполнение неравенства $|E(G)| \leqslant |V(G)|$, равносильного, очевидно, неравенству

$$\gamma(G) \leqslant 1. \tag{2}$$

Другими словами, для существования *р-вип* необходимо, чтобы граф G содержал не более одного цикла. Покажем, что это условие является и достаточным.

Рассмотрим два случая.

С л у ч а й 1: связный граф G содержит единственный цикл C.

Сориентировав рёбра цикла C, получим ориентированный цикл, для которого сохраним обозначение C. Каждой дуге цикла C сопоставим её концевую вершину, после чего удалим из G все такие вершины цикла C, для которых $d_G v = 2$.

Если граф G является циклом, искомое *р-вип* построено. В противном случае рассмотрим лес T, который получится после процедуры удаления. Заметим, что каждое

из деревьев t, образующих лес T, имеет точно одну вершину r_t, общую с циклом C; выбрав r_t в качестве корня дерева t, сориентируем рёбра дерева так, чтобы получить ориентированное корневое дерево; затем каждой дуге сопоставим её концевую вершину. В результате получим искомое *р-вип*.

С л у ч а й 2: связный граф G является деревом. Для построения *р-вип* достаточно применить к G рассуждения, приведённые в предыдущем абзаце для дерева t.

Замечание 1. За исключением тривиального случая, когда G является деревом, построенное отображение является биекцией: в нём участвует не только каждая дуга, но и каждая вершина.

Таким образом, доказано следующее

Утверждение 1. Условие (2) необходимо и достаточно для существования *р-вип* у графа G.

Замечание 2. Заметим, что ограничение $\Delta(G) = 3$ в доказательстве утверждения не использовано; другими словами, утверждение 1 справедливо для любого $\Delta(G)$. Вопросы существования *р-вип* и других близких по смыслу паросочетаний рассмотрены в [1, с. 93–94].

Набор пар вида «учитель–класс», индуцированный построенным *р-вип*, составляет второе по порядку из трёх занятий искомого расписания; во втором занятии задействованы все учителя и все классы (кроме тривиального исключения; см. замечание 1).

Любая корректная достройка построенной части расписания до всего расписания приведёт к искомому расписанию без окон. Для выполнения достройки заметим, что в результате упомянутых выше ориентаций рёбер у каждой невисячей вершины орграфа G имеются либо два потомка («левый» и «правый»), либо единственный потомок («левый»). Рассмотрим класс c, соответствующий вершине u: если вершина v — левый потомок вершины u, то в качестве первого занятия классу c назначим занятие с учителем $a = (u, v)$; если вершина u обладает также и правым потомком w, то в качестве третьего занятия назначим классу c занятие с учителем $b = (u, w)$. Таким образом, доказана следующая

Теорема 3. Для существования безоконного расписания длины 3, соответствующего связному графу G с $\Delta(G) = 3$, необходимо и достаточно выполнение условия $\gamma(G) \leqslant 1$.

Следствие 1. Пусть условие (2) выполнено. Если G не является деревом, то существует безоконное расписание длины 3, во втором занятии которого задействованы не только все учителя (для безоконного расписания длины 3 с двумя занятиями у каждого учителя это свойство, очевидно, всегда выполнено), но и все классы. Если G — дерево, v_0 — произвольно выбранная вершина G, а c_0 — класс, соответствующий вершине v_0, то существует безоконное расписание длины 3, во втором занятии которого задействованы все учителя и все классы, отличные от c_0.

Следствие 2. Если условие (2) выполнено, то существует безоконное расписание длины 3, где третье занятие проводится лишь в тех классах, которые соответствуют вершинам степени 3.

Заключение

Условия существования *р-вип* получены новым (по сравнению с [1]) способом. В теореме 3 выявлена связь *р-вип* с существованием безоконного расписания длины 3. Дополнение теорем 1 и 2 теоремой 3 открывает перспективы для исследования условий существования безоконных расписаний (нечётной длины) в общем случае.

ЛИТЕРАТУРА

1. *Оре О.* Теория графов. М.: Наука, 1980.
2. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.
3. *Магомедов А. М., Магомедов Т. А.* Интервальная на одной доле правильная рёберная 5-раскраска двудольного графа // Прикладная дискретная математика. 2011. № 5. С. 85–91.
4. *Магомедов А. М., Сапоженко А. А.* Условия существования непрерывных расписаний длительности пять // Вестник МГУ. Сер. Вычислительная математика и кибернетика. 2010. № 1. С. 39–44.
5. *Магомедов А. М., Магомедов Т. А.* О приложении алгоритма вычисления подграфа максимальной плотности к задаче оптимизации расписания // Матзаметки. 2013. Т. 93. № 2. С. 313–315.

REFERENCES

1. *Ore O.* Teorija grafov. Moscow, Nauka Publ., 1980. (in Russian)
2. *Geri M., Johnson D.* Vychislitel'nye mashiny i trudnoreshaemye zadachi. Moscow, Mir Publ., 1982. (in Russian)
3. *Magomedov A. M., Magomedov T. A.* Interval'naja na odnoj dole pravil'naja rjobernaja 5-raskraska dvudol'nogo grafa. Prikladnaya Diskretnaya Matematika, 2011, no. 5, pp. 85–91. (in Russian)
4. *Magomedov A. M., Sapozhenko A. A.* Uslovija sushhestvovanija nepreryvnyh raspisanij dlitel'nosti pjat'. Vestnik MSU. Ser. Vychislitel'naya Matematika i Kibernetika, 2010, no. 1, pp. 39–44. (in Russian)
5. *Magomedov A. M., Magomedov T. A.* O prilozhenii algoritma vychislenija podgrafa maksimal'noj plotnosti k zadache optimizacii raspisanija. Matzametki, 2013, vol. 93, no. 2, pp. 313–315. (in Russian)

УДК 519.171.2 + 519.175

О ПРЕДСТАВЛЕНИИ ГРАФОВ В ВИДЕ ГРУППОИДОВ СПЕЦИАЛЬНОГО ВИДА

М. Н. Назаров

Национальный исследовательский университет «МИЭТ», г. Москва, Россия

Рассмотрен альтернативный способ задания графов путём представления множества вершин графа в виде группоида. Для полученных группоидов описаны конгруэнции, идеалы и подалгебры, а также установлено, когда они являются полугруппами. Дополнительно к этому рассмотрено практическое применение группоидов графов для сжатия данных.

Ключевые слова: *алгебраическая теория графов, группоид графа, конгруэнции на графе, идеалы графа, компактное хранение графа.*

DOI 10.17223/20710410/27/11

ON THE REPRESENTATION OF GRAPHS IN THE FORM OF A SPECIAL TYPE OF BINARY ALGEBRA

M. N. Nazarov

National Research University of Electronic Technology, Moscow, Russia

E-mail: Nazarov-Maximilian@yandex.ru

An alternative way to define graphs as binary algebras on a set of vertices is considered. For the resulting algebras, we describe congruences, ideals and subalgebras, and obtain criterion for such a graph algebra to be a semigroup. In addition, we consider a practical application of graph algebras for data compression.

Keywords: *algebraic graph theory, graph algebra, congruence and ideal on graph, compact storage of graphs.*

Введение

Рассмотрим только конечные классические графы, исключая все остальные случаи: ориентированные, кратные, а также графы с петлями и бесконечным числом вершин.

Определение 1. *Классическим графом* (или просто *графом*) будем называть пару $G = (V, E)$, где множество вершин V — любое конечное множество; множество рёбер $E \subseteq V \times V$ — бинарное отношение, для которого выполняется:

1) $\forall a, b \in V \quad ((a, b) \in E \Rightarrow (b, a) \in E)$ — отношение симметрично;
2) $\forall a \in V \quad ((a, a) \notin E)$ — отношение антирефлексивно.

Фактически это означает, что из рассмотрения исключаются рёбра-петли (b, b), а все остальные рёбра $(a, b) \in E$ можно считать неупорядоченными парами.

Определение 2. Пусть $G = (V, E)$ — произвольный[1] граф. Назовём *частичным группоидом* графа множество $(V, \cdot)$, определив операцию как

$$\begin{cases} a \cdot b = a, & \text{если } (a, b) \in E, \\ a \cdot b = \theta, & \text{если } (a, b) \notin E. \end{cases} \tag{1}$$

Группоиды вида (1) впервые предложены в работе [1] в 1983 г. и впоследствии нашли широкое применение на стыке теории графов и других математических дисциплин, таких, как алгебра [2, 3], теория языков и автоматов [4], топология [5]. Однако у данного определения есть ряд недостатков, которые делают его менее ценным с алгебраической точки зрения; в частности, не представляется возможным связать понятие конгруэнции с нетривиальными свойствами структуры графов. Для преодоления этого недостатка предлагается альтернативное определение группоида для классических графов.

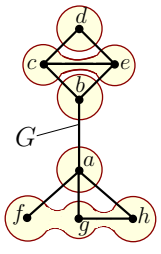
Определение 3. Пусть $G = (V, E)$ — классический граф. Будем называть множество $(V, \circ)$ *группоидом классического графа*, определив операцию как

$$\begin{cases} a \circ b = a, & \text{если } (a, b) \in E, \\ a \circ b = b, & \text{если } (a, b) \notin E. \end{cases} \tag{2}$$

Замечание 1. Отметим, что по группоиду $(V, \circ)$, заданному на основе (2), можно восстановить как граф без петель, так и граф, у которого все вершины имеют петли, так как все вершины являются идемпотентами: $a \circ a = a$. Поскольку рассматриваются только классические графы, случай с петлями $(a, a) \in E$ отбрасывается.

1. Общие алгебраические свойства группоидов графов

Напомним, что конгруэнцией на группоиде называется такое отношение эквивалентности ρ, которое сохраняет операцию: $\forall a, b, c\ ((a, b) \in \rho \Rightarrow (ac, bc) \in \rho \wedge (ca, cb) \in \rho)$. Классом $[a]$ конгруэнции ρ называется множество $[a] = \{a^* : (a, a^*) \in \rho\}$. Понятие конгруэнции определено для произвольной алгебраической системы; в частности, можно его применить для группоидов $(V, \circ)$. В этом случае конгруэнция ρ задаёт разбиение множества вершин V графа на классы эквивалентности (пример такого разбиения см. на рис. 1).



G	a	b	c	d	e	f	g	h
a	0	**1**	0	0	0	**1**	**1**	**1**
b	**1**	0	**1**	0	**1**	0	0	0
c	0	**1**	0	**1**	**1**	0	0	0
d	0	0	**1**	0	**1**	0	0	0
e	0	**1**	**1**	**1**	0	0	0	0
f	**1**	0	0	0	0	0	0	0
g	**1**	0	0	0	0	0	0	**1**
h	**1**	0	0	0	0	0	**1**	0

Рис. 1. Пример конгруэнции на группоиде графа с классами $\{a\}$, $\{b\}$, $\{c, e\}$, $\{d\}$, $\{f, g, h\}$

Теорема 1. Пусть $G = (V, E)$ — произвольный классический граф. Тогда для любого элемента $c \in V$ и любого класса $[a]$ произвольной конгруэнции ρ выполняется одно из трёх условий:

1) $c \in [a]$;

[1] Данное определение применимо и для графов с петлями, а также для ориентированных.

2) $(c, a^*) \in E$ для всех $a^* \in [a]$;
3) $(c, a^*) \notin E$ для всех $a^* \in [a]$.

Доказательство. По определению конгруэнции для любых вершин графа выполняется $(a, b) \in \rho \Rightarrow (a \circ c, b \circ c) \in \rho \wedge (c \circ a, c \circ b) \in \rho$. Рассмотрим все варианты значений произведений $a \circ c$ и $b \circ c$ на группоиде графа и проверим, когда эти значения лежат в одном классе конгруэнции ρ.

С л у ч а й 1: обе пары вершин связаны рёбрами: $(a, c) \in E$ и $(b, c) \in E$. В этом случае $a \circ c = a$ и $b \circ c = b$, и поскольку $(a, b) \in \rho$, результаты умножения лежат в одном классе без дополнительных ограничений. Если рассмотрим другой элемент $d \in [a]$, то, с одной стороны, при $d \circ c = d$ получим $(d, c) \in E$ без дополнительных условий на ρ. С другой стороны, в случае $d \circ c = c$ получаем, что ρ является конгруэнцией тогда и только тогда, когда $(a \circ c, d \circ c) = (a, c) \in \rho$. Продолжая итерационно процесс для всех элементов класса $[a]$ конгруэнции ρ, получим, что либо на каком-то шаге $c \in [a]$, либо для всех $a^* \in [a]$ выполняется $(c, a^*) \in E$.

С л у ч а й 2: $(a, c) \in E$ и $(b, c) \notin E$. Тогда $a \circ c = a$ и $b \circ c = c$. Как следствие, результаты будут в одном классе конгруэнции, только если $(a, c) \in \rho$. По определению получаем, что $c \in [a]$.

С л у ч а й 3: $(a, c) \notin E$ и $(b, c) \in E$. Этот вариант полностью аналогичен случаю 2, за тем лишь исключением, что необходимо потребовать, чтобы $(b, c) \in \rho$. Пользуясь транзитивностью отношения ρ, вновь получаем, что $c \in [a]$.

С л у ч а й 4: $(a, c) \notin E$ и $(b, c) \notin E$. По определению получаем $a \circ c = b \circ c = c$, и так как $(c, c) \in \rho$, не требуется дополнительных ограничений для того, чтобы произведения $a \circ c$ и $b \circ c$ лежали в одном классе конгруэнции. Если рассмотрим другой элемент $d \in [a]$, то, с одной стороны, при $d \circ c = c$ получим $(d, c) \notin E$ без дополнительных условий на ρ. С другой стороны, в случае $d \circ c = d$ получаем, что ρ есть конгруэнция тогда и только тогда, когда $(a \circ c, d \circ c) = (c, d) \in \rho$. Продолжая итерационно процесс для всех элементов класса $[a]$ конгруэнции ρ, получим, что либо на каком-то шаге $c \in [a]$, либо для всех $a^* \in [a]$ имеет место $(c, a^*) \notin E$.

Рассмотрев все четыре возможных значения для произведений $c \circ a$ и $c \circ b$, получим в точности аналогичный результат. ■

Напомним, что правыми конгруэнциями называются такие отношения эквивалентности ρ, для которых выполняется $\forall a, b, c\ ((a, b) \in \rho \Rightarrow (ac, bc) \in \rho)$, а левыми — такие отношения эквивалентности μ, для которых $\forall a, b, c\ ((a, b) \in \mu \Rightarrow (ca, cb) \in \mu)$.

Следствие 1. На любом группоиде графа все левые конгруэнции являются одновременно правыми, а все правые — левыми.

Доказательство. Результат в доказательстве теоремы 1 получен независимо для случая умножения на c как слева, так и справа. Это означает, что структура классов не зависит от того, является ли конгруэнция правой или левой, а условие теоремы 1 выполняется для обоих типов конгруэнций. ■

Определение 4. Пусть $G = (V, E)$ — классический граф, а ρ — конгруэнция на его группоиде. Назовём *фактор-графом* по ρ граф $G/\rho = (V_\rho, E_\rho)$, где

1) V_ρ — множество классов конгруэнции ρ;
2) $([a], [b]) \in E_\rho$ тогда и только тогда, когда $(a, b) \in E$.

Пример построения фактор-графа для конгруэнции ρ с классами $\{a\}$, $\{b\}$, $\{c, e\}$, $\{d\}$, $\{f\}$, $\{h, g, k\}$, $\{l\}$ представлен на рис. 2.

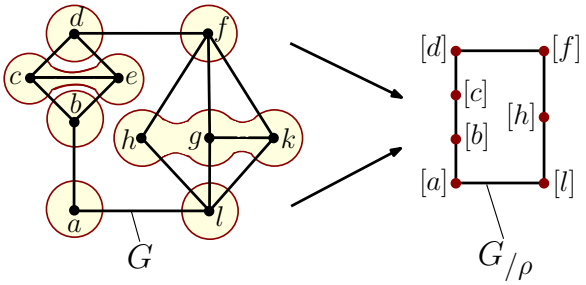


Рис. 2. Пример фактор-графа

Как известно, идеалом на группоиде $(D, \cdot)$ называется такое множество I, для которого любые произведения элементов группоида на элементы идеала лежат в идеале I. Можно по отдельности определить односторонние идеалы:

1) I_L — левый идеал, если $d \cdot i \in I_L$ для любых $d \in D$ и $i \in I_L$;
2) I_R — правый идеал, если $i \cdot d \in I_R$ для любых $d \in D$ и $i \in I_R$.

Понятия левого и правого идеалов можно, в частности, применить для группоидов графов $(V, \circ)$. На рис. 3 представлены примеры левых идеалов на G_1 и правых идеалов на G_2.

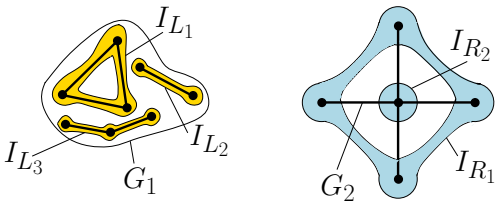


Рис. 3. Примеры левых и правых идеалов на графах

Напомним, что компонентой связности графа $G = (V, E)$ называется такое подмножество вершин $I \subseteq V$, что одновременно выполняются следующие два условия:

— любые две вершины $u, v \in I$ можно соединить путём;
— множество I максимально по включению.

Теорема 2. Минимальный по включению левый идеал I_L — это компонента связности графа. Любой другой левый идеал является объединением минимальных.

Доказательство. Компонента связности I_L является левым идеалом, так как вершины из I_L не связаны ни с одной другой вершиной графа $G = (V, E)$, и как следствие $V \circ I_L \subseteq I_L$ (примеры: $I_{L_1}, I_{L_2}, I_{L_3}$ на рис. 3). Если допустить, что существует меньший по включению идеал $I_L^* \subset I_L$, то найдётся вершина $u \in I_L \setminus I_L^*$, которая связана ребром с некоторой вершиной i из I_L^*. В результате получим противоречие с определением идеала: $u \circ i = u \notin I_L^*$.

Аналогично доказывается вторая часть теоремы. Если допустить, что произвольный левый идеал I_L — это не объединение компонент связности, то в множестве $V \setminus I_L$ найдётся вершина u, которая связана ребром хотя бы с одной вершиной i из предполагаемого идеала I_L: $u \circ i = u \notin I_L$. ■

Определение 5. Пусть дан граф $G = (V, E)$. Подмножество вершин $I \subset V$ будем называть *долей* графа G, если для любых $i \in I$ и $v \in V \setminus I$ верно, что $(i, v) \in E$.

Теорема 3. Минимальный по включению правый идеал I_R — это доля графа. Любой другой правый идеал является объединением долей графа.

Доказательство. Аналогично доказательству теоремы 2. ■

Теорема 4. Любой произвольный левый I_L (правый I_R) идеал на графе является классом некоторой конгруэнции ρ.

Доказательство. В качестве классов конгруэнции ρ рассмотрим I_L, а остальные классы возьмём одноэлементными. Из теоремы 2 следует, что ни одна вершина из множества $V \setminus I_L$ не связана ребром ни с одной вершиной из идеала I_L. В результате получим корректное разбиение на классы, согласно теореме 1, и определяющее условие конгруэнции будет выполнено. Аналогично доказывается утверждение и для случая правых идеалов I_R, за той лишь разницей, что все вершины идеала I_R связаны со всеми вершинами из множества $V \setminus I_R$. ■

Следствие 2. У произвольного графа $G = (V, E)$ не может быть левого идеала $I \neq V$, который одновременно был бы правым.

Доказательство. Если допустить, что такой идеал I существует, то он одновременно является объединением компонент связности и объединением долей. Это возможно только в случае $V \setminus I = \varnothing$. ■

Теорема 5. Группоид графа G является полугруппой тогда и только тогда, когда G — это либо полный граф K_n, либо пустой граф O_n.

Доказательство. Необходимость очевидна, так как для полного графа K_n группоид $(V, \circ)$ является полугруппой левых нулей, а для O_n — полугруппой правых нулей.

Доказательство достаточности проведём перебором всех вариантов произведений для троек вершин a, b, c с проверкой на ассоциативность.

С л у ч а й 1: три вершины не связаны ни одним ребром: $(a, b) \notin E$, $(b, c) \notin E$, $(a, c) \notin E$. Ассоциативность выполняется: $a \circ (b \circ c) = c = (a \circ b) \circ c$.

С л у ч а й 2: три вершины связаны ровно одним ребром: $(a, b) \notin E$, $(b, c) \in E$, $(a, c) \notin E$. Ассоциативность нарушена, так как $a \circ (b \circ c) = c \neq b = (a \circ b) \circ c$.

С л у ч а й 3: три вершины связаны ровно двумя рёбрами: $(a, b) \in E$, $(b, c) \in E$, $(a, c) \notin E$. Ассоциативность также нарушена, так как $a \circ (b \circ c) = a \neq c = (a \circ b) \circ c$.

С л у ч а й 4: три вершины связаны тремя рёбрами: $(a, b) \in E$, $(b, c) \in E$, $(a, c) \in E$. Ассоциативность выполняется: $a \circ (b \circ c) = a = (a \circ b) \circ c$.

Таким образом, для любых трёх вершин графа для выполнения условия ассоциативности они должны быть либо соединены тремя рёбрами друг с другом, либо не соединены ни одним ребром. Подобное условие верно для всех вершин только в случае, если граф G является полным K_n либо пустым O_n. ■

Класс группоидов классических графов можно задать аксиоматически. Для этого достаточно потребовать выполнения следующих трёх аксиом:

аксиома 1: $\forall a \quad (a^2 = a)$ (идемпотентность);

аксиома 2: $\forall a, b \quad (a \neq b \Rightarrow ab \neq ba)$ (антикоммутативность);

аксиома 3: $\forall a, b \quad (ab = a \vee ab = b)$.

Продемонстрируем, что если группоид $(V_s, \circ)$ удовлетворяет аксиомам 1–3, то он порождает некоторый граф $G_s = (V_s, E_s)$. Для этого нужно гарантировать однозначное восстановление множества рёбер E_s на основе множества с операцией $(V_s, \circ)$.

Определение 6. Назовём граф $G_s = (V_s, E_s)$ *порождённым* на основе группоида $(V_s, \circ)$, если его множество рёбер E_s задано по правилу

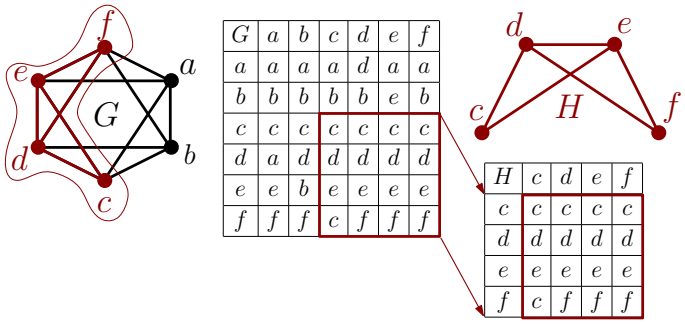
$$\forall a \quad ((a, a) \notin E_s(G)) \wedge (\forall b \neq a \quad (a, b) \in E_s(G) \Leftrightarrow a \circ b = a)\,.$$

Достаточно показать, что определение порождённого графа корректно при условии, что группоид V_s удовлетворяет аксиомам 1–3. Пусть $a \circ b = a$, тогда по аксиомам 2 и 3 получим $b \circ a = b$, а ребро будет задано корректно для классического графа: $(a, b) \in E_s$ и $(b, a) \in E_s$. Аналогично рассматривается случай $a \circ b = b$.

В свою очередь, аксиома 1 позволяет гарантировать, что у итогового графа все вершины не имеют петель в соответствии с замечанием 1 к определению 3.

Напомним, что в теории универсальных алгебр многообразием называется такой класс алгебр, который замкнут относительно взятия подалгебр, фактор-алгебр и прямого произведения алгебр. Под прямым произведением двух группоидов $D_1 \times D_2 = \{(d_1, d_2) : d_1 \in D_1, d_2 \in D_2\}$ подразумевается группоид, для которого умножение определено покомпонентно для всех его элементов $(d_1, d_2) \cdot (e_1, e_2) = (d_1 e_1, d_2 e_2)$ через умножения на D_1 и D_2. Отметим, что полученный на основе аксиом 1–3 класс объектов не является многообразием, так как он замкнут только относительно подалгебр и фактор-алгебр, а прямое произведение в классическом смысле не определено для графов. Действительно, если допустить, что у некоторых двух графов $ab = a$ для $a, b \in V(G_1)$ и $cd = d$ для $c, d \in V(G_2)$, то для прямого произведения получим $(a, c) \cdot (b, d) = (a, d)$, что является нарушением аксиомы 3.

В теории графов понятие подграфа вводится двумя разными способами. Подграфом в слабом смысле $G_s \subseteq G$ называется такой граф, для которого $V_s \subseteq V$ и $E_s \subseteq E$. Подграфом в сильном смысле называется такой подграф, для которого дополнительно требуется, чтобы E_s было максимальным по включениям, т. е. содержало бы все рёбра, которые соединяют вершины из $V_s \subseteq V$ в исходном графе G (пример на рис. 4).



G	a	b	c	d	e	f
a	a	a	a	d	a	a
b	b	b	b	b	e	b
c	c	c	c	c	c	c
d	a	d	d	d	d	d
e	e	b	e	e	e	e
f	f	f	c	f	f	f

H	c	d	e	f
c	c	c	c	c
d	d	d	d	d
e	e	e	e	e
f	c	f	f	f

Рис. 4. Пример подграфа $H \subset G$ в сильном смысле

Теорема 6. Для любого графа $G = (V, E)$ и любого непустого подмножества вершин $V_s \subseteq V$ верно:

1) $(V_s, \circ)$ — подгруппоид исходного группоида $(V, \circ)$;
2) граф $G_s = (V_s, E_s)$, порождённый $(V_s, \circ)$, является подграфом в сильном смысле для G.

Доказательство. Для группоида $(V, \circ)$ выполняются аксиомы 1–3. Поскольку они определены для всех элементов $a, b \in V$, они также выполняются и на произвольном подмножестве $V_s \subseteq V$. Аксиома 3 гарантирует, что при умножении элементов выйти за пределы V_s не получится, а значит, V_s замкнут относительно операции, и как следствие — это подгруппоид для V.

Порождённым графом на основе $(V_s, \circ)$ по определению 6 является такой граф $G_s = (V_s, E_s)$, у которого рёбра заданы правилом: $(a, b) \in E_s \Leftrightarrow a \circ b = a$. Очевидно, что данный граф является подграфом в сильном смысле графа G, так как он содержит все рёбра, которые соединяют вершины из V_s в исходном графе G. ■

2. Практическое приложение группоидов графов

Наиболее часто для представления графов в памяти компьютера используется матрица смежности для вершин графа. Напомним, что матрицей смежности графа G называется такая булева матрица $A_{n\times n}$, которая индексирована множеством вершин $V(G)$ и для которой $A(x,y)=1 \Leftrightarrow (x,y)\in E(G)$. С точки зрения компактного хранения данный способ является сильно избыточным. В первую очередь это связано с тем, что матрица смежности любого классического графа симметрична, а на её главной диагонали стоят только нули. Однако даже хранение только верхней части матрицы избыточно, так как хранить в общем случае имеет смысл только реально существующие рёбра $(x,y)\in E(G)$, для которых $A(x,y)=1$, а остальные по умолчанию можно считать отсутствующими ($A(x,y)=0$). Это подводит нас к рассмотрению первого примера реализации компактного хранения.

Пример 1. Вводим на множестве вершин $V(G)$ любой линейный порядок $(V,<)$, например, перейдя к канонической форме графа $\mathrm{Canon}(G)$ или любым другим методом [6]. Для компактного хранения в память заносим список рёбер E_m, пользуясь правилом $(x,y)\in E_m \Leftrightarrow ((x,y)\in E(G)\wedge x<y)$. В результате в память будут занесены все рёбра графа G, и каждое ровно по одному разу.

Отметим, что способ примера 1 не позволяет полностью избавиться от избыточности в хранении графа. В частности, вершина с первым номером будет многократно повторена в записи $(x,y_1),\ldots,(x,y_k)$. Более экономично указывать её один раз, а затем перечислять все связанные с ней вершины.

Пример 2. Вводим на множестве вершин графа $V(G)$ ($|V|=n$) любую взаимно-однозначную индексацию $N: V\to\{1,\ldots,n\}$. Для компактного хранения будем последовательно заносить в память двойки $(x_i,U(x_i))$ следующего вида:

$$x_i : N(x_i)=i,\quad U(x_i)=\{y:(x,y)\in E(G)\wedge\forall j<i\ (y\notin U(x_j))\}\,.$$

Для дополнительной экономии при хранении графа можно оборвать запись в память на первой паре $(x_i,U(x_i))$, для которой $U(x_i)=\varnothing$.

От элементарных примеров сжатия данных для графов перейдём непосредственно к приложению конгруэнций и фактор-графов для компактного хранения графов. Общая идея заключается в том, чтобы вместо самого графа G хранить фактор-граф G/ρ по максимальной нетривиальной конгруэнции ρ, а также все нетривиальные (содержащие больше одной вершины) классы $[a]$ конгруэнции ρ как подграфы G.

Ш а г 1: пользуясь результатом теоремы 1, ищем максимальную по включениям конгруэнцию ρ, исключая тривиальный случай разбиения на один класс $[a]=V$;

Ш а г 2: определяем, какие из классов состоят более чем из одного элемента;

Ш а г 3: для всех нетривиальных классов $[a]$, определённых на шаге 2, рассматриваем подграфы $G_1,\ldots,G_k\subset G$, порождённые группоидами $([a],\circ)$;

Ш а г 4: в каждом классе $[a]$ конгруэнции ρ выбираем произвольного представителя $a^*\in[a]$;

Ш а г 5: вводим новый граф $G^*/\rho=(V^*_\rho,E^*_\rho)$, заменяя в фактор-графе G/ρ классы вершин $[a]$ на представителей a^*, выбранных на шаге 4;

Ш а г 6: заменяем исходный граф G полученным набором графов $(G^*/\rho,G_1,\ldots,G_k)$.

Согласно теореме 1, исходный граф G можно однозначно восстановить на основе $(G^*/\rho,G_1,\ldots,G_k)$. Наличие ребра в G^*/ρ между двумя представителями a^* и b^* разных классов означает, что все элементы из класса $[a^*]$ попарно смежны со всеми

элементами из класса $[b^*]$. Аналогично, если ребра между a^* и b^* нет в G^*/ρ, то классы $[a^*]$ и $[b^*]$ также не связаны друг с другом ни одним ребром. Сжатие данных при этом достигается за счёт удаления из рассмотрения всех «лишних» рёбер, которые связывают элементы различных классов (остаётся лишь один экземпляр такого ребра). Естественно, что положительный результат с точки зрения сжатия достигается лишь в том случае, если для хранения $(G^*/\rho, G_1, \ldots, G_k)$ использован способ примера 1 или примера 2.

Пример работы алгоритма сжатия представлен на рис. 5. Важно отметить, что в общем случае если исходный граф G связный, то граф G^*/ρ также связный. Однако при этом подграфы $G_1, \ldots, G_k$, которые соответствуют нетривиальным классам конгруэнции ρ, вполне могут получиться несвязными (см. в качестве примера G_1 на рис. 5).

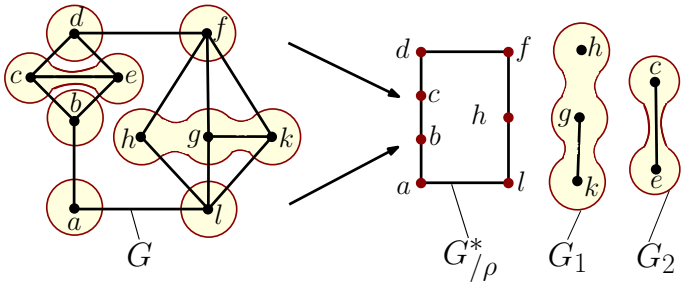


Рис. 5. Пример использования алгоритма сжатия графов

Замечание 2. Применение алгоритма сжатия для несвязных графов является нецелесообразным. Это связано с тем, что компоненты связности, согласно теоремам 2 и 4, являются классами конгруэнций, так же как и объединение компонент связности.

Заключение

Предложенный способ описания графов может быть также полезен при решении других задач теории графов. Например, его можно использовать для оптимизации решения задачи о клике. В классической постановке данной задачи необходимо найти внутри произвольного графа G максимальный полный подграф K_n. Согласно теореме 6, группоид для такого подграфа является полугруппой, а значит, можно воспользоваться для его поиска тестами на ассоциативность (тестами Лайта или их вероятностными модификациями [7]). Можно также переформулировать задачу о восстановлении графа по подграфам на языке алгебры, что потенциально может упростить её решение (см. подробнее о задаче восстановления в [8]).

В работе [9] предложен способ задания метрических пространств (D, ρ_R) и (D, ρ_L) на основе бинарной операции на группоиде D. Метрические пространства, которые получены с помощью определения из [9], для рассмотренных в данной работе группоидов графов обладают следующим свойством: если две вершины графа автоморфны $(x \sim y)$, то для любой другой вершины z расстояния до x и y совпадают: $\rho_R(x, z) = \rho_R(y, z)$ и $\rho_L(x, z) = \rho_L(y, z)$. В результате по отношению к группоидам графов сформулирована следующая гипотеза.

Гипотеза 1. Если применить к группоидам графов алгоритм поиска метрики, изложенный в работе [9], то две вершины графа автоморфны тогда и только тогда, когда для любой вершины z выполняется $\rho_R(x, z) = \rho_R(y, z) \wedge \rho_L(x, z) = \rho_L(y, z)$.

ЛИТЕРАТУРА

1. *McNulty G. F. and Shallon C. R.* Inherently nonfinitely based finite algebras // Universal algebra and lattice theory. Lecture Notes in Math. 1983. V. 1004. P. 206–231.
2. *Lee S. M.* Simple graph algebras and simple rings // Southeast Asian Bull. Math. 1991. V. 15. P. 117–121.
3. *Oates-Williams S.* On the variety generated by Murskii's algebra // Algebra Universalis. 1984. V. 18(2). P. 175–177.
4. *Kelarev A. V., Miller M., and Sokratova O. V.* Languages recognized by two-sided automata of graphs // Proc. Estonian Acad. Sci. 2005. V. 54(1). P. 46–54.
5. *Trent Y.* Groupoid models for the $C*$-algebras of topological higher-rank graphs // J. Operator Theory. 2006. No. 4. P. 95–120.
6. *Назаров М. Н.* Альтернативные подходы к описанию классов изоморфных графов // Прикладная дискретная математика. 2014. № 3. С. 86–97.
7. *Rajagopalan S. and Schulman L. J.* Verification of identities // SIAM J. Comput. 2000. V. 29. P. 1155–1163.
8. *Harary F.* A survey of the reconstruction conjecture // Graphs and Combinatorics. Lecture Notes in Math. 1974. V. 406. P. 18–28.
9. *Назаров М. Н.* Собственная метрика на группоидах и её приложение к анализу межклеточных взаимодействий в биологии // Фундамент. и прикл. матем. 2013. № 3. С. 149–160.

REFERENCES

1. *McNulty G. F. and Shallon C. R.* Inherently nonfinitely based finite algebras. Universal algebra and lattice theory. Lecture Notes in Math., 1983, vol. 1004, pp. 206–231.
2. *Lee S. M.* Simple graph algebras and simple rings. Southeast Asian Bull. Math., 1991, vol. 15, pp. 117–121.
3. *Oates-Williams S.* On the variety generated by Murskii's algebra. Algebra Universalis, 1984, vol. 18(2), pp. 175–177.
4. *Kelarev A. V., Miller M., and Sokratova O. V.* Languages recognized by two-sided automata of graphs. Proc. Estonian Acad. Sci., 2005, vol. 54(1), pp. 46–54.
5. *Trent Y.* Groupoid models for the $C*$-algebras of topological higher-rank graphs. J. Operator Theory, 2006, no. 4, pp. 95–120.
6. *Nazarov M. N.* Al'ternativnye podhody k opisaniju klassov izomorfnyh grafov. Prikladnaya Diskretnaya Matematika, 2014, no. 3, pp. 86–97. (in Russian)
7. *Rajagopalan S. and Schulman L. J.* Verification of identities. SIAM J. Comput., 2000, vol. 29, pp. 1155–1163.
8. *Harary F.* A survey of the reconstruction conjecture. Graphs and Combinatorics. Lecture Notes in Math., 1974, vol. 406, pp. 18–28.
9. *Nazarov M. N.* Sobstvennaja metrika na gruppoidah i ejo prilozhenie k analizu mezhkletochnyh vzaimodejstvij v biologii. Fundament. i Prikl. Matem., 2013, no. 3, pp. 149–160. (in Russian)

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

УДК 621.391.1:004.7

РЕЖИМЫ ФУНКЦИОНИРОВАНИЯ АСИНХРОННЫХ КЛЕТОЧНЫХ АВТОМАТОВ, МОДЕЛИРУЮЩИХ НЕЛИНЕЙНУЮ ПРОСТРАНСТВЕННУЮ ДИНАМИКУ[1]

О. Л. Бандман

Институт вычислительной математики и математической геофизики СО РАН, г. Новосибирск, Россия

Сдвиг научного интереса от физических явлений, подчиняющихся законам термодинамики, к нелинейным диссипативным процессам, содержащим химические и биологические превращения, привёл к аналогичному повороту в математическом моделировании: от решения дифференциальных уравнений к прямому дискретному стохастическому моделированию. Математическим фундаментом дискретного моделирования является асинхронный клеточный автомат — стохастический аналог клеточного автомата фон Неймана. Систематической методологии построения асинхронного клеточного автомата, моделирующего процессы, состоящие из многих действий, совместно преобразующих общее дискретное пространство, пока не существует. Нет ответа на вопрос, насколько и чем различаются результаты моделирования при разных способах организации (режимах) взаимодействий локальных операторов, составляющих сложный процесс. В работе делается попытка ответить на этот вопрос путём проведения серии вычислительных экспериментов по моделированию трёх типовых реакционно-диффузионных процессов при разных асинхронных режимах и сравнительного анализа их эволюций. Результат состоит в том, что качественный характер процессов не зависит от способа композиции, а количественные различия могут быть скорректированы.

Ключевые слова: *дискретное математическое моделирование, асинхронный клеточный автомат, режимы функционирования, реакционно-диффузионные процессы, пространственная самоорганизация.*

DOI 10.17223/20710410/27/12

FUNCTIONING MODES OF ASYNCHRONOUS CELLULAR AUTOMATA SIMULATING NONLINEAR SPATIAL DYNAMICS

O. L. Bandman

Institute of Computational Mathematics and Mathematical Geophysics SB RAS, Novosibirsk, Russia

E-mail: bandman@ssd.sscc.ru

[1]Работа поддержана грантами Президиума РАН (Проект 15.9, 2014) и СО РАН (Интеграционный проект ИП-47, 2011).

The shift of scientific interest from physical phenomena obeying laws of thermodynamics towards nonlinear dissipative processes containing chemical and biological transformations stimulates a similar turn in mathematical modeling: from differential equation solution to direct and stochastic simulation. A foundation for discrete simulation is the asynchronous cellular automaton — a stochastic analogue of von-Neumann's cellular automaton. For the time being, there is no systematic methodology for constructing asynchronous cellular automata simulating processes composed of many actions transforming a common discrete space. It is not known, how different are simulation results obtained by different ways of composing simple operations for organizing a complex computational process. In the paper, an attempt is made to answer this question by means of performing a series of simulation of three typical reaction-diffusion processes with different asynchronous modes of functioning, and comparative analysis of their evolutions and invariants. The obtained result shows that qualitative character of the process under simulation does not depend on the composition mode, and quantitative differences may be corrected.

Keywords: *discrete mathematical modeling, asynchronous cellular automaton, modes of functioning, reaction-diffusion processes, spacial self organization.*

Введение

Наряду с теоретическими и экспериментальными видами научной деятельности развивается третья её составляющая — компьютерное моделирование исследуемых процессов. В частности, с помощью имеющихся мощных компьютеров стало возможным изучение механизмов химических и биологических процессов на микро- и наноуровнях, которые трудно или невозможно моделировать, основываясь на традиционных моделях математической физики, так как исследуемые явления нелинейны, разрывны и диссипативны. Поиски новых нетрадиционных моделей привели к переосмысливанию идеи клеточного автомата (КА) [1] и появлению множества его модификаций. Среди них значительное место занимают КА-модели явлений, которые могут быть представлены композицией простейших действий типа «движение» и «превращение» элементарных частиц и составляют класс *реакционно-диффузионных* процессов. Движения обычно подчиняются законам диффузии или конвекции, а превращения имитируют химические реакции. Все действия представляются как случайные процессы [2], поскольку в естественных условиях нет для них специальной синхронизации. Известно несколько методов моделирования случайных процессов, происходящих в пространстве. В разных предметных областях они имеют свои названия и отличаются способами объединения элементарных действий в единый пространственно-распределённый процесс. В материаловедении и микроэлектронике — это «кинетический метод Монте-Карло» [3, 4]. В каталитической химии — это просто «метод Монте-Карло» [2, 5]. На самом деле они все являются вариантами асинхронного КА, отличающимися способами построения правил перехода.

Математические модели реакционно-диффузионных явлений, выраженные в терминах асинхронных КА [6, 7], а также исследование методов композиции КА [8] позволили обобщить накопленный опыт построения сложных КА-моделей и выделить три главных режима взаимодействия элементарных операторов, называемых *подстановками*:

— *стохастический режим*, когда каждая случайно выбранная подстановка применяется к случайно выбранной клетке, и так для всех подстановок и всех клеток;

— *локальная суперпозиция*, когда все подстановки в случайном порядке применяются к одной и той же случайно выбранной клетке, и так для всех клеток;
— *глобальная суперпозиция*, когда каждая случайно выбранная подстановка применяется ко всем случайно выбираемым клеткам, и так для всех подстановок.

Для правильного выбора способа композиции при синтезе КА-модели полезно знать, как этот выбор влияет на результат моделирования, т. е. насколько различны эволюции асинхронных КА, отличающихся только способом композиции подстановок. Есть предположение, что влияние это незаметно или очень мало. В каких случаях это предположение подтверждается — на этот вопрос далее делается попытка ответить путём проведения вычислительных экспериментов над несколькими типовыми КА-моделями.

Работа организована следующим образом. В п. 2 дана формальная постановка задачи. В п. 3, 4 и 5 приводятся результаты экспериментального моделирования для процессов движения фронта, агрегации вещества и самоорганизации соответственно. Заключение содержит сравнительный анализ полученных результатов.

1. Формальное представление асинхронных КА-моделей

Формально асинхронный КА задаётся тройкой понятий $\aleph = \langle A, X, \Theta(X)\rangle$, где A — *алфавит состояний клеток*, т. е. множество символов или чисел, обозначающих вещества, участвующие в процессе, или условия, определяющие их свойства; $X = \{x_k : k = 1, \ldots, N\}$ — *множество имён клеток*, которое обычно задаётся множеством координат дискретного пространства конечных размеров; $\Theta(X)$ — *глобальный оператор*, определяющий функционирование асинхронного КА. Пара (u, x), где $u \in A$, $x \in X$, называется *клеткой*. Множество клеток $\Omega = \{(u_k, x_k) : u_k \in A, x_k \in X, \forall k, l\ (k \neq l \Rightarrow x_k \neq x_l)\}$ образует *клеточный массив*, а перечень состояний всех клеток массива $\Omega_A = (u_1, u_2, \ldots, u_{|X|})$ — *глобальное состояние*.

В пространстве X определены подмножества имён клеток, называемые *шаблонами соседства*:

$$T_n(x) = \{x, x + a_1, \ldots, x + a_{n-1}\},$$

где a_j — вектор смещения; $n = |T_n(x)|$. Шаблон $T_n(x_k)$ соседства выделяет в клеточном массиве Ω подмножество клеток-соседей для конкретной клетки x_k, состояния которых составляют *локальную конфигурацию*

$$S(x_k) = \{u_0, u_1, \ldots, u_{n-1}\},$$

где $u_0, u_1, \ldots, u_{n-1}$ — состояния клеток $x_k, x_k + a_1, \ldots, x_k + a_{n-1}$ соответственно.

Элементарная операция, изменяющая состояние клеток-соседей $x \in \Omega$, имеет вид *подстановки*

$$\theta(x) : S(x) \xrightarrow{p} S'(x),$$

где p — вероятность применения подстановки, вычисляемая исходя из известных скоростей моделируемых элементарных действий.

Применение подстановки θ к клетке x_k сводится к замене всех или некоторых состояний $u_j \in S(x_k)$ на новые значения $u'_j \in S'(x_k)$:

$$u'_j = f_j(u_0, \ldots, u_{n-1}), \quad n = |S(x_k)|, \tag{1}$$

где $f_j(u_0, \ldots, u_{n-1})$ — *функция перехода*.

Применение подстановки к клетке $x_k \in X$ считается успешным, если все клетки с именами из $T_n(x_k)$ содержатся в Ω:

$$\{(u_0, x_k), \ldots, (u_{n-1}, x_k + a_{n-1})\} \subseteq \Omega. \tag{2}$$

При этом клетка (u, x) с переменным состоянием u считается принадлежащей Ω, если u определено в A.

Простым далее называется такой КА, у которого глобальный оператор $\Theta(X) = \Psi(\theta)$ состоит из одной подстановки. Асинхронный режим простого КА предполагает следующий алгоритм применения подстановки:

1) с вероятностью $p = 1/|X|$ выбирается клетка $(u, x_k) \in \Omega$;
2) к выбранной клетке применяется подстановка $\theta(x)$;
3) если условие (2) для $\theta(x)$ выполнено, то состояния $u_j \in S(x_k)$ немедленно меняются на значения функций переходов (1);
4) условно принимается, что $|X|$ повторений п. 1 и 2 составляет одну итерацию.

Сложная асинхронная КА-модель обычно задаётся не одной, а *набором подстановок* $\Theta = \{\theta_1, \ldots, \theta_m\}$ и *способом их композиции* $\Psi(\Theta)$. Набор подстановок соответствует набору элементарных действий в моделируемом процессе, причём так как скорости $K_1, \ldots, K_m$ выполнения этих действий различны, то каждая подстановка θ_i снабжается вероятностью своего применения

$$p_i = \frac{K_i}{K_1 + K_2 + \ldots + K_m}. \tag{3}$$

Поскольку $\sum\limits_{1}^{m} p_i = 1$, значения вероятностей в интервале $(0, 1)$ можно расположить так, чтобы каждому p_i назначался подинтервал $\pi_i = \left[\sum\limits_{j=1}^{i-1} p_j, \sum\limits_{j=1}^{i} p_j\right)$. *Случайным выбором* подстановки $\theta_i \in \Theta$ далее называется такой её выбор, что случайное число $\eta \in \pi_i$.

Применение глобального оператора $\Theta(X)$ к массиву $\Omega(t)$ изменяет его глобальное состояние $\Omega(t) \to \Omega(t+1)$, составляя одну итерацию. Последовательность

$$\Omega(0), \ldots, \Omega(t), \ldots, \Omega(T)$$

называется *эволюцией КА*.

Способ композиции подстановок $\Psi_z(\Theta)$ в глобальном операторе определяет алгоритм их применения к клеткам клеточного массива $\Omega(t)$ в течение одной итерации. Далее изучаются три основных способа композиции: стохастический ($z = S$), локальный ($z = L$) и глобальный ($z = G$), на которых могут строиться ещё более сложные композиционные конструкции.

Стохастическая композиция Ψ_S предусматривает следующий алгоритм применения подстановок:

1) с вероятностью $p = 1/|X|$ выбирается клетка $(u, x_k) \in \Omega$;
2) случайно выбирается подстановка θ_i, которая сразу применяется к x_k;
3) условно принимается, что $|X| \cdot m$ повторений п. 1 и 2 составляют одну итерацию.

Из приведённого алгоритма следует, что при стохастической композиции каждая случайно выбранная подстановка $\theta_i \in \Theta$ в течение одной итерации выполняется $p_i \cdot |X|$ раз, всякий раз для случайно выбранной клетки $x_k \in X$.

Локальная суперпозиция Ψ_L предусматривает следующий алгоритм применения подстановок:

1) с вероятностью $p = 1/|X|$ выбирается клетка $(u, x_k) \in \Omega$;
2) случайно выбирается подстановка $\theta_i \in \Theta$ и применяется к клетке x_k, затем выбирается следующая подстановка $\theta_j \in \Theta$, которая применяется к той же самой клетке, и так m раз;
3) условно принимается, что $|X|$ повторений п. 1 и 2 составляют одну итерацию.

Из приведённого алгоритма следует, что при локальной суперпозиции каждая случайно выбранная подстановка $\theta_i \in \Theta$ в течение одной итерации выполняется $p_i \cdot |X|$ раз, как и при стохастической композиции. Однако отличие состоит в том, что здесь все подстановки применяются к одной и той же случайно выбранной клетке.

Глобальная суперпозиция Ψ_G предусматривает следующий порядок применения подстановок:

1) случайно выбирается подстановка $\theta_i \in \Theta$;
2) θ_i применяется последовательно к случайно выбираемым с вероятностью $p = 1/|X|$ клеткам $(u, x_k) \in \Omega$;
3) условно принимается, что m повторений п. 1 и 2 составляют одну итерацию.

Из приведённого алгоритма следует, что при глобальной суперпозиции каждая случайно выбранная подстановка $\theta_i \in \Theta$ в течение одной итерации выполняется $p_i \cdot |X|$ раз, так же, как в обоих предыдущих случаях. Однако отличие состоит в том, что здесь одна и та же случайно выбранная подстановка применяется ко всем случайно выбираемым клеткам.

Три приведённых способа композиции подстановок в асинхронных КА-моделях различаются степенью вводимого в алгоритмы порядка, который можно оценивать вероятностью q_z каждого применения подстановки в течение одной итерации. Эта вероятность равна обратной величине числа возможностей. Легко подсчитать, что для каждого способа композиции она равна

$$q_S = \frac{2(Q-2)!}{Q!}, \quad q_L = q_G = \frac{m!(Q-m)!}{Q!},$$

где $Q = |X| \cdot m$.

Сравнение эволюций КА-моделей при трёх приведённых способах композиции локальных операторов выполнялось для трёх типовых реакционно-диффузионных процессов: распространение фронта, агрегация вещества и самоорганизация в системе «хищник — жертва». Вычислительные эксперименты были поставлены следующим образом:

1) для каждого процесса были выбраны одна или несколько основных величин, характеризующих его эволюции;
2) каждый процесс моделировался трижды; КА-модели отличались только способом композиции подстановок. На каждой итерации выводились значения выбранных характеристик;
3) исследовались различия полученных значений для трёх способов композиции.

2. Распространение фронта двумерной волны

Первая математическая модель процесса распространения фронта волны исследована в [10, 11]. В [10] процесс называется «диффузией, соединенной с возрастанием количества вещества». Результаты оказались необычайно плодотворными не только в части математического анализа этого нелинейного явления, но и в части применения их для моделирования подобных процессов, например распространения огня,

распространения сорняков и эпидемий, химических превращений веществ в активных средах. КА-модели процесса распространения фронта также предлагались и изучались для разных применений [12]. Для современного моделирования процесс «распространение фронта» может рассматриваться как типовая составляющая более сложных явлений [13] и, следовательно, должен быть изучен подробно.

Кинетика процесса представлена как множество частиц, распределённых по пространству с неравномерной плотностью. Частицы диффундируют из области с большей плотностью на свободные места. Однако плотность в каждой точке изменяется не только в результате диффузионного перемещения, но также из-за реакции среды на эти изменения. Реакция описывается логистической функцией, имеющей вид полинома n-го порядка. В простейшем случае это функция следующего вида:

$$F(u,x) = \alpha\langle u(x)\rangle(1 - \langle u(x)\rangle), \tag{4}$$

где $\langle u(x)\rangle$ — плотность вещества в клетке x, равная осреднённому значению состояния по окрестности осреднения:

$$\langle u(x)\rangle = \frac{\sum\limits_{x_j \in \mathrm{Av}(x)} u(x_j)}{|\mathrm{Av}|}. \tag{5}$$

Здесь $\mathrm{Av}(x)$ — окрестность осреднения, состоящая их множества клеток, отдалённых от x не более чем на заданное l.

Асинхронный КА, моделирующий распространение фронта волны в двумерном пространстве $\aleph = \langle A, X, \Theta(X)\rangle$, в своем классическом виде работает с булевым алфавитом $A = \{0,1\}$, множеством имён клеток $X = \{(i,j) : i,j = 0,\ldots,N\}$ и глобальным оператором $\Theta(X) = \Psi_z(\theta_\mathrm{d}(x), \theta_\mathrm{r}(x))$, где Ψ_z — один из способов композиции Ψ_S, Ψ_L или Ψ_G; θ_d — локальный оператор диффузии, θ_r — локальный оператор реакции, которые могут быть выражены одноимёнными элементарными подстановками.

Подстановка $\theta_\mathrm{d}(x)$ определена на пятиточечном шаблоне

$$T_5(i,j) = \{(i,j),(i,j+1),(i+1,j),(i,j-1),(i-1,j)\} \tag{6}$$

и имеет вид

$$\theta_\mathrm{d} : \{u_0,u_1,u_2,u_3,u_4\} \xrightarrow{p_\mathrm{d}} \{u_0', u_1'u_2', u_3', u_4'\} \tag{7}$$

Применение θ_d к случайно выбранной клетке $(u_0, x_k) \in \Omega$ состоит в замене её состояния u_0 на состояние u_l одной из соседних клеток, выбранных равновероятно, т. е.

$$(u_0' = u_l)\ \&\ (u_l' = u_0),\ \text{если}\ (l-1)/4 < \mathrm{rand}_1 < l/4\ \&\ \mathrm{rand}_2 < p_\mathrm{d}, \quad l = 1,2,3,4,$$

где rand_1, rand_2 — случайные числа в интервале (0,1).

Начальным глобальным состоянием выбран клеточный массив размера 701×701. В центре массива находится круг радиуса $R = 30$, в котором все клетки имеют состояния $v = 1$, в остальных клетках массива состояния $v = 0$. При функционировании КА круг расширяется, постепенно заполняя единицами всю область. Вычислительный эксперимент состоял из запуска параллельной программы моделирования эволюций трёх КА, отличающихся способами композиции глобального оператора. Каждому способу композиции Ψ_z, $z \in \{\Psi_S, \Psi_L, \Psi_G\}$, отводился один OpenMP-поток на четырёхядерном компьютере Intel Core i7 920. В эксперименте выполнялось по 100 прогонов с разными начальными значениями генератора случайных чисел и последующим вычислением математического ожидания $\bar{u}(x)$ результирующих состояний. Для каждого способа

композиции на t-й итерации выводилось по два числа, характеризующих моделируемый процесс:

$$\Gamma_z(t) = \sum_{x \in X} \bar{u}(x), \quad V_z(t) = \frac{1}{\sqrt{\pi}} \left(\sqrt{\Gamma_z(t)} - \sqrt{\Gamma_z(t-1)} \right),$$

где Γ_z — суммарное состояние; V_z — скорость распространения фронта. Вычислительные эксперименты различались соотношением вероятностей диффузии и реакции $(p_\mathrm{d}; p_\mathrm{r})$, которые равнялись $(0{,}1; 0{,}9)$, $(0{,}2; 0{,}8)$, $(0{,}5; 0{,}5)$, $(0{,}9; 0{,}1)$, $(0{,}95; 0{,}05)$. Полученные значения $\Gamma_z(t)$ и $V_z(t)$ (рис. 1) показывают, что все три способа композиции глобального оператора на качественном уровне неразличимы, так как разность между суммарными состояниями $\Gamma_S(t) - \Gamma_L(t)$, $\Gamma_S(t) - \Gamma_G(t)$ ни в одном эксперименте ни при одном t не превышает 3 %. На размер разницы не влияет также соотношение вероятностей $(p_\mathrm{d}; p_\mathrm{r})$, от которого зависит скорость распространения фронта (рис. 2).

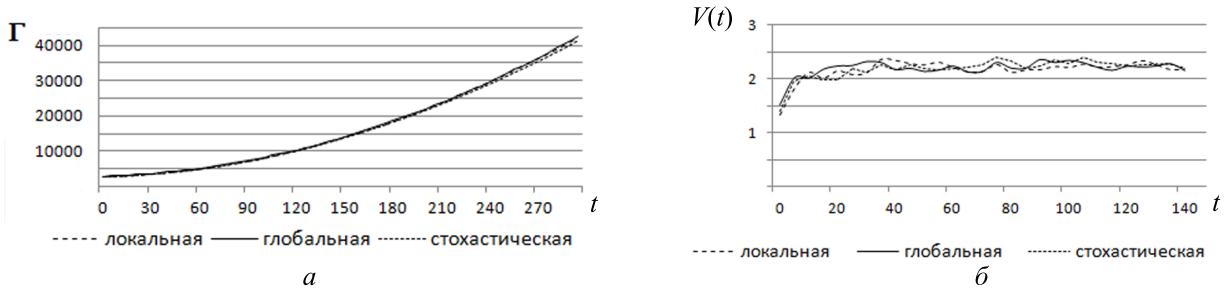


Рис. 1. Результаты вычислительного эксперимента при $p_\mathrm{d} = p_\mathrm{r} = 0{,}5$: *а* — суммарные состояния в зависимости от времени; *б* — скорости распространения фронта волны от времени

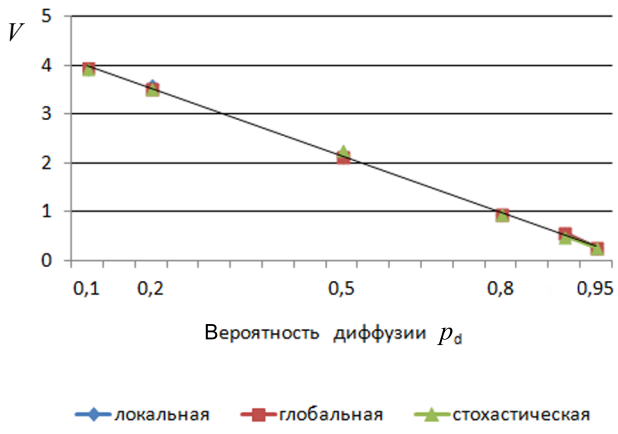


Рис. 2. Зависимость скорости распространения фронта волны V от значения вероятности применения подстановки диффузии p_d. Значения V_S, V_L, V_G для всех случаев совпадают

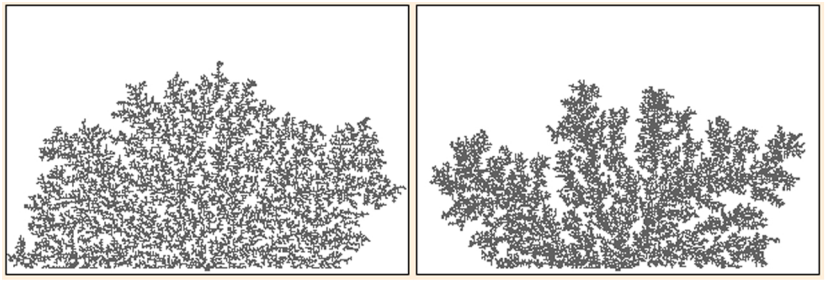
3. Агрегация, ограниченная диффузией

Явление, которое называется «агрегация, ограниченная диффузией» (diffusion limited aggregation, DLM), далее — просто *агрегация*, не может быть представлено в виде дифференциального уравнения. Его первая модель была описана в виде взаимодействий и движений частиц в дискретном пространстве и сразу реализована на компьютере [14]. В [14] модель не была причислена ни к какому направлению математического моделирования, хотя по сути является асинхронным КА. Модель агрегации является абстракцией таких процессов, как электрогальванизация [15], образование кристаллических структур [16], рост городов [17] и др. Наиболее известны асинхронные КА-модели, в которых диффузионная составляющая описывает случайное блуждание частиц в пространстве, а реакционная составляющая преобразует блуждающую частицу в неподвижную, если она оказывается достаточно близко к другой неподвижной (явление «прилипания»).

Процессу соответствует эволюция асинхронного КА $\aleph = \langle A, X, \Theta(X)\rangle$, где $A = \{0, 1, b\}$, $X = \{(i, j)\}$. Локальный оператор $\Theta(i, j) = \Phi_z(\theta_{\mathrm{d}}(i, j), \theta_{\mathrm{r}}(i, j))$, где $\theta_{\mathrm{d}}(i, j)$ — подстановка наивной диффузии (7), $\theta_{\mathrm{r}}(i, j)$ — подстановка прилипания. Обе подстановки вероятностные, значения вероятностей p_{d}, p_{r} определяются по (3), исходя из известных значений коэффициентов диффузии и прилипания. Подстановка прилипания построена на шаблоне T_5 (6) и имеет тот же вид, что и $\theta_{\mathrm{d}}(i, j)$, отличаясь только функцией перехода, которая здесь равна

$$u_0' = \begin{cases} b, & \text{если } (u_0 = 1)\ \&\ (u_l = b)\ \&\ (\mathrm{rand} < p_{\mathrm{r}}), \\ u_0 & \text{в остальных случаях,} \end{cases} \qquad l = 1, 2, 3, 4.$$

Исходное глобальное состояние $\Omega(0)$ — равномерное с плотностью 0,5 распределение «единиц» по всему массиву, кроме пятна из клеток-зародышей в состоянии $v(i, j) = b$ размера 2×4, расположенного в середине нижней границы массива. В процессе эволюции вокруг зародышей образуется растущая древовидная структура (рис. 3), похожая на коралл или мох.



а *б*

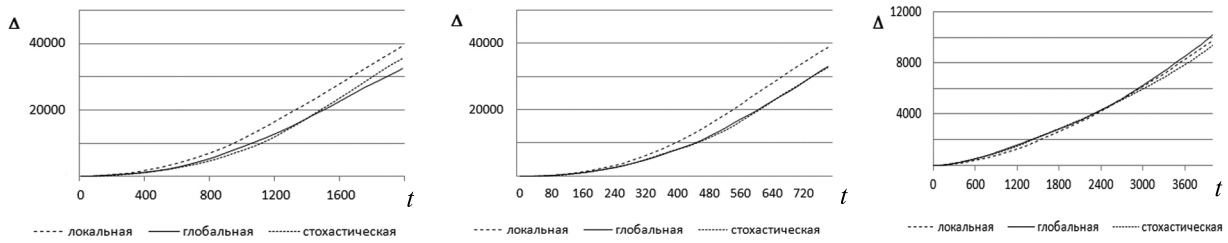
Рис. 3. Древовидные структуры, построенные асинхронным КА агрегации при стохастической композиции подстановок $\theta_{\mathrm{d}}(i, j)$ и $\theta_{\mathrm{r}}(i, j)$: *а* — при $(p_{\mathrm{d}}; p_{\mathrm{r}}) = (0{,}5; 0{,}5)$ и $t = 520$; *б* — при $(p_{\mathrm{d}}; p_{\mathrm{r}}) = (0{,}9; 0{,}1)$ и $t = 2500$

Вычислительные эксперименты проводились для клеточного массива размера 500×200. Промоделированы три случая, отличающиеся соотношениями вероятностей $(p_{\mathrm{d}}; p_{\mathrm{r}}) = (0{,}5; 0{,}5), (0{,}8; 0{,}2)$ и $(0{,}95; 0{,}05)$. Во всех случаях каждому способу композиции Ψ_z, $z \in \{S, L, G\}$, отводился один OpenMP-поток на четырёхъядерном компьютере Intel Core i7 920. В эксперименте выполнялось по 100 прогонов с разными начальными значениями генератора случайных чисел и последующим вычислением

математического ожидания состояний $\bar{u}(x)$. Для каждого способа композиции выводились зависимости $\Delta_z(t)$ для $z \in \{S, L, G\}$ (рис. 4) и вычислялись значения $\delta_z(t)$ при двух значениях радиуса $R = 30$ и 60:

$$\Delta_z(t) = \sum_{x \in X} \bar{u}(x), \quad \delta_z(t) = \log(N_z(R))/\log(\pi R^2),$$

где $\Delta_z(t)$ — суммарная масса на t-й итерации; δ_z — фрактальная размерность построенной структуры; $N_z(R)$ — количество клеток в состоянии b, находящихся на расстоянии не более чем R от зародыша (таблица).



а *б* *в*

Рис. 4. Зависимости суммарных масс $\Delta_L(t)$, $\Delta_G(t)$ и $\Delta_S(t)$ для трёх случаев соотношения интенсивностей диффузии и прилипания: *а* — $(p_\mathrm{d}; p_\mathrm{r}) = (0{,}5; 0{,}5)$; *б* — $(p_\mathrm{d}; p_\mathrm{r}) = (0{,}8; 0{,}2)$; *в* — $(p_\mathrm{d}; p_\mathrm{r}) = (0{,}95; 0{,}05)$

Фрактальные размерности древовидных структур, построенных в ходе моделирования процесса агрегации

R	30		60	
$(p_\mathrm{d}; p_\mathrm{r})$	(0,5; 0,5)	(0,95; 0,05)	(0,5; 0,5)	(0,95; 0,05)
Ψ_L	1,65621	1,64746	1,65243	1,69751
Ψ_G	1,65953	1,64608	1,6517	1,70208
Ψ_S	1,64146	1,6474	1,65126	1,69346

Полученные результаты показывают, что кривые суммарных масс для локальной Ψ_L, глобальной Ψ_G и стохастической Ψ_S композиций для каждого случая $(p_\mathrm{d}; p_\mathrm{r})$ имеют одинаковый характер, но различаются при разных соотношениях интенсивности диффузии и прилипании. Так, при $(p_\mathrm{d}; p_\mathrm{r}) = (0{,}5; 0{,}5)$ и $(0{,}8; 0{,}2)$ скорость роста суммарной массы при локальной композиции больше, чем при стохастической, примерно на 5 %, тогда как при $(p_\mathrm{d}; p_\mathrm{r}) = (0{,}95; 0{,}05)$ разницы в скоростях роста суммарной массы незаметно.

Различия в значениях фрактальных размерностей $\delta_z(t)$ от способа композиции не заметны ($< 1\,\%$). То же самое можно сказать и по поводу пространственного образа древовидной структуры (см. рис. 3).

Общий вывод из проведённого вычислительного эксперимента состоит в том, что свободный выбор способа композиции локальных операторов допустим, если нет сильных ограничений по точности. Кроме того, всегда возможна корректировка масштабов при переходе от модельных к физическим шагам по времени и пространству. Важно, что инвариант КА одинаков при разных способах композиции.

4. Самоорганизация в системе «хищник — жертва»

Исследование взаимоотношений хищников с жертвами [18], обитающих совместно в замкнутом пространстве, является типовой задачей самоорганизации [19], которая привлекает внимание не только экологов, но и математиков, физиков, химиков и даже социологов. В традиционной математике системы «хищник — жертва» описываются дифференциальными уравнениями в частных производных с полиномиальными нелинейными функциями. Поведенческие свойства изучаются при помощи качественной теории нелинейных систем. Компьютерная имитация выполняется путём решения систем нелинейных дифференциальных уравнений [18]. Возможности этих методов ограничены, во-первых, размерностью фазового пространства, во-вторых, трудностями решения нелинейных уравнений на суперкомпьютерах. Клеточно-автоматные модели систем «хищник — жертва» изучались также в синхронном [20] и асинхронном вариантах [21].

Взаимодействия между хищниками и жертвами происходят следующим образом. Хищники (щуки, лисы) питаются жертвами (планктоном, зайцами). Если в каком-то месте пищи достаточно (плотность жертв больше, чем плотность хищников), то плотность хищников увеличивается: хищники размножаются с вероятностью, пропорциональной их плотности. Если пищи не хватает (плотность жертв меньше, чем плотность хищников), то плотность хищников уменьшается: они умирают от голода с вероятностью, пропорциональной недостатку пищи. Жертвы всегда пытаются размножаться с вероятностью, пропорциональной логистической функции [18]. И хищники, и жертвы перемещаются в пространстве по закону диффузии, причём хищники более подвижны, чем жертвы.

Асинхронный КА, моделирующий систему из одного вида хищников и одного вида жертв, описывается параллельной композицией из двух диффузионно-реакционных КА $\aleph_v = \langle A, X_v, \Theta_v(X)\rangle$ и $\aleph_u = \langle A, X_u, \Theta_u(X)\rangle$, где A — булев алфавит; $X_v = \{(i,j)_v\}$ и $X_u = \{(i,j)_u\}$ — два изоморфных друг другу множества, определяющих клеточные массивы Ω_v и Ω_u, на которых отображаются эволюции хищника и жертвы соответственно. Пара клеток, связанных отношением изоморфизма, обозначается (i,j) (без индексов) и называется парой клеток-близнецов.

Глобальный оператор $\Theta(X)$ является композицией следующих подстановок:

- $\theta_{\mathrm{d}v}((i,j)_v)$ — диффузия хищника по массиву Ω_v;
- $\theta_{\mathrm{d}u}((i,j)_u)$ — диффузия жертв по массиву Ω_v;
- $\theta_{\mathrm{r}v}((i,j)_v)$ — реакция (изменение плотности) хищников;
- $\theta_{\mathrm{r}u}((i,j)_u)$ — реакция жертв.

Подстановки наивной диффузии (7) $\theta_{\mathrm{d}v}((i,j)_v)$ и $\theta_{\mathrm{d}u}(i,j)_u)$ применяются каждая на своём клеточном массиве, различаясь только коэффициентами диффузии ($D_v \gg D_u$).

Подстановки реакций построены на шаблоне $T_2 = \{(i,j)_v, (i,j)_u\}$, содержащем пары близнецов:

$$\begin{aligned} \theta_{\mathrm{r}v}((i,j)_v): &\quad (\langle v\rangle, \langle u\rangle) \xrightarrow{p_{\mathrm{r}}} (v', u'), \\ \theta_{\mathrm{r}u}((i,j)_u): &\quad (\langle u\rangle, \langle v\rangle) \xrightarrow{p_{\mathrm{r}}} (u', v'), \end{aligned} \tag{8}$$

где $\langle v\rangle$ и $\langle u\rangle$ — осреднённые по окрестности $\mathrm{Av} = \{(i+a, j+b) : a, b = -r, \ldots, 0, \ldots, r\}$ величины, имеющие смысл плотности (5) организмов в точках, соответствующих координатам клеток $(i,j)_v$ и $(i,j)_u$.

Новые состояния u', v' в (8) зависят от плотностей обоих организмов следующим образом:

$$v'_0 = \begin{cases} 0, & \text{если} \quad \langle u\rangle > \langle v\rangle \quad \& \quad \text{rand} < p_{v\to 0}, \\ 1, & \text{если} \quad \langle v\rangle > \langle u\rangle \quad \& \quad \text{rand} < p_{v\to 1}, \end{cases} \tag{9}$$

где вероятности $p_{v\to 0}$ и $p_{v\to 1}$ определяются на основе следующих соображений. Если $\langle v\rangle > \langle u\rangle$, то избыток хищников $(\langle v\rangle - \langle u\rangle)$ на площади $\mathrm{Av}((i,j)_v)$ не имеет пищи и умирает. Следовательно, $(\langle v\rangle - \langle u\rangle)$ клеток из $T((i,j)_v)$ должны сменить состояния $v = 1$ на $v = 0$. Если $\langle u\rangle > \langle v\rangle$, то хищнику достаточно пищи, он размножается в соответствии с логистической функцией $F_v(\langle v\rangle)$ вида (4). Отсюда вероятности в (9) равны

$$\begin{aligned} p_{v\to 0} &= \langle v\rangle - \langle u\rangle, \quad \text{если} \quad \langle v\rangle > \langle u\rangle, \\ p_{v\to 1} &= F_v(\langle v\rangle), \quad \text{если} \quad \langle u\rangle > \langle v\rangle. \end{aligned}$$

Функция перехода $\theta_{\mathrm{r}u}$ выглядит так же, как (8), отличаясь только вероятностями $p_{u\to 0}$ и $p_{u\to 1}$, значения которых определяются на основе следующих соображений. Если $\langle u\rangle < \langle v\rangle$ (жертва поедается хищником), её плотность уменьшается пропорционально плотности хищника. Если же $\langle u\rangle > \langle v\rangle$, то жертва размножается с вероятностью, пропорциональной $(\langle u\rangle - \langle v\rangle)$:

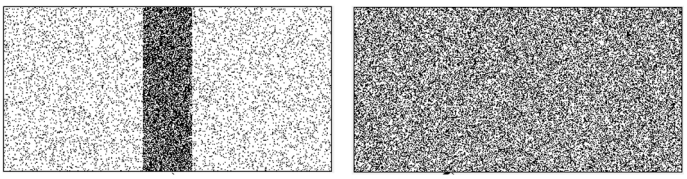
$$\begin{aligned} p_{u\to 0} &= \langle v\rangle, \quad \text{если} \quad \langle v\rangle > \langle u\rangle, \\ p_{u\to 1} &= F(\langle u\rangle - \langle v\rangle), \quad \text{если} \quad \langle u\rangle > \langle v\rangle. \end{aligned}$$

Вычислительные эксперименты проводились для клеточного массива $\Omega(0) = \Omega_v(0) \cup \Omega_u(0)$ размера $|X_v| = |X_u| = 400 \times 800$ (рис. 5). В начальном состоянии жертвы распределены по пространству равномерно: $\forall(u,(i,j)_u) \in \Omega_u(0)$ $(\langle u\rangle = 0{,}4)$. Хищник же собран в плотную полосу в середине области:

$$\langle v\rangle = \begin{cases} 0{,}6 & \text{для всех } (i,j)_v : i = 0,\ldots,399, j = 369,\ldots,439, \\ 0{,}2 & \text{в остальных} \quad (i,j)_v \in \Omega_u(0). \end{cases}$$

Константы скоростей для диффузии и реакций приняты равными $K_{\mathrm{d}v} = 10$, $K_{\mathrm{d}u} = 0{,}1$, $K_{\mathrm{r}v} = 0{,}2$, $K_{\mathrm{r}u} = 0{,}2$, что соответствует следующим вероятностям (3) применения локальных операторов $\theta_{\mathrm{d}v}$, $\theta_{\mathrm{d}u}$, $\theta_{\mathrm{r}v}$, $\theta_{\mathrm{r}u}$:

$$p_{\mathrm{d}v} = 0{,}952;\ p_{\mathrm{d}u} = 0{,}00952;\ p_{\mathrm{r}v} = 0{,}01904;\ p_{\mathrm{r}u} = 0{,}01904.$$



а *б*

Рис. 5. Начальное состояние $\Omega(0)$ КА, моделирующего самоорганизацию в системе «хищник — жертва» при появлении «косяка» хищника в виде полосы шириной 60 клеток и плотностью $\langle v\rangle = 0{,}6$ при исходной плотности хищника $\langle v\rangle = 0{,}2$ (*а*) и исходной плотности жертвы $\langle u\rangle = 0{,}4$ (*б*)

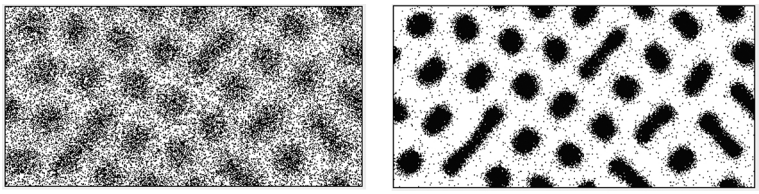
Моделирование проводилось для трёх исследуемых способов композиции подстановок, которые для случая двух организмов и двух клеточных массивов выполняются по следующим алгоритмам.

1. Стохастическая композиция Ψ_S. Случайно выбирается клетка $(i,j) \in X$. В соответствии с распределением вероятностей из четырёх подстановок $\theta_{\mathrm{d}v}$, $\theta_{\mathrm{d}u}$, $\theta_{\mathrm{r}v}$, $\theta_{\mathrm{r}u}$ выбирается одна, которая применяется к соответствующей клетке-близнецу ($(i,j)_v$ или $(i,j)_u$). Итерация содержит $4|X|$ таких шагов.

2. Локальная композиция Ψ_L. Случайно выбирается клетка $(i,j) \in X$. Все четыре подстановки применяются к этой клетке последовательно в случайно выбранном порядке, каждая — к соответствующему близнецу. Итерация содержит X таких шагов.

3. Глобальная композиция Ψ_G. Случайно выбирается одна из подстановок и применяется ко всем случайно выбираемым клеткам соответствующего ей подмассива. Итерация содержит 4 таких шага.

В процессе эволюции происходит постепенное перераспределение хищников и жертв по пространству, в результате которого достигается устойчивое равновесие в виде скоплений хищников и жертв, имеющих форму круглых или овальных пятен (рис. 6).



а *б*

Рис. 6. Глобальные устойчивые состояния хищника (*а*) и жертвы (*б*) при стохастической композиции, полученные в результате моделирования

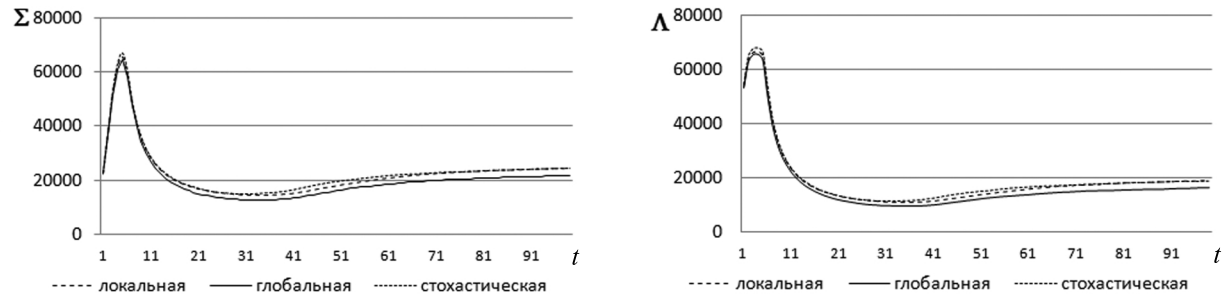
Каждому способу композиции Ψ_z, $z \in \{S, L, G\}$, отводился один OpenMP-поток на четырёхъядерном компьютере Intel Core i7 920. В эксперименте выполнялось по 100 прогонов с разными начальными значениями генератора случайных чисел и последующим вычислением математического ожидания $\bar{u}(x)$ и $\bar{v}(x)$. На каждой итерации в файл выводились суммарные массы хищников и жертв:

$$\Sigma_z(t) = \sum_{(i,j)_v \in X_v} (\bar{v}, (i,j)_v), \quad \Lambda_z(t) = \sum_{(i,j)_u \in X_u} (\bar{u}, (i,j)_v).$$

Сравнение эволюций для трёх способов композиции проводилось по суммарным массам $\Sigma_z(t)$ хищников и $\Lambda_z(t)$ жертв (см. рис. 7) , а также по количеству элементов связности (плотных скоплений) σ_z и λ_z в устойчивом состоянии. Сравнение по суммарным массам показывает максимальную разницу не более 3 %. Количество скоплений в устойчивых состояниях везде равно 23.

Заключение

Проведено исследование способов построения глобального оператора асинхронного КА, моделирующего реакционно-диффузионный процесс. Цель исследования — ответить на вопрос, насколько отличаются эволюции асинхронного КА при трёх способах композиции подстановок при построении глобального оператора: стохастическом, локальном и глобальном. Исследование проведено методом вычислительного



а *б*

Рис. 7. Зависимости суммарных масс хищников (*а*) и жертв (*б*) от времени, полученные в результате экспериментального моделирования

моделирования для трёх типовых реакционно-диффузионных процессов: распространение фронта, агрегация вещества из раствора, самоорганизация в системе «хищник — жертва». Возможность выбора способа композиции полезна при синтезе сложных КА-моделей, так как позволяет разработчику согласовать вычислительный процесс с архитектурой суперкомпьютера, а также рационально встраивать его в систему более сложных моделей.

Главный вывод из проведённого исследования состоит в том, что результаты моделирования при выбранных способах построения глобального оператора качественно совпадают. Более того, количественные различия заметны ($> 5\,\%$) только для процесса агрегации. Следует отметить, что в случае моделирования естественных процессов качественные совпадения часто вполне достаточны, а расхождения количественных значений получаемых характеристик до $10\,\%$ считаются допустимыми. В тех особых случаях, когда полученные количественные расхождения недопустимы, можно внести коррекцию в масштабы шагов по времени или пространству. Качественная идентичность эволюций позволяет это сделать, хотя потребует дополнительных исследований.

ЛИТЕРАТУРА

1. *Фон Нейман Дж.* Теория самовоспроизводящихся автоматов. М.: Мир, 1971. 384 с.
2. *Metropolis N. and Ulam S.* The Monte Carlo method // Amer. Statist. Assoc. 1949. V. 44. No. 247. P. 335–341.
3. *Chatterjee A. and Vlaches D. G.* An overview of spatial microscopic and accelerated kinetic Monte-Carlo methods // J. Computer-Aided Mater. Des. 2007. V. 14. P. 253–308.
4. *Nurminen L., Kuonen A., and Kaski K.* Kinetic Monte-Carlo simulation on patterned substrates // Phys. Rev. B63, O35407. 29 December 2000.
5. *Matveev A. V., Latkin E. I., Elokhin V. I, and Gorodetskii V. V.* Turbulent and stripes wave patterns caused by limited CO_{ads} diffusion during CO oxidation over Pd(110) surface: kinetic Monte Carlo studies // Chem. Eng. J. 2005. V. 107. P. 181–189.
6. *Бандман О. Л.* Дискретное моделирование физико-химических процессов // Прикладная дискретная математика. 2009. № 3. С. 33–49.
7. *Kireeva A.* Parallel implementation of totalistic cellular automata model of stable patterns formation // 12th Int. Conf. “Parallel Computing Technologies”, St.-Petersbourg, 2013. LNCS. 2013. V. 7979. P. 347–360.

8. *Бандман О. Л.* Методы композиции клеточных автоматов для моделирования пространственной динамики // Вестник Томского государственного университета. 2004. Приложение № 9(1). С. 183–193.
9. *Achasova S., Bandman O., Markova V., and Piskunov S.* Parallel Substitution Algorithm. Theory and Application. Singapore: World Scientific, 1994. 180 p.
10. *Колмогоров А. Н., Петровский И. Г., Пискунов И. С.* Исследование уравнения диффузии, соединенной с возрастанием количества вещества, и его применение к одной биологической проблеме // Бюллетень МГУ. Секция А. 1937. Вып. 6. С. 1–25.
11. *Fisher R. A.* The genetical theory of natural selection. Oxford: Univ. Press, 1930. 58 p.
12. *Szakàly T., Lagzi I., Izsàk F., et al.* Stochastic cellular automata modelling excitable systems // Central Eur. J. Phys. 2007. No. 5(4). P. 471–486.
13. *Van Saarloos W.* Front propagation into unstable states // Phys. Rep. 2003. V. 386. P. 29–222.
14. *Witten T. A., Jr. and Sander L. M.* Diffusion-limited aggregation, a kinetic critical phenomenon // Phys. Rev. Lett. 1981. V. 47. No. 19. P. 1400–1403.
15. *Ackland G. J. and Tweedie E. S.* Microscopic model of diffusion limited aggregation and electrodeposition in the presence of leveling molecules // Phys. Rev. E73, 011606. 26 January 2006.
16. *Bogoyavlenskiy V. A. and Chernova N. A.* Diffusion-limited aggregation: a relationship between surface thermodynamics and crystal morphology // Phys. Rev. E. 2000. No. 61(2). P. 1629–1633.
17. *Batty M. and Longley P.* Urban growth and form: scaling, fractal geometry, and diffusion-limited aggregation // Environment and Planning. 1989. V. 21(11). P. 1447–1472.
18. *Свирежев Ю. М.* Нелинейные волны, диссипативные структуры и катастрофы в экологии. М.: Наука, 1987. 368 с.
19. *Nicolis G. and Prigogine I.* Self-organization in Nonequilibrium Systems: From Dissipative Structures to Order through Fluctuations. N.Y.: Wiley, 1977.
20. *Kutson J. D.* A survey of the use of cellular automata and cellular automata like models for simulating a population of biological cells. Iowa State University, 2011. Graduate Thesis and Dissertations. Paper 10133. `http://lib.dr.iastate.edu/efd`
21. *Chen Q., Mao J., and Li W.* Stability analysis of harvesting strategies in a cellular automata based predator — prey model // Cellular Automata. LNCS. 2006. V. 4173. P. 268–376.

REFERENCES

1. *Von Neumann J.* Teoriya samovosproizvodjashhihsja avtomatov. Moscow, Mir Publ., 1971. 384 p. (in Russian)
2. *Metropolis N. and Ulam S.* The Monte Carlo method. Amer. Statistical Assoc., 1949, vol. 44, no. 247, pp. 335–341.
3. *Chatterjee A. and Vlaches D. G.* An overview of spatial microscopic and accelerated kinetic Monte-Carlo methods. J. Computer-Aided Mater. Des., 2007, vol. 14, pp. 253–308.
4. *Nurminen L., Kuonen A., and Kaski K.* Kinetic Monte-Carlo simulation on patterned substrates. Phys. Rev. B63, O35407. 29 December 2000.
5. *Matveev A. V., Latkin E. I., Elokhin V. I, and Gorodetskii V. V.* Turbulent and stripes wave patterns caused by limited CO_{ads} diffusion during CO oxidation over Pd(110) surface: kinetic Monte Carlo studies. Chem. Eng. J., 2005, vol. 107, pp. 181–189.
6. *Bandman O. L.* Diskretnoe modelirovanie fiziko-himicheskih processov. Prikladnaya Diskretnaya Matematika, 2009, no. 3, pp. 33–49. (in Russian)

7. *Kireeva A.* Parallel implementation of totalistic cellular automata model of stable patterns formation. 12th Int. Conf. "Parallel Computing Technologies", St.-Petersbourg, 2013. LNCS, 2013, vol. 7979, pp. 347–360.
8. *Bandman O. L.* Metody kompozicii kletochnyh avtomatov dlja modelirovanija prostranstvennoj dinamiki. Vestnik Tomskogo gosudarstvennogo universiteta, 2004, Prilozhenie no. 9(1), pp. 183–193. (in Russian)
9. *Achasova S., Bandman O., Markova V., and Piskunov S.* Parallel Substitution Algorithm. Theory and Application. Singapore, World Scientific, 1994. 180 p.
10. *Kolmogorov A. N., Petrovskij I. G., Piskunov I. S.* Issledovanie uravnenija diffuzii, soedinennoj s vozrastaniem kolichestva veshhestva, i ego primenenie k odnoj biologicheskoj probleme. MSU Bull., Sec. A, 1937, no. 6, pp. 1–25. (in Russian)
11. *Fisher R. A.* The genetical theory of natural selection. Oxford, Univ. Press, 1930. 58 p.
12. *Szakàly T., Lagzi I., Izsàk F., et al.* Stochastic cellular automata modelling excitable systems. Central Eur. J. Phys., 2007, no. 5(4), pp. 471–486.
13. *Van Saarloos W.* Front propagation into unstable states. Phys. Rep., 2003, vol. 386, pp. 29–222.
14. *Witten T. A., Jr. and Sander L. M.* Diffusion-limited aggregation, a kinetic critical phenomenon. Phys. Rev. Lett., 1981, vol. 47, no. 19, pp. 1400–1403.
15. *Ackland G. J. and Tweedie E. S.* Microscopic model of diffusion limited aggregation and electrodeposition in the presence of leveling molecules. Phys. Rev. E73, 011606. 26 January 2006.
16. *Bogoyavlenskiy V. A. and Chernova N. A.* Diffusion-limited aggregation: a relationship between surface thermodynamics and crystal morphology. Phys. Rev. E. 2000, no. 61(2), pp. 1629–1633.
17. *Batty M. and Longley P.* Urban growth and form: scaling, fractal geometry, and diffusion-limited aggregation. Environment and Planning, 1989, vol. 21(11), pp. 1447–1472.
18. *Svirezhev Ju. M.* Nelinejnye volny, dissipativnye struktury i katastrofy v jekologii. Moscow, Nauka Publ., 1987. 368 p. (in Russian)
19. *Nicolis G. and Prigogine I.* Self-organization in Nonequilibrium Systems: From Dissipative Structures to Order through Fluctuations. N.Y., Wiley, 1977.
20. *Kutson J. D.* A survey of the use of cellular automata and cellular automata like models for simulating a population of biological cells. Iowa State University, 2011. Graduate Thesis and Dissertations. Paper 10133. `http://lib.dr.iastate.edu/efd`
21. *Chen Q., Mao J., and Li W.* Stability analysis of harvesting strategies in a cellular automata based predator — prey model // Cellular Automata, LNCS, 2006. vol. 4173, pp. 268–376.

УДК 519.856, 519.854.3

ГЕНЕРАЦИЯ КОМПЬЮТЕРНОГО ПРЕДСТАВЛЕНИЯ ПОРИСТОЙ СТРУКТУРЫ С ПОМОЩЬЮ ТОТАЛИСТИЧЕСКОГО КЛЕТОЧНОГО АВТОМАТА[1]

А. Е. Киреева

Институт вычислительной математики и математической геофизики СО РАН, г. Новосибирск, Россия

Описывается двухслойный тоталистический клеточный автомат, позволяющий генерировать компьютерное представление пористых сред со сложной неоднородной морфологией. Двухслойный клеточный автомат представляет собой композицию двух клеточных автоматов: тоталистического (первого слоя) и асинхронного (второго слоя). Наличие второго слоя даёт возможность формировать сложные неоднородные структуры, похожие на наблюдаемые в природе. Для анализа формируемых структур в процессе моделирования вычисляются численные характеристики: пористость, перколяция, процент единичных (заполненных) клеток, на основании которых может быть выбран пористый материал с нужной морфологией.

Ключевые слова: *тоталистический клеточный автомат, параллельная композиция клеточных автоматов, активатор, ингибитор, устойчивые структуры, пористые среды.*

DOI 10.17223/20710410/27/13

GENERATION OF POROUS MEDIA COMPUTER REPRESENTATION BY TWO-LAYER TOTALISTIC CELLULAR AUTOMATON

A. E. Kireeva

Institute of Computational Mathematics and Mathematical Geophysics SB RAS, Novosibirsk, Russia

E-mail: kireeva@ssd.sscc.ru

In the paper, two-layer totalistic cellular automaton allowing to generate porous materials computer representation is presented. Two-layer cellular automaton is constructed as a parallel composition of a totalistic cellular automaton and an asynchronous cellular automaton. The second layer gives an opportunity to form complex inhomogeneous structures similar to a patterns emerging in natural phenomena. The investigation aims to create a method for porous media morphology synthesis according to a given set of properties such as porosity, percolation, density, etc. Two-layer totalistic cellular automaton allows to obtain a set of patterns representing different porous media morphology. In addition, a porous medium characteristics such as percolation degree, porosity, the number of connected components are calculated and can be used for the analysis and selection of materials with necessary morphology.

Keywords: *totalistic cellular automaton, parallel composition of cellular automata, activator, inhibitor, porous media, stable patterns.*

[1]Работа поддержана грантом РФФИ № 14-01-31425 мол-а.

Введение

Пористые материалы — это твердые тела, содержащие в своем объёме свободное пространство в виде полостей, каналов и пор. Исследование пористых материалов представляет интерес для многих областей науки и техники. В промышленности пористые материалы применяются в качестве фильтров, теплоизоляционных материалов, катализаторов и осушителей. По сравнению с плотными материалами пористые структуры являются более износоустойчивыми и могут подвергаться воздействию более высоких и низких температур, благодаря чему они эффективно используются в автомобиле- и самолётостроении. Кроме того, пористые материалы являются незаменимыми в медицине и фармацевтике для изготовления имплантов, повязок, протезов и других инновационных биотехнологических продуктов. Эффективность применения материалов зависит от их пористых характеристик: диаметра и объёма пор, наименьшего сквозного диаметра, проницаемости, распределения пор, гидрофобности и гидрофильности пор. Важно также знать, как структура вещества может меняться при внешнем воздействии, например при влиянии температуры и давления.

Компьютерное моделирование позволяет конструировать виртуальные пористые материалы с различной морфологией, исследовать их и подбирать образцы с нужными характеристиками. Однако построение неоднородных пористых сред со сложной морфологией сопряжено с определёнными трудностями, так как пористые среды — это сложная нерегулярная система сообщающихся пустот, трещин и каверн, в которой трудно выделить отдельные поровые каналы. В простых случаях для описания пористых сред часто используют идеализированные модели, например представление среды в виде множества шаров и трубок различного диаметра. Для конструирования пористых материалов со сложной морфологией более эффективным является клеточно-автоматный (КА) подход.

КА-метод получения компьютерного представления пористых сред [1] основан на формировании устойчивых структур в результате эволюции КА. В основе КА-моделей структурообразования [2 – 4] лежит активаторно-ингибиторный механизм, описанный в [5 – 7]. Суть этого механизма заключается в том, что новые состояния клеток вычисляются в зависимости от взвешенной суммы состояний соседних клеток. Такие КА называются тоталистическими (ТКА). Для создания компьютерного представления пористых сред со сложной неоднородной морфологией в работе предлагается использовать двухслойный ТКА, который позволяет формировать устойчивые структуры, сходные с реальными паттернами, возникающими в природе.

Целью работы является разработка двухслойной ТКА-модели процессов структурообразования, позволяющей генерировать компьютерное представление пористой среды, а также исследование зависимости морфологии генерируемой среды от значений активаторов и ингибиторов.

В п. 1 приводятся определения ТКА и двухслойного ТКА. В п. 2 представлены устойчивые структуры, формирующиеся в результате эволюции ТКА в двумерном и трёхмерном случае, приведены примеры компьютерного представления пористых сред для различных значений активаторов и ингибиторов, а также описаны характеристики пористых сред, вычисляющиеся в течение эволюции КА.

1. Двухслойный тоталистический клеточный автомат

1.1. Определение тоталистического клеточного автомата ТКА, согласно [2, 8], определяется следующими понятиями:

$$\aleph_{\mathrm{TCA}} = \langle A_{\mathrm{TCA}}, X^d_{\mathrm{TCA}}, \Theta_{\mathrm{TCA}}, \nu \rangle, \tag{1}$$

где A_{TCA} — алфавит состояний клеток; X^d_{TCA} — конечное множество имён клеток, определяющих координаты клеток в дискретном пространстве; Θ_{TCA} — локальный оператор, задающий правила изменения состояний клеток; ν — режим функционирования клеточного автомата.

Каждая *клетка* КА определяется парой $(a, \mathbf{x})$, где $a \in A_{\mathrm{TCA}}$ — состояние клетки; $\mathbf{x} \in X^d_{\mathrm{TCA}}$ — имя клетки. Множество клеток, не содержащее клеток с одинаковыми именами, называется *клеточным массивом* Ω. Алфавит состояний ТКА булев: $A_{\mathrm{TCA}} = \{0, 1\}$. Множество имён X^d_{TCA} в двумерном случае $(d = 2)$ представимо в виде решётки $X^2_{\mathrm{TCA}} = \{(i, j) : i = 1, \ldots, M_i, j = 1, \ldots, M_j\}$, а в трёхмерном $(d = 3)$ — в виде куба $X^3_{\mathrm{TCA}} = \{(i, j, k) : i = 1, \ldots, M_i, j = 1, \ldots, M_j, k = 1, \ldots, M_k\}$. На множестве имён X^d_{TCA} задаются именующие функции $\varphi_k : X^d_{\mathrm{TCA}} \to X^d_{\mathrm{TCA}}$, определяющие для клетки $\mathbf{x} \in X^d_{\mathrm{TCA}}$ одного из её соседей. Конечное множество именующих функций называется *шаблоном соседства* $T_{\mathrm{TCA}}(\mathbf{x})$. Далее в качестве шаблона соседства используется квадрат $K \times K$ клеток в двумерном случае и куб $K \times K \times K$ в трёхмерном случае:

$$T_{\mathrm{TCA}}(\mathbf{x}) = \{\mathbf{x}\} \cup \{\mathbf{x} + \mathbf{a} : \mathbf{a} \in \{-\lfloor K/2 \rfloor, \ldots, 0, \ldots, \lfloor K/2 \rfloor\}^d\}.$$

Локальный оператор $\Theta_{\mathrm{TCA}}(\mathbf{x})$ определяется на основании активаторно-ингибиторного механизма формирования структур; он вычисляет новое состояния клетки $\mathbf{x}$ в зависимости от взвешенной суммы состояний соседних клеток $(u_k, \varphi_k(\mathbf{x}))$, $k = 1, \ldots, |T_{\mathrm{TCA}}(\mathbf{x})|$, по следующей формуле:

$$\Theta_{\mathrm{TCA}}(\mathbf{x}) : (u, \mathbf{x}) \to (u', \mathbf{x}), \text{где } u' = \begin{cases} 0, \text{ если } s(\mathbf{x}) = \sum\limits_{k=0}^{|T_{\mathrm{TCA}}(\mathbf{x})|} w_k u_k \leqslant B, \\ 1 \text{ иначе.} \end{cases}$$

Здесь w_k — это элементы матрицы весов W, $|W| = |T_{\mathrm{TCA}}(\mathbf{x})|$. Константа $B \in \mathbb{R}$ — порог функции $s(\mathbf{x})$, далее в экспериментах используется $B = 0$. Весовые коэффициенты $w_k \in W$ принимают положительные и отрицательные значения. Положительные коэффициенты играют роль *активаторов* (p), а отрицательные — *ингибиторов* (n). Активаторы отвечают за распространение и рост устойчивых структур, а ингибиторы являются фактором, сдерживающим их рост.

Применение локального оператора $\Theta_{\mathrm{TCA}}(\mathbf{x})$ ко всем клеткам $\mathbf{x} \in X_{\mathrm{TCA}}$ называется *итерацией*. Далее используются синхронный (σ) и асинхронный (α) режимы применения локального оператора $\Theta_{\mathrm{TCA}}(\mathbf{x})$ к клеткам массива. При *синхронном* режиме для вычисления новых состояний клеток используются состояния, полученные на предыдущей итерации, и только после применения $\Theta_{\mathrm{TCA}}(\mathbf{x})$ ко всем клеткам массива $\mathbf{x} \in X_{\mathrm{TCA}}$ их состояния одновременно изменяются. При *асинхронном* режиме локальный оператор применяется к случайно выбранным клеткам массива, сразу же изменяя их состояния, таким образом, новые состояния клеток вычисляются от состояний, полученных на предыдущей и на текущей итерациях.

Множество состояний всех клеток $\mathbf{x} \in X_{\mathrm{TCA}}$ на t-й итерации называется *глобальной конфигурацией* клеточного массива $\Omega(t)$. Последовательность глобальных состояний

$\Sigma(\Omega) = \Omega(0), \ldots, \Omega(t), \ldots, \Omega(t_{\text{fin}})$, полученная в результате итеративного функционирования КА, называется *эволюцией*, $\Omega(0)$ — это исходное состояние клеточного массива, $\Omega(t)$ — состояние массива на t-й итерации, t_{fin} — число итераций.

1.2. Определение двухслойного тоталистического клеточного автомата

Двухслойный тоталистический КА является однонаправленной параллельной композицией двух КА [9]: тоталистического $\aleph_{\text{TCA}}$ и асинхронного КА второго слоя $\aleph_{2L}$:

$$\aleph_S = \Upsilon(\aleph_{\text{TCA}}, \aleph_{2L}).$$

Между множествами имён X_{2L} и X_{TCA} определяется взаимно-однозначное соответствие: $X^d_{\text{TCA}} = \gamma(X^d_{2L})$, $|X^d_{\text{TCA}}| = |X^d_{2L}|$. Состояния клеток $\aleph_{\text{TCA}}$ зависят не только от состояний их соседних клеток, но и от состояний клеток второго слоя $\aleph_{2L}$.

В результате исследования эволюции двухслойного ТКА при различных $\aleph_{2L}$ в качестве второго слоя выбран КА «Лесной пожар» (Forest fire) [10], так как в общем случае эволюция этого КА имитирует пространственно-неоднородное динамически изменяющееся распределение трёх произвольных веществ: химических реагентов, молекул либо атомов.

КА-модель распространения огня в лесу, описанная в [10], определяется следующими понятиями:

$$\aleph_{2L} = \langle A_{2L}, X^d_{2L}, \Theta_{2L}, \alpha \rangle.$$

Алфавит состояний клеток $A_{2L} = \{0, 1, 2\}$, где 0 — это свободный участок поверхности, 1 — дерево, 2 — горящее дерево. Режим функционирования — асинхронный. Шаблон соседства $T_{2L}(\mathbf{y}) = \{\mathbf{y} + \mathbf{a}\}$, где $\mathbf{a}$ — вектор сдвига: $\mathbf{a} \in \{(-1, 0), (0, 1), (1, 0), (0, -1)\}$ для $d = 2$ и $\mathbf{a} \in \{(-1, 0, 0), (1, 0, 0,), (0, -1, 0), (0, 1, 0), (0, 0, -1), (0, 0, 1)\}$ для $d = 3$. Локальный оператор $\Theta_{2L}(\mathbf{y})$ вычисляет новое состояние клетки $\mathbf{y}$ по формуле

$$\Theta_{2L}(\mathbf{y}) : (v, \mathbf{y}) \to (v', \mathbf{y}),$$

$$\text{где } v' = \begin{cases} 0, \text{ если } v = 2, \\ 1, \text{ если } v = 0 \quad \& \quad \text{rand}_1 < P_t, \\ 2, \text{ если } v = 1 \ \& \ \exists (v_k, \varphi_k(\mathbf{y}))\ (v_k = 2, \varphi_k(\mathbf{y}) \in X_{2L}) \quad \& \quad \text{rand}_2 < P_f. \end{cases}$$

Здесь $\varphi_k(\mathbf{y}) \in T_{2L}(\mathbf{y})$ определяет для клетки $\mathbf{y}$ одну из соседних клеток, выбираемых равновероятно по шаблону $T_{2L}(\mathbf{y})$; $\text{rand}_1, \text{rand}_2 \in \mathbb{R}$ — случайные числа в интервале (0, 1); P_f и P_t — вероятности самовозгорания и появления дерева соответственно.

Тоталистический КА $\aleph_{\text{TCA}} = \langle A_{\text{TCA}}, X^d_{\text{TCA}}, \Theta'_{\text{TCA}}, \nu \rangle$ определяется аналогично (1), за исключением локального оператора $\Theta'_{\text{TCA}}(\mathbf{x})$, который вычисляет новые состояния клеток в зависимости от коэффициентов, являющихся функцией $f(v_k)$ от состояний клеток $\aleph_{2L}$:

$$\Theta'_{\text{TCA}}(\mathbf{x}) : (u, \mathbf{x}) \to (u', \mathbf{x}), \quad \text{где } u' = \begin{cases} 0, \text{ если } \sum\limits_{k=0}^{|T_{\text{TCA}}(\mathbf{x})|} f(v_k) u_k \leqslant B, \\ 1 \text{ иначе.} \end{cases}$$

Здесь v_k — состояние k-й клетки с именем $\mathbf{y} = \gamma(\mathbf{x})$ для $\mathbf{x} \in T_{\text{TCA}}(\mathbf{x}) \subset X_{\text{TCA}}$.

Функция $f(v_k)$ используется следующая:

$$f(v_k) = \begin{cases} \dfrac{N(1) - N(2)}{|T_{\text{TCA}}|}, \text{ если } w_k > 0 \quad (\text{активатор}), \\ w_k, \text{ если } w_k \leqslant 0 \quad (\text{ингибитор}), \end{cases} \tag{2}$$

где $N(1)$ и $N(2)$ — количества клеток $\mathbf{y} = \gamma(\mathbf{x})$ с состояниями $v = 1$ и $v = 2$ соответственно, $\mathbf{x} \in T_{\mathrm{TCA}}(\mathbf{x})$.

2. Генерация компьютерного представления пористой среды с помощью двухслойного тоталистического клеточного автомата $\aleph_S$

2.1. Устойчивые структуры, формируемые с помощью тоталистического клеточного автомата $\aleph_{\mathrm{TCA}}$

Основными параметрами, влияющими на эволюцию $\aleph_{\mathrm{TCA}}$, являются начальное состояние клеточного массива $\Omega(0)$, значения весовых коэффициентов $w_k \in W$ и размер шаблона соседства K.

В качестве начального состояния $\Omega(0)$ в вычислительных экспериментах используются следующие глобальные конфигурации:

- Ω_1: одна клетка с состоянием $u = 1$ в центре клеточного массива, состояния остальных клеток — нулевые;
- Ω_2: случайное равномерное распределение клеток с состоянием $u = 1$ с вероятностью P_{Ω_1};
- Ω_3: случайное неравномерное распределение клеток с состоянием $u = 1$. Клеточный массив делится на $m \in \mathbb{N}$ частей, в каждой из которых задаётся своя вероятность распределения единичных клеток $P^l_{\Omega_3}, l \in m$.

Весовые коэффициенты w_k задаются с помощью матрицы весов W, имеющей следующий вид:

$$W = \begin{pmatrix} n & n & n & \cdots & n & n & n \\ n & n_1 & n_1 & \cdots & n_1 & n_1 & n \\ n & n_1 & p & \cdots & p & n_1 & n \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\ n & n_1 & p & \cdots & p & n_1 & n \\ n & n_1 & n_1 & \cdots & n_1 & n_1 & n \\ n & n & n & \cdots & n & n & n \end{pmatrix},$$

где $n \leqslant 0$; $n_1 \leqslant 0$; $p > 0$.

Таким образом, в двумерном случае ($d = 2$) матрица весов определяется выражением

$$w_{kl} = \begin{cases} p, \text{ если } |k| < (\lfloor K/2 \rfloor - 1) \quad \& \quad |l| < (\lfloor K/2 \rfloor - 1), \\ n_1, \text{ если } |k| = (\lfloor K/2 \rfloor - 1) \quad \& \quad |l| = (\lfloor K/2 \rfloor - 1), \\ n \text{ иначе}, \end{cases}$$

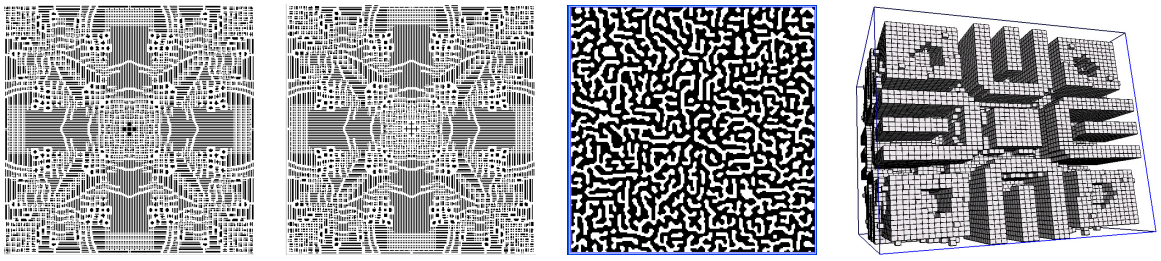
а в трёхмерном случае ($d = 3$) — выражением

$$w_{klm} = \begin{cases} p, \text{ если } |k| < (\lfloor K/2 \rfloor - 1) \,\&\, |l| < (\lfloor K/2 \rfloor - 1) \,\&\, |m| < (\lfloor K/2 \rfloor - 1), \\ n_1, \text{ если } |k| = (\lfloor K/2 \rfloor - 1) \,\&\, |l| = (\lfloor K/2 \rfloor - 1) \,\&\, |m| = (\lfloor K/2 \rfloor - 1), \\ n \text{ иначе}. \end{cases}$$

Здесь $k, l, m = -\lfloor K/2 \rfloor, \ldots, 0, \ldots, \lfloor K/2 \rfloor$.

Размер шаблона соседства K выбран равным 7, так как экспериментально установлено, что такой размер шаблона является оптимальным для получения большого многообразия устойчивых структур. При моделировании используются периодические (B_p) и нулевые (B_0) граничные условия.

Эволюция тоталистического КА $\aleph_{\text{TCA}}$ (1) моделирует процессы структурообразования. С помощью проведения вычислительных экспериментов при различных начальных состояниях, матрицах весов и режимах функционирования в результате эволюции $\aleph_{\text{TCA}}$ получено большое многообразие различных устойчивых структур (рис. 1).



а *б* *в* *г*

Рис. 1. Устойчивые состояния $\aleph_{\text{TCA}}$ при B_p: *а*, *б* — чередование двух структур при $\mu = \sigma$ для $|X^2_{\text{TCA}}| = 500 \times 500$ клеток, $\Omega(0) = \Omega_1$, $n = n_1 = -1, p = 0{,}54$; *в* — структура, формирующаяся при $\mu = \alpha$ для $|X^2_{\text{TCA}}| = 200 \times 200$ клеток, $\Omega(0) = \Omega_1$, $n = -0{,}27$, $n_1 = -0{,}07$, $p = 1$; *г* — структура, формирующаяся при $\mu = \sigma$ для $|X^3_{\text{TCA}}| = 50 \times 50 \times 50$ клеток, $\Omega(0) = \Omega_1$, $n = n_1 = -1$, $p = 1{,}6$

Для графического представления глобального состояния клеточного массива клетки с состоянием $u = 1$ отображаются чёрным цветом, а клетки с состоянием $u = 0$ — белым цветом.

В результате вычислительных экспериментов обнаружено, что при синхронном режиме функционирования $\aleph_{\text{TCA}}$ сходится преимущественно к чередованию двух устойчивых структур, т. е. через определённое число итераций t' происходит чередование двух глобальных состояний: $\Omega(t' + 2k) = \Omega(t')$ и $\Omega(t' + 2k + 1) = \Omega(t' + 1)$, $k \in \mathbb{N}$. При асинхронном режиме $\aleph_{\text{TCA}}$ сходится к одному устойчивому состоянию, т. е. через определённое число итераций t' глобальное состояние клеточного массива не изменяется: $\Omega(t) = \Omega(t')$ для всех $t > t'$.

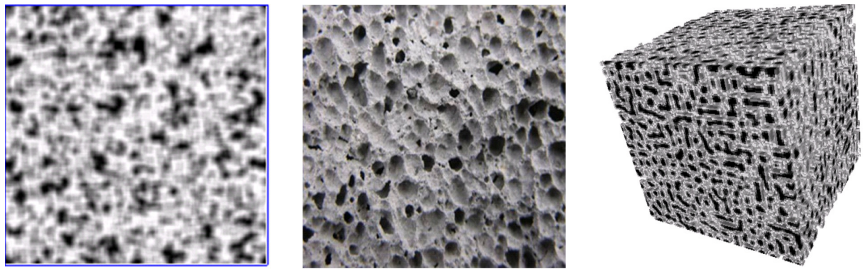
Устойчивые структуры, формирующиеся в результате эволюции $\aleph_{\text{TCA}}$, даже при неоднородном начальном распределении единичных клеток являются довольно простыми (рис. 2). Использование двухслойного ТКА $\aleph_S$ позволяет получать более сложные пространственно-неоднородные мотивы, похожие на наблюдаемые в природе.

а *б* *в*

Рис. 2. Структуры, формирующиеся с помощью $\aleph_{\text{TCA}}$ при $|X^2_{\text{TCA}}| = 500 \times 500$ клеток и B_0: *а* — начальное состояние клеточного массива $\Omega(0) = \Omega_3$, $P^1_{\Omega_3} = 0{,}0005$, $P^2_{\Omega_3} = 0{,}0001$; *б* — устойчивое состояние $\aleph_{\text{TCA}}$ при $\mu = \alpha$, $n = -0{,}5$, $n_1 = -0{,}1$, $p = 1$; *в* — устойчивое состояние $\aleph_{\text{TCA}}$ при $\mu = \sigma$, $n = -0{,}5$, $n_1 = -0{,}1$, $p = 2$

2.2. Устойчивые структуры, формируемые с помощью двухслойного тоталистического КА $\aleph_S$

Двухслойный ТКА $\aleph_S$ при различных значениях весовых коэффициентов позволяет генерировать компьютерное представление пористых материалов с различной морфологией. Например, в результате эволюции $\aleph_S$ при начальном состоянии $\Omega(0) = \Omega_2$, $P_{\Omega_2} = 0{,}01$, значениях весовых коэффициентов $n = -0{,}5$, $n_1 = -0{,}1$, $p = 3$ и $P_f = 0{,}01$, $P_t = 0{,}7$ возникают структуры, похожие на изображение бетона (рис. 3, *а*, *б*). Аналогично в трёхмерном случае при значениях весовых коэффициентов $n = -0{,}5$, $n_1 = -0{,}1$, $p = 2$ и начальном состоянии $\Omega(0) = \Omega_3$ с вероятностями распределения единичных клеток $P^1_{\Omega_3} = 0{,}01$, $P^2_{\Omega_3} = 0{,}1$, $P^3_{\Omega_3} = 0{,}3$ в результате эволюции $\aleph_S$ формируется пористая структура, представленная на рис. 3, *в*. На рис. 3 представлены осреднённые глобальные состояния $\aleph_S$, серый цвет соответствует меньшей концентрации единичных клеток, чёрный — большей концентрации.



а *б* *в*

Рис. 3. Структура, формирующаяся в результате эволюции $\aleph_S$ при $\mu = \alpha$ в двумерном случае $|X^2_{\mathrm{TCA}}| = 200 \times 200$ для $n = -0{,}5$, $n_1 = -0{,}1$, $p = 3$ и $P_f = 0{,}01$, $P_t = 0{,}7$ (*а*); фотография пористого материала (*б*); структура, формирующаяся в трёхмерном случае при $|X^3_{\mathrm{TCA}}| = 100 \times 100 \times 100$, $n = -0{,}5$, $n_1 = -0{,}1$, $p = 2$ и $P_f = 0{,}5$, $P_t = 5 \cdot 10^{-5}$ (*в*)

Морфология формирующихся пористых структур меняется в течение эволюции $\aleph_S$. Для её анализа на каждой итерации вычисляются следующие численные характеристики:

1) $L(1)$ и $L(0)$ — число компонент связности для единиц и нулей. Компонента связности – это множество клеток с одинаковыми состояниями ($u = 1$ либо $u = 0$), в котором для всех клеток есть путь из одной клетки в другую;
2) $P_v(1)$, $P_g(1)$ и $P_v(0)$, $P_g(0)$ — степень перколяции вдоль клеток с $u = 1$ и с $u = 0$ по вертикали (P_v) и горизонтали (P_g). Степень перколяции — это количество клеток, принадлежащих правой (или нижней) границе массива, в которые есть путь из клеток, принадлежащих противоположной границе;
3) Porosity — пористость; вычисляется как отношение количества клеток с $u = 0$ к размеру всего массива;
4) $Np(1)$ — процент клеток с состоянием $u = 1$; вычисляется как отношение количества единичных клеток к размеру всего массива, умноженное на 100 %;
5) Tortuosity — степень извилистости; вычисляется как число углов на границах связных компонент.

Возможность визуального наблюдения за эволюцией $\aleph_S$ и вычисления значений характеристик в процессе моделирования позволяет получать компьютерные представления пористых материалов с нужной морфологией.

При заданных начальном распределении единичных клеток, значениях активаторов и ингибиторов на каждой итерации формируются структуры с различными характеристиками (рис. 4). При получении компьютерного представления пористого материала с требующимися характеристиками вычислительный процесс может быть остановлен, а глобальное состояние $\aleph_S$ сохранено в файл для дальнейшего анализа.

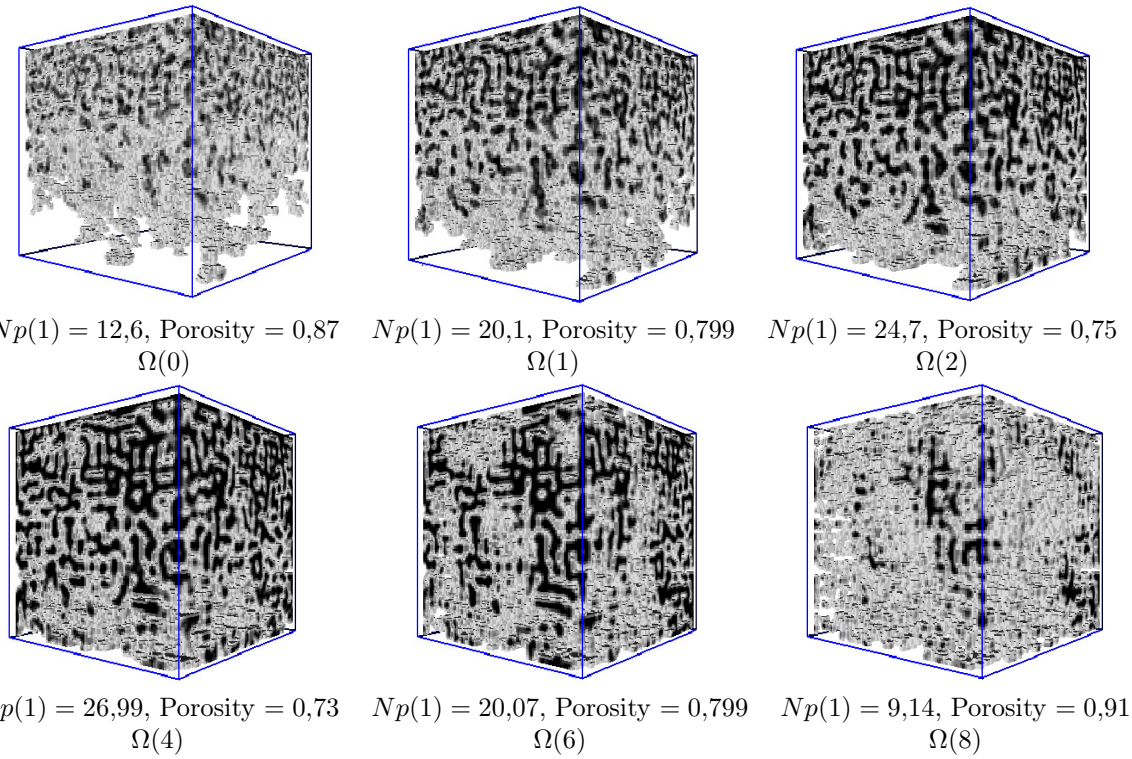


Рис. 4. Изменение морфологии компьютерного представления пористого материала, формирующегося в течение эволюции $\aleph_S$ при начальном распределении $\Omega(0) = \Omega_3$ с $P^1_{\Omega_3} = 0{,}05$, $P^2_{\Omega_3} = 0{,}001$, $P^3_{\Omega_3} = 0{,}0001$ и $|X^3_{\mathrm{TCA}}| = 100 \times 100 \times 100$, $n = -0{,}5$, $n_1 = -0{,}1$, $p = 3$ и $P_f = 0{,}5$, $P_t = 5 \cdot 10^{-5}$

Заключение

Разработана двухслойная тоталистическая КА-модель $\aleph_S$ процессов структурообразования, являющаяся параллельной композицией тоталистического КА $\aleph_{\mathrm{TCA}}$ и асинхронного КА второго слоя. Предложенная КА-модель $\aleph_S$ позволяет генерировать компьютерное представление двумерных и трёхмерных пористых материалов с различной морфологией. В зависимости от начального распределения единичных клеток, значений активаторов и ингибиторов в результате эволюции $\aleph_S$ формируется большое многообразие различных устойчивых структур. Для анализа формирующихся структур в процессе моделирования вычисляются численные характеристики глобального состояния КА: число компонент связности, степень перколяции, пористость, процент единичных клеток. Двухслойный ТКА $\aleph_S$ является эффективным инструментом для генерации компьютерного представления пористых материалов с нужной морфологией, так как визуальное отображение глобальных состояний $\aleph_S$ и вычисление значений характеристик на каждом шаге моделирования позволяет подбирать пористые структуры с требующейся морфологией.

ЛИТЕРАТУРА

1. *Bandman O. L.* Using Cellular Automata for porous media simulation // J. Supercomputing. 2011. V. 57. No. 2. P. 121–131.
2. *Бандман О. Л.* Метод построения клеточно-автоматных моделей процессов формирования устойчивых структур // Прикладная дискретная математика. 2010. № 4. С. 91–99.
3. *Chua L. O., Hasler M., Moschytz G. S., and Neirynck J.* Autonomous cellular neural networks: A unified paradigm for pattern formation and active wave propagation // IEEE Trans. Circuits and Systems. 1995. V. 42. P. 559–577.
4. *Young D. A.* A local activator-inhibitor model of vertebrate skin patterns // Math. Biosciences. 1984. V. 72. P. 51–58.
5. *Turing A. M.* The chemical basis of morphogenesis // Philosophical Transactions of the Royal Society of London. Ser. B. Biol. Sci. 1952. V. 237. No. 641. P. 37–72.
6. *Gierer A. and Meinhardt H.* A theory of biological pattern formation // Kybernetik. 1972. V. 12. No. 1. P. 30–39.
7. *Gierer A.* Generation of biological patterns and form: Some physical, mathematical and logical aspects // Progress in Biophysics and Molecular Biology. 1981. V. 37. P. 1–47.
8. *Бандман О. Л.* Клеточно-автоматные модели пространственной динамики // Системная информатика. Методы и модели современного программирования. 2006. № 10. С. 59–113.
9. *Bandman O. L.* Cellular Automata composition techniques for spatial dynamics simulation // Bulletin of the Novosibirsk Computing Center. Ser. Comp. Sci. 2008. V. 27. P. 1–39.
10. *Chopard B. and Droz M.* Cellular Automata Modeling of Physical Systems. Cambridge University Press, 1998. 337 p.

REFERENCES

1. *Bandman O. L.* Using Cellular Automata for porous media simulation. J. Supercomputing, 2011, vol. 57, no. 2, pp. 121–131.
2. *Bandman O. L.* Metod postroenija kletochno-avtomatnyh modelej processov formirovanija ustojchivyh struktur. Prikladnaya Diskretnaya Matematika, 2010, no. 4, pp. 91–99. (in Russian)
3. *Chua L. O., Hasler M., Moschytz G. S., and Neirynck J.* Autonomous cellular neural networks: A unified paradigm for pattern formation and active wave propagation. IEEE Trans. Circuits and Systems, 1995, vol. 42, pp. 559–577.
4. *Young D. A.* A local activator-inhibitor model of vertebrate skin patterns. Math. Biosciences, 1984, vol. 72, pp. 51–58.
5. *Turing A. M.* The chemical basis of morphogenesis. Philosophical Transactions of the Royal Society of London. Ser. B. Biol. Sci., 1952, vol. 237, no. 641, pp. 37–72.
6. *Gierer A. and Meinhardt H.* A theory of biological pattern formation. Kybernetik, 1972, vol. 12, no. 1, pp. 30–39.
7. *Gierer A.* Generation of biological patterns and form: Some physical, mathematical and logical aspects. Progress in Biophysics and Molecular Biology, 1981, vol. 37, pp. 1–47.
8. *Bandman O. L.* Kletochno-avtomatnye modeli prostranstvennoj dinamiki. Sistemnaja Informatika. Metody i Modeli Sovremennogo Programmirovaniya, 2006, no. 10, pp. 59–113. (in Russian)
9. *Bandman O. L.* Cellular Automata composition techniques for spatial dynamics simulation. Bulletin of the Novosibirsk Computing Center. Ser. Comp. Sci., 2008, vol. 27, pp. 1–39.
10. *Chopard B. and Droz M.* Cellular Automata Modeling of Physical Systems. Cambridge University Press, 1998. 337 p.

СВЕДЕНИЯ ОБ АВТОРАХ

БАНДМАН Ольга Леонидовна — доктор технических наук, профессор, главный научный сотрудник Института вычислительной математики и математической геофизики СО РАН, г. Новосибирск. E-mail: **bandman@ssd.sscc.ru**

ГАНОПОЛЬСКИЙ Родион Михайлович — кандидат физико-математических наук, директор Центра коллективного пользования высокопроизводительных и инфокоммуникационных технологий Тюменского государственного университета, г. Тюмень. E-mail: **rodion@utmn.ru**

ЕРМИЛОВ Дмитрий Михайлович — сотрудник лаборатории ТВП, г. Москва. E-mail: **wwwermilov@gmail.com**

КИРЕЕВА Анастасия Евгеньевна — кандидат физико-математических наук, младший научный сотрудник Института вычислительной математики и математической геофизики СО РАН, г. Новосибирск. E-mail: **kireeva@ssd.sscc.ru**

КОЖУХОВ Игорь Борисович — доктор физико-математических наук, профессор Национального исследовательского университета «МИЭТ», г. Москва.
E-mail: **kozhuhov_i_b@mail.ru**

КУЗЬМИН Сергей Алексеевич — г. Москва. E-mail: **kzmn_sr@mail.ru**

МАГОМЕДОВ Абдулкарим Магомедович — доктор физико-математических наук, доцент, заведующий кафедрой дискретной математики и информатики Дагестанского государственного университета, г. Махачкала.
E-mail: **magomedtagir1@yandex.ru**

МАГОМЕДОВ Тагир Абдулкаримович — аспирант кафедры дискретной математики и информатики Дагестанского государственного университета, г. Махачкала. E-mail: **magomedtagir1@yandex.ru**

МЕЖЕННАЯ Наталья Михайловна — кандидат физико-математических наук, доцент кафедры прикладной математики Московского государственного технического университета им. Н. Э. Баумана, г. Москва. E-mail: **natalia.mezhennaya@gmail.com**

МИХАЙЛОВИЧ Анна Витальевна — кандидат физико-математических наук, доцент общеуниверситетской кафедры высшей математики Национального исследовательского университета Высшая школа экономики, г. Москва.
E-mail: **avmikhailovich@gmail.com**

НАЗАРОВ Максим Николаевич — старший преподаватель Национального исследовательского университета «МИЭТ», г. Москва.
E-mail: **Nazarov-Maximilian@yandex.ru**

ПУДОВКИНА Марина Александровна — кандидат физико-математических наук, доцент Национального исследовательского ядерного университета «МИФИ», г. Москва. E-mail: **maricap@rambler.ru**

РОЖКОВ Михаил Иванович — доцент Московского института электроники и математики Национального исследовательского университета Высшая Школа Экономики, г. Москва. E-mail: **rozhkov.m.i@yandex.ru**

СОПИН Валерий Валерьевич — магистр Московского государственного университета им. М. В. Ломоносова, г. Москва. E-mail: **VvS@myself.com**

ТОКТАРЕВ Александр Валентинович — аспирант Национального исследовательского ядерного университета «МИФИ», г. Москва. E-mail: **toktarev@gmail.com**

ХАЛИУЛЛИНА Айгуль Римзиловна — аспирантка Национального исследовательского университета «МИЭТ», г. Москва. E-mail: **haliullinaar@gmail.com**