2014 Прикладная теория графов №1(23)

DOI 10.17223/20710410/23/10

УДК 519.174

СТРУКТУРА ФУНКЦИОНАЛЬНЫХ ГРАФОВ ДЛЯ ЦИРКУЛЯНТОВ С ЛИНЕЙНЫМИ БУЛЕВЫМИ ФУНКЦИЯМИ В ВЕРШИНАХ[1]

А. С. Корниенко

Институт математики СО РАН, г. Новосибирск, Россия

E-mail: anastasia.s.kornienko@gmail.com

Исследуется функциональный граф дискретной динамической системы, заданной на циркулянте с линейной булевой функцией от трёх аргументов в вершинах сети. Получено описание структуры деревьев и циклов функционального графа.

Ключевые слова: *дискретная динамическая система, циркулянт, генная сеть, регуляторный контур, функциональный граф.*

Введение

Генные сети служат основой для моделирования процессов, протекающих в клетке: поддерживают в организме устойчивые состояния, характеризующиеся постоянством концентрации веществ (стационарные состояния); обеспечивают периодические незатухающие колебания концентрации определённых групп веществ (контуры); контролируют необратимые процессы развития и роста [1].

Контуры с положительными и отрицательными обратными связями обеспечивают управление генной сетью. Некоторые структурные особенности строения регуляторных контуров естественно формулируются в терминах ориентированных графов и дискретных моделей регуляторных контуров.

В работе рассматривается дискретная динамическая система, которая является одной из таких моделей регуляторного контура генной сети. Функционирование контура определяется сменой его состояний и полностью характеризуется структурой функционального графа заданного преобразования $A_{f,2}\colon F_2^n \to F_2^n$. Метки вершин задают уровень концентрации веществ (гены, белки и др.), сопоставляемых этим верши нам [2 – 4]. В отличие от [2 – 4], где функции в вершинах являются пороговыми, в настоящей работе исследуется случай линейных функций.

Для характеризации функционального графа с заданной линейной функцией в вершинах используются циклические коды и техника их порождения с помощью полиномов [5]. Описывается структура деревьев функционального графа и изучаются его контуры: неподвижные точки, длины контуров. Рассматривается некоторое обобщение преобразования $A_{f,2}$.

В основе данной работы лежит защищённая магистерская диссертация [6].

1. Постановка задачи

Используем основные определения и понятия из работы [5], необходимые для постановки задачи.

Пусть даны $n \geqslant 3$, $1 \leqslant k \leqslant n$, $\{d_1, d_2, \ldots, d_k\} \subseteq \{0, 1, \ldots, n-1\}$ и ориентированный граф $G_{n;d_1,d_2,\ldots,d_k}$ с множествами вершин $\{0, 1, \ldots, n-1\}$ и дуг $\{(i, j) : (j - i) \equiv$

[1]Работа поддержана грантом РФФИ № 14-01-00507 и междисциплинарным интеграционным проектом СО РАН № 80.

$\equiv d_r \pmod n,\ r = 1, 2, \ldots, k\}$. Матрица смежности таких графов называется циркулянтом. Эти графы также принято называть *циркулянтами* [7].

Рассмотрим следующую дискретную динамическую систему. В каждый момент времени вершины циркулянта $G_{n;d_1,d_2,\ldots,d_k}$ помечены элементами $v_0, v_1, \ldots, v_{n-1}$ из конечного поля F_q порядка q. Набор $\widetilde{v} = (v_0, v_1, \ldots, v_{n-1}) \in F_q^n$ назовём *состоянием системы*. В следующий момент времени (такт работы системы) состояние системы меняется и динамика его изменения определяется отображением

$$A_{f,q}\colon F_q^n \to F_q^n,$$

где $f = (f_0, f_1, \ldots, f_{n-1})$ и новая метка каждой вершины $i \in \{0, 1, \ldots, n-1\}$ является значением функции $f_i\colon F_q^k \to F_q$, аргументы которой принимают значения старых меток в тех вершинах, дуги из которых входят в вершину i.

Функциональным графом $G_{f,q}$ называется ориентированный граф, вершинами которого являются элементы F_q^n, причём дуга из вершины $\widetilde{v}$ идёт в вершину $\widetilde{u}$ тогда и только тогда, когда $A_{f,q}(\widetilde{v}) = \widetilde{u}$. Известно, что функциональный граф любого преобразования конечного множества состоит из нескольких (быть может, одной) компонент связности. Каждая компонента содержит единственный контур (в частности, петлю, соответствующую неподвижной точке отображения). Некоторые вершины контура являются корнями деревьев, все дуги которых ориентированы к корню [8].

В работе исследуется структура функционального графа в случае, когда $q = 2$ (то есть действия происходят над полем F_2), все функции f_i равны между собой и линейны и отображение $A_{f,2}$ действует следующим образом:

$$\begin{gathered} A_{f,2}(v_0, v_1, \ldots, v_{n-1}) = (u_0, u_1, \ldots, u_{n-1}), \\ u_i = v_{i-1} + v_i + v_{i+1},\ i = 0, 1, \ldots, n-1, \\ \text{где } v_{-1} = v_{n-1}, v_n = v_0. \end{gathered} \tag{1}$$

2. Структура деревьев в функциональном графе

Линейное подпространство C векторного пространства F_2^n называется *циклическим кодом длины* n над F_2^n, если из $(v_0, v_1, \ldots, v_{n-1}) \in C$ следует $(v_1, \ldots, v_{n-1}, v_0) \in C$ [9].

Каждому набору $\widetilde{v} = (v_0, v_1, \ldots, v_{n-1})$ из F_2^n поставим в соответствие многочлен $v(x) = v_0 + v_1 x + \ldots + v_{n-1}x^{n-1}$ из кольца многочленов $F_2[x]$ над полем F_2. Известно [9], что при таком соответствии действие отображения $A_{f,2}(\widetilde{v}) = \widetilde{u}$, определяемое линейной рекуррентностью (1), можно записать в следующем виде.

Предложение 1 [9]. *$A_{f,2}(\widetilde{v}) = \widetilde{u}$ тогда и только тогда, когда*

$$v(x)(x^{n-1} + x + 1) \equiv u(x) \pmod{x^n - 1}.$$

Теперь в качестве состояний системы будем рассматривать элементы фактор-кольца $F_2[x]/(x^n - 1)$, а изменение состояния определяется умножением в этом фактор-кольце на многочлен

$$A(x) = x^{n-1} + x + 1.$$

Такую динамическую систему обозначим через $(n, 2, A(x))$ и далее будем называть *моделью*.

Известно [9], что если $C \subseteq F_2^n$ является циклическим кодом, то соответствующее ему подпространство (обозначать будем той же буквой C) фактор-кольца $F_2[x]/(x^n - 1)$

является идеалом. Порождающий многочлен $g(x)$ этого идеала называют *порождающим* кода C. Тогда если $\deg g(x) = r$, то $C = \{g(x)f(x) : f(x) \in F_2[x], \deg f(x) < n-r\}$. Многочлен $h(x)$, заданный соотношением $g(x)h(x) = x^n-1$, является *проверочным* циклического кода C. Таким образом, $c(x) \in C$ тогда и только тогда, когда $c(x)h(x) = 0$ в $F_2[x]/(x^n - 1)$.

Утверждение 1 [5, следствие 1]. Если $A(x)$ и $x^n - 1$ взаимно просты в кольце $F_2[x]$, то отображение $A_{f,2}$ обратимо и функциональный граф $G_{f,2}$ является дизъюнктивным объединением простых контуров.

Предложение 2. При n не кратном 3 отображение $A_{f,2}$ обратимо и функциональный граф $G_{f,2}$ является дизъюнктивным объединением простых контуров.

Доказательство. По утверждению 1 достаточно показать, что если n не кратно 3, то $(A(x), x^n - 1) = 1$ над полем F_2. Действительно, по алгоритму Евклида имеем

$$(A(x), x^n - 1) = (x^{n-1} + x + 1, x^n - 1) = (x^{n-1} + x + 1, (x^{n-1} + x + 1)x + x^2 + x + 1) = \\ = (x^{n-1} + x + 1, x^2 + x + 1).$$

Из разложения $x^{n-1}+x+1 = (x^2+x+1)(x^{n-3}+x^{n-4})+x^{(n-1)-3}+x+1$ следует сравнение $x^{n-1}+x+1 \equiv x^{(n-1)-3}+x+1 \pmod{x^2+x+1}$. Продолжая аналогичные рассуждения, видим что $x^{n-1}+x+1 \equiv x^{(n-1) \bmod 3}+x+1 \pmod{x^2+x+1}$. Таким образом, получаем

$$n \equiv 0 \pmod 3 \Rightarrow x^{n-1} + x + 1 \equiv 0 \pmod{x^2 + x + 1},$$
$$n \equiv 1 \pmod 3 \Rightarrow x^{n-1} + x + 1 \equiv x \pmod{x^2 + x + 1},$$
$$n \equiv 2 \pmod 3 \Rightarrow x^{n-1} + x + 1 \equiv 1 \pmod{x^2 + x + 1}.$$

Предложение доказано. ■

На рис. 1 изображён функциональный граф модели $(5, 2, A(x))$, который представляет из себя дизъюнктивное объединение простых контуров. Здесь двоичные наборы длины 5, соответствующие вершинам, записаны их десятичными представлениями.

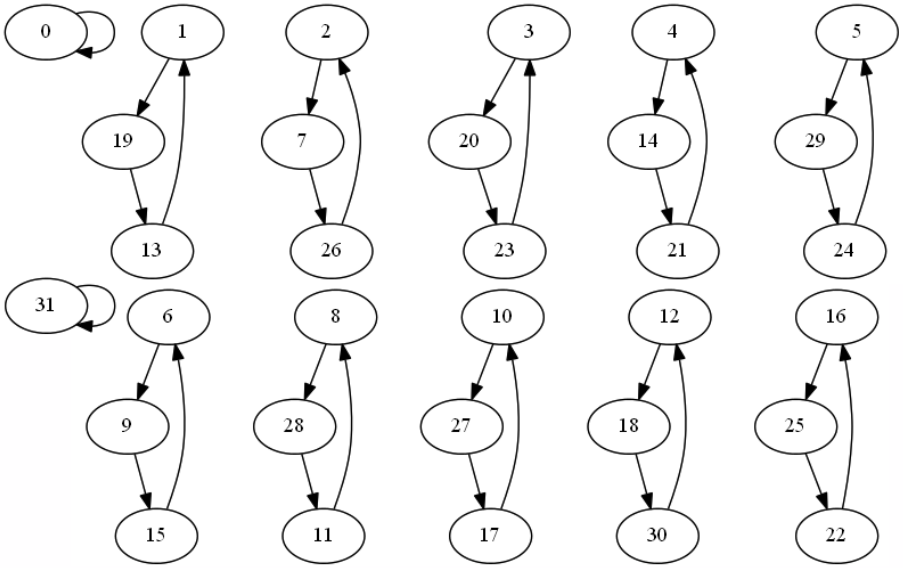

Рис. 1. Функциональный граф $G_{f,2}$ при $n = 5$

Пусть $(A(x), x^n - 1) \neq 1$, т. е. n кратно 3 по предложению 2. Рассмотрим, как в [5], последовательность циклических кодов $C_0 = F_2[x]/(x^n - 1)$, C_1, $C_2, \ldots, C_t$, таких, что

код C_i имеет порождающий и проверочный многочлены $g_i(x)$ и $h_i(x)$, $i = 1, 2, \ldots, t$, соответственно, где

$$g_1(x) = (A(x), x^n - 1),\ h_1(x) = (x^n - 1)/g_1(x),$$
$$g_i(x) = g_{i-1}(x)(g_1(x), h_{i-1}(x)),\ h_i(x) = (x^n - 1)/g_i(x),\ i = 2, 3, \ldots, t,$$

и t — такое минимальное число, что $(g_1(x), h_t(x)) = 1$.

Пусть $S_i = C_i \setminus C_{i+1},\ i = 0, 1, \ldots, t-1$, и $S_t = C_t$.

Утверждение 2 [5, теорема 2]. В функциональном графе $G_{f,2}$ вершины, принадлежащие контурам, образуют множество S_t. Множество вершин, принадлежащих деревьям, разбивается на t уровней S_0, $S_1, \ldots$, S_{t-1}, таких, что S_0 — множество листьев, а вершины из S_i находятся на расстоянии i от вершин из S_0, $1 \leqslant i \leqslant t-1$.

Теорема 1. При $n = 3 \cdot 2^k(2m+1)$, где $k, m \geqslant 0$, в функциональном графе $G_{f,2}$ множество вершин, принадлежащих деревьям, разбивается на 2^k уровней, причём каждая вершина дерева, кроме листьев, имеет ровно четырёх предков.

Доказательство. Из доказательства предложения 2 имеем $g_1(x) = x^2 + x + 1$. Используя неприводимость многочлена $g_1(x)$ над F_2, получаем, что для всех $i = 2, 3, \ldots, t$ порождающие многочлены $g_i(x) = g_{i-1}(x)(g_1(x), h_{i-1}(x))$ имеют вид $g_i(x) = g_{i-1}(x)g_1(x) = g_1^i(x) = (x^2 + x + 1)^i$, пока многочлен $x^n - 1$ делится на $(x^2 + x + 1)^i$, так как $h_i(x) = (x^n - 1)/g_i(x)$. Таким образом, $(g_1(x), h_t(x))$ впервые равен 1, когда t равно максимальной степени вхождения многочлена $x^2 + x + 1$ в разложение $x^n - 1$ на неприводимые множители над F_2.

Сначала докажем индукцией по k, что множество вершин, принадлежащих деревьям, разбивается на 2^k уровней.

Пусть $k = 0$, т. е. $n = 3(2m + 1)$. Покажем, что в этом случае $t = 1$. Допустим обратное, тогда $x^n - 1$ должно делиться без остатка на $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. Из представления $x^n - 1 = (x^4 + x^2 + 1)(x^{n-4} + x^{n-6}) + x^{n-6} - 1$ получаем, что $x^n - 1 \equiv x^{n-6} - 1 \equiv \ldots \equiv x^{n \bmod 6} - 1 \equiv 0 \pmod{x^4 + x^2 + 1}$. Но $n = 3(2m + 1) = 6m + 3 \equiv 3 \pmod 6$, противоречие. База индукции доказана.

Предположим, что для $n_k = 3 \cdot 2^k(2m + 1)$ максимальная степень вхождения $x^2 + x + 1$ в разложение на неприводимые множители $x^{n_k} - 1$ над F_2 равна $t_k = 2^k$. Пусть теперь $n = 3 \cdot 2^{k+1}(2m + 1)$. Из разложения $x^n - 1 = x^{2n_k} - 1 = (x^{n_k} - 1)(x^{n_k} + 1)$ и предположения индукции получаем, что $t = 2t_k = 2^{k+1}$. Таким образом, первая часть теоремы доказана.

Теперь, используя мощностные оценки, докажем, что каждая вершина в дереве, кроме листьев, имеет ровно четырёх предков.

Найдём мощность множества S_t вершин, принадлежащих контурам. Из утверждения 2 это множество совпадает с циклическим кодом C_t с порождающим многочленом $g_t(x)$. Из доказанного выше знаем, что при $n = 3 \cdot 2^k(2m + 1)$ имеем $t = 2^k$ и $g_t(x) = (x^2 + x + 1)^t$. Степень порождающего многочлена равна $2t$, значит, циклический код C_t имеет мощность 2^{n-2t}.

Заметим, что уравнение $A_{f,2}(\widetilde{v}) = \widetilde{u}$ с неизвестным $\widetilde{v}$ имеет не более четырёх решений. Действительно, из равенств (1) получаем, что решение $\widetilde{v}$, если оно существует, можно представить в следующем рекуррентном виде:

$$v_i = u_{i-1} + v_{i-1} + v_{i-2},\ i = 2, 3, \ldots, n-1,$$

если v_0, v_1 заданы. Так как v_0 и v_1 из F_2, то начальное условие, которое полностью задаёт решение, можно выбрать четырьмя различными способами.

Другими словами, доказано, что каждая вершина функционального графа $G_{f,2}$ имеет не более четырёх прообразов. Корень каждого дерева имеет не более трёх предков в своём дереве, так как он уже является образом некоторой вершины из контура. Оставшиеся вершины дерева, кроме листьев, имеют не более четырёх предков. Тогда весь функциональный граф имеет вершин не более, чем

$$2^{n-2t} + \sum_{l=0}^{t-1} 4^l \cdot 3 \cdot 2^{n-2t} = 2^{n-2t} + 3 \cdot 2^{n-2t} \sum_{l=0}^{t-1} 4^l =$$
$$= 2^{n-2t} + 3 \cdot 2^{n-2t} \cdot \frac{4^t - 1}{3} = 2^{n-2t} + 2^{n-2t} \cdot 4^t - 2^{n-2t} = 2^{n-2t} \cdot 2^{2t} = 2^n.$$

Но именно столько элементов в пространстве F_2^n. Значит, каждая вершина функционального графа, не являющаяся листом, имеет ровно четыре прообраза, и теорема полностью доказана. ■

На рис. 2 изображено дерево, притягиваемое вершиной $\widetilde{v} = (0, 0, \ldots, 0)$, в функциональном графе $G_{f,2}$ при $n = 6$. Двоичные наборы длины 6, соответствующие вершинам, записаны их десятичными представлениями.

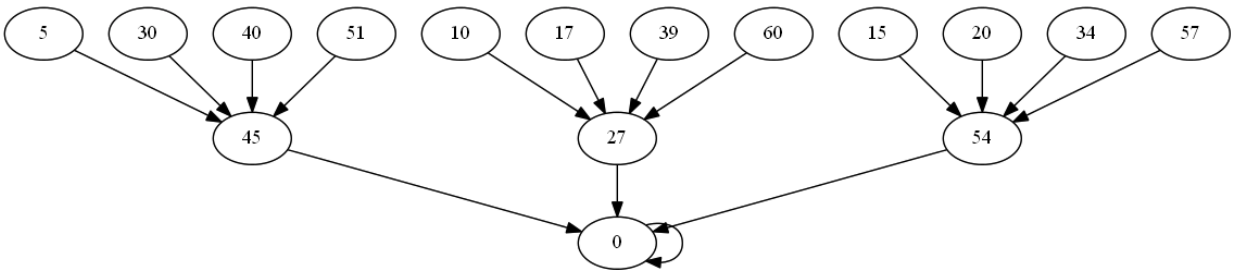

Рис. 2. Дерево, притягиваемое вершиной $\widetilde{v} = (0, 0, \ldots, 0)$, в функциональном графе $G_{f,2}$ при $n = 6$

3. Контуры в функциональном графе

Рассмотрим неподвижные точки и длины контуров в функциональном графе $G_{f,2}$.

Утверждение 3 [5, следствие 4]. Неподвижные точки функционального графа $G_{f,2}$ образуют циклический код с проверочным многочленом $(A(x) - 1, x^n - 1)$. Если степень этого многочлена равна r, то число неподвижных точек равно 2^r.

Предложение 3. При чётном n функциональный граф $G_{f,2}$ содержит четыре неподвижные точки, в противном случае — две.

Доказательство. По утверждению 3 для того, чтобы найти неподвижные точки функционального графа, необходимо и достаточно найти проверочный многочлен $h(x) = (A(x) - 1, x^n - 1)$ циклического кода, состоящего из неподвижных точек функционального графа $G_{f,2}$. Используя алгоритм Евклида, получаем

$$(A(x) - 1, x^n - 1) = (x^{n-1} + x, x^n - 1) = (x^{n-2} + 1, x^n - 1) =$$
$$= (x^{n-2} + 1, (x^{n-2} + 1)x^2 + x^2 + 1) = (x^{n-2} + 1, x^2 + 1) = x^{2-n \bmod 2} + 1.$$

В зависимости от чётности n имеем

$$n \equiv 0 \pmod 2 \Rightarrow h(x) = (A(x) - 1, x^n - 1) = x^2 + 1,$$
$$n \equiv 1 \pmod 2 \Rightarrow h(x) = (A(x) - 1, x^n - 1) = x + 1.$$

Рассмотрим каждый вариант по отдельности.

В первом случае проверочный многочлен циклического кода $h(x) = x^2+1$. По определению $g(x)h(x) = x^n-1$, значит, порождающий многочлен $g(x) = x^{n-2}+x^{n-4}+\ldots+1$, и порождающая матрица циклического кода, состоящего из неподвижных точек функционального графа $G_{f,2}$, имеет вид

$$\begin{pmatrix} 1 & 0 & 1 & 0 & \ldots & 1 & 0 \\ 0 & 1 & 0 & 1 & \ldots & 0 & 1 \end{pmatrix}.$$

Таким образом, имеем четыре неподвижные точки: 0, $x^{n-2} + x^{n-4} + \ldots + 1$, $x^{n-1} + {}+x^{n-3}+\ldots+x$, $x^{n-1}+x^{n-2}+\ldots+1$. В F_2^n неподвижные точки соответствуют элементам $(0,0,\ldots,0)$, $(1,0,\ldots,1,0)$, $(0,1,\ldots,0,1)$, $(1,1,\ldots,1)$.

Во втором случае $h(x) = x+1$ и порождающий многочлен $g(x) = x^{n-1}+x^{n-2}+\ldots+1$. Существуют всего две неподвижные точки: 0 и $x^{n-1}+x^{n-2}+\ldots+1$. В F_2^n неподвижные точки соответствуют элементам $(0,0,\ldots,0)$ и $(1,1,\ldots,1)$. ■

Утверждение 4 [5, теорема 3]. Для любого целого положительного l все вершины функционального графа, принадлежащие контурам длины, делящей l, образуют циклический код с проверочным многочленом $(A^l(x) - 1, x^n - 1)$.

Утверждение 5 [5, теорема 4]. Если наибольшая длина контура функционального графа модели $(n, 2, A(x))$ равна l и $h_t(x)$ является порождающим многочленом циклического кода, образованного вершинами всех контуров, то максимальная длина контура функционального графа модели $(2n, 2, A(x))$ не изменится тогда и только тогда, когда $h_t^2(x)$ делит $A^l(x) - 1$. В противном случае наибольшая длина контура удвоится.

Теорема 2. Если $n = 2^k(2m + 1)$, где $k, m \geqslant 0$, то все длины контуров функционального графа $G_{f,2}$ являются делителями $2^k(2^s - 1)$, где

$$s = \min\bigl\{j : j > 0,\ 2^j \equiv 1 \pmod{2m+1} \text{ или } 2^j \equiv -1 \pmod{2m+1}\bigr\}.$$

Доказательство. Пусть n — нечётное число. Положим $l = 2^s - 1$, где

$$s = \min\bigl\{j : j > 0,\ 2^j \equiv 1 \pmod{n} \text{ или } 2^j \equiv -1 \pmod{n}\bigr\}.$$

Так как сложение происходит по модулю 2, то имеем следующие сравнения:

$$A^{2^s}(x) = (x^{n-1} + x + 1)^{2^s} = x^{2^s(n-1)} + x^{2^s} + 1 \equiv x^{n-1} + x + 1 = A(x) \pmod{x^n - 1},$$
$$A(x)(A(x)^{2^s-1} - 1) \equiv 0 \pmod{x^n - 1},$$
$$A(x)(A^l(x) - 1) \equiv 0 \pmod{x^n - 1}.$$

Так как по предложению 2 выполняется $(A(x), x^n - 1) = 1$ при n, не кратном 3, то

$$A^l(x) - 1 \equiv 0 \pmod{x^n - 1},\ \text{то есть}\ (A^l(x) - 1, x^n - 1) = x^n - 1 = h_t(x).$$

В случае же, когда n делится на 3, имеем

$$(A(x), x^n - 1) = x^2 + x + 1,$$
$$(A^l(x) - 1, x^n - 1) = \frac{x^n - 1}{x^2 + x + 1} = h_t(x).$$

По утверждению 4 получаем, что для нечётного n теорема доказана. Из утверждения 5 следует истинность и для чётного n. ■

Утверждение 6 [5, следствие 6]. Если в модели $(n, 2, A(x))$ наибольшая длина l контура чётна, то в модели $(2n, 2, A(x))$ наибольшая длина контура равна $2l$.

Теорема 3. Пусть в модели $(n, 2, A(x))$ наибольшая длина контура равна l, тогда в модели $(2n, 2, A(x))$ наибольшая длина контура не изменится, если $n \in \{1, 3\}$, в противном случае она удвоится.

Доказательство. Пусть n нечётное. По теореме 2 и утверждению 5, если длина контура в модели $(2n, 2, A(x))$ не удваивается, то $h_t^2(x)$ должен делить $A^l(x) - 1$ и $A^{2^s-1}(x) - 1$, поскольку l — делитель числа $2^s - 1$ по теореме 2, где s удовлетворяет сравнению

$$2^s \equiv \pm 1 \pmod{n}, \text{ так как } n \text{ нечётное},$$
$$2^s \equiv n \pm 1 \pmod{2n}.$$

Рассмотрим при $n \neq 1$ в модели $(2n, 2, A(x))$ более подробно разность

$$A^{2^s}(x) - A(x) = (x^{2^s \cdot (2n-1)} + x^{2^s} + 1) - (x^{2n-1} + x + 1) \equiv$$
$$\equiv x^{(n-1)(2n-1)} + x^{n-1} - x^{2n-1} - x \equiv x^{n+1} + x^{n-1} - x^{2n-1} - x \equiv$$
$$\equiv x^{2n-2} + x^n + x^{n-2} + 1 \pmod{x^{2n} - 1}, \text{ если } 2^s \equiv n - 1 \pmod{2n};$$
$$A^{2^s}(x) - A(x) = (x^{2^s \cdot (2n-1)} + x^{2^s} + 1) - (x^{2n-1} + x + 1) \equiv$$
$$\equiv x^{(n+1)(2n-1)} + x^{n+1} - x^{2n-1} - x \equiv x^{n-1} + x^{n+1} - x^{2n-1} - x \equiv$$
$$\equiv x^{2n-2} + x^n + x^{n-2} + 1 \pmod{x^{2n} - 1}, \text{ если } 2^s \equiv n + 1 \pmod{2n}.$$

Для n, не кратного 3, порождающий многочлен циклического кода, образованного вершинами всех контуров функционального графа модели $(n, 2, A(x))$, равен $h_t(x) = x^n - 1$, и

$$A^{2^s-1}(x) - 1 \equiv 0 \pmod{x^{2n} - 1},$$
$$A^{2^s}(x) - A(x) \equiv 0 \pmod{x^{2n} - 1},$$
$$x^{2n-2} + x^n + x^{n-2} + 1 \equiv 0 \pmod{x^{2n} - 1},$$
$$(x^{n-2} + 1)(x^n + 1) \equiv 0 \pmod{(x^n - 1)(x^n + 1)},$$
$$x^{n-2} + 1 \equiv 0 \pmod{x^n - 1} \Rightarrow x^{n-2} + 1 = 0.$$

Равенство верно только при $n = 2$. Для n, кратного 3, порождающий многочлен равен $h_t(x) = (x^n - 1)/(x^2 + x + 1)$, $(A(x), x^{2n} - 1) = x^2 + x + 1$, и

$$A^{2^s-1}(x) - 1 \equiv 0 \pmod{(x^{2n} - 1)/(x^2 + x + 1)^2},$$
$$(A^{2^s-1}(x) - 1)(x^2 + x + 1)^2 \equiv 0 \pmod{x^{2n} - 1},$$
$$(A^{2^s-1}(x) - 1)(x^2 + x + 1)^2 A(x)/(x^2 + x + 1) \equiv 0 \pmod{x^{2n} - 1},$$
$$(A^{2^s}(x) - A(x))(x^2 + x + 1) \equiv 0 \pmod{x^{2n} - 1},$$
$$(x^{2n-2} + x^n + x^{n-2} + 1)(x^2 + x + 1) \equiv 0 \pmod{x^{2n} - 1},$$
$$(x^{n-2} + 1)(x^n + 1)(x^2 + x + 1) \equiv 0 \pmod{(x^n - 1)(x^n + 1)},$$
$$(x^{n-2} + 1)(x^2 + x + 1) \equiv 0 \pmod{x^n - 1},$$
$$x^n + x^{n-1} + x^{n-2} + x^2 + x + 1 \equiv 0 \pmod{x^n - 1},$$
$$x^{n-1} + x^{n-2} + x^2 + x \equiv 0 \pmod{x^n - 1} \Rightarrow (x^{n-3} + 1)(x + 1)x = 0.$$

Равенство верно только при $n = 3$.

Легко проверить, что у моделей $(1, 2, A(x))$ и $(2, 2, A(x))$, как и у моделей $(3, 2, A(x))$ и $(6, 2, A(x))$, максимальные длины контуров одинаковы и равны 1. А у моделей $(4, 2, A(x))$ и $(12, 2, A(x))$ максимальные длины контуров равны 2.

Таким образом, теорема доказана для нечётного l. Для чётного l истинность следует из утверждения 6. ■

Утверждение 7 [5, следствие 5]. Наибольшая длина контура в функциональном графе равна минимальному l, для которого

$$(A^l(x) - 1, x^n - 1) = h_t(x).$$

Следствие 1. Если $n = 2^k(2^m \pm 1)$, $k \geqslant 0$ и $m > 2$, то наибольшая длина контура в $G_{f,2}$ равна $2^k(2^m - 1)$.

Доказательство. Следует из теорем 2, 3 и утверждения 7. ■

Предложение 4. Если $n \neq 3$ — простое число, то все контуры в $G_{f,2}$, кроме двух неподвижных точек, имеют одинаковую длину.

Доказательство. Допустим, что существует контур, длина l которого отлична от максимальной длины всех контуров. Тогда по утверждению 7 должно выполняться

$$(A^l(x) - 1, x^n - 1) \neq h_t(x), \text{ то есть } (A^l(x) - 1, x^n - 1) \neq x^n - 1,$$

для простого $n \neq 3$ проверочный многочлен $h_t(x) = x^n - 1$. Разложим на множители $x^n - 1 = (x-1)(x^{n-1} + \ldots + x + 1)$. Известно [10], что многочлен $x^{n-1} + \ldots + x + 1$ является неприводимым над полем F_2. Таким образом, получаем, что $(A^l(x) - 1, x^n - 1) = x - 1$, так как

$$A(x) = x^{n-1} + x + 1 \equiv 1 \pmod{x - 1},$$
$$A^l(x) - 1 \equiv 0 \pmod{x - 1}.$$

Но $x - 1$ — это проверочный многочлен для циклического кода, состоящего из неподвижных точек функционального графа $G_{f,2}$. Тем самым предложение доказано. ■

4. Смещённое преобразование

Отображение $A_{f,2}\colon F_2^n \to F_2^n$, определённое равенством (1), можно записать в следующем виде: $A_{f,2} = I_n + L_n + R_n$, где I_n, L_n и R_n — тождественный оператор, операторы левого и правого сдвигов пространства F_2^n соответственно.

Рассмотрим отображения $A_{f_L,2} = L_n \cdot A_{f,2}$ и $A_{f_R,2} = R_n \cdot A_{f,2}$ и назовём их *смещёнными влево* и *вправо* относительно отображения $A_{f,2}$ соответственно. В силу симметрии структуры функциональных графов этих отображений совпадают, поэтому достаточно изучить структуру функционального графа только одного преобразования, например $A_{f_R,2}$.

4.1. Структура деревьев

Отображение $A_{f_R,2}\colon F_2^n \to F_2^n$, действующее следующим образом:

$$A_{f_R,2}(v_0, v_1, \ldots, v_{n-1}) = (u_0, u_1, \ldots, u_{n-1}),$$
$$u_i = v_{i-2} + v_{i-1} + v_i, \ i = 0, 1, \ldots, n-1,$$
$$v_{-2} = v_{n-2}, v_{-1} = v_{n-1},$$

в фактор-кольце $F_2[x]/(x^n-1)$ определяется как умножение элементов фактор-кольца на многочлен $A_R(x) = x^2+x+1$. Значит, порождающие $g_i(x)$ и проверочные $h_i(x)$ многочлены отображений $A_{f_R,2}$ и $A_{f,2}$ совпадают. Таким образом, можем описать структуру деревьев функционального графа отображения $A_{f_R,2}$.

Предложение 5. При n, не кратном 3, отображение $A_{f_R,2}$ обратимо и функциональный граф $G_{f_R,2}$ является дизъюнктивным объединением простых контуров.

Предложение 6. При $n = 3\cdot 2^k(2m+1)$, где $k, m \geqslant 0$, в функциональном графе $G_{f_R,2}$ множество вершин, принадлежащих деревьям, разбивается на 2^k уровней, причём каждая вершина дерева, кроме листьев, имеет ровно четырёх предков.

4.2. К о н т у р ы

В отличие от структур деревьев функциональных графов преобразований $A_{f_R,2}(x)$ и $A_{f,2}(x)$, которые совпадают, структуры контуров имеют различия.

Предложение 7. Функциональный граф $G_{f_R,2}$ содержит две неподвижные точки.

Доказательство. По утверждению 3, для того, чтобы найти неподвижные точки функционального графа, необходимо и достаточно найти проверочный многочлен $h(x)$:

$$h(x) = (A_R(x)-1, x^n-1) = (x^2+x, x^n-1) = (x+1, x^n-1) = x+1.$$

По определению $g(x)h(x) = x^n-1$, значит, порождающий многочлен циклического кода, состоящего из неподвижных точек функционального графа $G_{f_R,2}$, равен $g(x) = x^{n-1}+x^{n-2}+\ldots+1$. Таким образом, имеем две неподвижные точки: 0 и $x^{n-1}+x^{n-2}+\ldots+1$, которые в F_2^n соответствуют элементам $(0,0,\ldots,0)$ и $(1,1,\ldots,1)$. ■

Предложение 8. Если $n = 2^k(2m+1)$, $k, m \geqslant 0$, то все длины контуров функционального графа $G_{f_R,2}$ являются делителями $2^k(2^s-1)$, где

$$s = \min\bigl\{j : j>0,\ \ 2^j \equiv 1 \pmod{2m+1}\bigr\}.$$

Доказательство. Пусть n — нечётное число. Положим $l = 2^s-1$, где

$$s = \min\bigl\{j : j>0,\ \ 2^j \equiv 1 \pmod{n}\bigr\}.$$

Так как сложение происходит по модулю 2, то имеем следующие сравнения:

$$A_R^{2^s}(x) = (x^2+x+1)^{2^s} = x^{2\cdot 2^s}+x^{2^s}+1 \equiv x^2+x+1 = A_R(x) \pmod{x^n-1},$$
$$A_R(x)(A_R(x)^{2^s-1}-1) \equiv 0 \pmod{x^n-1},$$
$$A_R(x)(A_R^l(x)-1) \equiv 0 \pmod{x^n-1}.$$

Так как $(A_R(x), x^n-1) = 1$ при n, не кратном 3, то

$$A_R^l(x)-1 \equiv 0 \pmod{x^n-1},$$
$$(A_R(x)^l-1, x^n-1) = x^n-1 = h_t(x).$$

В случае же, когда n делится на 3, имеем

$$(A_R(x), x^n-1) = x^2+x+1,$$
$$(A_R(x)^l-1, x^n-1) = \frac{x^n-1}{x^2+x+1} = h_t(x).$$

По утверждению 4 получаем, что для нечётного n предложение доказано. Из утверждения 5 следует истинность и для чётного n. ■

Предложение 9. Наибольшая длина контура в модели $(2n, 2, A_R(x))$ в 2 раза больше, чем в модели $(n, 2, A_R(x))$.

Доказательство. Пусть n нечётное. По предложению 8 и утверждению 5, если длина контура в модели $(2n, 2, A_R(x))$ не удваивается, то $h_t^2(x)$ должен делить $A_R^l - 1$ и $A_R^{2^s-1} - 1$, поскольку l — делитель числа $2^s - 1$ по предложению 8, где s удовлетворяет сравнению

$$2^s \equiv 1 \pmod{n}, \text{ так как } n \text{ нечётное},$$
$$2^s \equiv n + 1 \pmod{2n}.$$

Рассмотрим более подробно разность

$$A_R^{2^s}(x) - A_R(x) = (x^{2\cdot 2^s} + x^{2^s} + 1) - (x^2 + x + 1) \equiv$$
$$\equiv x^{2(n+1)} + x^{n+1} - x^2 - x \equiv x^2 + x^{n+1} - x^2 - x \equiv x^n + 1 \pmod{x^{2n} - 1}.$$

Для n, не кратного 3, получаем, что $h_t(x) = x^n - 1$ и

$$A_R^{2^s-1}(x) - 1 \equiv 0 \pmod{x^{2n} - 1},$$
$$A_R^{2^s}(x) - A_R(x) \equiv 0 \pmod{x^{2n} - 1},$$
$$x^n + 1 \equiv 0 \pmod{x^{2n} - 1}.$$

Для n, кратного 3, получаем, что $h_t(x) = (x^n - 1)/(x^2 + x + 1)$ и

$$(A_R^{2^s-1}(x) - 1)(x^2 + x + 1)^2 \equiv 0 \pmod{x^{2n} - 1},$$
$$(A_R^{2^s}(x) - A_R(x))(x^2 + x + 1) \equiv 0 \pmod{x^{2n} - 1},$$
$$(x^n + 1)(x^2 + x + 1) \equiv 0 \pmod{x^{2n} - 1},$$
$$x^{n+2} + x^{n+1} + x^n + x^2 + x + 1 \equiv 0 \pmod{x^{2n} - 1}.$$

В обоих случаях полученные сравнения не верны для любого n.

Таким образом, предложение доказано для нечётного l. Для чётного l предложение следует из утверждения 6. ■

Следствие 2. Если $n = 2^k(2^m - 1)$, $k, m \geqslant 0$ и $m \neq 2$, то наибольшая длина контура в $G_{f_R,2}$ равна n.

Доказательство. Следует из предложений 8, 9 и утверждения 7. ■

Предложение 10. Если $n \neq 3$ — простое число, то все контуры в $G_{f_R,2}$, кроме двух неподвижных точек, имеют одинаковую длину.

Доказательство. Допустим, что существует контур, длина l которого отлична от максимальной длины всех контуров. Тогда по утверждению 7 должно выполняться

$$(A_R^l(x) - 1, x^n - 1) \neq h_t(x), \text{ то есть}$$
$$(A_R^l(x) - 1, x^n - 1) \neq x^n - 1,$$

для простого $n \neq 3$ проверочный многочлен $h_t(x) = x^n - 1$. Разложим на множители $x^n - 1 = (x-1)(x^{n-1} + \ldots + x + 1)$. Как было замечено ранее, многочлен $x^{n-1} + \ldots + x + 1$ неприводим над полем F_2. Таким образом, $(A_R^l(x) - 1, x^n - 1) = x - 1$, так как

$$A_R = x^2 + x + 1 \equiv 1 \pmod{x - 1},$$
$$A_R^l(x) - 1 \equiv 0 \pmod{x - 1}.$$

Но $x-1$ — это проверочный многочлен циклического кода, состоящего из неподвижных точек функционального графа $G_{f_R,2}$. Тем самым предложение доказано. ■

Предложение 11. Функциональный граф $G_{f_R,2}$ содержит контур длины 2, причём только один, тогда и только тогда, когда n чётное.

Доказательство. По утверждению 4 все вершины функционального графа, принадлежащие контурам длины, делящей 2, образуют циклический код с проверочным многочленом

$$(A_R^2(x)-1, x^n-1) = ((x^2+x+1)^2-1, x^n-1) =$$
$$= (x^4+x^2, x^n-1) = (x^2+1, x^n-1) = x^{2-n \bmod 2}-1.$$

В случае нечётного n проверочный многочлен равен $x-1$ и является проверочным для кода, состоящего из неподвижных точек. В случае чётного n имеем x^2-1, и такой проверочный многочлен образует циклический код из четырёх элементов, два и только два из которых — неподвижные точки. Значит, оставшиеся два элемента образуют один цикл длины 2. ■

5. Некоторое обобщение

Отображение $A_{f,2}\colon F_2^n \to F_2^n$ можно записать в виде $A_{f,2} = I_n + L_n + R_n$.

Рассмотрим отображение более общего вида $A_{f,2}(k) = I_n + L_n^k + R_n^k$.

Теорема 4. Пусть $(n,k)=1$. Тогда $A_{f,2}(k)$ является алгебраическим сопряжением к $A_{f,2}$.

Доказательство. Пусть $\widetilde{v} = (v_0, v_1, \ldots, v_{n-1}) \in F_2^n$. Определим отображение $\sigma\colon F_2^n \to F_2^n$ следующим образом:

$$\sigma(\widetilde{v}) = (v_{\pi(0)}, v_{\pi(1)}, \ldots, v_{\pi(n-1)}), \text{ где } \pi(jk \bmod n) = j,\ j = 0, \ldots, n-1.$$

Так как $(n,k)=1$, π является перестановкой $(0,1,\ldots,n-1)$, а $\pi^{-1}(j) = jk \bmod n$ — обратная к ней перестановка. Таким образом, имеем

$$(A_{f,2}(k)\sigma(\widetilde{v}))_{jk \bmod n} = v_j + v_{j+1} + v_{j-1},$$
$$(\sigma^{-1}A_{f,2}(k)\sigma(\widetilde{v}))_j = v_j + v_{j+1} + v_{j-1}, \text{ где } v_{-1} = v_{n-1}, v_n = v_0.$$

Отсюда получаем $\sigma^{-1}A_{f,2}(k)\sigma = A_{f,2}$, что и требовалось доказать. ■

Следствие 3. При $(n,k) = 1$ структура функционального графа отображения $A_{f,2}(k)$ совпадает со структурой функционального графа отображения $A_{f,2}$.

Заключение

В работе рассмотрена дискретная динамическая система, являющаяся моделью регуляторного контура генной сети, функционирование которого определяется сменой его состояний и полностью характеризуется структурой функционального графа $G_{f,2}$ заданного преобразования $A_{f,2}\colon F_2^n \to F_2^n$.

Для характеризации функционального графа $G_{f,2}$ с заданной линейной функцией в вершинах использованы циклические коды и техника их порождения с помощью полиномов. Описана структура деревьев функционального графа и изучены некоторые свойства контуров: найдены неподвижные точки; найдено число, делителями которого являются все длины контуров функционального графа; для некоторого вида n найдена максимальная длина контуров. Данные результаты удалось распространить на более общий вид преобразования $A_{f,2}$.

Доказаны также аналогичные свойства деревьев и контуров функциональных графов преобразований, смещённых относительно $A_{f,2}$.

ЛИТЕРАТУРА

1. *Лихошвай В. А., Матушкин Ю. Г., Фадеев С. И.* Задачи теории функционирования генных сетей // Сиб. журн. индустр. математики. 2003. Т. 6. № 2 (14). С. 64–80.
2. *Григоренко Е. Д., Евдокимов А. А., Лихошвай В. А., Лобарева И. А.* Неподвижные точки и циклы автоматных отображений, моделирующих функционирование генных сетей // Вестник ТГУ. 2005. Приложение № 14. С. 206–212.
3. *Евдокимов А. А.* Дискретные модели генных сетей: анализ и сложность функционирования // Вычислительные технологии. 2008. Т. 13. № 3. С. 31–37.
4. *Евдокимов А. А., Лиховидова Е. О.* Дискретная модель генной сети циркулянтного типа с пороговыми функциями // Вестник ТГУ. Управление, вычислительная техника и информатика. 2008. № 2. С. 18–21.
5. *Евдокимов А. А., Пережогин А. Л.* Дискретные динамические системы циркулянтного типа с линейными функциями в вершинах сети // Дискретный анализ и исследование операций. 2011. Т. 18. № 3. С. 39–48.
6. *Корниенко А. С.* Структура функциональных графов для циркулянтов с линейными булевыми функциями в вершинах: магистерская диссертация / Новосибирский государственный университет. Новосибирск, 2013. 22 с.
7. *Харари Ф.* Теория графов. М.: УРСС, 2003. 300 с.
8. *Оре О.* Теория графов. М.: Наука, 1980. 336 с.
9. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
10. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1. М.: Мир, 1988. 430 с.