ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Май—июнь 2011. Том 18, № 3. С. 39–48

УДК 519.174

ДИСКРЕТНЫЕ ДИНАМИЧЕСКИЕ СИСТЕМЫ ЦИРКУЛЯНТНОГО ТИПА С ЛИНЕЙНЫМИ ФУНКЦИЯМИ В ВЕРШИНАХ СЕТИ *)

А. А. Евдокимов, А. Л. Пережогин

Аннотация. Получено описание функционального графа дискретной динамической системы, заданной на циркулянте с линейной функцией в вершинах сети. Для случая булева оператора получены оценки наибольшей длины контура в функциональном графе.

Ключевые слова: дискретная динамическая система, циркулянт, генная сеть, регуляторный контур, кольцо многочленов, линейное пространство, функциональный граф, циклический код, орбита состояний.

1. Общая модель

Пусть даны $n \geqslant 3$, $\{d_1, d_2, \ldots, d_k\} \subseteq \{0, 1, \ldots, n-1\}$ и ориентированный граф $G_{n;d_1,d_2,\ldots,d_k}$ с множествами вершин $\{0, 1, \ldots, n-1\}$ и дуг $\left\{\overrightarrow{ij} \mid j - i \equiv d_r \pmod n,\ r = 1, 2, \ldots, k\right\}$. Матрица смежности таких графов является циркулянтом. Эти графы также принято называть *циркулянтами* [8].

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

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

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

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 09–01–00070 и 11–01–00997) и интеграционного проекта СО РАН № 119.

Функциональным графом $G_{f,q}$ называется ориентированный граф, вершинами которого являются элементы из 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 [7].

Определённая выше дискретная динамическая система является моделью регуляторного контура генной сети, функционирование которого определяется сменой его состояний и полностью характеризуется структурой функционального графа преобразования $A_{f,q} : F_q^n \to F_q^n$. Метки вершин характеризуют уровень концентрации веществ (гены, белки и др.), сопоставляемых этим вершинам [2, 4, 10]. Подробнее о дискретных моделях генных сетей можно прочесть в [3, 5, 11, 12]. Заметим, что в отличие от [2, 4, 10], где функции в вершинах являются пороговыми, в настоящей работе исследуется случай линейных функций, зависящих от фиксированного числа переменных, определяемого степенями вершин графа сети, которым эти функции сопоставлены. Для циркулянтного графа $G_{n;d_1,d_2,\ldots,d_k}$ степени всех вершин сети равны k. Для характеризации функциональных графов сетей с линейными функциями в вершинах оказалось удобно использовать циклические коды и технику их порождения с помощью полиномов. Такой подход основывается на действии оператора $A_{f,q}$, определяемого с помощью рекурсивной схемы с линейными рекуррентными последовательностями, алгебраическая техника оперирования с которыми хорошо развита (см., например, [9]). Наш интерес к исследуемой модели, помимо указанного выше, объясняется и тем, что в этом случае удаётся глубже и полнее охарактеризовать динамику системы и структуру её функционального графа.

В статье исследуется структура функционального графа в случае, когда все функции f_i равны между собой и линейны. Таким образом, везде далее если $A_{f,q}(v_0, v_1, \ldots, v_{n-1}) = (u_0, u_1, \ldots, u_{n-1})$, то

$$u_i = v_{(i-d_1) \bmod n} + v_{(i-d_2) \bmod n} + \cdots + v_{(i-d_k) \bmod n}, \quad i = 0, 1, \ldots, n-1. \quad (1)$$

Линейное подпространство C векторного пространства F_q^n называется *циклическим кодом длины* n над F_q, если из $(v_0, v_1, \ldots, v_{n-1}) \in C$ следует $(v_1, \ldots, v_{n-1}, v_0) \in C$ [6].

Каждому набору $\widetilde{v} = (v_0, v_1, \ldots, v_{n-1})$ из F_q^n поставим в соответствие многочлен $v(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}$ из кольца многочленов $F_q[x]$

над полем F_q. Известно, что при таком соответствии действие отображения $A_{f,q}(\widetilde{v}) = \widetilde{u}$, определяемое линейной рекуррентностью (1), можно записать в следующем виде.

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

$$v(x)(x^{d_1} + x^{d_2} + \cdots + x^{d_k}) \equiv u(x) \pmod{x^n - 1}.$$

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

$$A(x) = A_{d_1,d_2,\ldots,d_k}(x) = x^{d_1} + x^{d_2} + \cdots + x^{d_k}.$$

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

Известно (см., например, [6]), что если $C \subseteq F_q^n$ является циклическим кодом, то соответствующее ему подпространство (обозначать будем той же буквой C) фактор-кольца $F_q[x]/(x^n - 1)$ является идеалом. Порождающий многочлен $g(x)$ этого идеала называют *порождающим* кода C. Тогда если $\deg g(x) = r$, то $C = \{g(x)f(x) \mid f(x) \in F_q[x],\ \deg f(x) < n - r\}$. 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 $F_q[x]/(x^n - 1)$.

Теорема 1. *Пусть $g(x)$ и $h(x)$ — порождающий и проверочный многочлены циклического кода C длины n соответственно. Тогда $g_1(x) = g(x)\gcd(A(x), h(x))$ для порождающего многочлена $g_1(x)$ циклического кода $C_1 = C \cdot A(x)$.*

Доказательство. Поскольку в фактор-кольце $F_q[x]/(x^n - 1)$ имеем $g(x)A(x) = \lambda(x) \in C_1$, для некоторого многочлена $\tau(x)$ в кольце $F_q[x]$ получаем

$$g(x)A(x) = \tau(x)(x^n - 1) + \lambda(x).$$

В правой части равенства оба слагаемых делятся на $g_1(x)$. Следовательно, $g(x)A(x)$ делится на $g_1(x)$.

С другой стороны, поскольку $g_1(x) \in C_1$, найдётся такой многочлен $c(x) \in C$, что в фактор-кольце $F_q[x]/(x^n - 1)$ имеем $c(x)g(x) = g_1(x)$. Тогда для некоторого многочлена $\nu(x)$ в кольце $F_q[x]$ верно равенство

$$c(x)g(x) = \nu(x)(x^n - 1) + g_1(x).$$

Но $c(x) = f(x)g(x)$, следовательно,

$$f(x)\frac{g(x)A(x)}{g_1(x)} - \nu(x)\frac{x^n-1}{g_1(x)} = 1.$$

Из последнего равенства имеем

$$\gcd\left(\frac{g(x)A(x)}{g_1(x)}, \frac{x^n-1}{g_1(x)}\right) = 1.$$

Следовательно, $g_1(x) = \gcd(g(x)A(x), x^n-1) = g(x)\gcd(A(x), h(x))$. Теорема 1 доказана.

Следствие 1. *Если $A(x)$ и $x^n - 1$ взаимно просты в кольце $F_q[x]$, то отображение $A_{f,q}$ обратимо и функциональный граф является дизъюнктным объединением простых контуров. Состояние $(1, 0, 0, \ldots, 0)$ принадлежит контуру наибольшей длины.*

Доказательство. Первая часть утверждения непосредственно следует из теоремы 1, поскольку $F_q[x]/(x^n-1)$ является циклическим кодом с порождающим многочленом $g(x) = 1$. Для доказательства второй части заметим, что если $g(x)A^l(x) = g(x)$ в $F_q[x]/(x^n-1)$, то и для любого $c(x) \in F_q[x]/(x^n-1)$ имеем

$$c(x)A^l(x) = f(x)g(x)A^l(x) = f(x)g(x) = c(x).$$

Следствие 1 доказано.

Пусть $\gcd(A(x), x^n - 1) \neq 1$. Рассмотрим последовательность циклических кодов $C_0 = F_q[x]/(x^n-1)$, 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

$$g_1(x) = \gcd(A(x), x^n-1), \quad h_1(x) = x^n - 1/g_1(x),$$

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

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

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

Теорема 2. *В функциональном графе $G_{f,q}$ 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, $1 \leqslant i \leqslant t-1$.*

Доказательство. Пусть при любом $i = 0, 1, \ldots t-1$ множество T_i состоит из вершин, достижимых за i тактов работы системы, но не достижимых за $i+1$ такт. Таким образом, имеем $T_i = A^i(t)C_0 \setminus A^{t+1}C_0$. Докажем индукцией по i, что $A^i(t)C_0 = C_i$. База очевидна. Пусть для некоторого i верно $C_i = A^i(t)C_0$. Тогда $A^{i+1}(t)C_0 = A(x)C_i$ — циклический код, порождающий многочлен которого по теореме 1 имеет вид $g(x) = g_i(x)\gcd(A(x), h_i(x))$. Остаётся заметить, что поскольку $h_i(x)$ делит $x^n - 1$, верно равенство

$$\gcd(A(x), h_i(x)) = \gcd(\gcd(A(x), x^n - 1), h_i(x)) = \gcd(g_1(x), h_i(x)).$$

Следовательно, при любом $i = 0, 1, \ldots, t-1$ множество T_i равно S_i. Наконец, если $\gcd(A(x), h_t(x)) = \gcd(g_1(x), h_t(x)) = 1$, то по теореме 1 имеем $A(x)C_t = C_t$, т. е. $S_t = C_t$, где C_t — множество вершин, принадлежащих контурам. Теорема 2 доказана.

Следствие 2. *Пусть $x^n - 1 = f_1^{m_1}(x) f_2^{m_2}(x) \ldots f_s^{m_s}(x)$ — разложение в $F_q[x]$ на неприводимые многочлены. Если для любого $i = 1, 2, \ldots, s$ многочлен $f_i(x)$ делит $A(x)$, то функциональный граф $G_{f,q}$ состоит из единственной компоненты связности, являющейся деревом с петлёй в корневой вершине* $(0, 0, \ldots, 0)$.

Доказательство. По теореме 2 множество вершин, принадлежащих контурам, образует циклический код C_t с порождающим многочленом $g_t(x) = x^n - 1$. Следовательно, C_t состоит из единственной вершины $(0, 0, \ldots, 0)$. Следствие 2 доказано.

Аналогично следствию 2 доказывается

Следствие 3. *Состояние $g_t(x)$ принадлежит контуру наибольшей длины в функциональном графе $G_{f,q}$.*

Теорема 3. *Для любого целого положительного l все вершины функционального графа, принадлежащие контурам длины, делящей l, образуют циклический код с проверочным многочленом* $\gcd(A^l(x) - 1, x^n - 1)$.

Доказательство. Многочлены $b(x)$, принадлежащие контурам длины, делящей l, удовлетворяют сравнению

$$b(x)A^l(x) \equiv b(x) \pmod{x^n - 1},$$

равносильному сравнению

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

которое, в свою очередь, равносильно сравнению

$$b(x)\,\mathrm{gcd}(A^l(x)-1, x^n-1) \equiv 0 \pmod{x^n-1}.$$

Последнее означает, что $b(x)$ принадлежит циклическому коду с проверочным многочленом $\mathrm{gcd}(A^l(x)-1, x^n-1)$. Теорема 3 доказана.

Следствие 4. *Неподвижные точки функционального графа $G_{f,q}$ образуют циклический код с проверочным многочленом* $\mathrm{gcd}(A(x)-1, x^n-1)$. *Если степень этого многочлена равна r, то число неподвижных точек равно q^r.*

Теорема 3 и следствие 4 непосредственно влекут

Следствие 5. *Наибольшая длина контура в функциональном графе равна минимальному l, для которого* $\mathrm{gcd}(A^l(x)-1, x^n-1) = h_t(x)$.

2. Случай $q = 2$

Везде далее $q = 2$. Рассмотрим модель $(6, 2, x+x^2)$. Поскольку $x^6-1 = (x+1)^2(x^2+x+1)^2$, по теореме 2 все вершины функционального графа, не являющиеся листьями, образуют циклический код C_1 с порождающим многочленом

$$g_1(x) = \mathrm{gcd}(x+x^2, x^6-1) = x+1,$$

т. е. являются булевыми наборами с чётным числом единиц. Также по теореме 2 имеем $t = 2$ и все наборы, принадлежащие контурам, образуют циклический код C_2 с порождающим и проверочным многочленами $g_2(x) = (x+1)^2$ и $h_2(x) = (x^2+x+1)^2$ соответственно.

По следствию 4 неподвижные точки образуют циклический код с проверочным многочленом

$$\mathrm{gcd}(A(x)-1, x^6-1) = x^2+x+1,$$

который состоит из многочленов $0,\ x^4+x^3+x+1,\ x^5+x^4+x^2+x,\ x^5+x^3+x^2+1$. По теореме 3 все вершины, принадлежащие контурам длины 1 и 2, образуют циклический код с проверочным многочленом

$$\mathrm{gcd}(A(x)^2-1, x^6-1) = (x^2+x+1)^2 = h_2(x).$$

Это код мощности 16, и, следовательно, в функциональном графе имеем 6 контуров длины 2. По следствию 5 граф не содержит контуров длины больше двух.

Таким образом, функциональный граф имеет десять компонент связности, четыре из которых содержат неподвижные точки, а шесть — контуры длины 2. Число вершин в этих компонентах равно соответственно четырём и восьми, а 32 набора с чётным числом единиц не являются листьями. На рис. 1 изображен функциональный граф модели $(6, 2, x+x^2)$. Двоичные наборы длины 6, соответствующие вершинам, записаны их десятичными представлениями.

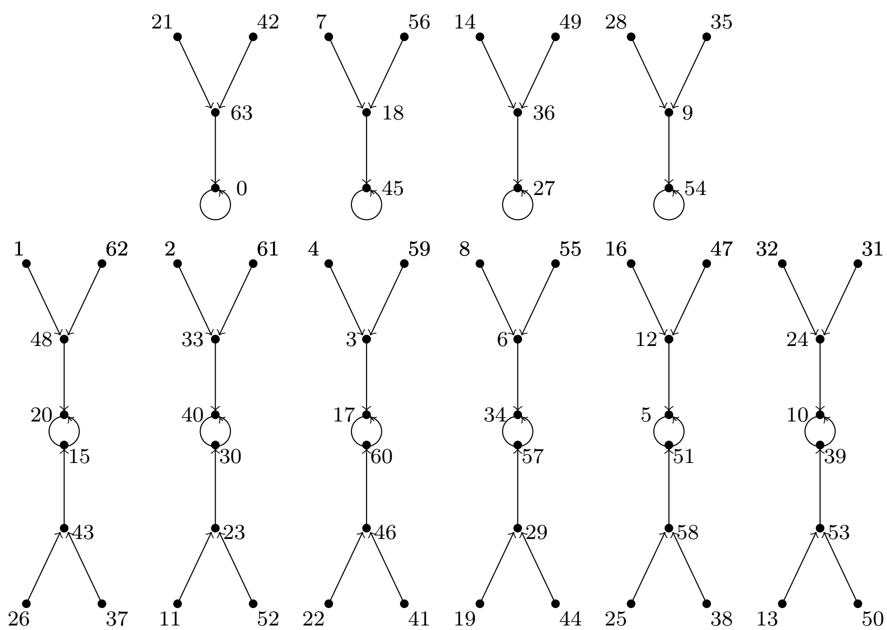

Рис. 1

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.*

Доказательство. Поскольку $x^{2n} - 1 = (x^n - 1)^2$ в поле характеристики 2, из теоремы 2 следует, что в модели $(2n, 2, A(x))$ многочлен $h_t^2(x)$ является проверочным для циклического кода, состоящего из наборов, принадлежащих контурам.

Пусть в модели $(2n, 2, A(x))$ наибольшая длина контура равна L. Тогда по следствию 5 L — минимальное число такое, что

$$\gcd(A^L(x)-1,(x^n-1)^2)=h_t^2(x).$$

Очевидно, что $L \leqslant 2l$. Заметим, что если набор $q(x)$ в модели $(n,2,A(x))$ принадлежит контуру длины l, то $q(x)+x^nq(x)$ в модели $(2n,2,A(x))$ также принадлежит контуру длины l. Следовательно, l делит L. Таким образом, либо $L=2l$, либо $L=l$, причём второе равенство справедливо тогда и только тогда, когда

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

Поскольку $x^n-1=h_t(x)g_t(x)$, равенство (2) имеет место тогда и только тогда, когда существует многочлен $a(x)\in F_2[x]$ такой, что

$$A^l(x)-1=h_t^2(x)a(x), \tag{3}$$
$$\gcd\big(a(x),g_t^2(x)\big)=1. \tag{4}$$

Поскольку наибольшая длина контура в модели $(n,2,A(x))$ равна l, по следствию 5 имеем

$$\gcd(h_t(x)a(x),g_t(x))=1,$$

и, следовательно, равенство (4) выполнено. Таким образом, $L=l$ тогда и только тогда, когда выполнено равенство (3). Теорема 4 доказана.

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 $2l$.*

Доказательство. Если в модели $(2n,2,A(x))$ наибольшая длина контура равна l, то по теореме 4 $h_t^2(x)$ делит $A^l(x)-1$. Поскольку l чётно, $h_t(x)$ делит $A^{l/2}(x)-1$; противоречие следствию 5. Следствие 6 доказано.

Заметим, что в модели $(2,2,1+x+x^2)$ наибольшая длина контура равна 2. По следствию 6 индукцией по r получаем, что в модели $(2^r,2,1+x+x^2)$ наибольшая длина контура равна 2^r.

Рассмотрим более подробно модель $(n,2,x+1)$. Функциональный граф такой модели рассматривался в [1], а в частном случае $n=2^m$ — в [13].

Теорема 5. *Для любого нечётного n наибольшая длина контура функционального графа модели $(n,2,1+x)$ является делителем числа 2^r-1, где $r=\min\{j\mid j>0,\ 2^j\equiv 1 \pmod n\}$.*

Доказательство. Пусть $x^n - 1 = f_1(x)f_2(x)\dots f_s(x)$ — разложение в $F_2[x]$ на неприводимые многочлены. Пусть $f_i(x)$ имеет степень r_i, $1 \leqslant i \leqslant s$. Известно (см., например, [6]), что $r = \text{НОК}(r_1, r_2, \dots, r_s)$. Пусть без ограничения общности $f_1(x) = x + 1$. Поскольку n нечётно, для рассматриваемой модели $t = 1$, $g_1(x) = A(x) = x + 1$, $h_1(x) = f_2(x)f_3(x)\dots f_s(x)$.

Известно [6], что многочлен $y^{2^r} + y$ равен произведению всех неприводимых над $GF(2)$ многочленов, степени которых делят r. Следовательно, $y^{2^r-1} + 1$ делится на многочлен $f_2(y+1)f_3(y+1)\dots f_s(y+1)$. Делая подстановку $y = x+1$, получаем, что $(x+1)^{2^r-1} + 1$ делится на $h_1(x)$. Тогда по следствию 5 наибольшая длина контура делит число $2^r - 1$. Теорема 5 доказана.

Следствие 7. *При любых $k \geqslant 2$, $m \geqslant 0$ для $n = 2^m(2^k - 1)$ наибольшая длина контура функционального графа модели $(n, 2, 1+x)$ равна n.*

Доказательство. Рассмотрим модель $(2^k - 1, 2, 1 + x)$. Пусть наибольшая длина контура для этой модели равна l. Поскольку

$$k = \min\{j \mid j > 0,\ 2^j \equiv 1 \pmod{2^k - 1}\},$$

l делит $2^k - 1$ по теореме 5. В этой модели $t = 1$, $g_1(x) = A(x) = x + 1$ и $h_1(x) = x^{2^k-2} + x^{2^k-3} + \dots + x + 1$. По следствию 4 набор $x+1$ принадлежит контуру длины l, следовательно,

$$(x+1)A^l(x) \equiv x + 1 \pmod{x^{2^k-1} - 1}.$$

Тем самым $h_1(x)$ делит многочлен $(x+1)^l + 1$, что возможно только при $l \geqslant 2^k - 2$. Таким образом, $l = 2^k - 1$. В модели $(2(2^k - 1), 1 + x)$ наибольшая длина контура равна $2l$ по теореме 4. Тогда из следствия 6 получаем искомое утверждение для произвольного m. Следствие 7 доказано.

ЛИТЕРАТУРА

1. **Арнольд В. И.** Топология и статистика формул арифметики // Успехи мат. наук. — 2003. — Т. 58, № 4. — С. 3–28.
2. **Григоренко Е. Д., Евдокимов А. А., Лихошвай В. А., Лобарева И. А.** Неподвижные точки и циклы автоматных отображений, моделирующих функционирование генных сетей // Вестн. ТГУ. — 2005. — № 14. — С. 206–212.
3. **Демиденко Г. В., Колчанов Н. А., Лихошвай В. А., Матушкин Ю. Г., Фадеев С. И.** Математическое моделирование регулярных контуров генных сетей // Журн. вычисл. математики и мат. физики. — 2004. — Т. 44, № 12. — С. 2276–2295.

4. **Евдокимов А. А., Лиховидова Е. О.** Дискретная модель генной сети циркулянтного типа с пороговыми функциями // Вестн. ТГУ. Управление, вычислительная техника и информатика. — 2008 — № 2. — С. 18–21.
5. **Лихошвай В. А., Голубятников В. П., Демиденко Г. В., Евдокимов А. А., Матвеева И. И., Фадеев С. И.** Теория генных сетей // Системная компьютерная биология. — Новосибирск: Изд-во СО РАН, 2008. — С. 397–480.
6. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. — М.: Связь, 1979. — 744 с.
7. **Оре О.** Теория графов. — М.: Наука, 1980. — 336 с.
8. **Харари Ф.** Теория графов. — М: УРСС, 2003. — 300 с.
9. **Цирлер Н.** Линейные возвратные последовательности // Кибернет. сб. — 1963. — № 6. — С. 55–79.
10. **Evdokimov A. A., Kutumova E. O.** The discrete model of the gene networks regulatory loops with the threshold functions // Proc. 7th Int. Conf. on bioinformatics of genom regulation and structure (Novosibirsk, June 20–27, 2010). — Novosibirsk: SB RAS, 2010. — P. 155.
11. **Kauffman S. A., Smith R. G.** Adaptive automata based on Darwinian selection // Physica D. — 1986. — Vol. 22, N 1–3. — P. 68–82.
12. **Kauffman S. A.** At home in the universe: the search for the laws of self-organization and complexity. — New York: Oxford Univ. Press, 1995. — 321 p.
13. **Merekin Yu. V.** On the computational complexity of the Arnold complexity of binary words // Asian–Eur. J. Math. — 2009. — Vol. 2, N 4. — P. 641–648.

Евдокимов Александр Андреевич,
e-mail: evdok@math.nsc.ru

Пережогин Алексей Львович,
e-mail: pereal@math.nsc.ru

Статья поступила
24 декабря 2010 г.

Переработанный вариант —
11 февраля 2011 г.