А. В. Б а б а ш (Москва, МЭСИ)**. Изопериод выходных последовательностей последовательного соединения полноциклового автомата с неавтономным перестановочным автоматом.**

Одним из требований к синтезу управляющих блоков многоалфавитных поточных шифров является требование, состоящее в том, что в управляющей гамме должны отсутствовать простые аналитические зависимости между близко расположенными знаками. Приводимые результаты тесно связаны с решением классической проблемы оценки периодов выходных последовательностей конечных автоматов (см. [1, 2]). Начало публикаций по вопросам оценок изопериодов выходных последовательностей некоторых классов автоматов осуществлено в [3, 4]. Пусть Y — конечный алфавит, $|Y| \geqslant 2$, σ — бинарное отношение на Y. Последовательность $Q = y_1, y_2, \ldots$ элементов алфавита Y называется *σ-периодической*, если существует натуральное число d, при котором $y_j \sigma y_{j+d}$ для любого $j \in \{1, 2, \ldots\}$. Число d называется *σ-периодом* последовательности Q. Если σ — отношение равенства, то $Q = y_1, y_2, \ldots$ — периодическая последовательность, и минимальное число d с указанным свойством является ее периодом. Если σ является отображением Y в Y, то последовательность $Q = y_1, y_2, \ldots$ будем называть *σ-изопериодической*, а минимальное число d — ее *σ-изопериодом*.

Введем обозначения: S — множество состояний автомата, X — входной алфавит, Y — выходной алфавит, h — функция переходов, $(h_x)_{x \in X}$ — частичные функции переходов, λ — функция выходов, $A_1 = (S_1, Y_1, h, \lambda)$ — полноцикловый приведенный автомат, $A_1({}^1s)$ — выходная последовательность A_1 при начальном состоянии ${}^1s \in S_1$, $A_2 = (X = Y_1, S_2, (h_x)_{x \in X})$— перестановочный коммутируемый автомат без выхода ($(h_x)_{x \in X}$ — биекции S_2 в S_2 и $h_x h_{x'} = h_{x'} h_x$ для любых $x, x' \in X$), $A_2({}^2s, P)$ — выходная последовательность автомата A_2 при входной последовательности P и начальном состоянии ${}^2s \in S_2$, $\Pi = h_{x(|S_1|)} h_{x(|S_1|)-1} \cdots h_{x(2)} h_{x(1)}$, где $A_1({}^1s) = x(1), x(2), \ldots$, $A_{\varphi,\Pi} = (S_2, \Pi, \varphi)$ — вспомогательный автономный автомат построенный для A_1 и A_2 с функцией переходов Π и выходов φ. Обозначим $A = A_1 \xrightarrow{\Phi} A_2$ последовательное соединение автомата $A_1 = (S_1, Y_1, h, \lambda)$ с автоматом $A_2 = (X, S_2, (h_x)_{x \in X})$. Символ Φ обозначает выходную функцию Φ: $S_1 \times S_2 \to Y$ этого последовательного соединения. Для описания класса рассматриваемых ниже функций Φ введем вспомогательные функции ψ: $S_1 \to Y'$, φ: $S_2 \to Y''$ и F: $Y' \times Y'' \to Y$. Будем считать, что функция F инъективна по последней переменной, в связи с чем удобно использовать обозначение $F_{y'}(y'') = F(y', y'')$, $(y', y'') \in Y' \times Y''$ для отображения $F_{y'}$ в Y.

Теорема. *Пусть $A = A_1 \xrightarrow{\Phi} A_2$ — полноцикловый автомат, $\Phi({}^1s, {}^2s) = F(\psi({}^1s), \varphi({}^2s))$, $({}^1s, {}^2s) \in S_1 \times S_2$, причем функция F инъективна по последней переменной, и период последовательности состояний $A_2({}^2s, P)$ автомата A_2 при выходной последовательности $P = A_1({}^1s)$, ${}^1s \in S_1$ кратен величине $|S_1|$, для автомата $A_{\varphi,\Pi} = (S_2, \Pi, \varphi)$ выполняется свойство: при фиксированной биекции σ Y в Y любой η-изопериод выходной последовательности $A_{\varphi,\Pi}({}^2s)$ автомата $A_{\varphi,\Pi}$ равен $|S_2|$ при $\eta \in \{F_{y'}^{-1} \sigma F_{\overline{y}'} \colon y', \overline{y}' \in Y'\}$. Тогда σ-изопериод выходной последовательности $A({}^1s, {}^2s)$ автомата A равен $|S_1|\,|S_2|$.*

СПИСОК ЛИТЕРАТУРЫ

1. *Бабаш А. В.* О периодах выходных последовательностей автоматов без потери информации при заданных периодических входных последовательностях. — Дискретн. матем., 2009, т. 21, в. 4.
2. *Бабаш А. В.* О периодичности выходных последовательностей автомата с потерей информации. — Ученые записки, 2010, № 3, с. 26–35.
3. *Бабаш А. В.* G-изопериод выходной последовательности автономного последовательного соединения автоматов. — Обозрение прикл. и промышл. матем., 2000, т. 7, в. 1.

4. *Babash A. V.* Isoperiods of output sequences of automata. — Probabilistic Methods in Discrete Mathematics. Utrecht: VSP, 2002, p. 147–158.