Math-Net.Ru

Общероссийский математический портал

А. В. Бабаш, О периодичности последовательности состояний автомата, отвечающей начальному состоянию и входной периодической последовательности, *Дискрет. матем.*, 2002, том 14, выпуск 2, 54–64

DOI: <https://doi.org/10.4213/dm241>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.198.187.58

26 апреля 2023 г., 16:15:43

О периодичности последовательности состояний автомата, отвечающей начальному состоянию и входной периодической последовательности

© 2002 г. А. В. Бабаш

Для интуитивного понятия почти периодичности последовательности элементов конечного алфавита введена его формализация — мера приближенного периода этой последовательности. Получена нижняя оценка меры приближенного периода последовательности состояний автомата при заданных начальном состоянии и входной периодической последовательности. На основании этой оценки для автоматов, моделирующих функционирование регистров сдвига, получена оценка снизу мер приближенных периодов их выходных последовательностей.

1. Введение

Основным результатом по оценке снизу периодов выходных последовательностей конечных автоматов, отвечающих начальным состояниям и выходным периодическим последовательностям, является результат, представленный в теореме 2.2 работы [1] и состоящий в том, что минимальный период W выходной последовательности автомата не превосходит величины $k\omega$, где k — число состояний автомата, а ω — минимальный период входной последовательности. В [2] и [3] приведены утверждения, суть которых состоит в том, что W является делителем числа $k'\omega$ при некотором $k' \leq k$.

В связи с большой сложностью проблемы нижней оценки периодов выходных последовательностей конечных автоматов при заданных начальном состоянии и входной периодической последовательности естественным подходом к ее удовлетворительному решению является выделение тех или иных классов автоматов в качестве объектов исследований. Например, ряд работ посвящен вопросам периодичности выходных последовательностей линейных автономных автоматов, в частности, в этом классе выделяются работы, в которых указываются способы построения линейных рекуррентных последовательностей максимального периода в разнообразных алгебраических структурах. В настоящей работе используется другой подход к решению поставленной проблемы, заключающийся в предварительном решении промежуточной задачи — задачи оценки снизу периода последовательности состояний автомата при заданных начальном состоянии и входной периодической последовательности. Эта задача решается в работе в более общей постановке, а именно, речь идет об оценке характеристик почти периодичности последовательностей состояний конечных автоматов.

Для периодической последовательности $\mathfrak{Z}$ периода ω элементов конечного алфавита I вводится понятие меры $\mu(\mathfrak{Z}, d)$ приближенного периода d . Качественно $\mu(\mathfrak{Z}, d)$ трактуется как минимальная часть знаков последовательности $\mathfrak{Z}$, которые необходимо изменить для получения из $\mathfrak{Z}$ последовательности периода d .

Основным результатом является теорема 1, дающая нижние оценки мер приближенных периодов последовательности состояний автомата, отвечающей его начальному состоянию и входной периодической последовательности. Следствие 1 дает нижние оценки периодов этих последовательностей. В следствии 2 указываются нижние оценки мер приближенных периодов выходной последовательности регистра сдвига, отвечающей его начальному состоянию и входной периодической последовательности.

2. Обозначения, основные понятия, вспомогательные результаты

Пусть I, S, O — произвольные непустые конечные множества такие, что $|I| \geq 2, |O| \geq 2$, где здесь и далее $|A|$ — число элементов конечного множества A ;

$$A = (I, S, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$$

— автомат с входным алфавитом I , множеством состояний S , выходным алфавитом O , частичными функциями переходов $(\delta_i)_{i \in I}$ и выходов $(\beta_i)_{i \in I}$; $\mathbf{N}$ — множество натуральных чисел, $N_0 = \mathbf{N} \cup 0$; I^* — множество всех слов в алфавите I ; I_p^∞ — множество всех смешанно-периодических последовательностей в алфавите I . Последовательность $\mathfrak{Z}$ из I_p^∞ называется чисто-периодической, если длина L ее предпериода равна нулю. Под периодом последовательности $\mathfrak{Z}$ здесь и далее будет пониматься ее минимальный период.

Пусть далее $I_{p,W}^\infty$ — множество всех последовательностей из I_n^∞ периода W ;

$$A_M(s, \mathfrak{Z}) = \{s_1, s_2, \dots\}$$

— последовательность состояний автомата A ;

$$A(s, \mathfrak{Z}) = \{y_1, y_2, \dots\}$$

— выходная последовательность автомата A ; для $\mathfrak{Z} = \{i_1, i_2, \dots\}$ и $s \in S$

$$s_j = \delta_{i_{j-1}} \dots \delta_{i_1} s, \quad y_j = \beta_{i_j} s_j, \quad s_1 = s;$$

$\rho(a, b)$ — расстояние Хемминга между словами a and b одинаковой длины из I^* ; $\rho_k(\mathfrak{Z}, \mathfrak{Z}')$ — расстояние Хемминга между начальными словами длины k последовательностей $\mathfrak{Z}, \mathfrak{Z}'$ из I_p^∞ ; (ω, ω') — наибольший общий делитель чисел ω, ω' ; $[\omega, \omega']$ — наименьшее общее кратное чисел ω, ω' ; $D \mid \omega$ означает, что D делит ω .

Для $\mathfrak{Z} = \{i_1, i_2, \dots\}$ из I_p^∞ положим

$$\begin{aligned} \mathfrak{Z}^j &= i_j, i_{j+1}, \dots, \quad \mathfrak{Z}^1 = \mathfrak{Z}, \\ \mathfrak{Z}^j|_k &= i_j, i_{j+1}, \dots, i_{j+k-1}, \\ \text{CON}(\mathfrak{Z}) &= \{i \in I : \exists j \in \mathbf{N}, i_j = i\}. \end{aligned}$$

Последнюю величину мы называем содержанием последовательности $\mathfrak{Z}$. Если понимать под последовательностью $\mathfrak{Z}$ элементов алфавита I отображение $\mathfrak{Z}: \mathbf{N} \rightarrow I$, то содержание $\mathfrak{Z}$ есть образ множества $\mathbf{N}$.

Пусть $\mathfrak{Z}, \mathfrak{Z}'$ — произвольные последовательности из I_p^∞ с длинами подходов L, L' и периодами ω, ω' соответственно. Легко доказывается следующее утверждение.

Предложение 1. При $k \rightarrow \infty$ предел

$$\lim \frac{1}{k} \rho_k(\mathfrak{Z}, \mathfrak{Z}')$$

существует и равен

$$\mu(\mathfrak{Z}, \mathfrak{Z}') = \frac{1}{[\omega, \omega']} \rho_{[\omega, \omega']}(\mathfrak{Z}^{\max(L, L') + 1}, \mathfrak{Z}'^{\max(L, L') + 1}).$$

Данное утверждение является частным случаем следствия 1 в [4].

Определение 1. Приближенным периодом последовательности $\mathfrak{Z} \in I_p^\infty$ называется любое число W из $\mathbb{N}$. Величина

$$\mu(\mathfrak{Z}, W) = \inf \mu(\mathfrak{Z}, \mathfrak{Z}'),$$

где нижняя грань берется по всем последовательностям $\mathfrak{Z}' \in I_{n, W}^\infty$, называется мерой приближенного периода W (мерой приближения приближенного периода W) последовательности $\mathfrak{Z}$.

Из предложения 1 следует, что величина $\mu(\mathfrak{Z}, \mathfrak{Z}')$ определена периодическими частями $\mathfrak{Z}^k, \mathfrak{Z}'^k$ последовательностей $\mathfrak{Z}, \mathfrak{Z}'$ при $k \geq \max(L, L') + 1$. Мощность множества всех чисто-периодических последовательностей периода W с элементами из алфавита I конечна. Поэтому

$$\inf \mu(\mathfrak{Z}, \mathfrak{Z}') = \min \mu(\mathfrak{Z}, \mathfrak{Z}').$$

Пусть N' — конечное подмножество $\mathbb{N}$.

Определение 2. Наилучшей мерой приближения приближенных периодов из множества N' последовательности $\mathfrak{Z}$ называется величина $\min \mu(\mathfrak{Z}, W')$, где минимум берется по всем $W' \in N'$.

Определение 3. Наилучшим приближенным периодом W среди периодов из N' последовательности $\mathfrak{Z}$ называется минимальное число $W \in N'$, при котором

$$\mu(\mathfrak{Z}, W) = \min \mu(\mathfrak{Z}, W'), \quad W' \in N'.$$

Определение 4. Наилучшей приближенной последовательностью

$$\text{BAS} \left(\mathfrak{Z}, \bigcup_{W' \in N'} I_{p, W'}^\infty \right)$$

из множества

$$\bigcup_{W' \in N'} I_{p, W'}^\infty$$

для последовательности $\mathfrak{Z}$ называется произвольная последовательность

$$\mathfrak{Z}' \in \bigcup_{W' \in N'} I_{p, W'}^\infty,$$

для которой

$$\mu(\mathfrak{Z}, \mathfrak{Z}') = \min_{W' \in N'} (\mathfrak{Z}, W').$$

Для формулировки приводимых ниже вспомогательных утверждений введем дополнительные обозначения. Для чисто периодической последовательности $\mathfrak{Z} = \{i_1, i_2, \dots\}$ из $I_{n,\omega}^\infty$, числа D , которое делит ω , и $j = 1, \dots, D$ обозначим $v_j(i)$ частоту встречаемости символа i в слове $i_j, i_{j+D}, \dots, i_{j+TD}$, $I(j, \mathfrak{Z})$ множество всех $i \in I$, для которых $v_j(i) = \max_{i \in I} v_j(i)$, и положим $T = (\omega/D - 1)$. Отметим, что $|I(j, \mathfrak{Z})| \geq 1$.

Через $\mathfrak{R}(\mathfrak{Z}, D)$ обозначим множество всех последовательностей $\mathfrak{Z}'' = \{i_1'', i_2'', \dots\}$ вида

$$i_j'' = i_{j+D}'', \quad j \in \mathbb{N}, \quad i_k'' \in I(k, \mathfrak{Z}), \quad k = 1, \dots, D.$$

Последние соотношения определяют $\mathfrak{Z}''$ однозначно лишь в случае $|I(k, \mathfrak{Z})| = 1$, $k = 1, \dots, D$. Очевидно, что $\text{CON}(\mathfrak{Z}'') \subseteq \text{CON}(\mathfrak{Z})$ для любой последовательности $\mathfrak{Z}''$ из $\mathfrak{R}(\mathfrak{Z}, D)$, а период каждой последовательности из $\mathfrak{R}(\mathfrak{Z}, D)$ является делителем числа D .

Лемма 1. Для $\mathfrak{Z} \in I_{p,\omega}^\infty$, $\mathfrak{Z}' \in I_{p,\omega'}^\infty$, $D = (\omega, \omega')$ величина $\mu(\mathfrak{Z}, \mathfrak{Z}'')$ не зависит от выбора $\mathfrak{Z}''$ из $\mathfrak{R}(\mathfrak{Z}, D)$ и

$$\mu(\mathfrak{Z}, \mathfrak{Z}'') \leq \mu(\mathfrak{Z}, \mathfrak{Z}'), \quad \mu(\mathfrak{Z}, \mathfrak{Z}'') \leq \mu(\mathfrak{Z}, \omega').$$

Доказательство. Из предложения 1 следует, что для доказательства леммы 1 достаточно доказать его для чисто периодических последовательностей $\mathfrak{Z}, \mathfrak{Z}'$. Пусть $\mathfrak{Z}, \mathfrak{Z}'$ — чисто периодические последовательности.

При $(\omega, \omega') = \omega$ утверждение леммы очевидно, так как множество $\mathfrak{Z}'' = \mathfrak{Z}$.

Пусть $(\omega, \omega') = D \neq \omega$, $\mathfrak{Z} = \{i_1, i_2, \dots\}$, $\mathfrak{Z}'' = \{i_1'', i_2'', \dots\}$ В силу предложения 1

$$\begin{aligned} \mu(\mathfrak{Z}, \mathfrak{Z}') &= \frac{1}{[\omega, \omega']} \rho_{[\omega, \omega']}(\mathfrak{Z}, \mathfrak{Z}') \\ &= \frac{1}{[\omega, \omega']} \sum_{j=1}^{[\omega, \omega']} \rho(i_j, i_j') = \frac{1}{[\omega, \omega']} \sum_{j=1}^{\omega'} \sum_{k=0}^{[\omega, \omega']/\omega'-1} \rho(i_j', i_{j+k\omega'}). \end{aligned}$$

Заметим, что $[\omega, \omega']/\omega' - 1 = \omega/D - 1$, а слова $i_j, i_{j+\omega'}, \dots, i_{j+C\omega'}, i_j, i_{j+D}, \dots, i_{j+CD}$, где $C = \omega/D - 1$, получаются друг из друга перестановкой символов, поэтому справедливо равенство

$$\sum_{k=0}^{\omega/D-1} \rho(i_j', i_{j+k\omega'}) = \sum_{k=0}^{\omega/D-1} \rho(i_j', i_{j+kD}).$$

Таким образом,

$$\mu(\mathfrak{Z}, \mathfrak{Z}') = \frac{1}{[\omega, \omega']} \sum_{j=1}^{\omega'} \sum_{k=0}^{\omega/D-1} \rho(i_j', i_{j+kD}) = \frac{1}{[\omega, \omega']} \sum_{j=1}^D \sum_{m=0}^{\omega'/D-1} \sum_{k=0}^{\omega/D-1} \rho(i_{j+mD}', i_{j+kD}).$$

Для произвольной последовательности $\mathfrak{Z}'' = i_1'', i_2'', \dots$ из $\mathfrak{R}(\mathfrak{Z}, D)$ справедливы равенства

$$\begin{aligned} \mu(\mathfrak{Z}, \mathfrak{Z}'') &= \frac{1}{\omega} \rho_\omega(\mathfrak{Z}, \mathfrak{Z}'') = \frac{1}{[\omega, \omega']} \rho_{[\omega, \omega']}(\mathfrak{Z}, \mathfrak{Z}'') \\ &= \frac{1}{[\omega, \omega']} \sum_{j=1}^{\omega'} \sum_{k=0}^{\omega/D-1} \rho(i_j'', i_{j+kD}) = \frac{1}{[\omega, \omega']} \sum_{j=1}^D \sum_{m=0}^{\omega'/D-1} \sum_{k=0}^{\omega/D-1} \rho(i_{j+mD}'', i_{j+kD}). \end{aligned}$$

Отсюда, во-первых, вытекает независимость значения $\mu(\mathfrak{Z}, \mathfrak{Z}'')$ от выбора $\mathfrak{Z}''$ из $\mathfrak{R}(\mathfrak{Z}, D)$ и, во-вторых, то, что при любых $j = 1, \dots, D$, $m = 0, 1, \dots, \omega'/D - 1$ справедливо неравенство

$$\sum_{k=0}^{\omega/D-1} \rho(i_{j+mD}'', i_{j+kD}) \leq \sum_{k=0}^{\omega/D-1} \rho(i_{j+mD}', i_{j+kD}).$$

Следовательно, $\mu(\mathfrak{Z}, \mathfrak{Z}'') \leq \mu(\mathfrak{Z}, \mathfrak{Z}')$. Откуда получаем неравенство $\mu(\mathfrak{Z}, \mathfrak{Z}'') \leq \mu(\mathfrak{Z}, \omega')$. Лемма 1 доказана.

Предложение 2. Пусть $\mathfrak{Z} \in I_{p,\omega}^\infty$ и $\omega' \in \mathbb{N}$. Наилучшая мера приближения $\min_{d': d'|\omega} \mu(\mathfrak{Z}, d')$ приближенных периодов из множества $\{d': d' \mid \omega'\}$ последовательности $\mathfrak{Z}$ равна величине $\mu(\mathfrak{Z}, \mathfrak{Z}'')$, где $\mathfrak{Z}'' \in \mathfrak{R}(\mathfrak{Z}, D)$ при $D = (\omega, \omega')$.

Доказательство. Пусть $\min_{d': d'|\omega'} \mu(\mathfrak{Z}, d'_0) = \mu(\mathfrak{Z}, d'_0)$, а $\mathfrak{Z}' = \text{BAS}(\mathfrak{Z}, I_{p,d'_0}^\infty)$ — наилучшая приближенная последовательность из множества I_{p,d'_0}^∞ к последовательности $\mathfrak{Z}$. Тогда $\mu(\mathfrak{Z}, \mathfrak{Z}') = \mu(\mathfrak{Z}, d'_0)$. По лемме 1 найдется $\mathfrak{Z}'' \in \mathfrak{R}(\mathfrak{Z}, D_0)$ периода d'' , $d'' \mid D_0$, $D_0 = (d'_0, \omega)$, для которой $\mu(\mathfrak{Z}, \mathfrak{Z}'') \leq \mu(\mathfrak{Z}, \mathfrak{Z}')$. Так как $D_0 \mid \omega'$, то $d'' \mid \omega'$. Из определения $\mu(\mathfrak{Z}, d'_0)$ и предыдущего неравенства получаем, что

$$\mu(\mathfrak{Z}, \mathfrak{Z}'') = \mu(\mathfrak{Z}, d'_0) = \mu(\mathfrak{Z}, \mathfrak{Z}').$$

Очевидно, что $\mu(\mathfrak{Z}, d'_0)$ является наилучшей мерой приближения приближенных периодов и из множества $\{d': d' \mid D\}$ последовательности $\mathfrak{Z}$, откуда вытекает, что $\mathfrak{Z}'' \in \mathfrak{R}(\mathfrak{Z}, D)$.

3. Нижние оценки мер приближенных периодов последовательностей состояний автоматов

Пусть $\mathfrak{Z} = \{i_1, i_2, \dots\}$ — входная смешанно-периодическая последовательность автомата $A = (I, S, 0, (\delta_i)_{i \in I}, (\beta_i)_{i \in I})$, а α — бинарное отношение эквивалентности на $\text{CON}(\mathfrak{Z})$, удовлетворяющее условию: произвольные элементы i, i' из разных классов эквивалентности таковы, что частичные функции переходов $\delta_i, \delta_{i'}$ автомата A не имеют общих переходов, то есть $\delta_i s \neq \delta_{i'} s$ при любом $s \in S$. Класс эквивалентности отношения α , содержащий элемент i , обозначим через $\alpha(i)$.

Теорема 1. Пусть $\mathfrak{Z} = \{i_1, i_2, \dots\}$ — входная смешанно-периодическая последовательность автомата A , $\alpha(\mathfrak{Z}) = \{\alpha(i_1)\alpha(i_2), \dots\}$ — соответствующая ей последовательность периода $\omega(\alpha)$ классов эквивалентности отношения α на $\text{CON}(\mathfrak{Z})$, $A_M(s, \mathfrak{Z})$ — последовательность состояний автомата A , отвечающая его начальному состоянию $s \in S$ и входной последовательности $\mathfrak{Z}$, τ' — приближенный период последовательности $A_M(s, \mathfrak{Z})$ с мерой приближения $\mu(A_M(s, \mathfrak{Z}), \tau')$, причем $(\tau', \omega(\alpha)) = t \neq \omega(\alpha)$. Тогда

$$\mu(A_M(s, \mathfrak{Z}), \tau') \geq \frac{1}{2} \min_{d': d'|\tau'} \mu(\alpha(\mathfrak{Z}), d).$$

Доказательство. Пусть $\text{BAS}(A_M(s, \mathfrak{Z}), I_{p,\tau'}^\infty) = \{s'_1, s'_2, \dots\}$ — наилучшая приближенная последовательность периода τ' из множества $I_{p,\tau'}^\infty$ к последовательности $A_M(s, \mathfrak{Z}) =$

$\{s_1, s_2, \dots\}$ периода τ , $s = s_1$. Определим вспомогательные последовательности

$$(A_M(s, \mathfrak{S}))_2 = \{s_1 s_2, s_2 s_3, \dots\},$$

$$(\text{BAS}(A_M(s, \mathfrak{S}), I_{p, \tau'}^\infty))_2 = \{s'_1 s'_2, s'_2 s'_3, \dots\}.$$

Очевидно, периоды этих последовательностей равны τ и τ' соответственно. Непосредственно проверяется, что

$$\begin{aligned} \mu((A_M(s, \mathfrak{S}))_2, \tau') &\leq \mu((A_M(s, \mathfrak{S}))_2, (\text{BAS}(A_M(s, \mathfrak{S}), I_{p, \tau'}^\infty))_2) \\ &\leq 2\mu(A_M(s, \mathfrak{S}), \text{BAS}(A_M(s, \mathfrak{S}), I_{p, \tau'}^\infty)) = 2\mu(A_M(s, \mathfrak{S}), \tau'). \end{aligned}$$

По предложению 2 найдется последовательность P'' периода d'' из $\mathfrak{R}((A_M(s, \mathfrak{S}))_2, D)$, $D = (\tau, \tau')$, для которой $d'' \mid D$ и выполняются соотношения

$$\mu((A_M(s, \mathfrak{S}))_2, d'') = \mu((A_M(s, \mathfrak{S}))_2, P'') \leq \mu((A_M(s, \mathfrak{S}))_2, \tau').$$

Отметим, что $\text{CON}(P'') \subseteq \text{CON}((A_M(s, \mathfrak{S}))_2)$.

На $\text{CON}((A_M(s, \mathfrak{S}))_2)$ определим функцию f . Для ss' из $\text{CON}((A_M(s, \mathfrak{S}))_2)$ положим $f(ss') = \alpha(i)$, если $\delta_i s = s'$. Рассмотрим последовательности

$$\begin{aligned} F((A_M(s, \mathfrak{S}))_2) &= \{f(s_1 s_2), f(s_2 s_3), \dots\}, \\ F(P'') &= \{\alpha(i''_1), \alpha(i''_2), \dots\}. \end{aligned}$$

Очевидно, что $F((A_M(s, \mathfrak{S}))_2) = \alpha(\mathfrak{S})$. Напомним, что период последовательности $\alpha(\mathfrak{S})$ равен $\omega(\alpha)$. Обозначим через $\omega''(\alpha)$ период последовательности $F(P'')$. Ясно, что $\omega''(\alpha) \mid d''$. Так как $(\omega(\alpha), \tau') = t \neq \omega(\alpha)$, то $(\omega(\alpha), \omega''(\alpha)) = d$, где $d \mid t$.

Очевидно, что

$$\mu(\alpha(\mathfrak{S}), F(P'')) \leq \mu((A_M(s, \mathfrak{S}))_2, P'').$$

Используя предложение 2, получаем, что

$$\min_{d: d \mid t} \mu(\alpha(\mathfrak{S}), d) \leq \mu(\alpha(\mathfrak{S}), F(P'')).$$

Следовательно,

$$\min_{d: d \mid t} \mu(\alpha(\mathfrak{S}), d) \leq \mu((A_M(s, \mathfrak{S}))_2, \tau') \leq 2\mu(A_M(s, \mathfrak{S}), \tau'),$$

что и требовалось доказать.

Эффективность теоремы 1 (рамки ее применения) определены условием $\omega(\alpha) > 1$. Таким образом, для нахождения нижней оценки меры приближенного периода последовательности $A_M(s, \mathfrak{S})$ состояний автомата A с помощью теоремы 1 необходимо предварительно построить какое-либо бинарное отношение типа α . В ряде случаев удобно сначала пытаться строить бинарное отношение эквивалентности σ^* на $\text{CON}(\mathfrak{S})$ следующим образом. Определяем бинарное отношение σ на $\text{CON}(\mathfrak{S})$, полагая, что i находится в отношении σ с i' тогда и только тогда, когда найдется $s \in S$, при котором $\delta_i s = \delta_{i'} s$. В качестве σ^* берем транзитивное замыкание отношения σ . Для повышения эффективности теоремы 1 удобно предварительно определить компоненту связности A_s автомата A , содержащую начальное состояние s , а затем проверять выполнение условий теоремы для автомата A_s .

Следствие 1. Пусть $\mathfrak{S} = \{i_1, i_2, \dots\}$ – входная смешанно-периодическая последовательность автомата A , $\alpha(\mathfrak{S}) = \{\alpha(i_1), \alpha(i_2), \dots\}$ – соответствующая ей последовательность периода $\omega(\alpha)$ классов эквивалентности отношения α на $\text{CON}(\mathfrak{S})$. Тогда период τ последовательности $A_M(s, \mathfrak{S})$ состояний автомата A , отвечающей начальному состоянию $s \in S$ и входной последовательности $\mathfrak{S}$, кратен $\omega(\alpha)$.

Доказательство. Предположим, что $(\tau, \omega(\alpha)) = t \neq \omega(\alpha)$. В качестве приближенного периода τ' последовательности $A_M(s, \mathfrak{S})$ рассмотрим период τ последовательности $A_M(s, \mathfrak{S})$. Тогда по теореме 1

$$\mu(A_M(s, \mathfrak{S}), \tau) \geq \frac{1}{2} \min_{d: d|t} \mu(\alpha(\mathfrak{S}), d).$$

Так как $t \neq \omega(\alpha)$, то очевидно, что правая часть неравенства больше нуля. Поэтому $\mu(A_M(s, \mathfrak{S}), \tau) > 0$, что противоречит тому, что τ – период последовательности $A_M(s, \mathfrak{S})$. Таким образом, τ кратен $\omega(\alpha)$.

Утверждение следствия 1 позволяет строить автоматы с гарантированными периодами последовательностей состояний, отвечающих их начальным состояниям и входным смешанно-периодическим последовательностям. Так, в частности, выбор частичных функций переходов автомата так, чтобы они попарно не имели общих переходов, гарантирует кратность периода последовательности его состояний величине периода входной последовательности при любом его начальном состоянии. Этот факт ранее был доказан В. А. Башевым.

Следующие две леммы, представляющие и самостоятельный интерес, являются вспомогательным инструментом для доказательства иной (чем в теореме 1) нижней оценки меры приближенного периода последовательности состояний автомата, отвечающей его начальному состоянию и входной смешанно-периодической последовательности.

Лемма 2. Пусть $\mathfrak{S} \in I_{p, \omega}^\infty$, $\mathfrak{S}' \in I_{p, \omega'}^\infty$, $(\omega, \omega') = d$ и L и L' – предпериоды последовательностей $\mathfrak{S}$ и $\mathfrak{S}'$ соответственно, $M = \max(L, L')$. Тогда

$$\mu(\mathfrak{S}, \mathfrak{S}') = \mu(\mathfrak{S}^{M+j}, \mathfrak{S}'^{M+j}) = \mu(\mathfrak{S}^{M+j+cd}, \mathfrak{S}'^{M+j}),$$

где $j \in \mathbb{N}$, $c \in \mathbb{N}_0$.

Доказательство. Так как $(\omega, \omega') = d$, найдутся k_1, k_2 , при которых $k_2\omega' - k_1\omega = d$. В силу предложения 1

$$\mu(\mathfrak{S}, \mathfrak{S}') = \frac{1}{[\omega, \omega']} \rho_{[\omega, \omega']}(\mathfrak{S}^{M+1}, \mathfrak{S}'^{M+1}).$$

Очевидно, что при любом $j \in \mathbb{N}$ и $c \in \mathbb{N}_0$ справедливы равенства

$$\begin{aligned} \frac{1}{[\omega, \omega']} \rho_{[\omega, \omega']}(\mathfrak{S}^{M+1}, \mathfrak{S}'^{M+1}) &= \frac{1}{[\omega, \omega']} \rho_{[\omega, \omega']}(\mathfrak{S}^{M+j}, \mathfrak{S}'^{M+j}) \\ &= \frac{1}{[\omega, \omega']} \rho_{[\omega, \omega']}(\mathfrak{S}^{M+j+ck_2\omega'}, \mathfrak{S}'^{M+j}) \\ &= \frac{1}{[\omega, \omega']} \rho_{[\omega, \omega']}(\mathfrak{S}^{M+j+ck_1\omega+cd}, \mathfrak{S}'^{M+j}) \\ &= \frac{1}{[\omega, \omega']} \rho_{[\omega, \omega']}(\mathfrak{S}^{M+j+cd}, \mathfrak{S}'^{M+j}). \end{aligned}$$

Несложно доказывается следующее утверждение.

Лемма 3. Для любых $\mathfrak{Z}, \mathfrak{Z}', \mathfrak{Z}'' \in I_p^\infty$ справедливо неравенство

$$\mu(\mathfrak{Z}, \mathfrak{Z}') + \mu(\mathfrak{Z}', \mathfrak{Z}'') \geq \mu(\mathfrak{Z}, \mathfrak{Z}'').$$

На множестве всех чисто периодических последовательностей функция μ является метрикой.

Теорема 2. Пусть $\mathfrak{Z} = \{i_1, i_2, \dots\}$ — входная смешанно-периодическая последовательность автомата A , $\alpha(\mathfrak{Z}) = \{\alpha(i_1), \alpha(i_2), \dots\}$ — соответствующая ей последовательность периода $\omega(\alpha)$ классов эквивалентности бинарного отношения α на $\text{CON}(\mathfrak{Z})$, $A_M(s, \mathfrak{Z})$ — последовательность периода τ состояний автомата A , отвечающая его начальному состоянию $s \in S$ и входной последовательности $\mathfrak{Z}$, τ' — приближенный период последовательности $A_M(s, \mathfrak{Z})$ с мерой приближения $\mu(A_M(s, \mathfrak{Z}), \tau')$, причем $(\tau, \tau') = d \neq \omega(\alpha)$. Тогда при любом $j \in \mathbb{N}$

$$\frac{1}{4} \mu(\alpha(\mathfrak{Z})^j, \alpha(\mathfrak{Z})^{j+cd}) \leq \mu(A_M(s, \mathfrak{Z}), \tau').$$

Доказательство. Пусть $\text{BAS}(A_M(s, \mathfrak{Z}), I_{p,\tau}^\infty) = \{s'_1, s'_2, \dots\}$ — наилучшая приближенная последовательность из множества последовательностей периода τ' к последовательности $A_M(s, \mathfrak{Z}) = \{s_1, s_2, \dots\}$. Обозначим через P максимальную длину из длин подходов последовательностей $\text{BAS}(A_M(s, \mathfrak{Z}), I_{p,\tau'}^\infty)$ и $A_M(s, \mathfrak{Z})$. Тогда $(\text{BAS}(A_M(s, \mathfrak{Z}), I_{p,\tau'}^\infty))^{P+1}$ и $(A_M(s, \mathfrak{Z}))^{P+1}$ — чисто периодические последовательности и первая последовательность является наилучшей приближенной последовательностью из множества последовательностей периода τ' ко второй последовательности. Пользуясь леммой 2 для $j \in \mathbb{N}$, $c \in \mathbb{N}_0$, получаем, что

$$\begin{aligned} \mu(A_M(s, \mathfrak{Z}), \tau') &= \mu((A_M(s, \mathfrak{Z}))^{P+1}, \tau') \\ &= \mu((A_M(s, \mathfrak{Z}))^{P+1}, (\text{BAS}(A_M(s, \mathfrak{Z}), I_{p,\tau'}^\infty))^{P+1}) \\ &= \mu((A_M(s, \mathfrak{Z}))^{P+j+cd}, (\text{BAS}(A_M(s, \mathfrak{Z}), I_{p,\tau'}^\infty))^{P+j}). \end{aligned}$$

В силу леммы 3 для c и c' из $\mathbb{N}_0$ справедливо неравенство

$$\mu((A_M(s, \mathfrak{Z}))^{P+j+cd}, (A_M(s, \mathfrak{Z}))^{P+j+c'd}) \leq 2\mu(A_M(s, \mathfrak{Z}), \tau').$$

Для последовательностей

$$\begin{aligned} (A_M(s, \mathfrak{Z}))^{P+j+cd} &= \{s_{P+j+cd}, s_{P+j+cd+1}, \dots\}, \\ (A_M(s, \mathfrak{Z}))^{P+j+c'd} &= \{s_{P+j+c'd}, s_{P+j+c'd+1}, \dots\} \end{aligned}$$

построим вспомогательные последовательности

$$\begin{aligned} ((A_M(s, \mathfrak{Z}))^{P+j+cd})_2 &= \{s_{P+j+cd} s_{P+j+cd+1}, s_{P+j+cd+1} s_{P+j+cd+2}, \dots\}, \\ ((A_M(s, \mathfrak{Z}))^{P+j+c'd})_2 &= \{s_{P+j+c'd} s_{P+j+c'd+1}, s_{P+j+c'd+1} s_{P+j+c'd+2}, \dots\} \end{aligned}$$

и функцию f на $\text{CON}(((A_M(s, \mathfrak{Z}))^{P+j+cd})_2)$, положив

$$f(s_k, s_{k+1}) = \alpha(i),$$

если $\delta_i s_k = s_{k+1}$. Из законов функционирования автомата A следует, что последовательности

$$\begin{aligned} F((A_M(s, \mathfrak{Z}))^{P+j+cd})_2 &= \{f(s_{P+j+cd} s_{P+j+cd+1}), f(s_{P+j+cd+1} s_{P+j+cd+2}), \dots\}, \\ F((A_M(s, \mathfrak{Z}))^{P+j+c'd})_2 &= \{f(s_{P+j+c'd} s_{P+j+c'd+1}), f(s_{P+j+c'd+1} s_{P+j+c'd+2}), \dots\} \end{aligned}$$

равны соответственно последовательностям

$$\begin{aligned} \alpha(\mathfrak{Z})^{P+j+cd} &= \{\alpha(i_{1+j+cd}), \alpha(i_{2+j+cd}), \dots\}, \\ \alpha(\mathfrak{Z})^{P+j+c'd} &= \{\alpha(i_{1+j+c'd}), \alpha(i_{2+j+c'd}), \dots\}. \end{aligned}$$

Очевидно, что

$$\begin{aligned} \mu(F((A_M(s, \mathfrak{Z}))^{P+j+cd})_2, F((A_M(s, \mathfrak{Z}))^{P+j+c'd})_2) \\ \leq \mu(((A_M(s, \mathfrak{Z}))^{P+j+cd})_2, ((A_M(s, \mathfrak{Z}))^{P+j+cd})_2) \\ \leq 2\mu((A_M(s, \mathfrak{Z}))^{P+j+cd}, (A_M(s, \mathfrak{Z}))^{P+j+c'd}). \end{aligned}$$

Из полученных оценок вытекает, что

$$\begin{aligned} \mu(\alpha(\mathfrak{Z})^{P+j+cd}, \alpha(\mathfrak{Z})^{P+j+c'd}) &\leq 2\mu((A_M(s, \mathfrak{Z}))^{P+j+cd}, (A_M(s, \mathfrak{Z}))^{P+j+c'd}) \\ &\leq 4\mu(A_M(s, \mathfrak{Z}), \tau'). \end{aligned}$$

Доказательство закончено.

Теорему 2 можно использовать и для оценки периода τ последовательности $A_M(s, \mathfrak{Z})$ состояний автомата A . Анализ доказательств теорем 1 и 2 показывает, что данные в них оценки меры $\mu(A_M(s, \mathfrak{Z}), \tau')$ приближенного периода τ' последовательности $A_M(s, \mathfrak{Z})$ несравнимы. На практике для получения оптимальной оценки следует использовать утверждения обеих теорем.

4. Нижние оценки мер приближенных периодов выходных последовательностей регистров сдвига

Рассмотрим регистр сдвига, то есть автомат

$$A = R(\varphi, I) = (i, S, O, (\delta_i)_{i \in I}, (\beta_i)_{i \in I}),$$

где $S = I^n$, $O = I$, для $i \in I$ и $\{i(n), i(n-1), \dots, i(1)\} \in I^n$

$$\delta_i(i(n), i(n-1), \dots, i(1)) = (\varphi(i, i(n), i(n-1), \dots, i(1)), i(n), i(n-1), \dots, i(2)),$$

где φ — функция $I^{n+1} \rightarrow I$; $\beta_i = \lambda$, $i \in I$,

$$\lambda(i(n), i(n-1), \dots, i(1)) = i(k)$$

для некоторого $k \in \{1, \dots, n\}$.

Пусть $\mathfrak{Z}$ — входная смешанно-периодическая последовательность автомата $A = R(\varphi, I)$. Период выходной последовательности $A(s, \mathfrak{Z})$ автомата $R(\varphi, I)$ совпадает с периодом его последовательности состояний $A_M(s, \mathfrak{Z})$, в связи с чем следствие 1 и

теорема 2 дают нижние оценки периода выходной последовательности $A(s, \mathfrak{Z})$ автомата $R(\varphi, I)$.

Рассмотрим вопрос о связях мер приближенных периодов последовательностей $A_M(s, \mathfrak{Z})$ и $A(s, \mathfrak{Z})$.

Предложение 3. Для любого $\tau' \in N$ справедливо неравенство

$$n\mu(A(s, \mathfrak{Z}), \tau') \geq \mu(A_M(s, \mathfrak{Z}), \tau').$$

Доказательство. Без ограничения общности будем предполагать, что входная последовательность $\mathfrak{Z}$ и выходная последовательность регистра сдвига

$$A(s, \mathfrak{Z}) = \{i(k), i(k+1), \dots, i(k+j), \dots\}$$

— чисто периодические последовательности (см. предложение 1). Последовательность $A_M(s, \mathfrak{Z})$ можно записать в виде

$$A_M(s, \mathfrak{Z}) = \{(i(n), i(n-1), \dots, i(1)), (i(n+1), i(n), \dots, i(2)), \dots, (i(n+j), \dots, i(j+1)), \dots\}.$$

Несовпадение состояний, слов

$$(i(n+j), \dots, i(j+1)), \quad (i'(n+j), \dots, i'(j+1)),$$

обуславливается несовпадением их компонент. Для последовательности

$$A(s, \mathfrak{Z}) = \{i(k), i(k+1), \dots, i(k+j), \dots\}$$

и чисто периодической последовательности

$$\mathfrak{Z}' = \{i'(k), i'(k+1), \dots, i'(k+j), \dots\}$$

периода τ' неравенство $i(k+j) \neq i'(k+j)$ для $j \geq k-1$ влечет n неравенств

$$\begin{aligned} & (i(k+j), i(k+j-1), \dots, i(k+j-n+1)) \\ & \quad \neq (i'(k+j), i'(k+j-1), \dots, i'(k+j-n+1)), \\ & (i(k+j+1), i(k+j), \dots, i(k+j-n+2)) \\ & \quad \neq (i'(k+j+1), i'(k+j), \dots, i'(k+j-n+2)), \\ & \quad \dots \\ & (i(k+j+n-1), i(k+j+n-2), \dots, i(k+j)) \\ & \quad \neq (i'(k+j+n-1), i'(k+j+n-2), \dots, i'(k+j)). \end{aligned}$$

Поэтому для последовательностей $A(s, \mathfrak{Z})$ периода τ и $\mathfrak{Z}'$ периода τ' справедливы соотношения

$$\begin{aligned} n\mu(A_M(s, \mathfrak{Z}), \mathfrak{Z}') &= \frac{n}{[\tau, \tau']} \rho_{[\tau, \tau']}(A_M(s, \mathfrak{Z}), \mathfrak{Z}') \geq \frac{1}{[\tau, \tau']} \rho_{[\tau, \tau']}(A_M(s, \mathfrak{Z}), R(\mathfrak{Z})) \\ &= \mu(A_M(s, \mathfrak{Z}), R(\mathfrak{Z})), \end{aligned}$$

где

$$R(\mathfrak{Z}') = \{(i'(k), i'(k+1), \dots, i'(k+n-1)), (i'(k+1), i'(k+2), \dots, i'(k+n)), \dots\}.$$

Справедливо неравенство

$$\mu(A_M(s, \mathfrak{S}), R(\mathfrak{S})) \geq \mu(A_M(s, \mathfrak{S}), \tau').$$

Следовательно, взяв в качестве $\mathfrak{S}'$ наилучшую приближенную последовательность периода τ' к $A(s, \mathfrak{S})$, получаем требуемое неравенство

$$n\mu(A(s, \mathfrak{S}), \tau') = n\mu(a(s, \mathfrak{S}), \mathfrak{S}') \geq \mu(A_M(s, \mathfrak{S}), R(\mathfrak{S})) \geq \mu(A_M(s, \mathfrak{S}), \tau').$$

Из теорем 1, 2 и предложения 3 вытекает следующее утверждение.

Следствие 2. Пусть $\mathfrak{S}$ — входная последовательность регистра сдвига $R(\varphi, I)$, $\alpha(\mathfrak{S})$ — соответствующая ей последовательность периода $\alpha(\omega)$ классов эквивалентности бинарного отношения α на $\text{CON}(\mathfrak{S})$, W' — приближенный период выходной последовательности $A(s, \mathfrak{S})$ периода W регистра сдвига $R(\varphi, I)$.

Тогда, если $(W, W') = d \neq \alpha(\omega)$, то при любых $j \in \mathbb{N}$ и $c \in \mathbb{N}_0$

$$\frac{1}{4}\mu(\alpha(\mathfrak{S})^j, \alpha(\mathfrak{S})^{j+cd}) \leq \mu(A(s, \mathfrak{S}), W');$$

если $(\alpha(\omega), W') = t \neq \alpha(\omega)$ и d — наилучший приближенный период последовательности $\alpha(\mathfrak{S})$ среди приближенных периодов из множества $\{d' : d' \mid t\}$, то

$$\frac{1}{2n}\mu(\alpha(\mathfrak{S}), d) \leq \mu(A(s, \mathfrak{S}), W').$$

Список литературы

1. Трахтенброт Б. А., Барздин Я. М., *Конечные автоматы (поведение и синтез)*. Наука, Москва, 1970.
2. Беркс А. В., Райт Д. Б., Теория логических сетей. *Киберн. сб.* (1962) 4, 233–255.
3. Кобринский Н. Е., Трахтенброт Б. А., *Введение в теорию конечных автоматов*. Наука, Москва, 1962.
4. Бабаш А. В., Приближенные модели перестановочных автоматов. *Дискретная математика* (1997) 9, №1, 103–123.

Статья поступила 17.05.2000.

Переработанный вариант поступил 14.02.2002.