Линейно реализуемые переходные системы

С. Б. Родин

Данная работа посвящена изучению «линейно реализуемых» переходных систем, то есть обладающих тем свойством, что существует кодирование, при котором порождаемый кодированием булевский оператор является линейным. В работе приведено необходимое условие линейной реализуемости переходной системы. Также приведены нижняя и верхняя оценка числа линейно реализуемых переходных систем.

Ключевые слова: теория автоматов, переходные системы, кодирование, сложность.

На практике часто необходимо решать задачу перехода от автоматного описания функционирования на язык схем. Например, при логическом синтезе чипов на первом этапе функционирование чипа описывается как конечный автомат. Переход к описанию на языке схем осуществляется с помощью кодирования алфавита состояний, входного алфавита и выходного алфавита в алфавите $\{0, 1\}$.

При этом важно выбрать кодирование, при котором достигается возможно меньшая сложность схемы.

В работе изучается сложность реализации автоматов специального вида, так называемых автоматов без выхода или переходных систем. С формальной точки зрения переходная система — это тройка $V = (A, Q, \varphi)$, где A — входной алфавит, Q — алфавит состояний, φ — функция, которая по текущему входу и состоянию определяет состояние переходной системы в следующий момент времени. Кодирование алфавита состояния — это отображение алфавита Q в ${E_2}^k$, при котором каждому состоянию из Q ставится в соотвествие вектор из ${E_2}^k$. Соотвественно кодирование входного алфавита — это отображение

алфавита A в ${E_2}^p$, при котором каждому элементу из A ставится в соотвествие вектор из ${E_2}^p$. При этом функции перехода φ преобразуется в булевский оператор $\phi : {E_2}^{p+k} \to {E_2}^k$, где p — длина кодового набора символов множества A, k — длина кодового набора символов множества Q. Данный оператор может быть рассмотрен как набор k булевских функций от $n + k$ переменных. А его сложность определить как максимальную сложность получаемых булевских функций. Как известно каждой булевской функции единственным образом соответствует полином Жегалкина. Мы будем понимать сложность оператора как максимальную из сложностей полиномов Жегалкина функций, задающих этот оператор, то есть максимальная степень полиномов. Таким образом, установив связь между переходной системой, кодировкой и возникающим полиномом, можно установить минимальную сложность реализации переходной системы.

Естественно начинать такого рода исследования с «простейших», линейных полиномов. Основной задачей данной работы было изучение переходных систем, у которых существует кодирование, такое что получаемые при данном кодировании, булевские функции являются линейными.

Вообще говоря, возникаемый при кодировании оператор, является частично определенным, так как значение оператора определенно только на кодирующих наборах. «Правильное» доопределение может как «упростить» оператор, так и «усложнить» его. В работе будут изучаться переходные системы мощность множества состояний есть степень 2. Зная какие переходные системы имеют линейную реализацию, можно доопределять частично определенные операторы до линейных или установить что это невозможно.

Введем некоторые понятия.

Определение 1. Нумерованной переходной системой назовем тройку (A, Q, φ), где A — входной алфавит, $Q = \{0, \ldots, n-1\}$, φ — функция переходов.

В работе изучаются нумерованные переходные системы с входным алфавитом $A = E_2$ и числом состояний $n = 2^k$.

Определение 2. Кодированием множества $Q = \{0, \ldots, n-1\}$ назовем взаимоднозначное отображение $F : \{0, \ldots, n-1\} \to {E_2}^k$.

Каждое кодирование F для переходной системы на множестве Q порождает булевский оператор $\phi : {E_2}^{k+1} \to {E_2}^k$, где

$$\phi(a, \alpha_1, \ldots, \alpha_k) = F(\varphi(a, F^{-1}(\alpha_1, \ldots, \alpha_k))), a \in A, \alpha_i \in E_2.$$

Данный оператор может быть рассмотрен как набор k булевских функций, зависящих от $k+1$ переменной. Обозначим этот набор через $\mathcal{F}_V(F)$.

Определение 3. Если для заданной нумерованной переходной системы V существует кодирование F, такое что все элементы $\mathcal{F}_V(F)$ являются линейными функциями алгебры логики, назовем такую переходную систему линейно реализуемой посредством кодирования F или просто линейно реализуемой.

Выделим из всех кодирований «стандартное» кодирование.

Определение 4. Кодирование $F_0 : \{0, \ldots, n-1\} \to {E_2}^k$ назовем стандартным, если код элемента есть его двоичное представление.

Каждому кодированию F можно сопоставить перестановку s_F на множестве $Q : \{0, \ldots, n-1\}$ по правилу $s_F(i) = {F_0}^{-1}(F(i))$.

Перейдем к изложению результатов.

Пусть задана переходная система $V = (E_2, Q, \varphi)$ и некоторое кодирование F. Обозначим через $\phi_V : {E_2}^{k+1} \to {E_2}^k$, булевский оператор, порождаемый кодированием F переходной системы V. Обозначим через $X_V = \{s : Q \leftarrow Q | \exists a \in E_2, s(q) = \varphi(a, q) \forall q\}$ А через $S_V =< X_V >$, замыкание множества X_V относительно операции умножения подстановок [4].

Определение 5. S_V назовем внутренней полугруппой переходной системы V. X_V порождающее множество внутренней полугруппы.

Поскольку входной алфавит E_2, то множество X_V состоит из двух элементов. Обозначим через p_0 подстановку, соответствующую входному символу 0, через p_1 подстановку, соответствующую входному символу 1. Пусть задана переходная система $V = (E_2, Q, \varphi)$ и некоторое кодирование F. Рассмотрим перестановку s_F. Обозначим через V_{s_F} переходную систему, с входным алфавитом E_2, алфавитом состояний $Q = \{0, \ldots, n-1\}$ и функцией φ, такой что

$\varphi(0,q) = s_F(p_0({s_F}^{-1}(q)))$ для любого $q \in Q$, $\varphi(1,q) = s_F(p_1({s_F}^{-1}(q)))$ для любого $q \in Q$.

Теорема 1. *Пусть задана переходная система $V = (E_2, Q, \varphi)$ и некоторое кодирование F. Тогда булевский оператор ϕ_V, порождаемый кодированием F равен булевскому оператору, порождаемому кодированием F_0 переходной системы V_{s_F}.*

Доказательство. Дана переходная система $V = (E_2, Q, \varphi)$ и кодирование $F : \{0, \ldots, n-1\} \to {E_2}^k$. Тогда соответствующий булевский оператор определяется как $\phi_V(a, \alpha_1, \ldots, \alpha_k) = F(\varphi(a, F^{-1}(\alpha_1, \ldots, \alpha_k)))$, $a \in A$, $\alpha_i \in E_2$. Несложно видеть, что булевский оператор, порождаемый кодированием F_0 переходной системы V_{s_F}, определяется как

$$V_{s_F}(a, \alpha_1, \ldots, \alpha_k) = F_0(s_F({s_F}^{-1}({F_0}^{-1}(\alpha_1, \ldots, \alpha_k))))).$$

Поскольку $s_F(i) = {F_0}^{-1}(F(i))$, то

$$V_{s_F}(a, \alpha_1, \ldots, \alpha_k) = F_0({F_0}^{-1}(F(\varphi(a, F^{-1}(F_0({F_0}^{-1}(\alpha_1, \ldots, \alpha_k))))))) = \\ = F(\varphi(a, F^{-1}(\alpha_1, \ldots, \alpha_k))).$$

Теорема доказана.

Обозначим через $V(n)$ множество нумерованных переходных систем со входным алфавитом E_2 и алфавитом состояний $Q = \{0, \ldots, n-1\}$.

Теорема 2. *Мощность множества $V(n)$ равна n^{2n}.*

Доказательство. Как несложно видеть нумерованная переходная система полностью определяется порождающими внутренней полугруппы. Число подстановок на множестве $Q = \{0, \ldots, n-1\}$ равно n^n. Поскольку в нашем случае число порождающих равно 2. То число возможных пар порождающих равно n^{2n}.

Теорема 3. *Число различных нумерованных переходных систем с n состояниями, линейно реализуемых посредством стандартного кодирования F_0, равно $n^{\log_2(n)+2}$.*

Доказательство. Пусть задана нумерованная переходная система с n состояниями, линейно реализуемая посредством стандартного кодирования F_0. Обозначим через $k = \log_2(n)$. Данное кодирование порождает булевский оператор $\phi : {E_2}^{k+1} \to {E_2}^k$. Рассмотрим этот оператор, как набор $\mathcal{F}_V(F_0)$. Поскольку переходная система линейно реализуема, то элементы $\mathcal{F}_V(F_0)$ есть линейные булевские функции от $k+1$ переменной, а именно $\mathcal{F}_V(F_0) = \{f_0, \ldots, f_{k-1}\}$,где $k = \log_2(n)$. Как известно, число различных линейных булевских функций зависящих от $k+1$ переменной равно 2^{k+2} [1]. Значит число различных наборов $\mathcal{F}_V(F_0)$ равно $\left(2^{k+2}\right)^k$, что равно $n^{\log_2(n)+2}$. Теперь покажем, что двум различным наборам соответсвуют две различные переходные системы, линейно реализуемые посредством стандартного кодирования F_0. Каждый набор соответствует булевскому оператору

$$\phi(a, \alpha_1, \ldots, \alpha_k) = (\beta_1, \ldots, \beta_k),$$

где $a, \alpha_i, \beta_i \in E_2$. Определим переходную систему по следующему правилу $V_\phi = (E_2, (0, \ldots, n-1), \varphi_\phi)$, где $\varphi_\phi(a, q) = {F_0}^{-1}(\phi(a, F_0(q))$. Несложно видеть, что линейный оператор, получаемый с помощью кодирования F_0 переходной системы V_ϕ равен оператору ϕ [5]. Пусть заданы два различных набора $\mathcal{F}_1$ и $\mathcal{F}_2$. Поскольку они различны, то найдутся две неравные функции ${f_i}^1 \in \mathcal{F}_1$ и ${f_i}^2 \in \mathcal{F}_2$ и набор $a, \alpha_1, \ldots, \alpha_k$, где $a, \alpha_i \in E_2$, такие что ${f_i}^1(a, \alpha_1, \ldots, \alpha_k) \neq {f_i}^2(a, \alpha_1, \ldots, \alpha_k)$. Следовательно операторы, соответствующие первому и второму набору, не равны на наборе $a, \alpha_1, \ldots, \alpha_k$. Обозначим булевский оператор соответствующий первому набору ϕ_1, а второму — ϕ_2. $\phi_1(a, \alpha_1, \ldots, \alpha_k) \neq \phi_2(a, \alpha_1, \ldots, \alpha_k)$. Обозначим через $q = F_0(\alpha_1, \ldots, \alpha_k)$. Тогда согласно построению переходной системы по булевскому оператору $\varphi_{\phi_1}(a, q) = {F_0}^{-1}(\phi_1(a, \alpha_1, \ldots, \alpha_k))$, а $\varphi_{\phi_2}(a, q) = {F_0}^{-1}(\phi_2(a, \alpha_1, \ldots, \alpha_k))$. Поскольку по определению кодирования, отображение F_0 взаимооднозначное, то $\varphi_{\phi_1}(a, q) \neq \varphi_{\phi_2}(a, q)$. Теорема доказана.

Перед формулировкой следующей теоремы введем несколько обозначений. Поскольку $n = 2^k$, то подстановки на множестве $Q = \{0, \ldots, n-1\}$ могут быть представлены как многочлены над полем Галуа F_{2^k} [1]. Обозначим через P_n множество подстановок на множестве

E_n. Обозначим через H_+ перестановки, соответствующие многочленам $x + c$ над полем Галуа F_n, где $c \in E_n$ — константа. Обозначим через H_* перестановки, соответствующие многочленам $c \cdot x$ над полем Галуа F_n, где $c \in E_n$ — константа. Обозначим через $H_L = \{s \in P_n$, такие что $\forall h \in H_+ \; \exists h' \in H_+,\; hs = sh'\}$. Порядок умножения подстановок слева направо. То есть если заданы перестановки p_1 и p_2, то значение их произведения на элементе i есть $(p_1 \cdot p_2)(i) = p_2(p_1(i))$.

Теорема 4. *Пусть задана переходная система $V = (E_2, Q, \varphi)$. Если V линейно реализуема посредством кодирования F, то существует подстановка c такая, что $p_0 = c \cdot h_1$, $p_1 = c \cdot h_2$, где $h_1, h_2 \in {s_F}^{-1} \cdot H_+ \cdot s_F$.*

Доказательство. Дана переходная система $V = (E_2, Q, \varphi)$ линейно реализуемая посредством кодирования F_0. Обозначим ее число состояний через n. Рассмотрим множество $\mathcal{F}_V(F_0) = \{h_1, h_2, \ldots, h_k\}$, где $k = \log_2(n)$. По определению булевского оператора и множества $\mathcal{F}_V(F_0)$ имеем $h_i : {E_2}^{k+1} \to {E_2}^k$. Поскольку h_i линейная булевская функция, то если первая переменная является существенной, то $h_i(0, \alpha_1, \ldots, \alpha_k) = h_i(1, \alpha_1, \ldots, \alpha_k) \oplus 1$,$\alpha_i \in E_2$. Если первая переменная является фиктивной, то по определению несущественной переменной $h_i(0, \alpha_1, \ldots, \alpha_k) = h_i(1, \alpha_1, \ldots, \alpha_k)$,$\alpha_i \in E_2$. Таким образом $h_i(0, \alpha_1, \ldots, \alpha_k) = h_i(1, \alpha_1, \ldots, \alpha_k) \oplus c_i$,$c_i \in E_2$. По определению булевского оператора, порождаемого кодированием F переходной системы V, множества $\mathcal{F}_V(F)$ и порождающих внутренней полугруппы имеем

$$
\begin{aligned}
p_0(q) &= {F_0}^{-1}(h_0(0, F_0(q)), h_1(0, F_0(q)), \ldots, h_{k-1}(0, F_0(q))),\\
p_1(q) &= {F_0}^{-1}(h_0(1, F_0(q)), h_1(1, F_0(q)), \ldots, h_{k-1}(1, F_0(q))) =\\
&= {F_0}^{-1}(h_0(0, F_0(q)) \oplus c_0, h_1(0, F_0(q)) \oplus c_1, \ldots, h_{k-1}(1, F_0(q)) \oplus c_{k-1}) =\\
&= p_0(q) + c,
\end{aligned}
$$

где $c = {F_0}^{-1}(c_0, c_1, \ldots, c_{k-1})$. Сумма понимается в смысле суммы в поле Галуа F_{2^k}. Обозначим перестановку, соответствующую многочлену $x + c$, через h_c. Тогда $p_1 = p_0 \cdot h_c$. Пусть переходная система линейно реализуема посредством кодирования F. Согласно теореме 1 булевский оператор, порождаемый кодированием F переходной

системы V, совпадает с булевским оператором, порождаемым кодированием F_0 переходной системы V_{s_F}. Тогда согласно определению ${p_0}^{V_{s_F}} = {s_F}^{-1} \cdot p_0 \cdot s_F$, ${p_1}^{V_{s_F}} = {s_F}^{-1} \cdot p_1 \cdot s_F$. Как только что было показано, ${p_1}^{V_{s_F}} = {p_0}^{V_{s_F}} \cdot h_c$. Следовательно ${s_F}^{-1} \cdot p_1 \cdot s_F = {s_F}^{-1} \cdot p_0 \cdot s_F \cdot h_c$. Отсюда имеем $p_1 = p_0 \cdot s_F \cdot h_c \cdot {s_F}^{-1}$. Что и требовалось доказать.

Теорема 5. *Число различных линейно реализуемых нумерованных переходных систем с n состояниями не превосходит* $n^{\log_2(n)+2} \cdot (n-2)!$.

Перед доказательством введем несколько определений. По аналогии с булевским оператором, построенным по заданной переходной системе с помощью некоторого кодирования, можно определить булевский оператор для отдельной подстановки. И ввести понятие линейной реализуемости подстановки.

Определение 6. Пусть задана некоторая подстановка на множестве $Q = \{0, \ldots, n-1\}$, $s : Q \to Q$. Кодирование F множества Q, определяет по подстановке s, булевский оператор ϕ_s по правилу

$$\phi_s(\alpha_1, \ldots, \alpha_{k-1}) = F(s(F^{-1}(\alpha_1, \ldots, \alpha_{k-1}))),$$

где $\alpha_1, \ldots, \alpha_{k-1} \in E_2$,$k = \log_2(n)$. Данный оператор может быть рассмотрен как набор k булевских функций, зависящих от k переменной. Обозначим этот набор через $\mathcal{F}_s(F)$.

Определение 7. Подстановка называется линейно реализуемой, посредством кодирования F, если набор $\mathcal{F}_s(F)$ состоит из линейных булевских функций.

Доказательство. Для доказательства теоремы докажем, что подстановка, линейно реализуема посредством стандартного кодирования F_0, тогда и только тогда, когда соответствующий ему многочлен над полем Галуа F_{2^k} является линейной комбинацией многочленов вида x^{2^i}, где $i = 0, \ldots, k-1$ и константы $c \in F_{2^k}$. Сначала докажем, что всякая подстановка, у которой соответствующий ей многочлен над полем Галуа имеет указаный вид является линейно реализуемой посредством стандартного кодирования F_0. Поле F_{2^k} является расширением поля F_2, образующим элементом которого является корень

неприводимого над F_2 многочлена степени k. Обозначим его через f. Его элементы могут быть рассмотрены как формальные многочлены [2]

$$q_{k-1} \cdot x^{k-1} + q_{k-2} \cdot x^{k-2} + \ldots + q_0. \qquad (*)$$

При этом данный многочлен соответствует элементу $q \in Q$, стандартный код которого равен $(q_0, q_1, \ldots, q_{k-1})$. Пусть многочлен, соответствующий подстановке s имеет вид

$$f_s(x) = c_0 + \sum_{i=1}^{k} c_i \cdot x^{2^{i-1}}.$$

Рассмотрим его значение на элементе q. Заметим, что умножение в поле Галуа $F_{2^k} \cong F_2[x]/(f)$ есть умножение многочленов вида (*) по модулю многочлена f. Также заметим, что для $g_1, g_2 \in F_{2^k}$ $(g_1 + g_2)^{2^i} = (g_1)^{2^i} + (g_2)^{2^i}$. Обозначим через f_c многочлен вида (*) константы $c \in F_{2^k}$. Тогда имеем

$$f_s(q) = f_{c_0} + \sum_{i=1}^{k} f_{c_i} \cdot {f_q}^{2^{i-1}} =$$

$$= f_{c_0} + \sum_{i=1}^{k} f_{c_i} \cdot (q_{k-1} \cdot x^{k-1} + q_{k-2} \cdot x^{k-2} + \ldots + q_0)^{2^{i-1}} =$$

$$= f_{c_0} + \sum_{i=1}^{k} f_{c_i} \cdot (q_{k-1} \cdot x^{k-1})^{2^{i-1}} + \sum_{i=1}^{k} f_{c_i} \cdot (q_{k-2} \cdot x^{k-2})^{2^{i-1}} + \ldots + \sum_{i=1}^{k} f_{c_i} \cdot (q_0)^{2^{i-1}} =$$

$$= f_{c_0} + \sum_{i=1}^{k} f_{c_i} \cdot q_{k-1} \cdot (x^{k-1})^{2^{i-1}} + \sum_{i=1}^{k} f_{c_i} \cdot q_{k-2} \cdot (x^{k-2})^{2^{i-1}} + \ldots + \sum_{i=1}^{k} f_{c_i} \cdot q_0 =$$

$$= f_{c_0} + \sum_{i=1}^{k} q_{k-1} \cdot f_{c_i} \cdot x^{(k-1) \cdot 2^{i-1}} + \sum_{i=1}^{k} q_{k-2} \cdot f_{c_i} \cdot x^{(k-2) \cdot 2^{i-1}} + \ldots + \sum_{i=1}^{k} q_0 \cdot f_{c_i} =$$

$$= f_{c_0} + q_{k-1} \cdot \sum_{i=1}^{k} f_{c_i} \cdot x^{(k-1) \cdot 2^{i-1}} + q_{k-2} \cdot \sum_{i=1}^{k} f_{c_i} \cdot x^{(k-2) \cdot 2^{i-1}} + \ldots + q_0 \cdot \sum_{i=1}^{k} f_{c_i}.$$

Результат умножения многочленов f_{c_i} на многочлен $x^{(k-j) \cdot 2^{i-1}}$, где $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant k$ есть опять многочлены вида (*) ${b_{k-1}}^{f_{c_i}, x^{(k-j) \cdot 2^{i-1}}}$.

$x^{k-1} + b_{k-2}{}^{f_{c_i},x^{(k-j)\cdot 2^{i-1}}} \cdot x^{k-2} + \ldots + b_0{}^{f_{c_i},x^{(k-j)\cdot 2^{i-1}}}$. Сгруппируем эту сумму по степеням x^l, где $0 \leqslant l \leqslant k-1$. Коэффициент при каждой степени есть линейная комбинация q_l,где $0 \leqslant l \leqslant k-1$. Коэффициент при степени x^l, есть значение l-ой функции из множества $\mathcal{F}_s(F_0)$. А следовательно данная функция является линейной булевской функцией переменных $q_0, \ldots, q_{k-1}$. Таким образом показано, что всякая подстановка, соответствующий многочлен над полем Галуа является линейной комбинацией многочленов вида x^{2^i}, где $i = 0, \ldots, k-1$ и константы $c \in F_{2^k}$, является линейно реализуемой посредством кодирования F_0. Посчитаем число таких многочленов. Мы имеем k степеней, каждая из которых может быть умножена на 2^k констант, и 2^k констант. Следовательно число таких многочленов равно $2^{k^{k+1}} = n^{\log_2(n)+1}$. Несложно видеть, что число различных подстановок на n-элементном множестве, линейно реализуемых посредством кодирования F_0 равно $n^{\log_2(n)+1}$. Действительно пусть задана подстановка на n-элементном множестве, линейно реализуемая посредством стандартного кодирования F_0. Обозначим через $k = \log_2(n)$. Данное кодирование порождает булевский оператор $\phi_s : {E_2}^k \to {E_2}^k$. Рассмотрим этот оператор, как набор $\mathcal{F}_s(F_0)$. Поскольку подстановка линейно реализуема, то элементы $\mathcal{F}_s(F_0)$ есть линейные булевские функции от k переменной, а именно $\mathcal{F}_s(F_0) = \{f_0, \ldots, f_{k-1}\}$,где $k = \log_2(n)$. Как известно, число различных линейных булевских функций зависящих от k переменной равно 2^{k+1} [1]. Значит число различных наборов $\mathcal{F}_s(F_0)$ равно $\left(2^{k+1}\right)^k$, что равно $n^{\log_2(n)+1}$. Теперь покажем, что двум различным наборам соответсвуют две различные подстановки, линейно реализуемые посредством стандартного кодирования F_0. Каждый набор соответствует булевскому оператору $\phi(\alpha_1, \ldots, \alpha_k) = (\beta_1, \ldots, \beta_k)$,где $\alpha_i, \beta_i \in E_2$. Определим подстановку по следующему правилу: $s_\phi(q) = {F_0}^{-1}(\phi(F_0(q))$. Несложно видеть, что линейный оператор, получаемый с помощью кодирования F_0 подстановки s_ϕ равен оператору ϕ. Пусть заданы два различных набора $\mathcal{F}_1$ и $\mathcal{F}_2$. Поскольку они различны, то найдутся две неравные функции ${f_i}^1 \in \mathcal{F}_1$ и ${f_i}^2 \in \mathcal{F}_2$ и набор $\alpha_1, \ldots, \alpha_k$, где $\alpha_i \in E_2$, такие что ${f_i}^1(\alpha_1, \ldots, \alpha_k) \neq {f_i}^2(\alpha_1, \ldots, \alpha_k)$. Следовательно операторы, соответствующие первому и второму набору, не равны на наборе

$\alpha_1, \ldots, \alpha_k$. Обозначим булевский оператор соответствующий первому набору ϕ_1, а второму — ϕ_2. $\phi_1(\alpha_1, \ldots, \alpha_k) \neq \phi_2(\alpha_1, \ldots, \alpha_k)$. Обозначим через $q = F_0(\alpha_1, \ldots, \alpha_k)$. Тогда согласно построению подстановки по булевскому оператору $s_{\phi_1}(q) = {F_0}^{-1}(\phi_1(\alpha_1, \ldots, \alpha_k))$, а $s_{\phi_2}(q) = {F_0}^{-1}(\phi_2(\alpha_1, \ldots, \alpha_k))$. Поскольку по определению кодирования, отображение F_0 взаимооднозначное, то $s_{\phi_1}(q) \neq s_{\phi_2}(q)$. В силу однозначности и единственности многочлена над полем Галуа, соответствующего данной подстановке, получаем, что для линейно реализуемых подстановок посредством кодирования F_0, соответствующий многочлен имеет указанный вид. Утверждение доказано.

Перестановка, соответствующий многочлен которой есть $c \cdot x$, есть $h_c \in H_*$. Поле Галуа F_n без элемента 0 относительно операции умножения представляет собой циклическую группу порядка $n-1$. Порождающий элемент мультипликативной группы поля Галуа обозначим ее через a_0,а h_{a_0} через h_m. Заметим, что для любого $a = {a_0}^i \in {F^*}_n$, $h_a = {h_m}^i$. Действительно, $h_a(q) = a \cdot q = {a_0}^i \cdot q = a_0 \cdot (a_0 \cdot (\ldots \cdot q)) = h_m(h_m(\ldots h_m(q))) = {h_m}^i(q)$ для любого $q \in Q$.

Обозначим через h_d, перестановку, такую что $h_d(q) = h_q(q) = {h_m}^i(q)$, где $q = {a_0}^i \in \{0, \ldots, n-1\}$. Перестановка, соответствующий многочлен, которой есть $c \cdot x^{2^i}$, есть ${h_d}^i \cdot h_c$, где $i = 0, \ldots, k-1$. Действительно для $i = 0$ многочлен имеет вид $c \cdot x$ и соответствующая ему подстановка есть h_c. Для $i = 1$ многочлен имеет вид $c \cdot x^2$. Рассмотрим заначение многочлена $c \cdot x^2$ на элементе $q \in Q$. $c \cdot x^2(q) = c \cdot q^2 = c \cdot (q \cdot q) = c \cdot h_q(q) = h_c(h_q(q))$. Таким образом показано, что для любого элемента $q \in Q$ значение многочлена $c \cdot x^2$ равно значение перестановки $h_d \cdot h_c$. Для произвольного i имеем $c \cdot x^{2^i}(q) = c \cdot x^{2^i}(q) = c \cdot q^{2^i} = h_c(h_d(h_d \ldots (q))) = h_c({h_d}^i(q))$.Таким образом показано, что для любого элемента $q \in Q$ значение многочлена $c \cdot x^{2^i}$ равно значению перестановки ${h_d}^i \cdot h_c$. Значение многочлена $\sum_{i=0}^{k-1} c_i \cdot x^{2^i}$ на элементе q, определяется перестановками ${h_d}^i \cdot h_{c_i}$, и таблицей суммы в поле Галуа F_{2^k}. Если подстановка s линейно реализуема посредством кодирования F, покажем, что булевский оператор, получаемый кодированием F подстановки s, совпадает с булевским оператором, получаемым посредством кодирования F_0 подстановки ${s_F}^{-1} \cdot s \cdot s_F$. Пусть задано кодирование $F : \{0, \ldots, n-1\} \to {E_2}^k$. Тогда соответствующий булевский оператор определяется как

$$\phi_s(\alpha_1,\ldots,\alpha_{k-1}) = F(s(F^{-1}(\alpha_1,\ldots,\alpha_{k-1}))),$$

где $\alpha_1,\ldots,\alpha_{k-1} \in E_2$, $k = \log_2(n)$. Несложно видеть, что булевский оператор, порождаемый кодированием F_0 перестаноки ${s_F}^{-1} \cdot s \cdot s_F$, определяется как

$$\phi_{s_F}(\alpha_1,\ldots,\alpha_k) = F_0(s_F(s({s_F}^{-1}({F_0}^{-1}(\alpha_1,\ldots,\alpha_k))))).$$

Поскольку $s_F(i) = {F_0}^{-1}(F(i))$, то

$$\phi_{s_F}(\alpha_1,\ldots,\alpha_k) = F_0({F_0}^{-1}(F(s(F^{-1}(F_0({F_0}^{-1}(\alpha_1,\ldots,\alpha_k))))))) = \\ = F(s(F^{-1}(\alpha_1,\ldots,\alpha_k))).$$

Покажем,что значение подстановки s определяется значениями перестановок $h_d^{{s_F}^i} \cdot h_{c_i}^{s_F}$ и таблицей суммы полученной из таблицей суммы в поле Галуа F_{2^k} следующим образом: строки и столбцы таблицы переставляются согласно перестановке ${s_F}^{-1}$, а элементы таблицы заменяются согласно перестановке s_F. Обозначим операцию задаваемую этой таблицей через $+_{s_F}$. Заметим,что $a +_{s_F} b = s_F({s_F}^{-1}(a) + {s_F}^{-1}(b))$. А следовательно, $a + b = {s_F}^{-1}(s_F(a) +_{s_F} s_F(b))$ Пусть h_f и h_g подстановки, соответствующие некоторым многочленам f и g. Для каждого $q \in Q$ покажем, что ${s_F}^{-1} \cdot (h_f + h_g) \cdot s_F = {h_f}^{s_F} +_{s_F} {h_g}^{s_F}$. Действительно

$$s_F(h_f + h_g({s_F}^{-1}(q))) = s_F(h_f({s_F}^{-1}(q)) + h_g({s_F}^{-1}(q))) = \\ = s_F({s_F}^{-1}(s_F(h_f({s_F}^{-1}(q))) +_{s_F} s_F(h_g({s_F}^{-1}(q))) = {h_f}^{s_F}(q) +_{s_F} {h_g}^{s_F}(q).$$

Заметим, что сопряжение произведения подстановок, есть произведение сопряжений. Покажем, что если $q = {a_0}^i$ верно равенство ${h_d}^{s_F}(q) = h_m^{{s_F}^i}(q)$. ${h_d}^{s_F}(q) = s_F({h_m}^i({s_F}^{-1}(q))) = s_F(h_m(h_m(\ldots({s_F}^{-1}(q))))) = {h_m}^{s_F}(q)$. Заметим, что ${h_c}^{s_F}(q) = s_F(h_c({s_F}^{-1}(q))) = s_F({h_m}^j({s_F}^{-1}(q))) = {h_m}^{{s_F}^i}(q)$.

Следовательно линейно реализуемые подстановки, полностью определяется перестановкой $h_m^{s_F}$. Данная перестановка есть цикл длины $n-1$. А таких перестановок $(n-2)!$ [3]. Следовательно число линейно реализуемых подстановок не превосходит $n^{\log_2(n)+1} \cdot (n-2)!$. Число линейно реализуемых переходных систем, не превосходит $n \cdot n^{\log_2(n)+1} \cdot (n-2)! = n^{\log_2(n)+2} \cdot (n-2)!$. Теорема доказана.

Теорема 6. *Число линейно реализуемых переходных систем с n состояниями есть $o(n^{2\cdot n})$.*

Доказательство. Обозначим через $N_L(n)$ число линейно реализуемых переходных систем с n состояниями. Согласно теореме 5

$$\frac{N_L(n)}{n^{2\cdot n}} \leqslant \frac{n^{\log_2(n)+2}\cdot(n-2)!}{n^{2\cdot n}},$$
$$\frac{n^{\log_2(n)+2}\cdot(n-2)!}{n^{2\cdot n}} \leqslant \frac{n^{\log_2(n)}\cdot(n-2)^{n-2}}{n^{2\cdot(n-1)}} \leqslant \frac{n^{\log_2(n)}}{n^{(n-1)}},$$
$$\lim_{n\to\infty}\frac{n^{\log_2(n)}}{n^{(n-1)}} = 0.$$

Отсюда следует уверждение теоремы $\lim\limits_{n\to\infty}\frac{N_L(n)}{n^{2\cdot n}} = 0$. Теорема доказана.

В заключение, автор выражет благодарность Станиславу Владимировичу Алёшину, чьи советы оказали неоценимую помощь в достижении результатов, изложенных в данной работе.

Список литературы

[1] Яблонский С. В. Введение в дискретную математику. М.: Наука, 1979.

[2] Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988.

[3] Карагаполов М. И., Мерзляков Ю. И. Основы теории групп / 3-е изд. М.: Наука, 1982.

[4] Арбиб М. А. Декомпозиция автоматов и расширение полугрупп // Алгебраическая теория автоматов, языков и полугрупп. М.: Статистика, 1975. С. 46–64.

[5] Родин С. Б. Переходные системы с максимальной вариантностью относительно кодирования состояний // Интеллектуальные системы. Т. 4, вып. 3–4. С. 335–352.