О периодичности в автономных автоматах

В. А. Носов

В статье приводятся общие конструкции, позволяющие гарантировать отсутствие эквивалентных состояний в автономных ячеечных автоматах, длину периодов последовательностей состояний, заданную степень нелинейности координатных функций и индекс линейности функции переходов.

1°. Всюду под термином автомат будем понимать автономный автомат $A(X, Y, \phi, f)$, где X — множество состояний автомата, Y — множество выходных символов, ϕ — функция переходов, f — функция выходов. Функционирование автомата определяется в дискретном времени следующими соотношениями:

$$\begin{aligned} x(t+1) &= \phi(x(t)), \quad t = 0, 1, \dots \\ y(t) &= f(x(t)), \end{aligned} \tag{1}$$

где $x(t)$, $y(t)$ — состояние автомата и выходной символ в такте t, соответственно.

В процессе функционирования автомата для начального состояния x_0 определены две последовательности состояний

$$x_s = \phi^s(x_0), \quad s = 0, 1, \dots, \tag{2}$$

и выходных символов

$$y_s = f(x_s), \quad s = 0, 1, \dots. \tag{3}$$

Будем рассматривать только регулярные автоматы, то есть автоматы, у которых функция ϕ является биективной. В этом случае обе

последовательности (2), (3) будут периодическими для любого начального состояния x_0; при этом, если T и R — периоды последовательностей (2) и (3), то R делит T.

Нашей задачей будет установление связей между периодами состояний и периодами выходов определенных классов автоматов. Для практических приложений важным является установить, имеет ли место случай $R < T$. Другой важной задачей является установление связи с известной задачей минимизации автомата, которая, в свою очередь, равносильна задаче определения классов эквивалентных состояний.

2°. Всюду в дальнейшем будем считать, что автомат $A(X, Y, \phi, f)$ обладает одноцикловой структурой, то есть период последовательности состояний (2) совпадает с мощностью множества состояний X. Положим $|X| = T$. В этом случае порядок отображения ϕ (в групповом смысле) равен T.

Обозначим через $G(\phi)$ циклическую группу порядка T, порожденную функцией перехода ϕ. Пусть $J(f)$ — группа инерции функции выхода f, то есть множество биективных отображений g множества X на себя, относительно которых функция f инвариантна, то есть справедливы соотношения для всех $x \in X$:

$$f(x) = f(gx). \tag{4}$$

Справедлива

Теорема 1. *Пусть автомат $A(X, Y, \phi, f)$ обладает одноцикловой структурой и $|X| = T$. Тогда выполнено:*

a) Если R — период выходной последовательности, то $\phi^R \in J(f)$;

b) R — наименьший делитель T, такой, что $\phi^R \in J(f)$.

Доказательство. Если $\phi^l \in J(f)$ для некоторого l, то $\phi^k \in J(f)$ для некоторого k, где $k|T$, так как из $\phi^l \in J(f)$ следует $G(\phi^l) \subset J(f)$. Но $G(\phi^l) = G(\phi^{(l,T)})$, где (l, T) — наибольший общий делитель l, T. Значит, можно ограничиться степенями ϕ^k, где $k|T$.

Пусть имеем соотношение $\phi^k \in J(f)$ и $k|T$. Тогда для любого $x \in X$ имеем

$$f(\phi^k x) = f(x). \tag{5}$$

Рассмотрим произвольное x_0 в качестве начального состояния и образуем последовательность

$$x_s = \phi^s(x_0), \quad s = 0, 1, \ldots.$$

Из (5) получаем

$$f(\phi^k x_s) = f(x_s) \quad \text{или} \quad f(\phi^k \phi^s x_0) = f(\phi^s x_0). \tag{6}$$

Отсюда получаем $y_{s+k} = y_s$, $s = 0, 1, \ldots$, и, значит, k кратно периоду выходной последовательности R, то есть $k = R \cdot i$.

Пусть теперь R — период выходной последовательности. Тогда имеем

$$y_{s+R} = y_s, \quad s = 0, 1, \ldots$$

или

$$f(\phi^{s+R} x_0) = f(\phi^s x_0), \quad s = 0, 1, \ldots.$$

В силу полноцикловости ϕ для любого x_0 последовательность $\phi^s(x_0)$ пробегает все множество X; значит, $f(\phi^R x) = f(x)$ для всех $x \in X$. Отсюда $\phi^R \in J(f)$.

Пусть теперь R — не наименьший делитель T, что выполнено $\phi^R \in J(f)$. Это значит, что существует k — делитель T, такой, что $\phi^k \in J(f)$ и $k < R$. Согласно установленному, из $\phi^k \in J(f)$ следует, что k кратно R, то есть $k \geqslant R$, что противоречит допущению.

Следствие 1. *Пусть автомат $A(X, Y, \phi, f)$ обладает одноцикловой структурой. Тогда имеет место сокращение периода ($R < T$) в том и только том случае, когда функция выхода f имеет нетривиальную группу инерции в группе $G(\phi)$.*

Доказательство. Действительно, период выхода R равен минимальному делителю $T = |X|$, такому, что $\phi^R \in J(f)$. Ясно, что $\phi^R \neq e$ тогда и только тогда, когда $R < T$.

3°. Рассмотрим вопрос нахождения преобразований множества состояний, которые не меняют выходов автомата для случая полноциклового автомата.

Определение 1. Биекция $\omega : X \to X$ множества состояний в себя автомата $A(X, Y, \phi, f)$ называется автоморфизмом автомата, если выполняются соотношения:

$$f(\phi^s x) = f(\phi^s \omega x) \quad \text{для всех} \quad s = 0, 1, \ldots, \ x \in X. \tag{7}$$

Ясно, что автоморфизмы автомата образуют группу, называемую группой автоморфизмов.

Напомним, что состояния x'_0 и x''_0 автомата $A(X, Y, \phi, f)$ называются эквивалентными, если они производят одинаковые выходные последовательности, то есть

$$f(\phi^s x'_0) = f(\phi^s x''_0) \quad \text{при всех} \quad s = 0, 1, \ldots. \tag{8}$$

Пусть ω — автоморфизм автомата A. Тогда согласно определению состояния x и ωx эквивалентны для любого $x \in X$. Обратно, если ω такая биекция X в себя, что для любого $x \in X$ состояния x и ωx эквивалентны, то ω — автоморфизм автомата. Значит, задача определения группы автоморфизмов равносильна задаче классификации эквивалентных состояний.

Теорема 2. *Пусть $A(X, Y, \phi, f)$ — произвольный одноцикловый автомат. Пусть R — период выходных символов. Тогда эквивалентные состояния образуют области транзитивности группы $G(\phi^R)$. При этом число классов эквивалентности равно $[G(\phi) : G(\phi^R)]$ — индексу группы $G(\phi^R)$ в группе $G(\phi)$ и равно R, а каждый класс эквивалентности содержит по $[G(\phi^R) : 1] = \frac{T}{R}$ состояний.*

Доказательство. Пусть состояния x'_0 и x''_0 эквивалентны. Тогда имеем по определению

$$f(\phi^s(x'_0)) = f(\phi^s(x''_0)), \quad s = 0, 1, \ldots.$$

Поскольку автомат $A(X, Y, \phi, f)$ полноцикловый, то существует k, такое, что $x''_0 = \phi^k x'_0$. Следовательно, выполнено соотношение

$$y_s = f(\phi^s(x'_0)) = f(\phi^s(\phi^k x'_0)) = y_{s+k}, \quad s = 0, 1, \ldots.$$

Отсюда следует, что k кратно периоду выхода R, то есть $k = k_1 \cdot R$ и, следовательно, $x_0'' = (\phi^R)^{k_1} x_0'$.

Обратно, пусть x_0' и x_0'' таковы, что $x_0'' = \phi^{k_1 R} x_0'$ для некоторого k_1. Тогда x_0' и x_0'' будут эквивалентны, так как

$$y_s'' = f(\phi^s x_0'') = f(\phi^s \phi^{k_1 R} x_0') = f(\phi^{k_1 R} \phi^s x_0') = f(\phi^s x_0') = y_s'.$$

Значит, эквивалентные состояния получаются одно из другого с помощью преобразования из группы $G(\phi^R)$. Отсюда получаем, что число состояний в классе эквивалентности равно $[G(\phi^R) : 1]$ — порядку группы $G(\phi^R)$, то есть $\frac{T}{R}$, $T = |X|$, а число классов эквивалентности равно $[G(\phi) : G(\phi^R)]$ — индексу группы $G(\phi^R)$ и равно R.

Следствие 2. *Полноцикловый автомат $A(X, Y, \phi, f)$ имеет эквивалентные состояния тогда и только тогда, когда имеет место сокращение периода выходных символов.*

Следствие 3. *Группа автоморфизмов полноциклового автомата $A(X, Y, \phi, f)$ есть прямое произведение групп подстановок классов эквивалентных состояний и имеет порядок*

$$\left(\frac{T}{R}!\right)^R, \quad T = |X|, \quad R \ - \text{период выходов.} \tag{9}$$

Следствие 4. *Минимальный автомат $\bar{A}(\bar{X}, \bar{Y}, \bar{\phi}, \bar{f})$ для одноциклового автомата $A(X, Y, \phi, f)$ имеет R состояний, где R — период выходных символов.*

4°. Специализируем теперь рассматриваемые автоматы, чтобы облегчить получение информации о группе инерции функции выхода f.

Определение 2. Автомат $A(X, Y, \phi, f)$ будем называть ячеечным, если $X = E_n^m$, то есть множество состояний есть множество n-мерных наборов $(x_1, \ldots, x_n)$, где $x_i \in [0, 1, \ldots, m-1]$, $i \in \overline{1, n}$. При этом $|X| = m^n$.

Теорема 3. *Пусть ячеечный автомат $A(E_n^m, Y, \phi, f)$ полноцикловый. Тогда функция выхода f имеет нетривиальную группу инерции в группе $G(\phi)$ тогда и только тогда, когда f имеет нетривиальную группу инерции в группе $G\left(\phi^{m^{n-1}}\right)$.*

Доказательство. Пусть f имеет нетривиальную группу инерции в группе $G(\phi)$, то есть существует R, что $\phi^R \in J(f)$, $\phi^R \neq e$. Согласно замечанию в доказательстве Теоремы 1 считаем, что $R|m^n$, $R < m^n$.

Поскольку R делит m^n, то $R = s_1 \dots s_n$, где s_i — делитель m, $1 \leqslant s_i \leqslant m$. Из того, что $R < m^n$ следует существование номера i, такого, что $s_i < m$. Пусть для определенности $s_1 < m$. Обозначим $P_i = \frac{m}{s_i}$, $i = \overline{1,n}$. Тогда R делит число $s_1 \cdot s_2 \cdot \dots \cdot s_n \cdot p_2 \cdot \dots \cdot p_n = s_1 \cdot m^{n-1}$, где $1 \leqslant s_1 \leqslant m$.

Если теперь $\phi^R \in J(f)$, то и $\phi^{R \cdot t} \in J(f)$ для любых целых t. Согласно доказанному, существует t, такое, что $R \cdot t = m^{n-1} \cdot k$, $1 \leqslant k < m$. Значит, $\phi^{m^{n-1} \cdot k} = \left(\phi^{m^{n-1}}\right)^k \in J(f)$. При этом $\phi^{m^{n-1} \cdot k} \neq e$, так как порядок ϕ равен m^n.

Обратное утверждение очевидно.

Следствие 5. *Для полноциклового ячеечного автомата $A(E_n^m, Y, \phi, f)$ период выхода сокращается тогда и только тогда, когда функция выхода f имеет нетривиальную группу инерции в группе $G\left(\phi^{m^{n-1}}\right)$.*

Замечание 1. Если m — простое число, то f имеет нетривиальную группу инерции в группе $G\left(\phi^{m^{n-1}}\right)$ тогда и только тогда, когда $\phi^{m^{n-1}} \in J(f)$, то есть $f(x) = f\left(\phi^{m^{n-1}} x\right)$ для всех $x \in X$.

Определение 3. Функция f на множестве E_n^m называется равномерной, если существует $d|m$, $d > 1$, такое, что каждое значение функции принимается кратное d число раз.

Теорема 4. *Если функция выходов f полноциклового ячеечного автомата $A(E_n^m, Y, \phi, f)$ не является равномерной, то группа инерции f в группе $G(\phi)$ тривиальна. Если функция выходов f является равномерной, то существует ϕ, такое, что f имеет нетривиальную группу инерции в группе $G(\phi)$.*

Доказательство. Пусть f имеет нетривиальную группу инерции в $G(\phi)$. Тогда по предыдущему f имеет нетривиальную группу инерции в $G\left(\phi^{m^{n-1}}\right)$. Значит, существует k, $1 \leqslant k < m$, $k|m$, такое, что

$\phi^{m^{n-1}\cdot k} \in J(f)$ или $f(x) = f\left(\phi^{m^{n-1}\cdot k}(x)\right)$ для всех $x \in E_n^m$. Тогда значения $f(x)$ совпадают в $d = \frac{m}{k} > 1$ точках, то есть функция f — равномерная.

Пусть f — равномерная функция. Значит, существует $d|m$, $d > 1$, что значения f принимаются кратное d число раз. Рассмотрим подстановку S множества E_n^m, которая состоит из $\frac{m^n}{d}$ циклов длины d и в состав каждого цикла входят только элементы E_n^m, на которых f принимает одинаковые значения. Согласно предположению о равномерности f такая подстановка S существует.

Теперь рассмотрим подстановку ϕ множества E_n^m, определенную равенством $\phi = \sqrt[m^{n-1}\cdot k]{S}$ ($\phi^{m^{n-1}\cdot k} = S$), где $k = \frac{m}{d}$. Ясно, что ϕ — полноцикловая подстановка множества E_n^m. Имеем по построению $\phi^{m^{n-1}\cdot k} \in J(f)$, так как значения f совпадают на циклах подстановки $\phi^{m^{n-1}\cdot k}$.

5°. Рассмотрим сначала ячеечные автоматы при $m = 2$. В этом случае функция переходов ϕ задается семейством булевых функций $\phi = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$ от n переменных. Пусть ϕ имеет «треугольный» тип, то есть

$$\begin{aligned} f_1 &= f_1(x_1) \\ f_2 &= f_2(x_1, x_2) \\ &\ldots \\ f_n &= f_n(x_1, \ldots, x_n). \end{aligned} \tag{10}$$

Индукцией по n легко доказывается ([3])

Теорема 5. *Отображение ϕ вида* (10) *биективно тогда и только тогда, когда оно представляется в виде*

$$\begin{aligned} y_1 &= x_1 + h_1 \\ y_2 &= x_2 + h_2(x_1) \\ &\ldots \\ y_n &= x_n + h_n(x_1, \ldots, x_{n-1}) \end{aligned} \tag{11}$$

(h_1 — константа).

Теорема 6. *Отображение ϕ вида (13) является полноцикловым тогда и только тогда, когда $h_1 = 1$ и вес функций $h_2, \dots, h_n$ нечетен.*

Доказательство легко осуществляется индукцией по n.

Следствие 6. *Пусть ϕ — полноцикловое преобразование вида* (11). *Тогда $\phi^{2^{m-1}}(x_1 \dots x_n) = (x_1 \dots x_{n-1}\bar{x}_n)$.*

Следствие 7. *Пусть $A(E_n^m, Y, \phi, f)$ — полноцикловый ячеечный автомат с функцией перехода вида* (11). *Тогда период выходов сокращается (существуют эквивалентные состояния) тогда и только тогда, когда функция выхода $f(x_1, \dots, x_n)$ зависит от x_n не существенно. (В этом случае период выхода R равен 2^i, где i — максимальный номер существенного переменного функции выхода $f(x_1, \dots, x_n)$.)*

Пусть теперь m — произвольное натуральное число. В этом случае функция переходов ϕ задается семейством (f_i), $i \in \overline{1,n}$, функций m-значной логики. Пусть семейство (f_i), $i \in \overline{1,n}$, может быть представлено в виде (11) (как функции m-значной логики).

Теорема 7. *Отображение ϕ множества E_n^m в себя вида* (11) *является полноцикловым тогда и только тогда, когда выполнены условия: $(h_1, m) = 1$, $(|h_2|, m) = 1$, $\dots$, $(|h_n|, m) = 1$, где $|h_i| = \sum_{x_1,\dots,x_{i-1}} h_i(x_1, \dots, x_{i-1})$ (сумма натуральных чисел по модулю m).*

Доказательство аналогично Теореме 6.

Следствие 8. *В условиях Теоремы 7 справедливо*

$$\phi^{m^{n-1}}(x_1, \dots, x_n) = (x_1, \dots, x_{n-1}, x_n + |h_n|).$$

Для некоторых случаев функций m-значной логики данный результат можно упростить.

Представление функций m-значной логики вида (11) будем называть псевдобулевым, если существуют константы a, b из $\{0, 1, \dots, m-1\}$, булевы функции $g_2, \dots, g_n$, функции $p_1, \dots, p_{n-1}$, где

$p_i : \{0,1,\dots,m-1\} \to \{0,1\}$, $i \in [1,n-1]$, такие, что выполнены равенства:

$$\begin{aligned} h_2(x_1) &= a + (b-a)g_2(p_1(x_1)) \\ h_3(x_1,x_2) &= a + (b-a)g_3(p_1(x_1),p_2(x_2)) \\ &\dots \\ h_n(x_1,\dots,x_{n-1}) &= a + (b-a)g_n(p_1(x_1),\dots,p_{n-1}(x_{n-1})). \end{aligned} \tag{12}$$

Теорема 8. *Пусть отображение ϕ множества E_n^m в себя имеет вид* (11) *и выполнено псевдобулево представление* (12). *Тогда ϕ является полноцикловым в том и только том случае, когда выполнены условия:* $(h_1,m) = 1$, $((b-a),m) = 1$, $(q_1,m) = 1$, $\dots$, $(q_{n-1},m) = 1$, $(C(g_2),m) = 1$, $\dots$, $(C(g_n),m) = 1$, *где* $q_i = \left|\left\{p_i^{-1}(1)\right\}\right|$, $i = \overline{1,n-1}$, $C(g_i)$ — *коэффициент Фурье функции* g_i, $i = \overline{2,n}$, *определяемый равенством* $C(g(x_1,\dots,x_n)) = \sum_{x_1,\dots,x_n}(-1)^{N(x_1,\dots,x_n)}$. $g(x_1,\dots,x_n)$ *(сумма действительная,* $N(x_1,\dots,x_n)$ — *число нулей в наборе* $(x_1,\dots,x_n)$*).*

Доказательство осуществляется индукцией по n.

Следствие 9. *В условиях Теоремы 8 справедливо*

$$\phi^{m^{n-1}}(x_1,\dots,x_n) = (x_1,\dots,x_{n-1},x_n + (b-a)q_1\dots q_{n-1}C(g_n)).$$

Таким образом, предложен класс преобразований, для которых эффективно решается вопрос о сокращении периода выхода и о наличии эквивалентных состояний в полноцикловом автомате.

Замечание 2. Для вычисления коэффициентов Фурье существуют эффективные алгоритмы, основанные на быстром преобразовании Фурье.

Замечание 3. Использованное свойство отображения ϕ, для которого $\phi^{m^{n-1}}(x_1,\dots,x_n) = (x_1,\dots,x_{n-1},x_n + c)$ может выполняться не только у полноцикловых преобразований треугольного вида. Рассмотрим отображение $\phi : E_3 \to E_3$ вида

$$\begin{aligned} f_1 &= x_2 \\ f_2 &= x_1 + 1 \\ f_3 &= x_1 + x_2 + x_3 + x_1x_2. \end{aligned} \tag{13}$$

Данное преобразование полноцикловое и выполнено $\phi^4(x_1, x_2, x_3) = (x_1, x_2, \bar{x}_3)$ для всех (x_1, x_2, x_3).

6°. Рассмотрим вопрос о сложности рассмотренных задач для булевских автоматов, то есть множества состояний и выходов кодируются двоичными наборами, а функции переходов и выходов задаются двоичными функциями. Как обычно, проблему называем NP-трудной, если из существования для нее разрешающего алгоритма полиномиальной сложности следует P=NP и NP-полной, если при этом она принадлежит классу NP. Для проблем Π_1, Π_2 мы пишем $\Pi_1 \leqslant \Pi_2$ если из полиномиальной разрешимости Π_2 следует полиномиальная разрешимость Π_1. В целях избежания неоднозначности толкования все задачи приводятся в единой стандартной форме.

1) Регулярность семейства булевских функций.
   Дано: Семейство из n булевских функций $\phi = (f_1, \ldots, f_n)$ от n переменных $x_1, \ldots, x_n$, каждая из которых задана в КНФ.
   Вопрос: Верно ли, что ϕ задает биекцию множества E_n?
2) Полноцикловость булевского отображения.
   Дано: Биективное булевское отображение $\phi : E_n \to E_n$, заданное семейством формул $\phi = (f_i)$, $i = \overline{1, n}$, в базисе $(+, \vee, \cdot, -)$.
   Вопрос: Верно ли, что ϕ является полноцикловым?
3) Существование эквивалентных состояний полноциклового булевского автомата.
   Дано: Автономный автомат $A(E_n^m, E_1, \phi, f)$, где ϕ — полноцикловое отображение E_n в себя, заданное семейством n булевых функций (f_i), $i = \overline{1, n}$, f — булева функция n переменных. Все функции заданы формулами в базисе $(+, \vee, \cdot, -)$.
   Вопрос: Верно ли, что автомат A имеет эквивалентные состояния?

Теорема 9. *Задачи 1)–3) являются NP-трудными.*

Доказательство. Пусть $f(x_1, \ldots, x_n)$ — произвольная индивидуальная задача «выполнимость КНФ». Образуем функцию

$$f^*(x_0, x_1, \ldots, x_n) = \bar{x}_0 f(x_1, \ldots, x_n) \vee x_0,$$

где x_0 — новое переменное. Функция f^* строится по функции f за полиномиальное время от длины задания f.

Рассмотрим отображение $\phi : E_{n+1} \to E_{n+1}$ вида

$$(x_0, x_1, \ldots, x_n) \to (f^*(x_0, x_1, \ldots, x_n), x_1, \ldots, x_n). \tag{14}$$

Отображение ϕ регулярно тогда и только тогда, когда функция $f(x_1, \ldots, x_n) \equiv 0$ (то есть задача не выполнима).

Действительно, рассмотрим два произвольные набора x'_0 и x''_0 из E_{n+1}. Если они различаются на координатах $x_1, \ldots, x_n$, то их образы при отображении ϕ различны. Если же $x'_1 = x''_1$, $\ldots$, $x'_n = x''_n$, то $f^*(x'_0, x'_1, \ldots, x'_n) = f^*(x''_0, x''_1, \ldots, x''_n)$, если $f(x'_1, \ldots, x'_n) = 1$ и $f^*(x_0, x'_1, \ldots, x'_n) \neq f^*(\bar{x}_0, x'_1, \ldots, x'_n)$, если $f(x'_1, \ldots, x'_n) = 0$. Если существует полиномиальный алгоритм проверки регулярности булевского отображения, то, применяя его к отображению (14), получаем полиномиальный алгоритм решения задачи «выполнимость». Поскольку задача «выполнимость» NP-полна, получаем противоречие.

Доказательство NP-трудности задач 2,3 аналогично.

В работе [4] представлен ряд NP-трудных задач теории автоматов, которые относятся к определению эквивалентных состояний, установлению цикловых структур и связи периодов состояний и выходов.

7°. Будем характеризовать функции переходов регулярных автоматов возможностью их включения (или их степеней) в группы преобразований множества состояний. Пусть $\delta : S \to S$ — регулярное (подстановочное) преобразование множества S. Пусть G — некоторая группа преобразований множества S.

Определение 4. Индексом преобразования δ относительно G будем называть минимальное натуральное число k, такое, что выполнено включение $\delta^k \in G$.

Обозначим индекс δ относительно G через $\operatorname{ind}_G \delta$. Ясно, что $\operatorname{ind}_G \delta$ делит $\operatorname{ord} G$ — порядок элемента δ. Легко устанавливается

Теорема 10. *Для любых двух групп преобразований G_1, G_2, таких, что $G_2 \subseteq G_1$, выполнено* $\operatorname{ind}_{G_1} \delta \,|\, \operatorname{ind}_{G_2} \delta$.

Доказательство. Ясно, что $\operatorname{ind}_{G_1} \delta \leqslant \operatorname{ind}_{G_2} \delta$. Представим $\operatorname{ind}_{G_2} \delta$ в виде $\operatorname{ind}_{G_2} \delta = \operatorname{ind}_{G_1} \delta \cdot p + q$, где $0 \leqslant q < \operatorname{ind}_{G_1} \delta$. Тогда имеем $\delta^{\operatorname{ind}_{G_2} \delta} =$

$\left(\delta^{\operatorname{ind}_{G_1}\delta}\right)\cdot\delta^q$. Отсюда следует, что $\delta^q\in G_1$. Поскольку $0\leqslant q<\operatorname{ind}_{G_1}\delta$, то $q=0$.

Аналогично устанавливается

Теорема 11. *Справедливо равенство*

$$\operatorname{ind}_G\delta=\operatorname{ord}\delta/\operatorname{ord}\delta^{\operatorname{ind}_G\delta}. \tag{15}$$

Определение 5. Преобразование δ назовем несовместимым с группой G, если $\operatorname{ind}_G\delta=\operatorname{ord}\delta$.

В качестве примера приложения данных понятий рассмотрим полноцикловое преобразование из п. 5° множества E_n вида

$$\begin{aligned}x_1'&=x_1+1\\x_2'&=x_2+\phi_2(x_1)\\&\dots\\x_n'&=x_n+\phi_n(x_1,\dots,x_{n-1}).\end{aligned}$$

Рассмотрим две группы преобразований E_n:

GL_n — группа линейных преобразований и Σ_n — группа отрицаний переменных. Легко видеть, что $\operatorname{ind}_{GL_n}\delta=2^n$, $\operatorname{ind}_{\Sigma_n}\delta=2^{n-1}$.

Заметим, что если длины всех циклов преобразования δ ограничены снизу величиной k, то выполнено $\operatorname{ind}_{GL_n}\delta\geqslant k$.

8°. С целью применения предыдущих результатов приведем конструкцию, позволяющую оценивать периоды регулярных преобразований снизу и тем самым оценивать снизу индекс регулярных преобразований. Будем рассматривать преобразования множества E_n^m, соответствующего состояниям ячеечного автомата. Укажем способ вычисления цикловой структуры преобразования треугольного вида

$$\delta:\quad\begin{aligned}x_1&+a_1\\x_2&+f_2(x_1)\\&\dots\\x_n&+f_n(x_1,\dots,x_{n-1}).\end{aligned}$$

Цикловую структуру Σ_n преобразования δ определим по индукции. Для $n=1$ Σ_1 состоит из m циклов длины 1 при $a_1=0$ и

(m, a_1) циклов длины $m/(m, a_1)$. Пусть для n структура Σ_n определена. Тогда Σ_{n+1} определяется так: для всякого l берем циклы длины l. Пусть это $C_1, \ldots, C_N$. Пусть $a_1, \ldots, a_N$ — веса функции $f_{n+1}(x_1, \ldots, x_n)$ на данных циклах. Вес функции f_{n+1} на цикле C_i есть $\sum_{x_1,\ldots,x_n} f(x_1, \ldots, x_n)$ (сумма в $\mathbb{Z}_m$). Тогда в Σ_{n+1} каждому циклу $(x_1, \ldots, x_n) \in C_i$ соответствует (a_i, m) циклов длины $(m/(a_i, m)) \cdot l$. Соответственно, N циклам длины l соответствует $(a_1, m) + \cdots + (a_N, m)$ циклов длин $(m/(a_1, m)) \cdot l$, $\ldots$, $(m/(a_N, m)) \cdot l$.

В [6] дан способ вычисления цикловой структуры прямого произведения отображений.

Рассмотрим преобразование множества E_n^m вида

$$\delta: \quad \begin{aligned} x_1' &= x_1 + f_1(x_1, \ldots, x_n) \\ &\ldots \\ x_n' &= x_n + f_n(x_1, \ldots, x_n). \end{aligned} \tag{16}$$

Предположим, что $f_1, \ldots, f_n$ — правильное семейство функций m-значной логики (см. [7]).

В этом случае преобразование E_n^m вида

$$\begin{aligned} x_1' &= x_1 + f_1(\phi_1(x_1), \ldots, \phi_n(x_n)) \\ &\ldots \\ x_n' &= x_n + f_n(\phi_1(x_1), \ldots, \phi_n(x_n)). \end{aligned} \tag{16'}$$

будет регулярным при любых функциях $\phi_1, \ldots, \phi_n$, где $\phi_i : \mathbb{Z}_m \to \mathbb{Z}_m$. Дадим рекурсивный способ построения правильных семейств функций.

Пусть имеется семейство функций $f' = (f'_{10}, \ldots, f'_{n0})$ от переменных $z_{10}, \ldots, z_{n0}$. Определим семейство из $n + s_1 + \cdots + s_n$ функций $f = (f_{ij})$ от переменных (z_{ij}), $i = 1, \ldots, n$, $j = 0, \ldots, s_i$, ($s_i, \ldots, s_n$ — произвольные $\geqslant 0$) соотношениями

$$\begin{aligned} f_{i1} &= \Phi_{i1}(f'_{i0}) \\ f_{i1} &= \Phi_{i2}(f'_{i0}, z_{i1}) \\ &\ldots \\ f_{is_i} &= \Phi_{is_i}(f'_{i0}, z_{i1}, \ldots, z_{is_i-1}) \\ f_{i0} &= \Phi_{i0}(f'_{i0}, z_{i1}, \ldots, z_{is_i}) \end{aligned} \tag{17}$$

($\Phi_{i1}\dots,\Phi_{is_i},\Phi_{i0}$ — произвольные функции от соответствующих (17) переменных).

Теорема 12. *Если f' — правильное семейство, то семейство f также правильное при любых функциях Φ_{ij}, $i\in\overline{1,n}$, $j\in\overline{0,s_i}$.*

Доказательство. Пусть семейство f не является правильным. Это значит, что существует пара различных наборов $z'=(z'_{ij})$, $i\in\overline{1,n}$, $j\in\overline{0,s_i}$, и $z''=(z''_{ij})$, $i\in\overline{1,n}$, $j\in\overline{0,s_i}$, таких, что для всех α,β, таких, что $z'_{\alpha\beta}\neq z''_{\alpha\beta}$ имеем $f_{\alpha\beta}(z')\neq f_{\alpha\beta}(z'')$.

Имеются два случая:

а) $z'_0\neq z''_0$, где $z'_0=(z'_{10},\dots,z'_{n0})$, $z''_0=(z''_{10},\dots,z''_{n0})$. В силу правильности семейства $f'=(f'_{10},\dots,f'_{n0})$ найдется $\alpha\in\overline{1,n}$, такое, что $z'_{\alpha0}\neq z''_{\alpha0}$ и $f'_{\alpha0}(z')=f'_{\alpha0}(z'')$. Из соотношений (17) получаем, что $f_{\alpha1}(z')=f_{\alpha1}(z'')$ и в силу предположения о неправильности семейства f имеем $z'_{\alpha1}=z''_{\alpha1}$. Снова из соотношений (17) имеем $f_{\alpha2}(z')=f_{\alpha2}(z'')$ и тогда имеем $z'_{\alpha2}=z''_{\alpha2}$. Продолжая таким образом, получим $z'_{\alpha s}=z''_{\alpha s}$ и из соотношений (17) имеем $f_{\alpha0}(z')=f_{\alpha0}(z'')$ и тогда $z'_{\alpha0}=z''_{\alpha0}$, что противоречит выбору α.

б) $z'_0=z''_0$. В этом случае из соотношений (17) имеем $f_{i1}(z')=f_{i1}(z'')$ для всех $i\in\overline{1,n}$. Отсюда по предположению о неправильности f имеем $z'_{i1}=z''_{i1}$ для всех $i\in\overline{1,n}$. Далее, из (17) имеем $f_{i2}(z')=f_{i2}(z'')$ для всех $i\in\overline{1,n}$. Отсюда получаем $z'_{i2}=z''_{i2}$ для всех $i\in\overline{1,n}$. Продолжая таким образом, получим, что $z'_{is_i}=z''_{is_i}$ для всех $i\in\overline{1,n}$ и, следовательно, $z'=z''$, что противоречит выбору пары z',z''. Значит, семейство f — правильное.

В качестве приложения рассмотрим семейство $f'=(f'_{10},\dots,f'_{n0})$ булевых функций от переменных $z_{10},\dots,z_{n0}$, где

$$\begin{aligned} f'_{10}&=1+\overline{z_{20}}z_{30}\cdots z_{n0}\\ &\dots\\ f'_{n0}&=1+\overline{z_{10}}z_{20}\cdots z_{n-10}\end{aligned}\qquad(18)$$

Легко установить правильность семейства (18). Применим к нему теорему 12, в которой положим $s_1=s,s_2=0,\dots,s_n=0$, в качестве функций Φ_{ij} возьмем конъюнкцию соответствующих переменных. Получим правильное семейство функций, каждая из которых

имеет степень нелинейности $\geqslant n-1$, размерность которого $n+s$ (n, s — произвольные натуральные).

Рассмотрим теперь в соотношении (16') функции ϕ_i такие, что

1) $\operatorname{Im}\phi_i = \{0,1\}$,

2) $\left(\left|\left\{\phi_i^{-1}(1)\right\}\right|, m\right) = 1$.

Модернизируя рассуждения теоремы 6 можно показать, что длина любого цикла преобразования (17) для данного семейства функций f не меньше, чем m^{s+1}. Если m — простое число, а GL_{n+s} — группа линейных преобразований над полем F_m, то получим $\operatorname{ind}_{GL_n}\delta \geqslant m^{s+1}$, при этом степень нелинейности каждой функции не меньше, чем $n-1$, число существенных переменных каждой функции не меньше, чем $n-1$.

Список литературы

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

[2] Huffman D. A. Canonical Forms for Information Lossless Finite-State Logical Machines // IRE Trans. Circ. Theory. 1959. V. 6. P. 41–59.

[3] Носов В. А. Специальные главы дискретной математики / Уч. пособие. М., 1990.

[4] Алексеев В. Б., Носов В. А. NP-полные задачи и их полиномиальные варианты. Обзор // Обозрение промышленной и прикладной математики. 1997. Т. 4. Вып. 2. С. 165–193.

[5] Клосс Б. М., Малышев В. А. Определение регулярности автомата по его каноническим уравнениям // ДАН СССР. 1967. Т. 172. № 3. С. 543–546.

[6] Gill A. Linear Sequential Circuits: Analysis, Synthesis, and Applications. New York: McGraw-Hill, 1966. [Рус. перевод: Гилл А. Линейные последовательные машины. М.: Наука, 1974].

[7] Носов В. А., Панкратьев А. Е. Латинские квадраты над абелевыми группами // Фундаментальная и прикладная математика. Т. 12. № 3. 2006. С. 65–71.