Math-Net.Ru

Общероссийский математический портал

В. И. Солодовников, Гомоморфизмы двоичных регистров сдвига, *Дискрет. матем.*, 2005, том 17, выпуск 1, 73–88

DOI: <https://doi.org/10.4213/dm89>

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: 35.173.219.149

26 апреля 2023 г., 03:49:53

Гомоморфизмы двоичных регистров сдвига

© 2005 г. В. И. Солодовников

В работе рассматриваются гомоморфизмы двоичных регистров сдвига с линейной по входной переменной функцией обратной связи, то есть гомоморфизмы автоматов, вырабатывающих двоичные линейно управляемые усложненные рекуррентные последовательности. Доказывается, что всякий гомоморфизм такого регистра разлагается в композицию гомоморфизма на регистр и некоторого гомоморфизма, близкого к изоморфизму. При описании этого разложения основную роль играет некая операция, распространяющая операцию произведения многочленов на множество всех двоичных функций. Вопрос о гомоморфизмах регистра сводится к вопросу о поиске общих делителей его функции обратной связи и выходной функции.

В работе приняты следующие обозначения: V_n — множество всех двоичных строк длины n , $n \geq 0$; F_n — множество всех двоичных функций n переменных $x_1, \dots, x_n$ (функции из F_n мы будем отождествлять с представляющими их многочленами Жегалкина); F_{n+1}^* — множество всех линейных по последней (то есть по $(n+1)$ -й) переменной функций из F_{n+1} , то есть функций вида $f = f^* \oplus x_{n+1}$, где $f^* \in F_n$.

Через $\psi\varphi$ обозначается композиция отображений ψ и φ , при которой отображение φ действует первым. Аналогично, BA — последовательное соединение автоматов A и B , при котором выход автомата A подается на вход автомата B .

Следуя терминологии работы [1], двоичным регистром сдвига длины n с функцией обратной связи f и выходной функцией h , где $f, h \in F_{n+1}$, будем называть автомат

$$R(h, f) = (V_1, V_n, V_1, \rho, \mu),$$

у которого функция переходов ρ и функция выходов μ определяются равенствами

$$\rho((x_1, \dots, x_n), x) = (x_2, \dots, x_n, f(x_1, \dots, x_n, x)),$$

$$\mu((x_1, \dots, x_n), x) = h(x_1, \dots, x_n, f(x_1, \dots, x_n, x))$$

для любых $x_1, \dots, x_n, x \in V_1$. Регистр сдвига без выхода с функцией обратной связи f будем обозначать через $R(f)$. Введем также обозначения

$$R_0(h) = R(h, x_{n+1}),$$

$$R'(f) = R(x_{n+1}, f).$$

Автомат $A = (X, S, Y, \delta, \lambda)$ называется обратимым, если все его автоматные отображения биективны (что равносильно биективности частичной функции выходов λ_s для всех $s \in S$). В этом случае обратным к автомату A называется автомат $A^{-1} = (Y, S, X, \delta', \lambda')$,

где $\delta'(s, y) = \delta(s, \lambda_s^{-1}(y))$, $\lambda'(s, y) = \lambda_s^{-1}(y)$ для всех $s \in S$, $y \in Y$. В частности, для $f, h \in F_{n+1}$ регистр $R(h, f)$ обратим тогда и только тогда, когда $f, h \in F_{n+1}^*$. При этом $R(h, f)^{-1} = R(f, h)$ и, следовательно, $R'(f)^{-1} = R_0(f)$.

Как и в статье [2], для любых $n_i \geq 0$, $f_i \in F_{n_i+1}$, $i = 1, 2$, определим функцию $f_2 \triangleleft f_1 \in F_{n_1+n_2+1}$ и отображение $\pi_{f_1, n_2}: V_{n_1+n_2} \rightarrow V_{n_2}$ равенствами

$$\begin{aligned} f_2 \triangleleft f_1(x_1, \dots, x_{n_1+n_2+1}) \\ = f_2(f_1(x_1, \dots, x_{n_1+1}), f_1(x_2, \dots, x_{n_1+2}), \dots, f_1(x_{n_2+1}, \dots, x_{n_1+n_2+1})), \\ \pi_{f_1, n_2}(x_1, \dots, x_{n_1+n_2}) \\ = (f_1(x_1, \dots, x_{n_1+1}), f_1(x_2, \dots, x_{n_1+2}), \dots, f_1(x_{n_2}, \dots, x_{n_1+n_2})) \end{aligned}$$

для любых $x_1, \dots, x_{n_1+n_2+1} \in V_1$, так что

$$f_2 \triangleleft f_1 = f_2 \pi_{f_1, n_2+1}.$$

Настоящая работа посвящена описанию гомоморфизмов двоичных регистров сдвига с линейной по входной (то есть последней) переменной функцией обратной связи в терминах операции $\triangleleft$, отображения π_{f_1, n_2} и бинарного отношения совпадения состояний с задержкой, которое будет введено позже.

Отметим, что, как и для любых автоматов, любой гомоморфизм $(\alpha, \beta, \gamma): R(h, f) \rightarrow A$ регистра $R(h, f)$ в автомат $A = (V_1, S, V_1, \delta, \lambda)$ сводится к внутреннему гомоморфизму (то есть такому, при котором на входном и выходном алфавитах соответствующие отображения действуют тождественно) $\beta: R(\gamma h, f) \rightarrow A'$, где $A' = (V_1, S, V_1, \delta', \lambda')$, $\delta'(s, x) = \delta(s, \alpha(x))$, $\lambda'(s, x) = \lambda(s, \alpha(x))$. Поэтому далее мы будем рассматривать только внутренние гомоморфизмы, причем термин внутренние будем опускать.

Начнем с описания гомоморфизмов регистра на регистр. В 1967 году К. Г. Тоболовым была обнаружена связь между операцией, схожей с операцией $\triangleleft$ и гомоморфизмами регистров без выхода на регистры без выхода. В идейном плане эту связь описывает следующая теорема, очевидным образом вытекающая из введенных определений.

Теорема 1. Пусть $n_i \geq 0$, $f_i \in F_{n_i+1}^*$, $i = 1, 2$. Тогда $\pi_{f_1, n_2}: R(f_2 \triangleleft f_1) \rightarrow R(f_2)$ — сюръективный гомоморфизм.

В. А. Башевым в 1972 году было доказано, что других гомоморфизмов регистра на регистр нет. Следующая теорема несколько уточняет этот результат.

Теорема 2. Пусть $n_1, n_2 \geq 0$, $f \in F_{n_1+n_2+1}^*$, $f_2 \in F_{n_2+1}$, $\beta: R(f) \rightarrow R(f_2)$ — гомоморфизм. Тогда $\beta = \pi_{f_1, n_2}$ для некоторой $f_1 \in F_{n_1+1}$. При этом, если $f_2 \in F_{n_2+1}^*$, то $f_1 \in F_{n_1+1}^*$ и $f = f_2 \triangleleft f_1$.

Доказательство. При $n_2 = 0$ теорема очевидна, так что далее $n_2 \geq 1$. Пусть $\beta_i \in F_{n_1+n_2}$, $i = 1, \dots, n_2$, — координатные функции отображения $\beta: V_{n_1+n_2} \rightarrow V_{n_2}$. По определению гомоморфизма

$$\begin{aligned} \beta(x_2, \dots, x_{n_1+n_2}, f(x_1, \dots, x_{n_1+n_2+1})) \\ = (\beta_2(x_1, \dots, x_{n_1+n_2}), \dots, \beta_{n_2}(x_1, \dots, x_{n_1+n_2}), f_2(\beta(x_1, \dots, x_{n_1+n_2}), x_{n_1+n_2+1})), \end{aligned}$$

то есть для $i = 1, \dots, n_2 - 1$

$$\beta_i(x_2, \dots, x_{n_1+n_2}, f(x_1, \dots, x_{n_1+n_2+1})) = \beta_{i+1}(x_1, \dots, x_{n_1+n_2}), \quad (1)$$

$$\beta_{n_2}(x_2, \dots, x_{n_1+n_2}, f(x_1, \dots, x_{n_1+n_2+1})) = f_2(\beta(x_1, \dots, x_{n_1+n_2}), x_{n_1+n_2+1}). \quad (2)$$

Индукцией по $i = n_2 - 1, \dots, 1$ докажем, что β_i не зависит от переменных с номерами $n_1 + i + 1, \dots, n_1 + n_2$. Поскольку $f \in F_{n_1+n_2+1}^*$, из (1) следует, что β_i не зависит от последней переменной и, следовательно, при $i = n_2 - 1$ утверждение верно. Допустим, что оно верно для некоторого i , $2 \leq i \leq n_2 - 1$. Тогда из (1) следует, что

$$\beta_i(x_1, \dots, x_{n_1+i}) = \beta_{i-1}(x_2, \dots, x_{n_1+n_2}),$$

так что доказываемое утверждение верно и для $i - 1$.

Итак, мы получили, что

$$\beta_1 = \beta_1(x_1, \dots, x_{n_1+1}).$$

Докажем теперь индукцией по $i = 1, \dots, n_2 - 1$, что

$$\beta_{i+1} = \beta_1(x_{i+1}, \dots, x_{n_1+i+1}).$$

При $i = 1$ это следует из (1). Допустим, что равенство верно для некоторого i , $1 \leq i \leq n_2 - 2$. Тогда из (1) следует, что

$$\beta_{i+2} = \beta_{i+1}(x_2, \dots, x_{n_1+n_2}) = \beta_1(x_{i+2}, \dots, x_{n_1+i+2}),$$

так что доказываемое равенство верно и для $i + 1$. Таким образом, мы показали, что

$$\beta = \pi_{f_1, n_2},$$

где $f_1 = \beta_1$.

Пусть теперь $f_2 \in F_{n_2+1}^*$. Из (2) получаем, что

$$f_1(x_{n_2+1}, \dots, x_{n_1+n_2}, f(x_1, \dots, x_{n_1+n_2+1})) = f_2(\pi_{f_1, n_2}(x_1, \dots, x_{n_1+n_2}), x_{n_1+n_2+1})$$

и, следовательно, $f_1 \in F_{n_1+1}^*$ и $f = f_2 \triangleleft f_1$. Теорема доказана.

Следующая теорема описывает гомоморфизмы регистров на регистры с произвольными выходными функциями.

Теорема 3. Пусть $n_1, n_2 \geq 0$, $f \in F_{n+1}^*$, $h \in F_{n+1}$, $f_2 \in F_{n_2+1}^*$, $h_2 \in F_{n_2+1}$, $\beta: V_n \rightarrow V_{n_2}$. Тогда следующие утверждения равносильны:

(1) $\beta: R(h, f) \rightarrow R(h_2, f_2)$ — гомоморфизм;

(2) $n \geq n_2$ и для некоторой $f_1 \in F_{n_1+1}^*$, где $n_1 = n - n_2$, выполняются равенства

$$\beta = \pi_{f_1, n_2},$$

$$f = f_2 \triangleleft f_1,$$

$$h = h_2 \triangleleft f_1.$$

Доказательство. Пусть выполнено (1). Автомат $R(h_2, f_2)$ является сильно связным, поэтому β сюръективно. Следовательно, $n \geq n_2$ и по теореме 2 $\beta = \pi_{f_1, n_2}$, $f_1 \in F_{n_1+1}^*$, $f = f_2 \triangleleft f_1$. Из гомоморфности по выходу следует, что

$$\begin{aligned} h(x_1, \dots, x_n, f(x_1, \dots, x_{n+1})) &= h_2(\pi_{f_1, n_2}(x_1, \dots, x_n), f_2(\pi_{f_1, n_2}(x_1, \dots, x_n), x_{n+1})) \\ &= h_2 \triangleleft f_1(x_1, \dots, x_n, f_2 \triangleleft f_1(x_1, \dots, x_{n+1})). \end{aligned}$$

Поскольку

$$f_2 \triangleleft f_1 = f \in F_{n+1}^*,$$

справедливо равенство

$$h = h_2 \triangleleft f_1.$$

Наоборот, пусть выполнено (2). Тогда по теореме 1 отображение β — гомоморфизм по состояниям. Поскольку $h = h_2 \triangleleft f_1$, аналогично предыдущему

$$h(x_1, \dots, x_n, f(x_1, \dots, x_{n+1})) = h_2(\pi_{f_1, n_2}(x_1, \dots, x_n), f_2(\pi_{f_1, n_2}(x_1, \dots, x_n), x_{n+1})),$$

так что β — гомоморфизм и по выходу. Теорема доказана.

Следствие 1. Пусть $n \geq 0$, $f, f' \in F_{n+1}^*$, $h, h' \in F_{n+1}$, $\beta: V_n \rightarrow V_n$. Тогда следующие утверждения равносильны:

- (1) $\beta: R(h, f) \rightarrow R(h', f')$ — изоморфизм;
- (2) для некоторого $c \in V_1$ и любых $x_1, \dots, x_{n+1} \in V_1$ выполняются равенства

$$\begin{aligned}\beta(x_1, \dots, x_n) &= (x_1 \oplus c, \dots, x_n \oplus c), \\ f(x_1, \dots, x_{n+1}) &= f'(x_1 \oplus c, \dots, x_{n+1} \oplus c), \\ h(x_1, \dots, x_{n+1}) &= h'(x_1 \oplus c, \dots, x_{n+1} \oplus c).\end{aligned}$$

Из этого следствия получаем, что для порядка группы автоморфизмов (не обязательно внутренних) регистра справедливо неравенство

$$|\text{Aut}(R(h, f))| \leq 2$$

для любых $f \in F_{n+1}^*$, $h \in F_{n+1}$.

Следующее утверждение описывает гомоморфизмы регистров на последовательное соединение регистров.

Следствие 2. Пусть $n, n_2, n'_2 \geq 0$, $f, h \in F_{n+1}^*$, $f_2, h_2 \in F_{n_2+1}^*$, $f'_2, h'_2 \in F_{n'_2+1}^*$, $\beta: V_n \rightarrow V_{n'_2} \times V_{n_2}$. Тогда следующие утверждения равносильны:

- (1) $\beta: R(h, f) \rightarrow R(h'_2, f'_2)R(h_2, f_2)$ — гомоморфизм;
- (2) $n_1 = n - n_2 \geq 0$, $n'_1 = n - n'_2 \geq 0$ и существуют $f_1 \in F_{n_1+1}^*$, $h'_1 \in F_{n'_1+1}^*$ такие, что выполняются равенства
 - (a) $\beta(\bar{x}) = (\pi_{h'_1, n'_2}(\bar{x}), \pi_{f_1, n_2}(\bar{x}))$ для любого $\bar{x} \in V_n$,
 - (b) $f = f_2 \triangleleft f_1$, $h = h'_2 \triangleleft h'_1$,
 - (c) $f'_2 \triangleleft h'_1 = h_2 \triangleleft f_1$.

Доказательство. Пусть $p: V_{n'_2} \times V_{n_2} \rightarrow V_{n_2}$, $p': V_{n'_2} \times V_{n_2} \rightarrow V_{n'_2}$ — проекции.

Пусть выполнено (1). Поскольку $p\beta: R(f) \rightarrow R(f_2)$ — гомоморфизм и $f_2 \in F_{n_2+1}^*$, по теореме 2

$$p\beta = \pi_{f_1, n_2}, \quad f = f_2 \triangleleft f_1.$$

Поскольку все три исходных регистра обратимы, переходя к обратным регистрам, получаем, что $p'\beta: R(h) \rightarrow R(h'_2)$ — гомоморфизм, и снова по теореме 2

$$p'\beta = \pi_{h'_1, n'_2}, \quad h = h'_2 \triangleleft h'_1.$$

Таким образом, (а) и (б) доказаны. Докажем (с). В силу (а) и (б) гомоморфность β по состояниям означает, что

$$\begin{aligned} & \beta(x_2, \dots, x_n, f_2 \triangleleft f_1(x_1, \dots, x_{n+1})) \\ &= ((h'_1(x_2, \dots, x_{n'_1+2}), \dots, h'_1(x_{n'_2+1}, \dots, x_n, f_2 \triangleleft f_1(x_1, \dots, x_{n+1}))), \\ & \quad (f_1(x_2, \dots, x_{n_1+2}), \dots, f_1(x_{n_2+1}, \dots, x_n, f_2 \triangleleft f_1(x_1, \dots, x_{n+1})))) \\ &= ((h'_1(x_2, \dots, x_{n'_1+2}), \dots, h'_1(x_{n'_2}, \dots, x_n), \\ & \quad f'_2(\pi_{h'_1, n'_2}(x_1, \dots, x_n), (h_2^* \oplus f_2^*)\pi_{f_1, n_2}(x_1, \dots, x_n) \oplus x_{n+1})), \\ & \quad (f_1(x_2, \dots, x_{n_1+2}), \dots, f_1(x_{n_2}, \dots, x_n), f_2(\pi_{f_1, n_2}(x_1, \dots, x_n), x_{n+1}))). \end{aligned}$$

Это равносильно равенству

$$\begin{aligned} & h'_1(x_{n'_2+1}, \dots, x_n, f_2 \triangleleft f_1(x_1, \dots, x_{n+1})) \\ &= f_2'^* \pi_{h'_1, n'_2}(x_1, \dots, x_n) \oplus h_2'^* \pi_{f_1, n_2}(x_1, \dots, x_n) \oplus f_2'^* \pi_{f_1, n_2}(x_1, \dots, x_n) \oplus x_{n+1}, \end{aligned}$$

то есть выполнено (с) и (2) доказано полностью.

Пусть теперь выполнено (2). Доказательство гомоморфности β по состояниям полностью аналогично доказательству пункта (с). Докажем гомоморфность по выходу:

$$\begin{aligned} & h_2'^* \pi_{h'_1, n'_2}(x_1, \dots, x_n) \oplus h_1'^* (x_{n'_2+1}, \dots, x_n) \oplus f_2'^* \pi_{f_1, n_2}(x_1, \dots, x_n) \\ & \quad \oplus f_1'^* (x_{n_2+1}, \dots, x_n) \\ & \quad \oplus x_{n+1} \\ &= h_2'^* \pi_{h'_1, n'_2}(x_1, \dots, x_n) \oplus f_2'^* \pi_{h'_1, n'_2}(x_1, \dots, x_n) \\ & \quad \oplus h_2'^* \pi_{f_1, n_2}(x_1, \dots, x_n) \\ & \quad \oplus f_2'^* \pi_{f_1, n_2}(x_1, \dots, x_n) \\ & \quad \oplus x_{n+1} \\ &= (h_2'^* \oplus f_2'^*) \pi_{h'_1, n'_2}(x_1, \dots, x_n) \\ & \quad \oplus (h_2'^* \oplus f_2'^*) \pi_{f_1, n_2}(x_1, \dots, x_n) \\ & \quad \oplus x_{n+1}. \end{aligned}$$

Следствие доказано.

Частным случаем этого следствия является следующее утверждение.

Следствие 3. Если $n_i \geq 0$, $f_i, h_i \in F_{n_i+1}^*$, $i = 1, 2$, и

$$f_2 \triangleleft h_1 = h_1 \triangleleft f_2,$$

то отображение $\beta: V_{n_1+n_2} \rightarrow V_{n_2} \times V_{n_1}$, определяемое равенством

$$\beta(\bar{x}) = (\pi_{h_1, n_2}(\bar{x}), \pi_{f_2, n_1}(\bar{x})),$$

является гомоморфизмом автоматов $\beta: R(h_2 \triangleleft h_1, f_1 \triangleleft f_2) \rightarrow R(h_2, f_2)R(h_1, f_1)$.

Состояние автомата A назовем существенным, если оно может появляться в любом такте его работы. Поскольку множество всех существенных состояний замкнуто относительно действия функции переходов, оно является множеством состояний подавтомата, который назовем существенным подавтоматом автомата A .

Следствие 4. Если $n_i \geq 0$, $f_i, h_i \in F_{n_i+1}^*$, $i = 1, 2$, и хотя бы одна из функций f_2^* , h_1^* нулевая, то отображение $\beta: V_{n_1+n_2} \rightarrow V_{n_2} \times V_{n_1}$, определяемое равенством

$$\beta(\bar{x}) = (\pi_{h_1, n_2}(\bar{x}), \pi_{f_2, n_1}(\bar{x})),$$

является гомоморфизмом автоматов $\beta: R(h_2 \triangleleft h_1, f_1 \triangleleft f_2) \rightarrow R(h_2, f_2)R(h_1, f_1)$, образ которого совпадает с существенным подавтоматом автомата $R(h_2, f_2)R(h_1, f_1)$, причем в автомате $R(h_2, f_2)R(h_1, f_1)$ после такта с номером $\max(n_1, n_2)$ появляются только существенные состояния.

Доказательство. Очевидно, что условие коммутативности следствия 3 выполнено. Поскольку автомат $R(h_2 \triangleleft h_1, f_1 \triangleleft f_2)$ сильно связан, его гомоморфный образ также сильно связан, так что все состояния образа существенны. Наоборот, пусть $\bar{y}$ — существенное состояние. Тогда для любого $l \geq 0$ оно является финальным для некоторых начального состояния $(\bar{s}_2, \bar{s}_1)$ и входной последовательности длины l .

При $f_2^* = 0$ возьмем $l = n_2$. Тогда $\beta(\bar{s}_1, \bar{x}) = \bar{y}$, где $\bar{x}$ — соответствующая последовательность, поступающая на вход накопителя (вектора текущего состояния) регистра $R(h_1, f_1)$.

При $h_1^* = 0$ возьмем $l = n_1$. Тогда $\beta(\bar{s}_2, \bar{x}) = \bar{y}$, где $\bar{x}$ — соответствующая последовательность, поступающая на вход накопителя регистра $R(h_2, f_2)$.

Следствие доказано.

Для того, чтобы перейти к описанию гомоморфизмов на произвольный автомат, нам потребуются следующие понятия.

Определение 1. Состояния $s, s' \in S$ автомата $A = (X, S, Y, \delta, \lambda)$ назовем совпадающими с задержкой k , $k \geq 0$, и в этом случае будем писать $s \simeq_k s'$, если любая входная последовательность длины k переводит их в одинаковые состояния. Соотношение $s \simeq s'$ будет обозначать тот факт, что $s \simeq_k s'$ для некоторого k , такие состояния назовем совпадающими с задержкой. Минимальное k , для которого $s \simeq_k s'$, назовем задержкой совпадения состояний в автомате A и обозначим через $\Delta(A)$.

Очевидно, что $\simeq_k$ и $\simeq$ являются бинарными отношениями эквивалентности на множестве S и для любого $k \geq 0$

$$\equiv = \simeq_0 \subseteq \simeq_k \subseteq \simeq_{k+1} \subseteq \simeq = \bigcup_{i=0}^{\infty} \simeq_i$$

(здесь и далее $\equiv$ означает совпадение состояний), причем, если $\simeq_{k'} = \simeq_{k'+1}$ для некоторого k' , то $\simeq_{k'} = \simeq_k = \simeq$ для любого $k \geq k'$. Следовательно,

$$0 \leq \Delta(A) \leq |S| - 1,$$

так что для автомата с конечным числом состояний задержка всегда конечна.

Определение 2. Внутренний гомоморфизм автоматов $\beta: A \rightarrow A'$ назовем изоморфизмом с задержкой, если отображение β сюръективно и все состояния любого полного прообраза совпадают с задержкой, то есть для любых $s, s' \in S$ из равенства $\beta(s) = \beta(s')$ следует, что $s \simeq s'$.

Если A — автомат без выхода, то отношения $\simeq_k$ и $\simeq$ являются конгруэнциями автомата A и, следовательно, естественные гомоморфизмы $\bar{\beta}_k: A \rightarrow A/\simeq_k$ и $\bar{\beta}: A \rightarrow A/\simeq$ являются изоморфизмами с задержкой. При этом любой изоморфизм с задержкой $\beta: A \rightarrow A'$ автоматов без выхода продолжается до гомоморфизма $\bar{\beta}$ (то есть $\beta'\beta = \bar{\beta}$ для некоторого изоморфизма с задержкой $\beta': A' \rightarrow A/\simeq$).

Следующие два очевидных утверждения описывают случаи, когда отношение $\simeq$ тривиально, то есть совпадает с отношением $\equiv$.

Предложение 1. Для любого автомата $A = (X, S, Y, \delta, \lambda)$ следующие свойства равносильны:

- (1) $\simeq = \equiv$;
- (2) $\Delta(A) = 0$;
- (3) для любых различных $s, s' \in S$ существует $x \in X$ такой, что $\delta(s, x) \neq \delta(s', x)$ (то есть все строки таблицы функции переходов δ различны).

Следствие 5. Если хотя бы одна из частичных функций переходов автомата A является подстановкой, то $\Delta(A) = 0$.

Следующее утверждение устанавливает связь отношения $\simeq$ с некоторыми характеристиками графа автомата.

Предложение 2. Пусть $A = (X, S, Y, \delta, \lambda)$ — произвольный автомат, $l \geq 1$, $\bar{x} = (x_1, \dots, x_l) \in X^l$, $c_{\bar{x}}$ — число циклических точек преобразования $\delta_{\bar{x}} = \delta_{x_l} \dots \delta_{x_1}$ множества S . Тогда $|S/\simeq| \geq c_{\bar{x}}$, причем выполняется равенство, если автомат A автономен. Если $l \geq \Delta(A)$, то $|S/\simeq| \geq |\delta_{\bar{x}}(S)|$.

Доказательство. Если s, s' — различные циклические точки преобразования $\delta_{\bar{x}}$, то последовательность $\bar{x}, \bar{x}, \dots$ переводит эти состояния в различные для любого числа повторений $\bar{x}$, так что $s \not\simeq s'$ и первое неравенство доказано. Для автономного автомата A оно превращается в равенство, поскольку в этом случае множество циклических точек преобразования $\delta_{\bar{x}}$ не зависит от $\bar{x}$ и l и всякая точка подхода преобразования δ совпадает с задержкой с некоторой циклической. Наконец, если $l \geq \Delta(A)$ и $\delta_{\bar{x}}(s) \neq \delta_{\bar{x}}(s')$, то $s \not\simeq s'$ по определению $\Delta(A)$ и, следовательно, выполняется второе неравенство. Предложение доказано.

В заключение рассмотрения общих свойств отношения $\simeq$ приведем один достаточно очевидный алгоритм получения фактор-автомата $A/\simeq$, который естественно назвать табличным. Пусть $A = (X, S, \delta)$ — произвольный автомат без выхода, который задан таблицей своей функции переходов δ , то есть матрицей размера $|S| \times |X|$, строки которой занумерованы элементами множества S , столбцы — элементами множества X , а на пересечении s -й строки и столбца с номером x стоит $\delta(s, x)$. В этой таблице выделим все классы одинаковых строк. В каждом классе выберем одну строку, а остальные удалим. В полученной таблице каждое состояние, являющееся номером удаленной строки, заменим на номер выбранной строки в классе, содержащем эту удаленную строку. Очевидно, что

мы получим таблицу автомата, изоморфного автомату $A/\simeq_1$. Ясно, что повторяя эту процедуру еще $\Delta(A) - 1$ раз (то есть пока не придем к таблице с различными строками) мы получим таблицу автомата, изоморфного автомату $A/\simeq$.

Вернемся теперь к регистрам сдвига. Всюду далее через $\sim$ обозначается отношение эквивалентности (неотличимости) состояний соответствующего автомата.

Теорема 4. Для любых $n \geq 0$ и $f \in F_{n+1}^*$ бинарные отношения $\simeq$ и $\sim$ для автомата $R'(f)$ совпадают и $\Delta(R(f)) \leq n$, причем равенство выполняется тогда и только тогда, когда функция f^* равна постоянной.

Прежде чем перейти непосредственно к доказательству теоремы, приведем следующее очевидное вспомогательное утверждение.

Лемма 1. Для любых $0 \leq k \leq n$, $\bar{s}, \bar{s}' \in V_n$, $\bar{s} = (s_1, \dots, s_n)$, $\bar{s}' = (s'_1, \dots, s'_n)$, $f \in F_{n+1}^*$ следующие утверждения для автомата $R(f)$ равносильны:

- (1) $\bar{s} \simeq_k \bar{s}'$;
- (2) $s_j = s'_j$ для всех $j = k + 1, \dots, n$ и

$$f(s_i, \dots, s_n, s_{n+1}, \dots, s_{n+i}) = f(s'_i, \dots, s'_n, s_{n+1}, \dots, s_{n+i})$$

для любых $i = 1, \dots, k$ и $s_{n+1}, \dots, s_{n+i} \in V_1$.

Доказательство теоремы 4. Пусть i_1 — минимальный номер существенной переменной функции f . Если $i_1 = n + 1$, то функция f^* равна постоянной и $\Delta(R(f)) = n$. Пусть $i_1 \leq n$. Допустим, что $\simeq_{n-1} \neq \simeq_n$, то есть существуют $\bar{s}, \bar{s}' \in V_n$ такие, что $\bar{s} \simeq_n \bar{s}'$ и $\bar{s} \not\simeq_{n-1} \bar{s}'$. В силу леммы 1

$$f(s_i, \dots, s_n, s_{n+1}, \dots, s_{n+i}) = f(s'_i, \dots, s'_n, s_{n+1}, \dots, s_{n+i})$$

для любых $i = 1, \dots, n$, $s_{n+1}, \dots, s_{n+i} \in V_1$, причем $s_n \neq s'_n$. Отсюда при $i = n - i_1 + 1$ получаем, что i_1 — номер несущественной переменной функции f , и мы приходим к противоречию. Следовательно, $\simeq_{n-1} = \simeq_n$, так что $\Delta(R(f)) \leq n - 1$, если $i_1 \leq n$.

Осталось доказать, что $\simeq = \sim$. Это следует из очевидных равенств $\sim = \sim_n = \simeq_n = \simeq$, где через $\sim_n$ обозначено отношение n -эквивалентности.

Теорема доказана.

Следствие 6. Если $n \geq 0$, $f \in F_{n+1}^*$, $\bar{s}, \bar{s}' \in V_n$, то для автомата $R(f)$ справедливы следующие утверждения:

- (1) если $f^*(\bar{s}) \neq f^*(\bar{s}')$, то $\bar{s} \not\simeq \bar{s}'$;
- (2) если f^* не является постоянной и последние координаты векторов $\bar{s}$ и $\bar{s}'$ различны, то $\bar{s} \not\simeq \bar{s}'$;
- (3) $|V_n/\simeq| = 1$ тогда и только тогда, когда f^* — постоянная;
- (4) $|V_n/\simeq| = 2^{n-1} + \|f_1\|$, где $f^*(x_1, \dots, x_n) = x_1 f_1(x_2, \dots, x_n) \oplus f_0(x_2, \dots, x_n)$, $\|f_1\| = |f_1^{-1}(1)|$.

Доказательство очевидно.

Следующее утверждение описывает все изоморфизмы с задержкой регистра на регистр.

Теорема 5. Пусть $n, n_2 \geq 0$, $f \in F_{n+1}^*$, $f_2 \in F_{n_2+1}^*$, $\beta: V_n \rightarrow V_{n_2}$. Тогда следующие утверждения равносильны:

- (1) $\beta: R(f) \rightarrow R(f_2)$ — изоморфизм с задержкой;
- (2) $n_1 = n - n_2 \geq 0$, $\beta = \pi_{f_1, n_2}$, $f = f_2 \triangleleft f_1$, где $f_1 = c \oplus x_{n_1+1}$, $c \in V_1$.

При этом, если функция f существенно зависит от первой переменной, то утверждение (1) равносильно утверждению, состоящему в том, что $\beta: R(f) \rightarrow R(f_2)$ — изоморфизм.

Доказательство. Пусть выполнено (1). Тогда по теореме 2

$$n_1 = n - n_2 \geq 0, \quad \beta = \pi_{f_1, n_2}, \quad f = f_2 \triangleleft f_1, \quad f_1 \in F_{n_1+1}^*.$$

Допустим, что f_1^* не равна постоянной, то есть существуют $\bar{s} = (s_1, \dots, s_{n_1})$ и $\bar{s}' = (s'_1, \dots, s'_{n_1})$ такие, что $f_1^*(\bar{s}) \neq f_1^*(\bar{s}')$. Тогда по следствию 6 получаем, что $\bar{s} \neq \bar{s}'$ в $R(f_1)$, так что существует входная последовательность $(\alpha_1, \dots, \alpha_{n-1})$, переводящая $\bar{s}$ и $\bar{s}'$ в различные состояния. Пусть

$$\begin{aligned} R'(f_1)_{\bar{s}}(\alpha_1, \dots, \alpha_{n-1}) &= (s_{n_1+1}, \dots, s_{n_1+n-1}), \\ R'(f_1)_{\bar{s}'}(\alpha_1, \dots, \alpha_{n-1}) &= (s'_{n_1+1}, \dots, s'_{n_1+n-1}) \end{aligned}$$

(здесь и далее через A_s обозначается автоматное отображение автомата A при начальном состоянии s). Тогда $s_{n+i_0} \neq s'_{n+i_0}$ для некоторого i_0 , $0 \leq i_0 \leq n_1 - 1$. Положим

$$\bar{s}_0 = (s_{1+i_0}, \dots, s_{n+i_0}), \quad \bar{s}'_0 = (s'_{1+i_0}, \dots, s'_{n+i_0}).$$

Тогда

$$\pi_{f_1, n_2}(\bar{s}_0) = (\alpha_{i_0+1}, \dots, \alpha_{i_0+n_2}) = \pi_{f_1, n_2}(\bar{s}'_0).$$

Поскольку $\beta = \pi_{f_1, n_2}$ — изоморфизм с задержкой, отсюда следует, что $\bar{s}_0 \simeq \bar{s}'_0$ в $R(f)$. Тогда f^* — постоянная в силу утверждения (2) следствия 6. Поскольку β сюръективно, все состояния автомата $R(f_2)$ совпадают с задержкой, и по следствию 6 f_2^* — постоянная. Поскольку $f = f_2 \triangleleft f_1$, то и f_1^* является постоянной. Получаем противоречие с исходным предположением.

Пусть выполнено (2). Тогда по теореме 1 отображение β является сюръективным гомоморфизмом и

$$f = f_2(c \oplus x_{n_1+1}, \dots, c \oplus x_{n_1+n+1}).$$

Поскольку для любого $(s_1, \dots, s_{n_2}) \in V_{n_2}$

$$\beta^{-1}(s_1, \dots, s_{n_2}) = \{(\alpha_1, \dots, \alpha_{n_1}, c \oplus s_1, \dots, c \oplus s_{n_2}) \mid (\alpha_1, \dots, \alpha_{n_1}) \in V_{n_1}\},$$

все состояния из $\beta^{-1}(s_1, \dots, s_{n_2})$ совпадают с задержкой n_1 , и (1) доказано.

В случае, когда f существенно зависит от 1-й переменной, из (2) следует, что $n_1 = 0$, так что β — изоморфизм.

Теорема доказана.

Центральным результатом настоящей работы является следующая теорема о разложении произвольного гомоморфизма регистра в композицию гомоморфизма на регистр и изоморфизма с задержкой, причем разложению, по существу, однозначному.

Теорема 6. Пусть $n \geq 0$, $f \in F_{n+1}^*$, $h \in F_{n+1}$, $A = (V_1, S, V_1, \delta, \lambda)$, $\bar{A} = (V_1, S, \delta)$, $\beta: R(f) \rightarrow \bar{A}$ — сюръективный гомоморфизм. Тогда существуют $n_1 \in \{0, 1, \dots, n\}$, $f_1 \in F_{n_1+1}^*$, $f_2 \in F_{n_2+1}^*$, где $n_2 = n - n_1$, и изоморфизм с задержкой $\beta_2: R(f_2) \rightarrow \bar{A}$ такие, что $f = f_2 \triangleleft f_1$, $\beta_1 = \pi_{f_1, n_2}: R(f) \rightarrow R(f_2)$ — сюръективный гомоморфизм и выполняются следующие свойства:

$$(1) \beta = \beta_2 \beta_1;$$

(2) если $\beta = \beta'_2 \beta'_1$, где $\beta'_1: R(f) \rightarrow R(f'_2)$ — гомоморфизм, $\beta'_2: R(f'_2) \rightarrow \bar{A}$ — изоморфизм с задержкой, $f'_2 \in F_{n'_2+1}^*$, $n'_2 \in \{0, 1, \dots, n\}$, то

$$m = n_2 - n'_2 \geq 0$$

и для некоторого $c \in V_1$ выполняются равенства

$$\begin{aligned} \beta'_1 &= \pi_{f'_1, n'_2} = \pi_{(c \oplus x_{m+1}), n'_2} \beta_1, & f'_1 &= (c \oplus x_{m+1}) \triangleleft f_1, \\ \beta_2 &= \beta'_2 \pi_{(c \oplus x_{m+1}), n_2}, & f_2 &= f'_2 \triangleleft (c \oplus x_{m+1}); \end{aligned}$$

(3) если $\beta: R(h, f) \rightarrow A$ — гомоморфизм, то существует $h_2 \in F_{n_2+1}$ такая, что $h = h_2 \triangleleft f_1$ и $\beta_1: R(h, f) \rightarrow R(h_2, f_2)$, $\beta_2: R(h_2, f_2) \rightarrow A$ — гомоморфизмы.

При этом, если f существенно зависит от первой переменной, то в пункте (2)

$$n_2 = n'_2, \quad f'_1 = f_1 \oplus c, \quad f'_2 = f_2(x_1 \oplus c, \dots, x_{n_2+1} \oplus c), \quad \beta'_2 = \beta_2(x_1 \oplus c, \dots, x_{n_2} \oplus c).$$

Доказательство. Рассмотрим автомат

$$M(f) = R'(f)R_0(f),$$

и пусть

$$T = \{(\bar{s}, \bar{s}') \mid \bar{s}, \bar{s}' \in V_n, \beta(\bar{s}) = \beta(\bar{s}')\}.$$

Поскольку β — гомоморфизм, то множество состояний T замкнуто относительно действия функции переходов автомата $M(f)$. Пусть B — подавтомат автомата $M(f)$ с множеством состояний T .

Нам потребуются терминология и результаты работы [2]. По теоремам 5 и 6 из [2] для длины транзитивности автомата $M(f)$ справедливо неравенство $t(M(f)) \leq n$, и следовательно, $t(B) \leq n$. Пусть $n_1 = t(B)$, f_1 — индикатор орбит автомата B на V_{n_1+1} . Тогда по теореме 9 из [2] существует $f_2 \in F_{n_2+1}$, где $n_2 = n - n_1$, такая, что $f = f_2 \triangleleft f_1$. Поскольку $f \in F_{n+1}^*$, то и $f_i \in F_{n_i+1}^*$, $i = 1, 2$, и по теореме 1 $\beta_1 = \pi_{f_1, n_2}: R(f) \rightarrow R(f_2)$ — сюръективный гомоморфизм.

Определим отображение $\beta_2: V_{n_2} \rightarrow S$ следующим образом. По теореме 9 из [2] $\{\beta_1^{-1}(\bar{\alpha}) \mid \bar{\alpha} \in V_{n_2}\}$ — множество всех орбит группы G_n подстановок множества V_n , порожденной множеством всех ограниченных на длине n автоматных отображений автомата B . Из определения автомата B следует, что если $\bar{s}$ и $\bar{s}'$ принадлежат одной орбите группы G_n , то $\beta(\bar{s}) = \beta(\bar{s}')$. Поэтому существует единственное отображение $\beta_2: V_{n_2} \rightarrow S$, для которого $\beta = \beta_2 \beta_1$, и это отображение определяется формулой $\beta_2(\bar{\alpha}) = \beta(\bar{s})$ для любых $\bar{\alpha} \in V_{n_2}$, $\bar{s} \in \beta_1^{-1}(\bar{\alpha})$. Поскольку β, β_1 — сюръективные гомоморфизмы автоматов, то и $\beta_2: R(f_2) \rightarrow \bar{A}$ — сюръективный гомоморфизм автоматов.

Докажем, что β_2 — изоморфизм с задержкой. Пусть ρ_f, ρ_{f_2} — функции переходов соответственно автоматов $R(f)$ и $R(f_2)$. Сначала заметим, что если $\beta(\bar{s}_1) = \beta(\bar{s}_2)$, то

для любого $\bar{x} \in V_n$ состояния $\rho_f(\bar{s}_1, \bar{x})$ и $\rho_f(\bar{s}_2, \bar{x})$ принадлежат одной орбите группы G_n , поскольку, подавая на вход автомата B в начальном состоянии $(\bar{s}_2, \bar{s}_1)$ последовательность $\rho_f(\bar{s}_1, \bar{x})$, получим на выходе последовательность $\rho_f(\bar{s}_2, \bar{x})$. Пусть теперь $\beta_2(\bar{\alpha}_1) = \beta_2(\bar{\alpha}_2)$. Возьмем $\bar{s}_i \in \beta_1^{-1}(\bar{\alpha}_i)$, $i = 1, 2$. Тогда

$$\beta(\bar{s}_1) = \beta(\bar{s}_2),$$

и следовательно, для любого $\bar{x} \in V_n$

$$\rho_{f_2}(\bar{\alpha}_1, \bar{x}) = \beta_1(\rho_f(\bar{s}_1, \bar{x})) = \beta_1(\rho_f(\bar{s}_2, \bar{x})) = \rho_{f_2}(\bar{\alpha}_2, \bar{x}),$$

то есть $\bar{\alpha}_1 \simeq_n \bar{\alpha}_2$. Пункт (1) теоремы доказан.

Докажем пункт (2). При $n'_2 = 0$ утверждение (2) очевидно в силу теоремы 5. Поэтому далее считаем, что $n'_2 \geq 1$. По теореме 2

$$\beta'_1 = \pi_{f'_1, n'_2}, \quad f'_1 \in F_{n'_1+1}^*, \quad n'_1 = n - n'_2, \quad f = f'_2 \triangleleft f'_1.$$

Пусть $(\bar{s}, \bar{s}') \in T$, то есть $\beta(\bar{s}) = \beta(\bar{s}')$. Тогда $\beta'_1(\bar{s}) \simeq \beta'_1(\bar{s}')$ и $\beta'_1(\bar{s}) \simeq_n \beta'_1(\bar{s}')$ по теореме 4. Отсюда и из гомоморфности β'_1 следует, что

$$\beta'_1(\rho_f(\bar{s}, \bar{x})) = \beta'_1(\rho_f(\bar{s}', \bar{x}))$$

для любого $\bar{x} \in V_n$.

Доказанное означает, что отображение β'_1 постоянно на орбитах группы G_n . Поскольку $\beta'_1 = \pi_{f'_1, n'_2}$ и $n'_2 \geq 1$, функция f'_1 постоянна на орбитах группы $G_{n'_1+1}$. Тогда по теореме 9 из [2] получаем, что

$$n'_1 \geq n_1, \quad f'_1 = \varphi \triangleleft f_1, \quad \varphi \in F_{m+1}^*, \quad m = n'_1 - n_1 = n_2 - n'_2 \geq 0.$$

Отсюда следует, что

$$\beta'_1 = \pi_{\varphi, n'_2} \pi_{f_1, n_2}.$$

Из равенств

$$f_2 \triangleleft f_1 = f = f'_2 \triangleleft \varphi \triangleleft f_1$$

получаем, что

$$f_2 = f'_2 \triangleleft \varphi.$$

Поскольку

$$\beta_2 \beta_1 = \beta = \beta'_2 \pi_{\varphi, n'_2} \beta_1$$

и β_1 сюръективно, то

$$\beta_2 = \beta'_2 \pi_{\varphi, n'_2}.$$

Отсюда следует, что π_{φ, n'_2} — изоморфизм с задержкой, так как β_2 — изоморфизм с задержкой, и по теореме 5

$$\varphi = c \oplus x_{m+1}, \quad c \in V_1.$$

Пункт (2) теоремы доказан.

Докажем пункт (3). Определим $h_2 \in F_{n_2+1}$, полагая

$$h_2(\bar{s}, x) = \lambda(\beta_2(\bar{s}), f_2(\bar{s}, x))$$

для любых $\bar{s} \in V_{n_2}$, $x \in V_1$. Тогда $\beta_2: R(h_2, f_2) \rightarrow A$ — гомоморфизм, так как $f_2 \in F_{n_2+1}^*$. Но тогда и $\beta_1: R(h, f) \rightarrow R(h_2, f_2)$ — гомоморфизм, и по теореме 3 получаем, что $h = h_2 \triangleleft f_1$. Пункт (3) теоремы доказан.

Наконец, в случае, когда f существенно зависит от 1-й переменной, получаем, что $m = 0$, так как

$$f = f'_2 \triangleleft (c \oplus x_{m+1}) \triangleleft f_1.$$

Теорема доказана.

Теорема 6 сводит описание гомоморфизмов регистров к описанию разложений функций обратной связи по операции $\triangleleft$ и описанию соответствующих изоморфизмов с задержкой. Одним из следствий этой теоремы является следующее утверждение. При $f \in F_{n+1}^*$ всякий сюръективный гомоморфизм регистра $R(f)$ может быть продолжен до гомоморфизма на фактор-автомат $R(f_2)/\simeq$, где $f = f_2 \triangleleft f_1$, а конгруэнция $\simeq$ описывается леммой из доказательства теоремы 4.

Автомат называют подстановочным, если все его частичные функции переходов являются подстановками множества состояний. Очевидно, что для двоичного регистра сдвига ненулевой длины подстановочность равносильна линейности функции обратной связи по 1-й переменной, а в случае линейности функции обратной связи по последней переменной равносильна еще и отсутствию различных совпадающих с задержкой состояний (утверждение (4) следствия 6). Следовательно, неподстановочный регистр сдвига без выхода длины 2 и более с линейной по последней переменной функцией обратной связи всегда имеет нетривиальные изоморфизмы с задержкой.

Следствие 7. *Любой гомоморфный образ подстановочного двоичного регистра сдвига с линейной по последней переменной функцией обратной связи изоморфен некоторому подстановочному двоичному регистру сдвига с линейной по последней переменной функцией обратной связи.*

Доказательство. Поскольку гомоморфный образ подстановочного автомата является подстановочным, подстановочным является регистр $R(h_2, f_2)$ из теоремы 6. Тогда β_2 — изоморфизм, так как для подстановочных автоматов $\simeq = \equiv$.

Следствие доказано.

Заметим, что следствие 7 для случая регистров без выхода было доказано А. Я. Прососовым в 1977 году.

Следствие 8. *Любой гомоморфный образ двоичного регистра сдвига с линейной по последней переменной функцией обратной связи и линейной по первой и последней переменным выходной функцией изоморфен некоторому двоичному регистру сдвига с линейной по последней переменной функцией обратной связи и линейной по первой и последней переменным выходной функцией.*

Доказательство. Поскольку гомоморфный образ обратимого автомата является обратимым и (в обозначениях теоремы 6) $\beta: R(f, h) \rightarrow A^{-1}$ — сюръективный гомоморфизм,

по следствию 7 автомат A^{-1} изоморфен некоторому обратимому подстановочному двоичному регистру сдвига. Обратимость двоичного регистра равносильна линейности его функций по последней переменной, а подстановочность — линейности по первой переменной функции обратной связи.

Следствие доказано.

Рассмотрим теперь множество всех двоичных функций

$$f = \bigcup_{n=0}^{\infty} F_{n+1}.$$

Относительно операции $\triangleleft$ оно является моноидом с единичным элементом $x_1 \in F_1$. Следовательно, на множестве F возникает соответствующее транзитивное и рефлексивное бинарное отношение делимости (справа) $|$, которое определяется следующим образом: $f_1 | f$ тогда и только тогда, когда $f = f_2 \triangleleft f_1$ для некоторой $f_2 \in F$ (которая называется частным от деления f на f_1 , а f_1 — делителем f). Это отношение не является симметричным, поскольку $f_1 | f$ и $f | f_1$ только в случае, когда f и f_1 являются функциями от одинакового количества переменных и $f \oplus f_1$ — функция, равная постоянной. Кроме того, частное не всегда определено однозначно. Точнее, справедливо следующее свойство: частное от деления на функцию f_1 всегда определено однозначно тогда и только тогда, когда f_1 является функцией без запретов (то есть отображение π_{f_1, n_2} является сюръективным для любого $n_2 \geq 0$, что равносильно возможности появления на выходе регистра $R_0(f_1)$ любой двоичной последовательности, см. [3]). В частности, все функции из подмоноида

$$F^* = \bigcup_{n=0}^{\infty} F_{n+1}^*$$

моноида F являются функциями без запретов.

Введенное отношение делимости функций является продолжением отношения делимости многочленов в следующем смысле. Обозначим через L^* подмоноид моноида F^* , состоящий из всех линейных функций из F^* , а через $GF(2)[x]^*$ — моноид всех ненулевых многочленов над полем $GF(2)$. Тогда отображение $GF(2)[x]^* \rightarrow L^*$, где $c_0 \oplus c_1x \oplus \dots \oplus c_nx^n \mapsto c_0x_1 \oplus c_1x_2 \oplus \dots \oplus c_nx_{n+1}$ является изоморфизмом и, следовательно, сохраняет отношение делимости.

Наибольшим общим делителем функций $h, f \in F$ назовем любой их общий делитель от наибольшего количества переменных. Множество всех наибольших общих делителей функций h и f обозначим через (h, f) . Оно не пусто, поскольку функции $x_1, 1 \oplus x_1 \in F_1$ являются делителями любой функции из F . Функции $h, f \in F$ назовем взаимно простыми, если

$$(h, f) = \{x_1, 1 \oplus x_1\}.$$

Теорема 7. Пусть $n \geq 0$, $f \in F_{n+1}^*$, $h \in F_{n+1}$. Тогда

$$(h, f) = \{f_1, 1 \oplus f_1\},$$

где $f_1 \in F_{n_1+1}^*$, $n_1 \leq n$, причем для любой функции $f'_1 \in F$ следующие утверждения

Рис. 1. Коммутативная диаграмма 1

Рис. 2. Коммутативная диаграмма 2

равносильны:

- (1) $f'_1 \mid h \ f'_1 \mid f$;
- (2) $f'_1 \mid f$.

При этом существует коммутативная диаграмма 1 гомоморфизмов автоматов (см. рис. 1), где β — естественный гомоморфизм автомата $R(h, f)$ на свою приведенную форму $R(h, f)/\sim$, $\beta_1 = \pi_{f_1, n_2}$, $n_2 = n - n_1$, $f_2 \in F_{n_2+1}^*$, $h_2 \in F_{n_2+1}$, $f = f_2 \triangleleft f_1$, $h = h_2 \triangleleft f_1$, β_2 — изоморфизм с задержкой.

Доказательство. Выберем в соответствии с пунктами (1) и (3) теоремы 6 указанную диаграмму с наибольшим n_1 . Осталось доказать утверждение о наибольшем общем делителе. Для этого достаточно показать, что из утверждения (1) следует утверждение (2). Пусть выполнено (1), то есть

$$\begin{aligned} f &= f'_2 \triangleleft f'_1, \\ h &= h'_2 \triangleleft f'_1. \end{aligned}$$

Поскольку β — естественный гомоморфизм, по теоремам 3 и 6 существует коммутативная диаграмма 2 (см. рис. 2), где

$$\begin{aligned} f'_2 &= f''_2 \triangleleft f''_1, \\ h'_2 &= h''_2 \triangleleft f''_1, \\ \beta'_1 &= \pi_{f''_1, n''_2}, \end{aligned}$$

β'_2 — изоморфизм с задержкой.

Если $n_2 = 0$, то

$$f_1 = c_0 \oplus f,$$

и утверждение (2) выполнено.

Пусть $n_2 \geq 1$. Тогда и $n_2'' \geq 1$, так как $n_1 \geq n_1''$ в силу максимальности n_1 . Тогда из пункта (2) теоремы 6 следует, что для некоторой функции f_0 выполняются равенства

$$\begin{aligned} f_1 &= (c \oplus x_{m+1}) \triangleleft f_0, \\ f_1'' \triangleleft f_1' &= (c' \oplus x_{m'+1}) \triangleleft f_0, \end{aligned}$$

где $m \geq m'$. Следовательно,

$$f_1 = (c \oplus c' \oplus x_{m-m'+1}) \triangleleft f_1'' \triangleleft f_1',$$

и утверждение (2) выполнено.

Теорема доказана.

Следствие 9. Пусть $n \geq 0$, $f \in F_{n+1}^*$, $h \in F_{n+1}$ и выполнено хотя бы одно из условий:

- (а) f линейна по первой переменной;
- (б) h линейна по первой и $(n+1)$ -й переменным.

Тогда следующие утверждения равносильны:

- (1) автомат $R(h, f)$ не имеет различных эквивалентных состояний (то есть минимален);
- (2) функции h и f взаимно просты.

Доказательство. По теореме 7 из (1) следует (2). Наоборот, пусть выполнено (2). Тогда при условии (а) гомоморфизмы β_1, β_2 из теоремы 7 являются изоморфизмами и (1) выполнено. Если же выполнено условие (б), то условие (а) выполнено для h , и следовательно, $R(f, h)$ минимален. Поскольку $R(h, f) = R(f, h)^{-1}$, то и $R(h, f)$ минимален.

Следствие доказано.

В качестве примеров применения теоремы 7 приведем еще два следствия, описывающие некоторые неэквивалентные состояния регистров.

Следствие 10. Пусть $n \geq 1$, $f, h \in F_{n+1}^*$, $f \oplus h$ не является постоянной. Тогда $(\alpha_1, \dots, \alpha_{n-1}, 0) \approx (\alpha_1, \dots, \alpha_{n-1}, 1)$ в $R(h, f)$ для любых $\alpha_1, \dots, \alpha_{n-1} \in V_1$.

Доказательство. Допустим противное. Тогда в обозначениях теоремы 7

$$\begin{aligned} (\gamma_1, \dots, \gamma_{n_2-1}, \gamma_{n_2}) &= \pi_{f_1, n_2}(\alpha_1, \dots, \alpha_{n-1}, 0) \\ &\simeq \pi_{f_1, n_2}(\alpha_1, \dots, \alpha_{n-1}, 1) = (\gamma_1, \dots, \gamma_{n_2-1}, \gamma_{n_2} \oplus 1) \end{aligned}$$

в $R(h_2, f_2)$, причем $n_2 \geq 1$, так как $f \oplus h$ не является постоянной. Тогда $f_2 = c \oplus x_{n_2+1}$ по следствию 6. Так как $(\gamma_1, \dots, \gamma_{n_2-1}, \gamma_{n_2}) \sim (\gamma_1, \dots, \gamma_{n_2-1}, \gamma_{n_2} \oplus 1)$ в $R(h_2, f_2)$, то $h_2 = c' \oplus x_{n_2+1}$, и следовательно, $f \oplus h = c \oplus c'$ не является постоянной.

Следствие доказано.

Следствие 11. Пусть $n \geq 1$, $f, h \in F_{n+1}^*$, $f \oplus h$ не является постоянной и выполнено одно из следующих условий:

(а) хотя бы одна из функций f , h принимает разные значения на векторах $(0, \dots, 0), (1, \dots, 1) \in V_{n+1}$;

(б) $f_1(0, \dots, 0) \neq f_1(1, \dots, 1)$, где $f_1 \in (h, f)$.

Тогда $(0, \dots, 0) \approx (1, \dots, 1)$ в $R(h, f)$.

Доказательство. Очевидно, что из (а) следует (б). Пусть выполнено (б). Допустим, что $(0, \dots, 0) \sim (1, \dots, 1)$ в $R(h, f)$. Отсюда следует, что в обозначениях теоремы 7 $(0, \dots, 0) \simeq (1, \dots, 1)$ в $R(h_2, f_2)$, где $n_2 \geq 1$. Далее доказательство полностью аналогично доказательству следствия 10.

В заключение укажем на возможные обобщения изложенных результатов на случай регистра $R(h, f)$, где $f: X^{n+1} \rightarrow X$, $h: X^{n+1} \rightarrow Y$, X, Y — произвольные конечные множества. Так, теоремы 1, 2, 3 без особых затруднений могут быть обобщены следующим образом.

Функцию $\varphi: X^{m+1} \rightarrow X$ назовем биективной по последней (то есть $(m+1)$ -й) переменной, если при любой фиксации всех остальных переменных получаемое отображение $X \rightarrow X$ является биекцией. В этом случае через φ^{-1} обозначим функцию, обратную к функции φ по последней переменной, то есть $\varphi^{-1}: X^{m+1} \rightarrow X$ и

$$\varphi^{-1}(x_1, \dots, x_m, \varphi(x_1, \dots, x_{m+1})) = x_{m+1}$$

для любых $x_1, \dots, x_{m+1} \in X$.

Теорема 8. Пусть $n, n_2 \geq 0$, $f: X^{n+1} \rightarrow X$, $f_2: X^{n_2+1} \rightarrow X$ — биективные по последней переменной функции, $h: X^{n+1} \rightarrow X$, $h_2: X^{n_2+1} \rightarrow X$, $\beta: X^n \rightarrow X^{n_2}$.

Тогда следующие утверждения равносильны:

(1) $\beta: R(h, f^{-1}) \rightarrow R(h_2, f_2^{-1})$ — гомоморфизм;

(2) $n \geq n_2$, $\beta = \pi_{f_1, n_2}$, $f = f_2 \triangleleft f_1$, $h = h_2 \triangleleft f_1$ для некоторой биективной по последней переменной функции $f_1: X^{n_1+1} \rightarrow X$, где $n_1 = n - n_2$.

Автор посвящает эту работу памяти своего отца Игоря Георгиевича Солодовникова, изобретателя и конструктора реальных автоматов.

Список литературы

1. Golomb S. W., *Shift register sequences*. Holden-Day, San Francisco, 1967.
2. Солодовников В. И., О полугруппе, порожденной автоматными отображениями обратимого автомата. *Труды по дискретной математике* (2001) 4, 231–242.
3. Сумароков С. Н., Запреты двоичных функций и обратимость для одного класса кодирующих устройств. *Обозрение прикладной и промышленной математики* (1994) 1, №1, 33–55.

Статья поступила 12.07.2004.