О восстановлении систем, моделируемых автоматами

А. А. Сытник, Т. Э. Шульга

Одной из основных математических моделей сложных систем дискретного типа является модель конечного автомата. Как правило, поведение моделируемых объектов рассматривается с преобразовательной точки зрения и изучается механизм преобразования входных последовательностей в выходные, то есть входно-выходное соответствие этих последовательностей. Важно при этом обратить внимание на множество входных последовательностей, преобразуемых в заданную выходную последовательность. Если при описании такого автомата ограничиться множеством выходных последовательностей, которые он генерирует, то говорят о перечислительной форме поведения автомата. В статье исследуется переход от преобразовательной формы к перечислительной.

Предлагается использовать элементы теории чисел для построения так называемой «числовой» модели поведения автомата, определяется преобразование, приводящее поведение автомата к эталонному виду, а затем осуществляется переход от преобразовательной формы поведения автомата к перечислительной.

Пусть дан конечный автомат $A = (X, S, Y, \delta, \lambda)$, где X и Y, соответственно, входной и выходной алфавиты, S — алфавит состояний, а δ и λ — функции переходов и выходов автомата соответственно. Если $S = Y$ и $\delta = \lambda$, то имеем так называемый *автомат Медведева* $A = (S, X, \delta)$.

Обозначим состояния $s \in S$ целыми числами от 0 до $m - 1$. Тогда $S = \{0, 1, \ldots, m - 1\} = GL(m)$, то есть S совпадает с полугруппой вычетов по модулю m.

Пусть $\{h_s\}_{s\in S}$ — множество автоматных отображений вида $h_s:\ X^*\to Y^*$, порождаемых автоматом A, где X^*, Y^* — множества входных и выходных слов в алфавитах X и Y, s — начальное состояние автомата. Перейдем к множеству автоматных отображений $\{g_s\}_{s\in S}$ вида $g_s:\ X^*\to Y$, где произвольному входному слову сопоставляется последний символ соответствующего выходного слова, то есть при соответствии $x_1x_2\dots x_n\to y_1y_2\dots y_n$ для $\{h_s\}_{s\in S}$ имеем $x_1x_2\dots x_n\to y_n$ для $\{g_s\}_{s\in S}$.

Под поведением автомата A как преобразователя понимается его множество автоматных отображений $\{g_s\}_{s\in S}$ (под множеством автоматных отображений $\{g_s\}_{s\in S}$ фактически понимается фактор-множество данного множества по отношению эквивалентности между множествами выходных слов автоматов). Под поведением автомата A как перечислителя понимается множество выходных последовательностей

$$L(X^*)=\{y_1y_2\dots y_n\in Y^*\,|\,(\forall i=1,\dots,n)\\ (\exists s_i\in S)(\exists\alpha_i\in X^*):\ g_{s_i}(\alpha_i)=y_i\},$$

генерируемых этим автоматом.

Задача синтеза автомата как перечислителя заключается в построении такого автомата, который перечисляет заданное множество автоматных отображений. При построении множества слов $L(X^*)$ по заданному множеству $\{g_s\}_{s\in S}$ будет использоваться специальная модель поведения автомата, построенная с учетом некоторых ограничений на вид элементов $\{g_s\}_{s\in S}$.

При фиксированном $x\in X$ функцию переходов δ можно считать обобщенной подстановкой вида

$$\delta_x:\ \begin{pmatrix} 0 & 1 & \dots & m-1\\ s_0 & s_1 & \dots & s_{m-1}\end{pmatrix}. \qquad (1)$$

Будем говорить, что автомат Медведева $A=(S,X,\delta)$, $S=\{0,1,\dots,m-1\}$ допускает моделирование степенными функциями, если для любой входной буквы $x\in X$ функция переходов δ_x может быть представлена полиномом $f_x(s)=a_0+a_1s+a_2s^2+\ldots+a_ls^l$, $s\in S$ с постоянными коэффициентами $\{a_0,a_1,\dots,a_{m-1}\}\in S$:

$$\delta_x(s) = f_x(s) \ (\mathrm{mod}\ m), \ \ s \in S. \tag{2}$$

Справедлива следующая

Лемма 1. *Если автомат $A = (S, X, \delta)$ допускает моделирование степенными функциями $\{f_x\}_{x \in X}$, то для любого $s \in S$ автоматное отображение g_s может быть представлено в виде композиции конечного числа полиномов из $\{f_x\}_{x \in X}$, взятой по модулю m.*

Доказательство. В самом деле, доопределим функцию переходов δ до отображения $\tilde{\delta}: \ S \times X^* \to S$ следующим образом:

$$\begin{cases} \tilde{\delta}(s, \Lambda) = s, \\ \tilde{\delta}(s, x\alpha) = \tilde{\delta}(\delta(s, x), \alpha), \end{cases}$$

$\forall s \in S$, $\forall x \in X$, $\forall \alpha \in X^*$, где Λ — пустое слово в X^*.

Тогда $g_s(\alpha) = \tilde{\delta}(s, \alpha)$, $\forall \alpha \in X^*$.

Вместе с тем, по условию теоремы

$$\forall s \in S, \ \ \forall x \in X \ \ \delta(s, x) = f_x(s) \ \mod \ m.$$

Пусть $\Delta(s) = s \ (\mathrm{mod}\ m)$. Тогда

$$\tilde{\delta}(s, \Lambda) = \Delta(s),$$

и $\forall s \in S$, $\forall x \in X$, $\forall \alpha \in X^*$

$$\begin{aligned} \tilde{\delta}(s, x_1 x_2 \ldots x_n) &= \tilde{\delta}(\delta(s, x_1), x_2 \ldots x_n) = \\ &= \delta(\delta(\ldots(\delta(s, x_1), \ldots), x_{n-1}), x_n) = \\ &= f_{x_n}(f_{x_{n-1}}(\ldots f_{x_1}(s) \ \mod \ m \ldots) \ \mod \ m) \mod \ m = \\ &= f_{x_n} \circ f_{x_{n-1}} \circ \ldots \circ f_{x_1}(s) \ \mod \ m \end{aligned}$$

Таким образом, $g_s(x_1 x_2 \ldots x_n) = f_{x_n} \circ f_{x_{n-1}} \circ \ldots \circ f_{x_1}(s) \ \mod \ m$, что и требовалось доказать.

Множество полиномов $\{f_x\}_{x \in X}$, моделирующих поведение автомата A, конечно, поскольку входной алфавит X конечен. Оценим сверху максимальную степень l' полиномов из $\{f_x\}_{x\in X}$. Можно считать, что $l' \leqslant l$, где $l = \min\{L | \forall n > L \quad \exists k < n : \quad x^k = x^n\}$. Действительно, если $l' > l$, можно конечным числом подстановок вида $x^n \to x^k$ привести полиномы из $\{f_x\}_{x\in X}$ степени, большей l, к полиномам степени, не превосходящей l, так что приведенная система полиномов будет по-прежнему моделировать поведение автомата A.

Множество степенных функций $\{x^0, x^1, x^2, \ldots, x^l\}$ над полем вычетов по модулю m составляет полугруппу отображений с константой $x^0 = 1 \pmod m$. Подполугруппа $\{x^1, x^2, \ldots, x^l\}$ этой полугруппы является периодической полугруппой, порождаемой x. По определению, индекс полугруппы — это наименьшее целое положительное число r_0 такое, что $x^{r_0} = x^{r_0+n}$ для некоторого натурального n, период полугруппы — это наименьшее положительное число m_0 из всех возможных n. Данным r_0 и m_0 соответствует единственная (с точностью до изоморфизма) полугруппа преобразований $\{x, x^2, \ldots, x^{r_0+m_0-1}\}$, то есть $l = r_0 + m_0 - 1$. Так как $x \in S$, то полугруппу $\{x, x^2, \ldots, x^{r_0+m_0-1}\}$ можно считать полугруппой m-мерных векторов вида $(0^k, 1^k \mod m, 2^k \mod m, \ldots, (m-1)^k \mod m)$. Эти вектора, фактически, являются нижними строками соответствующих подстановок вида (1).

Замечание 1. В полугруппе векторов умножение определяется покомпонентно, поэтому все i-тые компоненты векторов полугруппы образуют подполугруппу полугруппы $\{0, 1, \ldots, m-1\}$, порожденную числом i. Следовательно, говоря о связи между индексами и периодами векторной и покомпонентной полугрупп, надо учитывать, что период векторной полугруппы должен содержать все периоды покомпонентных полугрупп, а значит, должен являться их наименьшим общим кратным. Индекс векторной полугруппы должен быть наибольшим из всех индексов покомпонентных полугрупп. Зависимость между числом m и парой r_0, m_0 определяет следующая теорема:

Теорема 1. *Если*

$$m = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} \; - \tag{3}$$

разложение числа m на простые множители, $\alpha_0 \geqslant 0$, $\alpha_i > 0$, $i = \overline{1,k}$, то индекс и период полугруппы $\{x, x^2, \ldots, x^{r_0+m_0-1}\}$ вычисляются по формулам:

$$\begin{aligned} &r_0 = \max(\alpha_0, \alpha_1, \ldots, \alpha_k), \\ &m_0 = p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1} \cdot \text{НОК}([2^{\alpha-2}], p_1 - 1, \ldots, p_k - 1). \end{aligned} \quad (4)$$

Доказательство. Согласно приведенному выше определению, r_0 и m_0 — это наименьшие положительные числа, удовлетворяющие сравнению

$$x^{r_0} = x^{r_0 + m_0} \pmod{m}, \quad \forall x \in \{0, 1, \ldots, m-1\}. \quad (5)$$

Можно считать (5) системой из m сравнений. Для удобства разобьем ее на три подсистемы.

В первую подсистему сравнений включим все сравнения для x, взаимно простых с m:

$$x \in I = \{a |\ \text{НОД}(a, m) = 1\}.$$

Во вторую — все сравнения для x, являющихся делителями числа m, то есть для x из множества $x \in II = \{a |\, a = 2^{\beta_0} p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$, $0 < \beta_i \leqslant \alpha_i$, $i = \overline{0, k}\}$.

В третью подсистему включим все оставшиеся сравнения, то есть сравнения для x, имеющих с m какой-либо общий делитель, отличный от единицы и $2 p_1 p_2 \ldots p_k$ (или $p_1 p_2 \ldots p_k$, в случае нечетного m): $x \in III = \{0, 1, \ldots, m-1\} \setminus (I \cup II)$.

Далее будем искать решение для каждой из этих трех подсистем отдельно.

I. Первая подсистема является приведенной системой вычетов по модулю m. Она допускает деление каждого сравнения на число x^{r_0}, взаимно простое с m. Получим $x^{m_0} = 1 \pmod{m}$, $\forall x \in I$. Для каждого x разложим каждое из сравнений первой подсистемы на систему из $k+1$ сравнений:

$$\begin{cases} x^{m_0} = 1 \pmod{2^{a_0}} \\ x^{m_0} = 1 \pmod{p_1^{a_1}} \\ \qquad \ldots\ldots\ldots \\ x^{m_0} = 1 \pmod{p_k^{a_k}}. \end{cases}$$

Далее, разобьем полученную систему на $k+1$ подсистему (по каждому из модулей $2^{\alpha_0}, p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$), в каждой из которых x

пробегает всю приведенную систему вычетов. Для первой подсистемы $x^{m_0} = 1 \pmod{2^{\alpha_0}}$, $\forall x \in I$ наименьшим возможным решением будет $m_0 = \begin{cases} 1, \ \alpha_0 = 0, 1 \\ 2^{\alpha_0 - 2}, \ \alpha_0 \geqslant 2 \end{cases}$, или $m_0 = [2^{\alpha-2}]$, где $[A]$ обозначает целую часть числа A. Решением подсистем сравнений вида $x^{m_0} = 1 \pmod{p_i^{\alpha_i}}$, $\forall x \in I$, $i = \overline{1,k}$, согласно теореме Эйлера, будет так называемая функция Эйлера $m_0 = \varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1} = (p_i - 1)p_i^{\alpha_i - 1}$. Искомое m_0 должно быть одновременно кратно всем числам $[2^{\alpha-2}], (p_1 - 1)p_1^{\alpha_1 - 1}, \ldots, (p_k - 1)p_k^{\alpha_k - 1}$, а, значит, оно является их наименьшим общим кратным. Поскольку все $p_i^{\alpha_i - 1}$ взаимно просты, они могут быть вынесены за знак НОК. Получим $m_0 = p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1} \cdot \text{НОК}([2^{\alpha-2}], p_1 - 1, \ldots, p_k - 1)$. Так как любое число из приведенной системы вычетов, будучи возведенным в степень, кратную значению его функции Эйлера, даст единицу, то решением первой подсистемы является число $r_0 = 1$.

II. Числа из множества II содержат все простые сомножители разложения числа m. После возведения любого такого числа в некоторую степень r^* получим 0, и все последующие возведения его в степень будут давать также 0. Число $2p_1p_2\ldots p_k$ (или $p_1p_2\ldots p_k$, в случае нечетного m), будет ненулевым, пока $r^* < \max(\alpha_0, \alpha_1, \ldots, \alpha_k)$, следовательно, r^* не меньше максимального показателя, вместе с тем ни одно из чисел множества II^* не останется ненулевым при достижении этого максимума. Следовательно, получаем, самое большее, $r^* - 1$ ненулевых степеней. По Замечанию 1 имеем $r_0 = \max(\alpha_0, \alpha_1, \ldots, \alpha_k)$ и $m_0 = 1$.

III. Каждое из $x \in III$ имеет с m по крайней мере один делитель, отличный от единицы и не кратный $2p_1p_2\ldots p_k$ (или $p_1p_2\ldots p_k$, в случае нечетного m). Каждое такое число является произведением какого-либо элемента p подполугруппы с единицей (приведенной полугруппы вычетов) на какой-либо элемент q подполугруппы с другим идемпотентом. Полугруппа, порожденная этим числом, имеет вид: $\{pq, p^2q^2, \ldots, p^{r_0}q^{r_0}, \ldots, p^{r_0+m_0-1}q^{r_0+m_0-1}\}$. Очевидно, что период данной полугруппы должен быть кратен периоду полугруппы, порожденной p, а индекс должен быть не меньше ее индекса (то есть не меньше единицы). Следовательно, нас интересуют только индекс и период полугруппы, порожденной q. Разобьем исходную систему сравнений на $k+1$ подсистему (по каждому из модулей $2^{\alpha_0}, p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$), в каждой из которых x пробегает всю приведенную систему вычетов.

Обозначим через d = НОД$(m, a^{r_0}, a^{r_0+m_0})$ наибольший общий делитель обеих частей сравнения и его модуля (одного из $2^{\alpha_0}, p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$). Согласно [3], мы можем поделить обе части сравнения и модуль на это число и перейти к эквивалентному сравнению:

$$x^* = \bar{x}^* \pmod{m^*}, \;\; x^*, \bar{x}^* \in I^*.$$

Заметим, что теперь обе части сравнения взаимно просты с полученным модулем, поэтому можно домножить обе части сравнения на число, обратное к x^* по модулю m^* в полугруппе GL(m), выделить степень и решать полученное сравнение методом, предложенным в пункте I. Полученное r_0^* будет не меньше индекса, найденного для подсистемы I, так как у модуля m^* все степени простых сомножителей в разложении (3) меньше либо равны всем степеням соответствующего разложения для m. Полученный модуль будет кратен модулю m_0 по способу построения.

Выбрав НОК модулей, полученных в каждом из пунктов I, II и III, убеждаемся, что он в точности равен $m_0 = p_1^{\alpha_1-1} \cdot \ldots \cdot p_k^{\alpha_k-1} \cdot$ НОК$([2^{\alpha-2}], p_1-1, \ldots, p_k-1)$, а максимальный из трех индексов равен соответственно $r_0 = \max(\alpha_0, \alpha_1, \ldots, \alpha_k)$, что и требовалось доказать.

Число $l = r_0 + m_0 - 1$ дает нам верхнюю оценку максимальной степени многочленов из $\{f_x\}_{x \in X}$. Непосредственный вид функций f_x, а также их степень можно найти при помощи метода Гаусса, модифицированного для работы над кольцом целых чисел ([4, 9, 10, 11]). При этом для определения коэффициентов всех функций $\{f_x\}_{x \in X}$ необходимо только один раз построить исходную матрицу метода Гаусса и, приписав к ней все вектора, соответствующие входам $x_1, x_2, \ldots, x_n$, осуществить прямой и обратный ход метода Гаусса.

Будем искать коэффициенты $a_0, a_1, \ldots, a_l$ полинома f_x: $f_x(s) = a_0 + a_1 s + a_2 s^2 + \ldots + a_l s^l$, $s \in S$, подставляя в f_x последовательно числа $0, 1, \ldots, m-1$ и приравнивая полученные результаты числам $s_0, s_1, \ldots, s_{m-1}$ из соответствующей обобщенной подстановки вида (1). Имеем систему линейных сравнений по модулю m:

$$\begin{cases} s_0 = a_0 \pmod m \\ s_1 = a_0 + a_1 + a_2 + \ldots + a_l \pmod m \\ s_2 = a_0 + a_1 2 + a_2 2^2 + \ldots + a_l 2^l \pmod m \\ \ldots\ldots\ldots \\ s_{m-1} = a_0 + a_1(m-1) + a_2(m-1)^2 + \ldots + a_l(m-1)^l \pmod m \end{cases} \tag{6}$$

или, в матричном виде, исключая первое уравнение как тривиальное и преобразуя соответствующим образом остальные:

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ 2 & 2^2 & \ldots & 2^l \\ \ldots & \ldots & \ldots & \ldots \\ (m-1) & (m-1)^2 & \ldots & (m-1)^l \end{bmatrix} \times \begin{bmatrix} a_1 \\ a_2 \\ \ldots \\ a_l \end{bmatrix} = \begin{bmatrix} s_1 - s_0 \\ s_2 - s_0 \\ \ldots \\ s_{m-1} - s_0 \end{bmatrix} \pmod m \tag{7}$$

В краткой записи: $Ma = s$.

Матрица M — это матрица Вандермонда,

$$M = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ 2 & 2^2 & \ldots & 2^l \\ \ldots & \ldots & \ldots & \ldots \\ (m-1) & (m-1)^2 & \ldots & (m-1)^l \end{bmatrix}, \tag{8}$$

где в качестве переменных взяты константы $1, \ldots, m-1$.

Данная матричная система уравнений позволяет выделить критерий моделируемости автомата множеством степенных функций, основанный на свойствах числа m и виде подстановок (1).

Теорема 2. *Автомат $A = (S, X, \delta)$ допускает моделирование множеством степенных функций $\{f_x\}_{x \in X}$ тогда и только тогда, когда ранг расширенной матрицы $[M|s]$ равен рангу матрицы M, а каждый элемент столбца свободных членов кратен наибольшему общему делителю всех элементов соответствующей строки матрицы M.*

Замечание 2. Если автомат A имеет несколько входов, под «столбцом свободных членов» можно понимать матрицу, составленную из столбцов свободных членов, соответствующих различным входам этого автомата.

Содержательно, теорема 2 означает, что матричная система уравнений не только должна быть совместна над полем действительных чисел (по [7] для этого требуется равенство рангов обычной и расширенной матриц), но и должна иметь решение в целых числах как система диофантовых уравнений. Последнее условие требует кратности свободного члена сравнения наибольшему общему делителю коэффициентов при переменных.

Второе условие теоремы 2 можно переформулировать следующим образом: для любого простого числа p, входящего в разложение (3), и натурального числа k, должна быть разрешима система сравнений $Ma \equiv \tilde{s} \pmod{p^k}$, $a \neq 0 \pmod{p}$.

Следствие 1. *Если m — простое, то любой автомат A с m состояниями допускает моделирование множеством степенных функций.*

Действительно, если модуль системы сравнений — простое число, то матрица M будет квадратной, и, по [12], ее ранг будет в точности равен рангу расширенной матрицы $[M|s]$.

Исследуем теперь структуру матрицы M с $m-1$ строками, где $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ — каноническое разложение числа m. Заметим, что i-тая строка матрицы M представляет собой элементы мультипликативной полугруппы, порожденной числом i. Строку матрицы, порожденную числом i, будем обозначать через $\mathbf{S}_i$.

Будем говорить, что строка $\mathbf{S}_{k+1}$ матрицы M линейно зависима от строк $\mathbf{S}_1, \ldots, \mathbf{S}_k$, если существуют целые числа $\alpha_1, \ldots, \alpha_k, \alpha_{k+1}$, не все равные нулю, такие, что выполняется векторное сравнение

$$\alpha_{k+1}\mathbf{S}_{k+1} \equiv \alpha_1 \mathbf{S}_1 + \ldots + \alpha_k \mathbf{S}_k \pmod{m},$$

то есть имеет место система сравнений вида:

$$\alpha_{k+1} s_{k+1,i} \equiv \alpha_1 s_{1,i} + \ldots + \alpha_k s_{k,i} \pmod{m}, \quad i = \overline{1,l},$$

где s_{ji} — i-тый элемент строки $\mathbf{S}_j$.

В противном случае строка $\mathbf{S}_{k+1}$ называется линейно независимой от строк $\mathbf{S}_1, \ldots, \mathbf{S}_k$.

Рассмотрим полугруппу $(S, \cdot)$, где $S = \{0, 1, \ldots, m-1\}$, $(\cdot)$ — операция умножения по модулю m. В дальнейшем вместо $(S, \cdot)$ будем сокращенно писать S, а знак $\cdot$ при записи опускать. Введем обозначение $m_j = p_1^{\alpha_1} \cdot \ldots \cdot p_j^{\alpha_j - 1} \cdot \ldots \cdot p_n^{\alpha_n}$, тогда $m_j p_j = m$. Очевидно, справедливо следующее утверждение.

Лемма 2. *Множества* $\mathbf{I}_j = \{0, m_j, 2m_j, \ldots, (p_j - 1)m_j\}$, *где* $j \in [1, n]$, *являются идеалами полугруппы* S.

Из леммы 2 следует, что строки $S_{p_1 k_j + j}$ и S_j, $i = \overline{1, l}$, $j = \overline{1, p_1 - 1}$ линейно зависимы, то есть $m_1 S_{p_1 k_j + j} = m_1 S_j \pmod{m}$.

Кроме того, можно выделить еще $m_1 - 1$ линейных зависимостей вида

$$m_1 S_{k_1^p} \equiv \bar{0} \pmod{m}.$$

Таким образом, от первых $p_1 - 1$ строк матрицы M линейно зависят все остальные. Напротив, строки $\mathbf{S}_1, \mathbf{S}_2, \ldots, \mathbf{S}_{p_1 - 1}$ матрицы M линейно независимы между собой. Основываясь на этих результатах, получаем следующую теорему.

Теорема 3. *Если* $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ *— каноническое разложение числа* m, $m_1 = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, *то для допуска автоматом* A *с* m *состояниями моделирования степенными функциями необходимо, чтобы любое его отображение переходов вида (1) удовлетворяло системе из* $m - p_1$ *сравнений, из которых* $m_1 - 1$ *имеют вид*

$$m_1 (s_{k p_1} - s_0) \equiv 0 \pmod{m}, \quad k = \overline{1, m_1 - 1}, \tag{9}$$

а остальные имеют вид

$$m_1 s_{k_j p_1 + j} \equiv m_1 s_j \pmod{m}, \quad j = \overline{1, p_1 - 1}, 1 \leqslant k_j \leqslant \frac{m - j}{p_1}. \tag{10}$$

Замечание 3. Приведенные выше условия в общем случае не являются достаточными. Исключениям служат лишь те случаи, когда все строки матрицы M являются линейно независимыми в поле рациональных чисел. Например, при $m = 4$ условия $2s_1 \equiv 2s_3 \pmod{4}$, $2s_2 \equiv 0 \pmod{4}$ являются необходимыми и достаточными условиями моделируемости автомата степенными функциями.

Пусть автомат A допускает моделирование степенными функциями. Вернемся к преобразованному матричному уравнению:

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 & \dots & 1 \\ 0 & 1 & m_{2,3} & \dots & m_{2,\mathrm{rang}} & \dots & m_{2,l} \\ 0 & 0 & 1 & \dots & m_{2,\mathrm{rang}} & \dots & m_{3,l} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & \dots & m_{\mathrm{rang},l} \\ 0 & 0 & 0 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & \dots & 0 \end{bmatrix} \times \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \dots \\ a_{\mathrm{rang}} \\ \dots \\ a_l \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \dots \\ s_{\mathrm{rang}} \\ s_{\mathrm{rang}+1} \\ \dots \\ s_{m-1} \end{bmatrix} \pmod m \tag{11}$$

Здесь, не ограничивая общности, мы предположили, что все линейно независимые степенные функции расположены в первых столбцах матрицы.

Матрица в левой части сравнения является верхнетреугольной, причем ее верхняя строка — единичная, а строки с номерами $\mathrm{rang}+1$ и ниже являются нулевыми. Для того, чтобы получить разложение строк матрицы M по базисным функциям, которых ровно rang, необходимо действовать следующим образом. Отбросим нулевые строки и соответствующие им элементы столбца свободных членов, а также столбцы с номерами $\mathrm{rang}+1$.

Далее будем вычитать последовательно:

– из предпоследней строки объединенной матрицы $[M|a]$ последнюю строку, домноженную на последний элемент предпоследней строки, при этом в предпоследней строке единственным ненулевым компонентом останется единица, стоящая на диагонали, а в столбце свободных членов появится соответствующий коэффициент разложения;

– из третьей снизу строки вначале последнюю строку, а потом предпоследнюю, домноженные на соответствующие элементы третьей снизу строки, так, чтобы единственным ненулевым элементом ее осталась единица, стоящая на диагонали, и так далее.

Теперь матрица M предельно упрощена:

$$\begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix} \times \begin{bmatrix} a_1 \\ a_2 \\ \dots \\ a_{\mathrm{rang}-1} \\ a_{\mathrm{rang}} \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ \dots \\ s_{\mathrm{rang}-1} \\ s_{\mathrm{rang}} \end{bmatrix} \pmod m \qquad (12)$$

и коэффициенты в столбце свободных членов — это коэффициенты разложения по базису из rang линейно независимых степенных функций.

Найденные коэффициенты $a_0, a_1, \dots, a_{\mathrm{rang}}$ являются коэффициентами разложения по линейно независимому базису, выделенному из множества $\{s, s^2, s^3, \dots, s^l\}$:

$$f_x(s) = a_0 + a_1 e_1 + a_2 e_2 + \dots + a_{\mathrm{rang}} e_{\mathrm{rang}} \pmod m, \quad e_i \in \{s, s^2, s^3, \dots, s^l\}.$$

Моделирование поведения автомата полиномами состоит в том, чтобы каждому входному слову $\alpha = x_1 x_2 \dots x_n \in X^*$ сопоставить выходное слово $g_s(\alpha) = f_{x_n} \circ f_{x_{n-1}} \circ \dots \circ f_{x_1}(s) \mod m$. В процессе прохождения метода Гаусса нами были найдены векторы разложения по базису $\{e_i\}_{i=\overline{0,\mathrm{rang}}}$ для всех входных букв. Пусть вектор $(a_0, a_1, \dots, a_{\mathrm{rang}})$ соответствует функции f_a для входной буквы a, вектор $(b_0, b_1, \dots, b_{\mathrm{rang}})$ — функции f_b для входной буквы b. Тогда функция $f_b(f_a(s))$ есть степенная функция с линейным образом преобразованными коэффициентами. Иначе говоря, можно подставить вектора $(a_0, a_1, \dots, a_{\mathrm{rang}})$ и $(b_0, b_1, \dots, b_{\mathrm{rang}})$ в некую матрицу-оператор и получить вектор коэффициентов итоговой функции $f_b(f_a(s))$. Следовательно, работая со словами произвольной конечной длины, мы будем ставить каждому слову в соответствие вектор из $\mathrm{rang}+1$ компонент. При этом метод Гаусса требует всего лишь одного прохода для определения коэффициентов степенных функций для каждой из входных букв $x \in X$, а для вычисления степенной функции, соответствующей данному слову α, матрица-оператор применяется столько же раз, сколько букв в этом слове.

Сопоставим входному слову $\alpha = x_1 x_2 \dots x_n$ индуцируемое им преобразование $f_{x_1 x_3 \dots x_k}(s) = \alpha_{i1} s^{\beta_{i1}} + \alpha_{i2} s^{\beta_{i2}} + \dots + \alpha_{ij} s^{\beta_{ij}} \pmod m$.

В качестве выходного слова автомата запишем коэффициенты и показатели базисных степенных функций, входящих в это разложение. Тем самым, выходным словом будет $\gamma = \beta_{i1}\alpha_{i1}\beta_{i2}\alpha_{i2}\ldots\beta_{ij}\alpha_{ij}$, составленное над алфавитом из m букв $\{\alpha_i\}_{i=\overline{0,m-1}}$, отвечающих за коэффициенты при степенных функциях (компоненты вектора a) и $\mathrm{rang}+1$ букв $\{\beta_j\}_{j=\overline{0,\mathrm{rang}}}$, отвечающих за показатели степеннных функций, входящих в базис $\{e_i\}_{i=\overline{0,\mathrm{rang}}}$.

Согласно Лемме 1, множество степенных функций $\{f_x\}_{x\in X}$ моделирует поведение автомата A в том смысле, что всякое его автоматное отображение g_s из $\{g_s\}_{s\in S}$ может быть представлено в виде композиции функций из $\{f_x\}_{x\in X}$. Так как каждому из автоматных изображений $g_s(x_1x_2\ldots x_k)$ однозначным образом сопоставлена своя степенная функция $f_{x_1x_3\ldots x_k}(s) = \alpha_{i1}s^{\beta_{i1}} + \alpha_{i2}s^{\beta_{i2}} + \ldots + \alpha_{ij}s^{\beta_{ij}} \pmod m$, а каждой из таких функций сопоставлено слово $\gamma = \beta_{i1}\alpha_{i1}\beta_{i2}\alpha_{i2}\ldots\beta_{ij}\alpha_{ij}$, составленное из обозначений коэффициентов и показателей степеней функции, то можно говорить, что порождающему множеству автоматных отображений $\{g_s\}_{s\in S}$, построенному для автомата, допускающего моделирование полиномами, равно как и множеству степенных функций $\{f_x\}_{x\in X}$, однозначно сопоставлено множество выходных слов $\{\gamma_x\}_{x\in X^*}$, то есть порождающее множество для всех слов $L(X^*)$, перечисляемых автоматом A.

Замечание. Ограничения, накладываемые на вид функции переходов автомата Теоремой 2, могут быть преодолены путем переобозначения состояний автомата или введением дополнительного внутреннего состояния, которое позволило бы перейти к случаю автомата с простым числом внутренних состояний, позволяющему решить задачу моделирования поведения автомата для произвольной функции переходов.

Список литературы

[1] Алгебраическая теория автоматов, языков и полугрупп. / Под ред. Арбиба М. А., пер. с англ. М.: Статистика, 1975.

[2] Боревич З. И., Шафаревич И. Р. Теория чисел. М.: Наука, 1985. 451 с.

[3] Виноградов И. М. Основы теории чисел. М.: Наука, 1965.

[4] Вотяков А. А., Фрумкин М. А. Алгоритмы нахождения общего целочисленного решения системы линейных уравнений // Исследования по дискретной оптимизации. М.: Наука, 1976. С. 128–140.

[5] Кострикин А. И. Введение в алгебру. М.: Наука, 1977. 495 с.

[6] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. М.: Наука, 1985.

[7] Курош А. Г. Курс высшей алгебры. М.: Наука, 1975.

[8] Сытник А. А. Перечислимость при восстановлении поведения автоматов. // Доклады РАН. 1993. Т. 238. С. 25–26.

[9] Фрумкин М. А. Алгоритмы решения систем линейных уравнений в целых числах // Исследования по дискретной оптимизации. М.: Наука, 1976. С. 97–127.

[10] Ху. Т. Целочисленное программирование и потоки в сетях. М.: Мир, 1974. 516 с.

[11] Borosh J., Frankel A. S. Exact solutions of linear equations rational coefficients by congruence techniques // Math. of Comput. 1966. 20:93. P. 107–112.

[12] Sytnik A. A. Methods and Models for Restoration on Automata Behaviour // Automation and remote control. Consultants Bureau. New York, 1993. P. 1781–1790.

[13] Sytnik A. A., Posohina N. I. On Some Methods Of Discret Systems Behaviour Simulation // The First International Conference CASYS'97 on Computing Anticipatory SYStems. Liege, Belgium, 1997.