ФГБОУ ВО «Московский государственный университет
имени М. В. Ломоносова»

Механико-математический факультет

На правах рукописи

Родин Сергей Борисович

Размещение состояний автоматов

01.01.09 — Дискретная математика и математическая кибернетика

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научные руководители:

д.ф.-м.н., профессор
Алешин С. В.

Москва – 2017

Содержание

Введение

Актуальность. Диссертация посвящена изучению задачи кодирования состояний автоматов.

Абстрактный автомат является достаточно мощным объектом для описания функционирования реальных устройств. Это понятие используется в таких областях как теория сложности, теория алгоритмов, теория языков, теория групп. На практике автомат используется в таких областях как синтез СБИС, теория кодирования, обработка изображений, передача данных. Однако, для практического применения необходимым этапом является синтез автоматов или переход с языка абстрактных автоматов на язык схем.

Переход на язык схем осуществляется посредством кодирования состояний, входных символов и выходных символов. В результате получаются описания, которые называются каноническими уравнениями. Часть уравнений описывают переходы состояний, другая часть описывает выходы. Таким образом, кодирование приводит к возникновению булевых операторов. Затем булевы операторы реализуются в виде схем из функциональных элементов. Набор функциональных элементов может содержать(и на практике обычно содержит) функции многих переменных, операторы и т.д.(этот набор называется библиотекой). На основе этой библиотеки строят схемы.

В описанной процедуре реализации абстрактного автомата видно много степеней свободы. Однако первый и, на наш взгляд, очень важный этап — это выбор кодирования состояний. После того как код выбран все остальные этапы детерминированы в известной степени.

В зависимости от условий, накладываемых на получаемую схему, воз-

никает ряд задач, связанных с кодированием состояний автомата: задача противогоночного кодирования, задача монотонного кодирования, задача экономичного кодирования и другие.

В случае противогоночного кодирования требуется найти такое кодирование, что при любом переходе автомата из одного состояния в другое переключается только один элемент памяти.

Задача монотонного кодирования состоит в нахождение такого кодирования, что возникаемые функции переходов являются монотонными функциями алгебры логики.

В данной работе основной задачей была задача экономичного кодирования, которая состоит в нахождении кодирования, при котором достигается возможно меньшая сложность схемы. Данную задачу можно решать с использованием эвристических алгоритмов построения кодирования состояний. Данные алгоритмы изучались в работе [1]. Особенностью данных методов является построение кодирований, приводящих к «достаточно простым» схемам, но не гарантирующим, что полученная схема будет «простейшей». Одним из основных подходов является построение кодирований, при котором уменьшается число существенных переменных у функций переходов, соответствующих переменным кодирования.

Вопрос «простой» реализации автоматов был рассмотрен в работах 60-х годов Стирнса и Хартманиса. В основе исследований лежал метод пар разбиений на множестве состояний автомата. Этот метод был в дальнейшем трансформирован в метод алгебры пар. Покрытием π множества Q называется разбиение множества Q на непересекающиеся подмножества, которые называются блоками [2]. На множестве покрытий вводится частичный порядок. Говорим, что покрытие $\pi_1 \geq \pi_2$, если каждый блок покрытия π_2 полностью содержится в некотором блоке π_1. С помощью порядка вводится операции сложения и умножения на покрытиях. По определению $\pi_1 + \pi_2$ — наименьшая верхняя грань покрытий π_1 и π_2, а $\pi_1 \cdot \pi_2$ — наибольшая нижняя грань покрытий π_1 и π_2. Упорядоченная пара (π, τ) покрытий множества Q автомата $\mathcal{A}$ образует пару покрытий, если для любых двух состояний q_i и q_j, лежащих в одном блоке покрытия π, и для любого входа $a \in A$, состоя-

ния в следующий момент времени $\varphi(a, q_i)$ и $\varphi(a, q_j)$ лежат в одном блоке покрытия τ. На основании понятия пары покрытий и введенного порядка для заданного покрытия π определяется «наименьшее» покрытие τ, составляющее пару покрытий (π, τ), такое покрытие обозначается $m(\pi)$. Для покрытия π наибольшее покрытие τ, такое что (τ, π) есть пара покрытий, обозначается $M(\pi)$. С каждым кодированием алфавита состояний Q векторами длины k можно связать k покрытий множества Q, пусть i-ой переменной соответствует покрытие π_i. Было доказано, что переменная, соответствующая покрытию τ, зависит от некоторого подмножества переменных с индексами $P \subset \{0, \ldots, k-1\}$ тогда и только тогда, когда $(\prod_{i \in P} \pi_i, \tau)$ есть пара покрытий. Существование кодирования с таким свойством эквивалентно существованию разложению(разбиению,декомпозиции) автомата на меньшие автоматы. Введенные понятия также могут быть использованы для изучения обратной связи в реализации автомата. С помощью разбиения множества вводится формализация переменной, участвующей в операции обратной связи. Разбиение π_f множества состояний называется разбиением обратной связи, если существует набор таких покрытий $\{\tau_i\}(1 \leq i \leq k)$, что $\prod_{i=1}^{k} \tau_i$ и $(\pi_f \cdot \prod_{i<j}, \tau_j)$ есть пара покрытий, $j = 1, \ldots, k$. Для покрытия π определен ряд покрытий $A^i(\pi)$ по следующему правилу $A^1(\pi) = \pi$ и $A^{i+1}(\pi) = \pi \cdot m(A^i(\pi))$. Если используется кодирование кодами длины n, обозначим $A(\pi) = A^n(\pi)$. С помощью введенных понятий сформулирован критерий, для автомата существует реализация, где переменная, соответствующая покрытию π_f, используется в операции обратной связи тогда и только тогда, когда $A(\pi_f) = 0$. Как следствие данного результата доказан критерий используется ли операция обратной связи в реализации автомата, а именно операция обратной связи не используется тогда и только тогда, когда $m^n(I) = 0$ или, что эквивалентно, $M^n(0) = I$

Также данная техника в отдельных случаях позволяет находить разложения автомата в последовательно-параллельное соединение двух автоматов, в одном из которых не используется операция обратной связи. Как видно, предложенная техника является довольно мощной, с одной стороны она позволяет абстрагироваться от конкретной реализации автомата, с

другой стороны позволяет находить декомпозицию автомата на более простые автоматы. В ее основе лежит понятие пары покрытий и введенные операции сложения и умножения. Данный подход может быть обобщен до рассмотрения пар объектов(не обязательно покрытий), удовлетворяющих ряду свойств. Таким образом возникло понятие алгебры пар. А именно, пусть L_1 и L_2 - конечные структуры, тогда подмножество Δ прямого произведения $L_1 \times L_2$ является алгеброй пар тогда и только тогда, когда выполнены свойства:

1. Если $(x_1, y_1), (x_2, y_2) \in \Delta$, то $(x_1 \cdot x_2, y_1 \cdot y_2) \in \Delta$ и $(x_1 + x_2, y_1 + y_2) \in \Delta$
2. $\forall x \in L_1$ и $\forall y \in L_2$, $(x, I) \in \Delta$ и $(0, y) \in \Delta$.

Под операцией умножения понимается операция взятия наибольшей нижней грани, под операцией сложения понимается операция взятия наименьшей верхней грани. Был доказан ряд результатов, связывающий возможность декомпозиции автомата в последовательно-параллельное соединение меньших автоматов с наличием пар покрытий множества состояний с определенными свойствами [3].

Тот или иной подход к реализации автоматов приводит к возникновению булевых операторов. Суммарная сложность этих операторов и задает сложность реализации автомата. Естественно начинать такого рода исследования с «простейших», линейных операторов. Наиболее полно линейные автоматы изучены в книге А. Гилла «Линейные последовательностные машины» [4]. Линейным автоматом называется шестерка $\mathcal{L} = (E_p^r, E_p^k, E_p^m, \varphi, \psi, q_0)$, где $\varphi(x, q) = Ax + Bq$, $\psi(x, q) = Cx + Dq$, сумма понимается в смысле суммы в поле Галуа $GF(p)$, где p — простое число. В книге введены и изучены понятия эквивалентности, подобия, минимальности, канонической формы, управляемости и предсказуемости линейных автоматов. Отдельно рассмотрены и изучены автономные линейные автоматы и автоматы с нулевым начальным состоянием. Для каждого из классов изучены проблемы анализа и синтеза автоматов. Также отдельно рассматриваются процессы изменения состояний автоматов и развивается теория множества циклов и деревьев.

И в частности, рассмотрен вопрос линейной реализуемости для автоматов, у которых множество входных сигналов — это множество l-мерных векторов над полем $GF(p)$, множество выходных сигналов — это множество m-мерных векторов над полем $GF(p)$, множество состояний содержит p^n элементов. Приводится метод, который в некоторых случаях дает ответ о линейной реализуемости. Для таких автоматов доказаны следующие утверждения. Пусть задано множества $S = \{s_1, s_2, \ldots, s_{n-1}\}$ и $y_0^j(t)$ — выход автомата в момент t при входном символе 0 и начальном состоянии s_j. Введем матрицу

$$L = \begin{pmatrix} y_0^1(0) & y_0^2(0) & \ldots & y_0^{p^n}(0) \\ y_0^1(1) & y_0^2(1) & \ldots & y_0^{p^n}(1) \\ \ldots & & & \\ y_0^1(n-1) & y_0^2(n-1) & \ldots & y_0^{p^n}(n-1) \end{pmatrix}$$

Составим из первых n линейно независимых строк матрицы L матрицу $\widetilde{L}$, а через s_j обозначим j-й вектор-столбец матрицы $\widetilde{L}$. Тогда, если существует изоморфный исходному линейный автомат $\mathfrak{A}$, состояние s_j заданного автомата эквивалентно состоянию $\mathbf{s}_j$ автомата $\mathfrak{A}$. У исходного автомата можно переобозначить каждое состояния s_j на $\mathbf{s_j}$ и пусть δ и λ его функция переходов и выходов. Введем обозначения

$$\mathbf{s'}_i = \delta(\mathbf{s}^i, \mathbf{0}), \quad \mathbf{s''}_i = \delta(\mathbf{0}, \mathbf{u}^i),$$

$$\mathbf{y'}_i = \lambda(\mathbf{s}^i, \mathbf{0}), \quad \mathbf{y''}_i = \lambda(\mathbf{0}, \mathbf{u}^i).$$

Верно утверждение, если существует изоморфный исходному линейный автомат $\mathfrak{A}$,

$$A = ||\mathbf{s'}_1, \mathbf{s'}_2, \ldots, \mathbf{s'}_n||,$$

$$B = ||\mathbf{s''}_1, \mathbf{s''}_2, \ldots, \mathbf{s''}_l||,$$

$$C = ||\mathbf{y'}_1, \mathbf{y'}_2, \ldots, \mathbf{y'}_n||,$$

$$D = ||\mathbf{y''}_1, \mathbf{y''}_2, \ldots, \mathbf{y''}_l||.$$

Таким образом, проверка линейной реализуемости автомата осуществляется проверкой, что состояние автомата в следующей момент времени вычисляется как $A\mathbf{s} + B\mathbf{u}$, а выход автомата определяется выражением $C\mathbf{s} + D\mathbf{u}$ для всех $\mathbf{s}$ и $\mathbf{u}$. Если это не верно, то исходный автомат не является линейно реализуемым. Однако, было замечено, что исходный автомат может превратиться в линейно реализуемый, если переобозначить входные и(или) выходные символы. Таким образом, данный результат не в полной мере решает вопрос о линейной реализуемости автомата.

Другой подход связан с рассмотрением свойств внутренней полугруппы. Внутренняя полугруппа определяется как замыкание отображений множества состояний в себя, определяемых входными символами [5]. Внутренняя полугруппа является инвариантом относительно кодирований состояний. Тогда вопрос линейной реализуемости можно решать через характеризацию внутренней полугруппы.

В работе Экера [6] был рассмотрен вопрос о линейно реализуемых автоматах с точки зрения внутренней полугруппы. В частности, приведена характеризация внутренней полугруппы линейно реализуемого автомата в случае, когда внутренняя полугруппа автомата — группа, а именно группа G изоморфна внутренней полугруппе линейного над полем $GF(p)$ автомата тогда и только тогда, когда:

1. G содержит нормальную, абелеву подгруппу N, у которой все элементы кроме единичного имеют порядок p;

2. существует такой элемент $c \in G$, что N и c образуют G.

Однако, данная теорема не в полной мере решает вопрос о линейно реализуемости автомата, так автомат, внутренняя полугруппа которого удовлетворяет условиям теоремы, не всегда является линейно реализуемым, что было показано в работе Хартманиса и Уолтера [7]. В этой же работе развит подход, предложенный Экером, и сформулирован критерий линейной реализуемости автомата в случае, когда автомат — перестановочный и сильно-связный. Также отметим, что в работе рассматриваются автоматы

без выходов или переходные системы. В случае, когда внутренняя полугруппа автомата V — это транзитивная группа G, состояния автомата V могут быть рассмотрены как левые смежные классы группы G по простой подгруппе H, т.е. переходная система автомата с точностью до изоморфизма определяется группой G, простой подгруппой H и подмножеством $I \subseteq G$, где G — внутренняя полугруппа, множество смежных классов — множество состояний, подмножество I — множество входов. Переходная система, задаваемая этими объектами, обозначается $V_{G,H,I}$. Тогда результат может быть сформулирован следующим образом, переходная система $V_{G,H,I}$ - линейно реализуема над полем $GF(p)$ тогда и только тогда, когда

1. G содержит нормальную, абелеву подгруппу N, у которой все элементы кроме единичного имеют порядок p;
2. существует такой элемент $c \in G$, что N и c образуют G;
3. $N \cap H = e$;
4. $I \subseteq Na$ для некоторого $a \in G$.

Данный результат ограничен перестановочными сильно-связными автоматами. Дальнейшее развитие изложенный подход получил в работе Хартфила и Максона [8]. В работе сформулированы две теоремы. Первая — это обобщение результата Экера на полугрупповой случай, а именно существует изоморфизм β между полугруппой $S =< \phi_0, \phi_1, \ldots, \phi_r >$ и внутренней полугруппой автомата, линейно реализуемого над полем $GF(p)$ тогда и только тогда, когда S — подполугруппа моноида $J =< \phi_0, N >$, где

1. N — абелева группа, содержащая единичный элемент моноида J, у которой все элементы имеют порядок p;
2. $\phi_0 N = N\phi_0$;
3. если для $\phi', \phi'' \in N$ верно $\phi'\phi_0^k = \phi''\phi_0^k$, то $\phi' = \phi''$;
4. $\{\phi_0, \phi_1, \ldots, \phi_r\} \subseteq N\phi_0$.

Вторая теорема обобщает результат Хартманиса и Уолтера на случай полугрупповых автоматов. Пусть задана полугруппа S, тогда автомат имеющий в качестве внутренней полугруппы полугруппу S определяется, с точность до изоморфизма, полугруппой S, множеством $I \subseteq S$, и левой конгруэнтностью ρ на S, где I — множество входов, классы эквивалентности, определяемые конгруэнтностью ρ — множество состояний, умножение в полугруппе S определяет функцию переходов. Такой автомат обозначен через $V_{S,I,\rho}$. В определенных терминах сформулирован критерий линейно реализуемости, а именно автомат $V_{S,I,\rho}$ линейно реализуем над полем $GF(p)$ тогда и только тогда, когда S — подполугруппа моноида $J =< \phi_0, N >$, где

1. N — абелева группа, содержащая единичный элемент моноида J, у которой все элементы имеют порядок p;
2. $\phi_0 N = N\phi_0$;
3. если для $\phi', \phi'' \in N$ верно $\phi'\phi_0^k = \phi''\phi_0^k$, то $\phi' = \phi''$;
4. $\{\phi_0, \phi_1, \ldots, \phi_r\} \subseteq N\phi_0$;
5. конгруэнтность ρ может быть доопределена до левой конгруэнтности $\bar{\rho}$ на J таким образом, что $\rho \cap \mu = id$, где μ — конгруэнтность на J, определяемая правилом: $s\mu t$ если существует такой элемент $\psi \in N$, что $s = \psi t$.

Данные результаты полно характеризуют внутреннюю полугруппу линейно реализуемых автоматов и дают критерий линейной реализуемости в терминах внутренней полугруппы. Однако, построение внутренней полугруппы автомата представляет собой нетривиальную задачу. В диссертации будет представлен критерий линейной реализуемости в терминах порождающих внутренней полугруппы. Такой подход представляется более «технологичным», так как анализ свойств порождающих существенно проще.

Предыдущие результаты относятся к случаю неизбыточных кодирований, т.е. когда состояния кодируются минимально возможными по длине

кодами. Однако, автомат может не являться линейно-реализуемым для неизбыточного кодирования, но «удлинение» кода приводит к линейной реализуемости автомата. С точки зрения полугрупповых свойств наличие такого более длинного кода, приводящего к линейной реализуемости автомата $\mathfrak{A}$, эквивалентно существованию линейно-реализуемого автомата, чей гомоморфный образ равен исходному автомату $\mathfrak{A}$. В работах [9], [7] исследуются гомоморфные образы линейно-реализуемых переходных систем. Доказан результат, гомоморфный образ линейно реализуемой переходной системы, не являющийся линейно-реализуемым, есть последовательно-параллельное соединение двух переходных систем, одна из которых либо не содержит обратных связей, либо функция переходов этой переходной системы зависит фиктивным образом от входной переменной. Заметим, что данные результаты приведены для группового случая, т.е. для переходных систем, чья внутренняя полугруппа является группой. Данные результаты задают критерий линейной реализуемости «длинными» кодированиями, однако, не приведены оценки на длину кода, приводящего к линейной реализуемости. А также нет оценок сложности реализации автоматов, не являющихся линейно реализуемыми.

Цель исследования. Основной целью настоящей работы является исследование и совершенствование математических методов, применяемых при решении задачи кодирования состояний автоматов. Тема, объект и предмет диссертационной работы соответствуют следующим пунктам паспорта специальности 01.01.09 — дискретная математика и математическая кибернетика: теория автоматов; теория кодирования (алгоритмические и комбинаторные вопросы, синтез и сложность управляющих систем), в частности, сложность алгоритмов и вычислений). Для достижения поставленной цели в работе сформулированы и решаются следующие задачи.

- Нахождение критерия линейной реализуемости автомата посредством неизбыточных кодирований в терминах порождающих внутренней полугруппы
- Теоретическая оценка сложности реализации автомата посредством

всевозможных однородных кодирований состояний, не обязательно неизбыточных

- Алгоритмическая разрешимость задачи распознавания свойства линейной реализуемости автомата посредством всевозможных однородных кодирований состояний автомата, не обязательно неизбыточных

- Нахождение критерия максимальной реализуемости автомата в терминах порождающих внутренней полугруппы

Научная новизна. Результаты диссертации являются новыми и получены автором самостоятельно. Основные результаты диссертации состоят в следующем:

- Сформулирован критерий линейной реализуемости автомата посредством неизбыточных кодирований в терминах порождающих внутренней полугруппы

- Получена оценка сложности реализации автомата посредством всевозможных однородных кодирований состояний, не обязательно неизбыточных

- Доказана алгоритмическая разрешимость задачи распознавания свойства линейной реализуемости автомата посредством всевозможных однородных кодирований состояний автомата, не обязательно неизбыточных

- Сформулирован критерий максимальной реализуемости автомата в терминах порождающих внутренней полугруппы

- С помощью полученных критериев установлено как взаимосвязаны классы линейно реализуемых автоматов и максимально реализуемых автоматов. Было показано, что данные классы имеют непустое пересечение, и ни один из классов не лежит в другом.

Метод исследования. В работе используются методы теории автоматов, теории сложности, теории кодирования, теории конечных полей, теории групп и теории полугрупп.

Теоретическая и практическая ценность. Работа носит теоретический характер. Результаты диссертации могут быть использованы в теории автоматов, теории кодирования, теории синтеза и сложности управляющих систем. С другой стороны, некоторые из полученных результатов могут быть использованы на практике при решении задачи перехода описания функционирования автомата с языка диаграмм или таблиц на язык схем.

Апробация. Основные результаты диссертации докладывались на семинарах и всероссийских и международных конференциях, включая:

- научный семинар «Теория автоматов» под руководством профессора В.Б. Кудрявцева, механико-математический факультет МГУ имени М.В. Ломоносова, 2016 г.;

- научный семинар «Теория дискретных функций и приложения» под руководством профессора Д.Н. Бабина, старшего научного сотрудника И.Л. Мазуренко механико-математический факультет МГУ имени М.В. Ломоносова, 2016 г.;

- научный семинар «Дискретная математика и математическая кибернетика» под руководством профессора В.Б. Алексеева, профессора А.А. Сапоженко, профессора С.А. Ложкина факультет ВМиК МГУ имени М.В. Ломоносова, 2016 г.;

- семинар «Дискретный анализ» под руководством профессора С.В. Алёшина, профессора В.А. Буевича, старшего научного сотрудника М.В. Носова, механико-математический факультет МГУ имени М.В. Ломоносова, 2014 г.;

- семинар «Компьютерная безопасность» под руководством старшего научного сотрудника А.В. Галатенко, механико-математический факультет МГУ имени М.В. Ломоносова, 2015 г.;

- научный семинар «Нейронные сети» под руководством профессора А.А. Часовских, научного сотрудника В.С. Половникова, старшего научного сотрудника А.А. Говорко механико-математический факультет МГУ имени М.В. Ломоносова, 2016 г.;

- XI международная конференция «Интеллектуальные системы и компьютерные науки», МГУ имени М.В. Ломоносова, 28 ноября - 2 декабря 2016 г.;

- Двенадцатый Международный научный семинар «Дискретная математика и ее приложения» имени академика О. Б. Лупанова, МГУ имени М.В. Ломоносова, 20-25 июня 2016 г.;

- Десятый международный научный семинар «Дискретная математика и ее приложения», МГУ имени М.В. Ломоносова, 1-5 февраля 2010 г.;

- Международная конференция «Современные проблемы математики, механики и их приложений», посвященная 70-летию ректора МГУ акад. В. А. Садовничего, МГУ имени М.В. Ломоносова, 1-5 мая 2009 г.;

- VII Международный семинар «Дискретная математика и ее приложения», МГУ имени М.В. Ломоносова, 9 января-2 февраля 2001 г.

Публикации. Основные результаты диссертации опубликованы в 4 печатных работах автора [28—31], из них 3 [28—30] в научных журналах из списка, рекомендованного ВАК РФ.

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения, списка литературы из 31 наименований. Общий объем диссертации составляет 108 страниц.

Краткое содержание диссертации

Во **введении** описаны структура диссертации и история рассматриваемых в ней вопросов. Обосновываются актуальность темы и научная новизна полученных результатов. Описаны основные результаты диссертации.

В **главе 1** сформулирована задача, решение которой представлено в настоящей диссертации.

В **главе 2** изучается сложность реализации автоматов, мощность множества состояний которых есть степень 2, посредством неизбыточных кодирований. Основным вопросом изучения является линейная реализуемость автомата. Так как каждый входной символ автомата порождает отображение на множестве состояний [5], в разделе 2.1 изучаются линейно реализуемые отображения. Приведен критерий линейной реализуемости отображения, а также приведены верхняя и нижняя оценка числа линейно реализуемых отображений. В разделе 2.2 сформулирован критерий линейной реализуемости переходной системы, а также верхняя и нижняя оценки числа линейно реализуемых переходных систем. В разделе 2.3 приведен критерий линейной реализуемости автомата, а также верхняя и нижняя оценки числа линейно реализуемых автоматов.

В **главе 3** изучается сложность реализации автоматов посредством всевозможных однородных кодирований состояний автомата. В разделе 3.1 доказано, что все отображения на множестве состояний являются линейно реализуемыми. В разделе 3.2 приведена оценка сложности реализации переходных систем, а также доказано, что вопрос линейной реализуемости переходной системы является алгоритмически разрешимым.

В **главе 4** изучаются максимально реализуемые автоматы, т.е. такие автоматы, что два различных неизбыточных кодирования состояний автомата порождают различные операторы. В разделе 4.1 приведен критерий максимальной реализуемости в терминах порождающих внутренней полугруппы. В разделе 4.2 устанавливается как связаны классы линейно реализуемых и максимально реализуемых автоматов.

В **заключении** представлены основные результаты диссертации.

Благодарности

Автор выражает глубокую благодарность своему научному руководителю — профессору Станиславу Владимировичу Алёшину за постановку задачи, обсуждение результатов и постоянное внимание к работе. Автор

благодарен всем сотрудникам кафедры Математической теории интеллектуальных систем Механико-математического факультета МГУ, в особенности заведующему кафедрой профессору Валерию Борисовичу Кудрявцеву, за поддержку работы и творческую атмосферу на кафедре.

Глава 1

Постановка задачи

С формальной точки зрения автомат — это пятерка $\mathfrak{A} = (A, Q, B, \varphi, \psi)$, где A — входной алфавит, Q — алфавит состояний, B — выходной алфавит, φ — функция, которая по текущему входу и состоянию определяет состояние автомата в следующий момент времени, ψ — выходная функция, которая по текущему входу и состоянию определяет выход автомата в текущий момент времени. Кодирование алфавита состояний — это отображение алфавита Q в E_2^k, при котором каждому состоянию из Q ставится в соответствие вектор из E_2^k. Кодирование входного алфавита — это отображение алфавита A в E_2^p, при котором каждому элементу из A ставится в соответствие вектор из E_2^p. Кодирование выходного алфавита — это отображение алфавита B в E_2^l, при котором каждому элементу из B ставится в соответствие вектор из E_2^l. Кодирования алфавита состояния, входного алфавита и выходного алфавита порождают булев оператор $\phi : E_2^{k+p} \to E_2^{k+l}$, где p — длина кодового набора для символов множества A, k — длина кодового набора для символов множества Q, l — длина кодового набора для символов множества B.

Оператор ϕ можно рассматривать как набор $k + l$ булевых функций от $k + p$ переменных. При этом важно выбрать кодирование, при котором достигается возможно меньшая сложность схемы.

Сложность такого оператора можно определить как максимальную сложность получающихся булевых функций. Как известно [10], каждой бу-

левой функции единственным образом соответствует полином Жегалкина. Мы будем понимать сложность оператора как максимальную из сложностей полиномов Жегалкина функций, задающих этот оператор, т.е. как максимальную степень полиномов, а сложность автомата — как сложность оператора ϕ. Таким образом, установив связь между автоматом, кодированием и возникающими полиномами, можно найти минимальную сложность реализации автомата. С теоретической точки зрения выбор базиса реализации булевой функции не принципиален, так как сложность реализации функции в разных базисах эквивалентна с точностью до константы [11]. С практической точки зрения при реализации автоматов схемами используются функциональные элементы из некоторого набора, называемого библиотекой. Эти библиотеки могут содержать функции многих переменных, операторы, структурные автоматы. В качестве элементов такой библиотеки могут быть взяты «просто» реализуемые автоматы с точки зрения сложности полиномов Жегалкина.

Одной из основных задач работы было изучение автоматов, у которых существует такое кодирование, что получаемые при данном кодировании, булевы функции являются линейными, т.е. вопрос является ли автомат изоморфным линейному автомату.

С другой стороны интерес представляют максимально реализуемые автоматы, т.е. такие автоматы, что все операторы, задаваемые всевозможными кодированиями, являются различными. Данное свойство называется свойством максимальности. В данном случае для нахождения «простейшего» оператора необходимо перебрать всевозможные кодирования.

В работе изучаются автоматы с входным алфавитом $A = E_2$ и выходным алфавитом $B = E_2$. Обозначим через P_n множество всех отображений множества $E_n = \{0, \ldots, n-1\}$ в себя, не обязательно взаимно-однозначных. Данное множество образует полугруппу преобразований множества E_n относительно операции суперпозиции отображений. Взаимно-однозначные преобразования множества E_n образуют группу подстановок на этом множестве [12].

Сформулируем центральную задачу, решаемую в данной диссертации.

Задача: Пусть задан автомат $\mathfrak{A} = (E_2, Q, E_2, \varphi, \psi)$. Найти минимальную сложность реализации автомата $\mathfrak{A}$ при всевозможных кодированиях алфавита Q. Найти критерий линейной реализуемости автомата $\mathfrak{A}$. Найти критерий максимальной реализуемости автомата $\mathfrak{A}$. Установить как связаны класс линейно реализуемых автоматов и максимально реализуемых автоматов.

Глава 2

Неизбыточные кодирования

В данной главе изучаются автоматы с числом состояний $n = 2^k$.

2.1 Линейно реализуемые элементы полугруппы P_n

В данном разделе изучается вопрос о линейной реализуемости преобразований множества $E_n = \{0, \ldots, n-1\}$.

Прежде чем перейти к вопросу линейной реализуемости, введем несколько общих определений.

Определение 1. *Кодированием множества* $E_n = \{0, \ldots, n-1\}$ назовем взаимно-однозначное отображение (вложение) $F : \{0, \ldots, n-1\} \to E_2^m$, где $m \geq]\log_2^n[$.

В данной главе рассматриваются кодирования $F : \{0, \ldots, n-1\} \to E_2^m$, где $m =]\log_2^n[$, или $m = k$ с учетом равенства $n = 2^k$.

Определение 2. Пусть $\phi : E_2^m \to E_2^k$ — булев оператор. Его можно рассматривать как набор k булевых функций, зависящих от m переменных, а именно, если $\phi(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) = (\beta_0, \beta_1, \ldots, \beta_{k-1})$, то $f_j(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) = \beta_j$, где $0 \leq j \leq k-1$. Обозначим этот набор че-

рез $\mathcal{F}_\phi = \{f_0, f_1, \ldots, f_{k-1}\}$.

Определение 3. Пусть $\mathcal{F} = \{f_0, f_1, \ldots, f_{k-1}\}$ — набор булевых функций, зависящих от m переменных. Данный набор определяет булев оператор $\phi_\mathcal{F} : E_2^m \to E_2^k$ по правилу

$$\begin{aligned}\phi_\mathcal{F}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) =&(f_0(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}), f_1(\alpha_0, \alpha_1, \ldots, \alpha_{m-1}),\\ &\ldots\\ &f_{k-1}(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})),\end{aligned}$$

где $\alpha_i \in E_2$.

Определение 4. Пусть $\phi : E_2^m \to E_2^k$ — булев оператор. *Сложностью оператора* назовем максимальную степень полиномов Жегалкина функций $\mathcal{F}_\phi$ или $L_{deg}(\phi) = max\{deg_{f_i \in \mathcal{F}_\phi} f_i\}$

Пример 1. В качестве примера кодирования можно рассмотреть следующее отображение E_8 в E_2^3:

q	0	1	2	3	4	5	6	7
$F_0(q)$	000	001	010	011	100	101	110	111

Определение 5. Пусть $s : E_n \to E_n$ — отображение множества $E_n = \{0, \ldots, n-1\}$ в себя. Кодирование F множества E_n сопоставляет отображению s булев оператор ϕ_s по правилу

$$\phi_s(\alpha_0, \ldots, \alpha_{k-1}) = F(s(F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))),$$

где $\alpha_0, \ldots, \alpha_{k-1} \in E_2$, $k = \log_2 n$. Этот оператор можно рассматривать как набор k булевых функций, зависящих от k переменных. Обозначим этот набор через $\mathcal{F}_s(F)$.

Пример 2. Пусть задана подстановка

$$p = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 7 \end{pmatrix}.$$

Тогда кодирование F_0 из примера 1 сопоставляет подстановке p следующий булев оператор

q_0	q_1	q_2	f_0	f_1	f_2
0	0	0	0	0	1
0	0	1	0	1	0
0	1	0	0	1	1
0	1	1	1	0	0
1	0	0	1	0	1
1	0	1	1	1	0
1	1	0	0	0	0
1	1	1	1	1	1

А множество булевых функций есть

$$\mathcal{F}_s(F) = \{f_0(q_0, q_1, q_2) = q_1 \cdot q_2 + q_0,$$

$$f_1(q_0, q_1, q_2) = q_2 + q_1 + q_0 \cdot q_1,$$

$$f_2(q_0, q_1, q_2) = 1 + q_2 + q_1 + q_0 \cdot q_2 + q_0 \cdot q_1 \cdot q_2\}.$$

Определение 6. Отображение $s : E_n \to E_n$ называется *линейно реализуемым* посредством кодирования F, если набор $\mathcal{F}_s(F)$ состоит из линейных булевых функций.

Пример 3. Подстановка из примера 2

$$p = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 7 \end{pmatrix}.$$

является линейно реализуемой.

Кодирование F

q	0	1	2	3	4	5	6	7
$F(q)$	001	010	100	011	110	111	101	000

сопоставляет подстановке p булев оператор

q_0	q_1	q_2	f_0	f_1	f_2
0	0	0	0	0	0
0	0	1	0	1	0
0	1	0	1	0	0
0	1	1	1	1	0
1	0	0	0	1	1
1	0	1	0	0	1
1	1	0	1	1	1
1	1	1	1	0	1

Множество булевых функций есть

$$\mathcal{F}_s(F) = \{f_0(q_0, q_1, q_2) = q_1, f_1(q_0, q_1, q_2) = q_0 + q_2, f_2(q_0, q_1, q_2) = q_0\}.$$

Выделим из всех кодирований «стандартное» кодирование.

Определение 7. Кодирование $F_0 : \{0, \ldots, n-1\} \to E_2^k$ назовем *стандартным*, если код элемента есть его двоичное представление.

Примером стандартного кодирования на множестве E_8 является кодирование из примера 1.

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

Пример 4. Рассмотрим кодирование F из примера 3

q	0	1	2	3	4	5	6	7
$F(q)$	001	010	100	011	110	111	101	000

Подстановка s_F имеет вид

$$s_F = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 3 & 6 & 7 & 5 & 0 \end{pmatrix}.$$

Введем несколько обозначений.

Если $n = 2^k$, то отображения множества $E_n = \{0, \ldots, n-1\}$ в себя могут быть представлены как многочлены над полем Галуа F_n [10].

Обозначим через $H_+ \subset P_n$ множество подстановок, соответствующих многочленам вида $x + c$ над полем Галуа F_n, где $c \in E_n$ — константа.

Обозначим через $H_* \subset P_n$ множество подстановок, соответствующих многочленам вида $c \cdot x$ над полем Галуа F_n, где $c \in E_n$ — константа.

Пример 5. Приведем пример множеств H_+ и H_* для $n = 8$, где F_8 есть расширение поля F_2 с помощью многочлена $x^3 + x + 1$. Обозначим отображение, соответствующее многочлену f над полем Галуа, через h_f.

$$H_+ = \{h_x = e, h_{x+1} = (0\,1)(2\,3)(4\,5)(6\,7), h_{x+2} = (0\,2)(1\,3)(4\,6)(5\,7),$$

$$h_{x+3} = (0\,3)(1\,2)(4\,7)(5\,6), h_{x+4} = (0\,4)(1\,5)(2\,6)(3\,7), h_{x+5} = (0\,5)(1\,4)(2\,7)(3\,6),$$

$$h_{x+6} = (0\,6)(1\,7)(2\,4)(3\,5), h_{x+7} = (0\,7)(1\,6)(2\,5)(3\,4)\},$$

$$H_* = \left\{ h_{0\cdot x} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, h_x = e, h_{2\cdot x} = (1\,2\,4\,3\,6\,7\,5),\right.$$

$$h_{3\cdot x} = (1\,3\,5\,4\,7\,2\,6), h_{4\cdot x} = (1\,4\,6\,5\,2\,3\,7), h_{5\cdot x} = (1\,5\,7\,6\,3\,4\,2),$$

$$\left. h_{6\cdot x} = (1\,6\,2\,7\,4\,5\,3), h_{7\cdot x} = (1\,7\,3\,2\,5\,6\,4) \right\}.$$

Пусть $H_L = \{s \in P_n : \forall h \in H_+ \, \exists h' \in H_+, \, hs = sh'\}$.

Замечание 1. Порядок умножения отображений «слева направо»: если заданы отображения p_1 и p_2, то значение их произведения на элементе i определяется равенством $(p_1 \cdot p_2)(i) = p_2(p_1(i))$.

Определение 8. Пусть заданы булев оператор $\phi(\alpha_0, \ldots, \alpha_{k-1}) = (\beta_0, \ldots, \beta_{k-1})$, где $\alpha_i, \beta_i \in E_2$, $k = \log_2 n$, и кодирование F. Определим отображение множества E_n в себя правилом $s_\phi^F(q) = F^{-1}(\phi(F(q)))$, $q \in E_n$.

Лемма 1. *Пусть задан булев оператор $\phi(\alpha_0, \ldots, \alpha_{k-1}) = (\beta_0, \ldots, \beta_{k-1})$, где $\alpha_i, \beta_i \in E_2$, $k = \log_2 n$. Оператор $\phi_{s_\phi^F}$, который сопоставляется кодированием F отображению s_ϕ^F, равен оператору ϕ .*

Доказательство. Согласно определению 5

$$\phi_{s_\phi^F}(\alpha_0, \ldots, \alpha_{k-1}) = F(s_\phi^F(F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))) \quad \forall(\alpha_0, \ldots, \alpha_{k-1}),$$

где $\alpha_i \in \{0, 1\}$. Согласно определению 8 отображения, определяемого по

оператору,

$$F(s_\phi^F(F^{-1}(\alpha_0,\ldots,\alpha_{k-1}))) = F(F^{-1}(\phi(F(F^{-1}(\alpha_0,\ldots,\alpha_{k-1}))))) =$$

$$= \phi(\alpha_0,\ldots,\alpha_{k-1}).$$

Следовательно,

$$\phi_{s_\phi^F}(\alpha_0,\ldots,\alpha_{k-1}) = \phi(\alpha_0,\ldots,\alpha_{k-1}) \quad \forall(\alpha_0,\ldots,\alpha_{k-1}),$$

где $\alpha_i \in \{0,1\}$. □

Лемма 2. *Число различных отображений множества* $Q = \{0,1,\ldots,n-1\}$ *в себя, где* $n = 2^k$*, линейно реализуемых посредством кодирования* F_0*, равно* $n^{\log_2(n)+1} = 2^{k(k+1)}$.

Доказательство. Пусть задано отображение n-элементного множества в себя, линейно реализуемое посредством стандартного кодирования F_0. Обозначим $k = \log_2 n$. Данное кодирование порождает булев оператор $\phi_s : E_2^k \to E_2^k$. Рассмотрим этот оператор как набор $\mathcal{F}_s(F_0)$.

Поскольку отображение линейно реализуемо, то элементы $\mathcal{F}_s(F_0)$ есть линейные булевы функции от k переменных, а именно $\mathcal{F}_s(F_0) = \{f_0,\ldots,f_{k-1}\}$, где $k = \log_2 n$. Как известно, число различных линейных булевых функций зависящих от k переменных, равно 2^{k+1} [10]. 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 соответствуют два различных отображения, линейно реализуемых посредством стандартного кодирования F_0. Пусть заданы два различных набора $\mathcal{F}_1$ и $\mathcal{F}_2$. Поскольку они различны, найдутся такие две различные функции $f_i^1 \in \mathcal{F}_1$ и $f_i^2 \in \mathcal{F}_2$ и набор $\alpha_0,\ldots,\alpha_{k-1}$, где $\alpha_i \in E_2$, что $f_i^1(\alpha_0,\ldots,\alpha_{k-1}) \neq f_i^2(\alpha_0,\ldots,\alpha_{k-1})$. Следовательно, операторы, соответствующие первому и второму наборам, не равны на наборе $\alpha_0,\ldots,\alpha_{k-1}$. Обозначим булев оператор, соответствующий первому набору, через ϕ_1, а второму — через ϕ_2, $\phi_1(\alpha_0,\ldots,\alpha_{k-1}) \neq \phi_2(\alpha_0,\ldots,\alpha_{k-1})$. Пусть $q = F_0(\alpha_0,\ldots,\alpha_{k-1})$. Тогда согласно построению отображения по булеву оператору $s_{\phi_1}(q) = F_0^{-1}(\phi_1(\alpha_0,\ldots,\alpha_{k-1}))$, а $s_{\phi_2}(q) =$

$F_0^{-1}(\phi_2(\alpha_0, \ldots, \alpha_{k-1}))$. Поскольку по определению кодирования отображение F_0 взаимно-однозначное, то $s_{\phi_1}(q) \neq s_{\phi_2}(q)$. □

Лемма 3. *Пусть задано отображение s множества $Q = \{0, 1, \ldots, n-1\}$ в себя, где $n = 2^k$. Булев оператор, сопоставляемый кодированием F отображению s, совпадает с булевым оператором, который кодирование F_0 сопоставляет отображению $s_F^{-1} \cdot s \cdot s_F$.*

Доказательство. Пусть задано кодирование $F : \{0, \ldots, n-1\} \to E_2^k$. Тогда соответствующий булев оператор определяется равенством

$$\phi_s(\alpha_0, \ldots, \alpha_{k-1}) = F(s(F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))),$$

где $\alpha_0, \ldots, \alpha_{k-1} \in E_2$, $k = \log_2 n$. Можно видеть, что булев оператор, сопоставляемый кодированием F_0 отображению $s_F^{-1} \cdot s \cdot s_F$, определяется правилом

$$\phi_{s_F}(\alpha_0, \ldots, \alpha_{k-1}) = F_0(s_F(s(s_F^{-1}(F_0^{-1}(\alpha_0, \ldots, \alpha_{k-1}))))).$$

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

$$\phi_{s_F}(\alpha_0, \ldots, \alpha_{k-1}) = F_0(F_0^{-1}(F(s(F^{-1}(F_0(F_0^{-1}(\alpha_0, \ldots, \alpha_{k-1}))))))) =$$

$$= F(s(F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))).$$

□

Пример 6. Рассмотрим подстановку

$$p = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 7 \end{pmatrix}$$

и кодирование

q	0	1	2	3	4	5	6	7
$F(q)$	001	010	100	011	110	111	101	000

Как было показано в примере 4

$$s_F = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 3 & 6 & 7 & 5 & 0 \end{pmatrix}$$

Тогда $s_F^{-1} \cdot s \cdot s_F = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 2 & 4 & 6 & 3 & 1 & 7 & 5 \end{pmatrix}$.

Стандартное кодирование F_0 сопоставляет подстановке $s_F^{-1} \cdot s \cdot s_F$ оператор

q_0	q_1	q_2	f_0	f_1	f_2
0	0	0	0	0	0
0	0	1	0	1	0
0	1	0	1	0	0
0	1	1	1	1	0
1	0	0	0	1	1
1	0	1	0	0	1
1	1	0	1	1	1
1	1	1	1	0	1

.

Как видно из примера 3 данный оператор совпадает с булевым оператором, сопоставляемым кодированием F подстановке p.

Лемма 4. *Отображение s линейно реализуемо 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 $c \in F_{2^k}$.*

Доказательство. Сначала докажем, что всякое отображение, у которого соответствующий ему многочлен над полем Галуа имеет указанный вид, является линейно реализуемым посредством стандартного кодирования F_0. Поле F_{2^k} — это расширение поля F_2, образующим элементом которого является корень неприводимого над F_2 многочлена степени k. Обозначим его через f. Его элементы можно рассматривать как формальные многочлены

$$q_{k-1} \cdot x^{k-1} + q_{k-2} \cdot x^{k-2} + \ldots + q_0, \tag{2.1}$$

см. [13]. При этом данный многочлен соответствует элементу $q \in Q$, стандартный код которого равен $(q_0, q_1, \ldots, q_{k-1})$.

Пусть многочлен, соответствующий отображению 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 (2.1) по модулю многочлена f. Также заметим, что $(f_1 + f_2)^{2^i} = (f_1)^{2^i} + (f_2)^{2^i}$ для $f_1, f_2 \in F_{2^k}$. Обозначим через g_c многочлен вида (2.1) соответствующий элементу $c \in F_{2^k}$. Тогда

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

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

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

$$\ldots$$

$$+ \sum_{i=1}^{k} g_{c_i} \cdot (q_0)^{2^{i-1}} =$$

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

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

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

Результат умножения многочленов g_{c_i} на многочлен $x^{(k-j)\cdot 2^{i-1}}$, где $1 \le i \le k$, $1 \le j \le k$, есть опять многочлены вида (2.1)

$$b_{k-1}^{g_{c_i}, x^{(k-j)\cdot 2^{i-1}}} \cdot x^{k-1} + b_{k-2}^{g_{c_i}, x^{(k-j)\cdot 2^{i-1}}} \cdot x^{k-2} + \ldots + b_0^{g_{c_i}, x^{(k-j)\cdot 2^{i-1}}}.$$

Сгруппируем эту сумму по степеням x^l, где $0 \leq l \leq k-1$. Коэффициент при каждой степени есть линейная комбинация q_l, где $0 \leq l \leq k-1$. Коэффициент при степени x^l есть значение l-й функции из множества $\mathcal{F}_s(F_0)$. А следовательно, данная функция является линейной булевой функцией переменных $q_0, \ldots, q_{k-1}$. Таким образом, показано, что всякое отображение, у которого соответствующий многочлен над полем Галуа — это линейная комбинация многочленов вида x^{2^i}, где $i = 0, \ldots, k-1$, и константы $c \in F_{2^k}$, является линейно реализуемым посредством кодирования F_0. Согласно лемме 2 число различных отображений на n-элементном множестве, линейно реализуемых посредством кодирования F_0, равно $n^{\log_2(n)+1}$. В силу однозначности и единственности многочлена над полем Галуа, соответствующего данному отображению, получаем, что для отображений, линейно реализуемых посредством кодирования F_0, соответствующий многочлен имеет указанный вид. Утверждение доказано. □

Как видно из примера 4 подстановка

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 2 & 4 & 6 & 3 & 1 & 7 & 5 \end{pmatrix}$$

линейно реализуема. Соответствующий ей многочлен над полем F_8 есть $2 \cdot x$.

Следствие 1. *Подстановки $h_c^+ \in H_+$ линейно реализуемы посредством кодирования F_0 и $\mathcal{F}_{h_c^+}(F_0) = \{x_0 + c_0, x_1 + c_1, \ldots, x_{k-1} + c_{k-1}\}$, $(c_0, c_1, \ldots, c_{k-1}) = F_0(c)$.*

Лемма 5. *Пусть заданы отображения p_1, p_2 множества E_n в себя и кодирование F. Тогда $\phi^F_{p_1 \cdot p_2} = \phi^F_{p_2}(\phi^F_{p_1})$.*

Доказательство. Согласно определению 5

$$\phi^F_{p_1 \cdot p_2}(\alpha_0, \ldots, \alpha_{k-1}) = F(p_1 \cdot p_2(F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))) \quad \forall(\alpha_0, \ldots, \alpha_{k-1}),$$

где $\alpha_i \in E_2, k = \log_2 n$, поэтому

$$F(p_1 \cdot p_2(F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))) = F(p_2(p_1(F^{-1}(\alpha_0, \ldots, \alpha_{k-1})))) =$$

$$= F(p_2(p_1(F^{-1}(\alpha_0, \ldots, \alpha_{k-1})))) = F(p_2(F^{-1}(F(p_1(F^{-1}(\alpha_0, \ldots, \alpha_{k-1})))))) =$$

$$= \phi^F_{p_2}(\phi^F_{p_1}(\alpha_0, \ldots, \alpha_{k-1})) \quad \forall(\alpha_0, \ldots, \alpha_{k-1}).$$

Лемма доказана. □

Следствие 2. *Пусть заданы отображения p_1, p_2 множества E_n в себя и кодирование F. Если*

$$\mathcal{F}_{p_1}(F) = \{f_0(x_0, x_1, \ldots, x_{k-1}), f_1(x_0, x_1, \ldots, x_{k-1}), \ldots, f_{k-1}(x_0, x_1, \ldots, x_{k-1})\}$$

и

$$\mathcal{F}_{p_2}(F) = \{h_0(x_0, x_1, \ldots, x_{k-1}), h_1(x_0, x_1, \ldots, x_{k-1}), \ldots, h_{k-1}(x_0, x_1, \ldots, x_{k-1})\},$$

то

$$\mathcal{F}_{p_1 \cdot p_2}(F) = \{h_0(f_0(x_0, x_1, \ldots, x_{k-1}), f_1(x_0, x_1, \ldots, x_{k-1}),$$

$$\ldots$$

$$f_{k-1}(x_0, x_1, \ldots, x_{k-1})),$$

$$h_1(f_0(x_0, x_1, \ldots, x_{k-1}), f_1(x_0, x_1, \ldots, x_{k-1}), \ldots, f_{k-1}(x_0, x_1, \ldots, x_{k-1})),$$

$$\ldots$$

$$h_{k-1}(f_0(x_0, x_1, \ldots, x_{k-1}), f_1(x_0, x_1, \ldots, x_{k-1}), \ldots, f_{k-1}(x_0, x_1, \ldots, x_{k-1}))\}.$$

Доказательство. Обозначим

$$\mathcal{F}_{p_1 \cdot p_2}(F) = \{g_0(x_0, x_1, \ldots, x_{k-1}), g_1(x_0, x_1, \ldots, x_{k-1}),$$

$$\ldots$$

$$g_{k-1}(x_0, x_1, \ldots, x_{k-1})\}.$$

Согласно лемме 5 верно равенство $\phi^F_{p_1 \cdot p_2} = \phi^F_{p_2}(\phi^F_{p_1})$. Следовательно, для любого набора $(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$, где $\alpha_i \in E_2$,

$$(g_0(\alpha_0, \alpha_1, \ldots, \alpha_{k-1}), g_1(\alpha_0, \alpha_1, \ldots, \alpha_{k-1}), \ldots, g_{k-1}(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})) =$$

$$= F(p_1 \cdot p_2(F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))) = \phi^F_{p_2}(\phi^F_{p_1}(\alpha_0, \ldots, \alpha_{k-1})) =$$

$$= (h_0(\phi^F_{p_1}(\alpha_0, \ldots, \alpha_{k-1})), h_1(\phi^F_{p_1}(\alpha_0, \ldots, \alpha_{k-1})), \ldots, h_{k-1}(\phi^F_{p_1}(\alpha_0, \ldots, \alpha_{k-1})) =$$

$$= (h_0(f_0(\alpha_0, \alpha_1, \ldots, \alpha_{k-1}), f_1(\alpha_0, \alpha_1, \ldots, \alpha_{k-1}), \ldots, f_{k-1}(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})),$$

$$h_1(f_0(\alpha_0, \alpha_1, \ldots, \alpha_{k-1}), f_1(\alpha_0, \alpha_1, \ldots, \alpha_{k-1}), \ldots, f_{k-1}(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})),$$

$$\ldots$$

$$h_{k-1}(f_0(\alpha_0, \alpha_1, \ldots, \alpha_{k-1}), f_1(\alpha_0, \alpha_1, \ldots, \alpha_{k-1}), \ldots, f_{k-1}(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})).$$

□

Лемма 6. *Отображение p линейно реализуемо посредством кодирования F тогда и только тогда, когда $H^{s_F}_+ p \subset p H^{s_F}_+$.*

Доказательство. Сначала докажем утверждение для случая линейной реализуемости отображения посредством кодирования F_0. Заметим, что s_{F_0} — тождественная подстановка.

Пусть p линейно реализуема посредством F_0. Согласно лемме 4 соответствующий ей многочлен над полем Галуа F_{2^k} является линейной комбинацией многочленов вида x^{2^i}, где $i = 0, .., k-1$, и константы $c \in F_{2^k}$. Пусть соответствующий многочлен имеет вид $f_p(x) = c_0 + \sum_{i=1}^{k} c_i \cdot x^{2^{i-1}}$.

Согласно определению H_+ — множество подстановок, соответствующих многочленам $x+c$ над полем Галуа F_n, где $c \in E_{2^k}$ — константа. Без ограничения общности рассмотрим подстановку h_c, соответствующую многочлену $x + c$.

Тогда

$$h \cdot p(q) = c_0 + \sum_{i=1}^{k} c_i \cdot (q + c)^{2^{i-1}} \quad \forall q \in E_{2^k}.$$

Так как $(a + b)^{2^j} = a^{2^j} + b^{2^j}$ [13], то

$$h_c \cdot p(q) = c_0 + \sum_{i=1}^{k} c_i \cdot (q + c)^{2^{i-1}} = c_0 + \sum_{i=1}^{k} c_i \cdot q^{2^{i-1}} + \sum_{i=1}^{k} c_i \cdot c^{2^{i-1}}.$$

Обозначим $\sum_{i=1}^{k} c_i \cdot c^{2^{i-1}}$ через c'. Можно заметить, что $c' = p(c) + p(0)$.

$$h_c \cdot p(q) = c_0 + \sum_{i=1}^{k} c_i \cdot (q+c)^{2^{i-1}} = p(q) + c' = p \cdot h_{c'}(q) \quad \forall q \in E_{2^k}.$$

Так как данное равенство верно для любого q и c' и не зависит от q, то $h_c \cdot p = p \cdot h_{c'}$. Следовательно, для каждого $c \in E_{2^k}$ существует такое c', что $h_c \cdot p = p \cdot h_{c'}$. Отсюда следует, что $H_+ p \subset pH_+$.

Докажем обратное утверждение. Пусть $H_+ p \subset pH_+$, т. е. для каждого $c \in E_{2^k}$ существует такое c', что $h_c \cdot p = p \cdot h_{c'}$. Предположим, что отображение p не является линейно реализуемым. Тогда среди функций $\mathcal{F}_p(F_0)$ найдется нелинейная функция f. Согласно следствию 1 и следствию 2

$$f(x_0 + c_0, x_1 + c_1, \ldots, x_{k-1} + c_{k-1}) = f(x_0, x_1, \ldots, x_{k-1}) + d,$$

где $c_0, c_1, \ldots, c_{k-1}, d \in E_2$. Поскольку функция f нелинейная, в ее полиноме Жегалкина найдется член, являющийся произведением не менее двух сомножителей. Без ограничения общности считаем, что среди этих множителей присутствуют x_0 и x_1. Тогда полином можно преобразовать следующим образом:

$$f(x_0, x_1, \ldots, x_{k-1}) = x_0 \cdot x_1 \cdot f_1(x_2, x_3, \ldots, x_{k-1}) + x_0 \cdot f_2(x_2, x_3, \ldots, x_{k-1}) +$$

$$+ x_1 \cdot f_3(x_2, x_3, \ldots, x_{k-1}) + f_4(x_2, x_3, \ldots, x_{k-1});$$

в силу единственности полинома $f_1(x_2, x_3, \ldots, x_{k-1}) \not\equiv 0$. Значит, найдется такой набор $\alpha_2, \alpha_3, \ldots, \alpha_{k-1}$, что $f_1(\alpha_2, \alpha_3, \ldots, \alpha_{k-1}) = 1$. Пусть $f_2(\alpha_2, \alpha_3, \ldots, \alpha_{k-1}) = \alpha$, $f_3(\alpha_2, \alpha_3, \ldots, \alpha_{k-1}) = \beta$, $f_4(\alpha_2, \alpha_3, \ldots, \alpha_{k-1}) = \gamma$ и $g(x_0, x_1) = f(x_0, x_1, \alpha_2, \ldots, \alpha_{k-1}) = x_0 \cdot x_1 + \alpha \cdot x_0 + \beta \cdot x_1 + \gamma$. Заметим, что для любых α_0, α_1 существует такое d, что $g(x_0 + \alpha_0, x_1 + \alpha_1) = g(x_0, x_1) + d$. Предположим, что либо α, либо β не равно 0. Значит, для β, α существует такое d, что $g(x_0 + \beta, x_1 + \alpha) = g(x_0, x_1) + d$. Тогда

$$g(x_0+\beta, x_1+\alpha) = (x_0+\beta)\cdot(x_1+\alpha)+\alpha\cdot(x_0+\beta)+\beta\cdot(x_1+\alpha)+\gamma = x_0\cdot x_1+\alpha\cdot\beta+\gamma,$$

$$g(x_0, x_1) + d = x_0 \cdot x_1 + \alpha \cdot x_0 + \beta \cdot x_1 + \gamma + d.$$

Из равенства $g(x_0 + \beta, x_1 + \alpha) = g(x_0, x_1) + d$ следует, что

$$\alpha \cdot \beta + \gamma = \alpha \cdot x_0 + \beta \cdot x_1 + \gamma + d.$$

Данное равенство означает, что $\alpha = \beta = 0$. Поэтому $g(x_0, x_1) = x_0 \cdot x_1 + \gamma$.

Для набора $(1, 0)$ существует такое d, что $g(x_0 + 1, x_1) = g(x_0, x_1) + d$. Следовательно,

$$g(x_0+1, x_1) = (x_0+1) \cdot x_1 + \gamma = x_0 \cdot x_1 + x_1 + \gamma = g(x_0, x_1) + d = x_0 \cdot x_1 + \gamma.$$

Равенство верно, если $x_1 \equiv 0$. Мы пришли к противоречию. Значит, функция f линейна.

Докажем утверждение в общем случае. Согласно лемме 3 булев оператор, который кодирование F сопоставляет отображению p, совпадает с булевым оператором, который кодирование F_0 сопоставляет отображению $s_F^{-1} \cdot p \cdot s_F$. Отображение $s_F^{-1} \cdot p \cdot s_F$ линейно реализуемо посредством кодирования F_0 тогда и только тогда, когда $H_+ s_F^{-1} \cdot p \cdot s_F \subset s_F^{-1} \cdot p \cdot s_F H_+$. Следовательно, для каждого $c \in E_{2^k}$ существует такое c', что $h_c \cdot s_F^{-1} \cdot p \cdot s_F = s_F^{-1} \cdot p \cdot s_F \cdot h_{c'}$; тогда

$$s_F \cdot h_c \cdot s_F^{-1} \cdot p \cdot s_F = p \cdot s_F \cdot h_{c'},$$

$$s_F \cdot h_c \cdot s_F^{-1} \cdot p = p \cdot s_F \cdot h_{c'} \cdot s_F^{-1}.$$

Заметим, что $s_F \cdot h_c \cdot s_F^{-1}, s_F \cdot h_{c'} \cdot s_F^{-1} \in H_+^{s_F}$. Так как подстановка s_F задает изоморфное отображение H_+ на $H_+^{s_F}$, то $H_+^{s_F} p \subset p H_+^{s_F}$. □

Лемма 7. *Пусть задано отображение p множества $Q = \{0, 1, \ldots, n-1\}$ в себя, где $n = 2^k$. Тогда $p = c \cdot h$, где $c(0) = 0$, $h \in H_+$.*

Доказательство. Так как $n = 2^k$, то отображение p можно представить как многочлен f_p над полем Галуа F_{2^k} [10], т. е. $f_p(q) = p(q)$ при любом $q \in Q = \{0, \ldots, n-1\}$. В общем виде многочлен имеет вид $f_p = \sum_{i=1}^{n-1} a_i \cdot x^i + a_0$, где $a_i \in Q$. Обозначим через c отображение, соответствующее многочлену $\sum_{i=1}^{n-1} a_i \cdot x^i$, а через h — подстановку соответствующую многочлену $x + a_0$.

Покажем, что $p = c \cdot h$. Действительно, при любом $q \in Q$

$$p(q) = f_p(q) = \sum_{i=1}^{n-1} a_i \cdot q^i + a_0,$$

$$c \cdot h(q) = h(c(q)) = \sum_{i=1}^{n-1} a_i \cdot q^i + a_0.$$

Отсюда следует, что $p(q) = c \cdot h(q)$ при любом $q \in Q$. □

Лемма 8. *Число различных линейно реализуемых отображений множества* $Q = \{0, 1, \ldots, n-1\}$ *в себя, где* $n = 2^k$, *не превосходит* $n^{\log_2(n)+1} \cdot (n-2)!$.

Доказательство. Подстановка, которой соответствует многочлен $c \cdot x$, есть $h_c \in H_*$.

Поле Галуа F_n без элемента 0 относительно операции умножения представляет собой циклическую группу порядка $n-1$ [13]. Порождающий элемент мультипликативной группы поля Галуа обозначим через m, а соответствующую ему подстановку — через h_m. Заметим, что $h_a = h_m^i$ для любого $a = m^i \in F_n^*$. Действительно, для любого $q \in Q$

$$h_a(q) = a \cdot q = m^i \cdot q = m \cdot (m \cdot (\ldots \cdot q)) = h_m(h_m(\ldots h_m(q))) = h_m^i(q).$$

Обозначим через h_d такое отображение, что $h_d(q) = h_q(q) = h_m^i(q)$, где $q = m^i \in \{0, \ldots, n-1\}$. Отображение, которому соответствует многочлен $c \cdot x^{2^i}$, есть $h_d^i \cdot h_c$, где $i = 0, \ldots, k-1$.

Действительно при $i = 0$ многочлен имеет вид $c \cdot x$, и соответствующая ему подстановка есть h_c.

При $i = 1$ многочлен имеет вид $c \cdot x^2$. Рассмотрим значение многочлена $c \cdot x^2$ на элементе $q \in Q$: $c \cdot q^2 = c \cdot (q \cdot q) = c \cdot h_q(q) = h_c(h_q(q))$. Таким образом, для любого элемента $q \in Q$ значение многочлена $c \cdot x^2$ равно значению отображения $h_d \cdot h_c$.

Для произвольного i имеем $c \cdot q^{2^i} = h_c(h_d(h_d \ldots (q))) = h_c(h_d^i(q))$. Таким образом, для любого элемента $q \in Q$ значение многочлена $c \cdot x^{2^i}$ равно

значению отображения ${h_d}^i \cdot h_c$.

Значение многочлена $\sum_{i=0}^{k-1} c_i \cdot x^{2^i}$ на элементе q определяется отображениями $h_d^i \cdot h_{c_i}$ и таблицей сложения в поле Галуа F_n. Покажем, что значение отображения s определяется значениями отображений $h_d^{{s_F}^i} \cdot h_{c_i}^{s_F}$ и таблицей сложения, полученной из таблицы сложения в поле Галуа F_n следующим образом: строки и столбцы таблицы переставляются согласно подстановке s_F^{-1}, а элементы таблицы заменяются согласно подстановке 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 — отображения, соответствующие некоторым многочленам f и g. Покажем, что $s_F^{-1} \cdot (h_f + h_g) \cdot s_F = h_f^{s_F} +_{s_F} h_g^{s_F}$ для каждого $q \in Q$. 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 отображений есть произведение сопряжений.

Покажем, что если $q = m^i$, то 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 реализуемое отображение полностью определяется подстановкой $h_m^{s_F}$. Данная подстановка есть цикл длины $n-1$. А таких подстановок $(n-2)!$ [14]. Следовательно, число линейно реализуемых отображений не превосходит $n^{\log_2(n)+1} \cdot (n-2)!$ □

2.2 Линейно реализуемые переходные системы

В данном разделе изучается вопрос о линейной реализуемости переходных систем.

Определение 9. *Нумерованной переходной системой* назовем тройку $V = (A, Q, \varphi)$, где A — входной алфавит, $Q = \{0, \ldots, n-1\}$, φ — функция переходов.

Пример 7. На рисунке 2.1 приведен пример переходной системы.

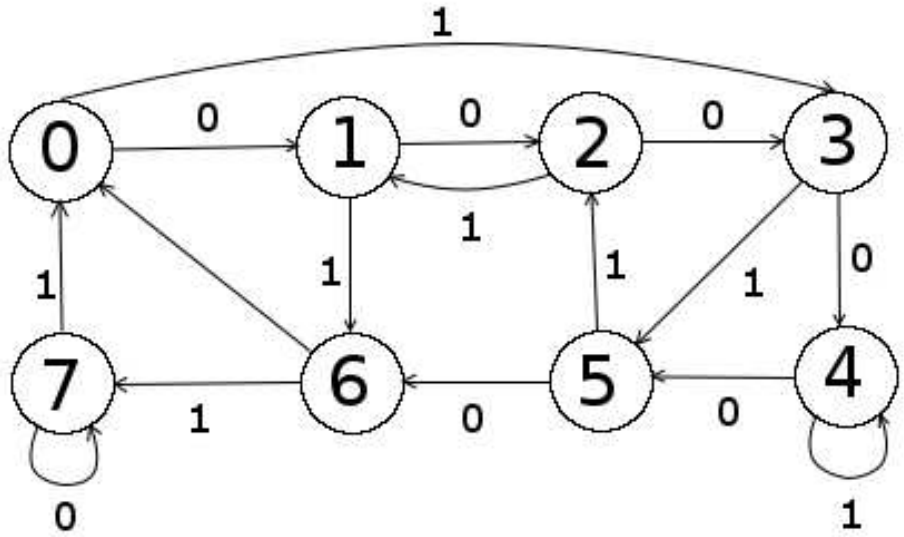

Рис. 2.1. Переходная система

Определение 10. Каждое кодирование F множества Q нумерованной переходной системы (A, Q, φ) порождает булев оператор $\phi_V^F : E_2^{k+1} \to E_2^k$ по правилу

$$\phi_V^F(a, \alpha_0, \ldots, \alpha_{k-1}) = F(\varphi(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))),$$

где $a \in E_2, \alpha_i \in E_2$. Этот оператор можно рассматривать как набор k булевых функций, зависящих от $k+1$ переменной. Обозначим этот набор через $\mathcal{F}_V(F)$.

Пример 8. Для переходной системы из примера 7 и кодирования

q	0	1	2	3	4	5	6	7
$F_0(q)$	000	001	010	011	100	101	110	111

соответствующий булев оператор есть

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$
0	0	0	0	0	0	1
0	0	0	1	0	1	0
0	0	1	0	0	1	1
0	0	1	1	1	0	0
0	1	0	0	1	0	1
0	1	0	1	1	1	0
0	1	1	0	0	0	0
0	1	1	1	1	1	1
1	0	0	0	0	1	1
1	0	0	1	1	1	0
1	0	1	0	0	0	1
1	0	1	1	1	0	1
1	1	0	0	1	0	0
1	1	0	1	0	1	0
1	1	1	0	1	1	1
1	1	1	1	0	0	0

Тогда канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = 0 \\ q_0(t+1) = q_1(t) \cdot q_2(t) + x(t) \cdot q_2(t) + q_0(t) + x(t) \cdot q_0(t) + x(t) \cdot q_1(t) \cdot q_2(t) \\ q_1(t+1) = q_2(t) + q_1(t) + q_0(t) \cdot q_1(t) + x(t) + x(t) \cdot q_3(t) + x(t) \cdot q_2(t) + \\ + x(t) \cdot q_1(t) \cdot q_2(t) + x \cdot q_0(t) + x \cdot q_0(t) \cdot q_2(t) \\ q_2(t+1) = 1 + q_2(t) + q_1(t) + q_0(t) \cdot q_2(t) + q_0(t) \cdot q_1(t) \cdot q_2(t) + \\ + x(t) \cdot q_1(t) \cdot q_2(t) + x(t) \cdot q_0(t) \cdot q_1(t) + x(t) \cdot q_0(t) \cdot q_1(t) \cdot q_2(t) \end{cases}$$

Определение 11. Назовем переходную систему *линейно реализуемой посредством кодирования* F, или просто *линейно реализуемой*, если для за-

данной нумерованной переходной системы V существует такое кодирование F, что все элементы $\mathcal{F}_V(F)$ являются линейными функциями алгебры логики.

Пример 9. Заметим, что переходная система из примера 7 является линейно реализуемой посредством кодирования F

q	0	1	2	3	4	5	6	7
$F(q)$	001	010	100	011	110	111	101	000

Данное кодирование порождает булев оператор

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$
0	0	0	0	0	0	0
0	0	0	1	0	1	0
0	0	1	0	1	0	0
0	0	1	1	1	1	0
0	1	0	0	0	1	1
0	1	0	1	0	0	1
0	1	1	0	1	1	1
0	1	1	1	1	0	1
1	0	0	0	0	0	1
1	0	0	1	0	1	1
1	0	1	0	1	0	1
1	0	1	1	1	1	1
1	1	0	0	0	1	0
1	1	0	1	0	0	0
1	1	1	0	1	1	0
1	1	1	1	1	0	0

.

Канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = 0 \\ q_0(t+1) = q_1(t) \\ q_1(t+1) = q_0(t) + q_2(t) \\ q_2(t+1) = q_0(t) + x(t) \end{cases}$$

Пусть заданы нумерованная переходная система $V = (E_2, Q, \varphi)$ и некоторое кодирование F. Пусть $X_V = \{s : Q \to Q | \exists a \in E_2, s(q) = \varphi(a, q) \quad \forall q \in Q\}$, а $S_V =< X_V >$ — замыкание множества X_V относительно операции суперпозиции отображений множества Q в себя [5].

Определение 12. Назовем S_V *внутренней полугруппой* переходной системы V, а X_V — *порождающим множеством* внутренней полугруппы.

Так как входной алфавит — это E_2, то множество X_V состоит из двух элементов. Обозначим через p_0 отображение, задаваемое входным символом 0, через p_1 — отображение, задаваемое входным символом 1.

Пример 10. Порождающее множество внутренней полугруппы переходной системы из примера 7 есть

$$\left\{ \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 7 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 1 & 5 & 4 & 2 & 7 & 0 \end{pmatrix} \right\}.$$

Определение 13. Пусть заданы булев оператор $\phi(a, \alpha_0, \ldots, \alpha_{k-1}) = (\beta_0, \ldots, \beta_{k-1})$, где $a, \alpha_i, \beta_i \in E_2$, $k = \log_2 n$, и кодирование F. Определим переходную систему $V_\phi^F = (E_2, E_n, \varphi)$, в которой функция переходов φ определяется следующим правилом

$$\varphi(a, q) = F^{-1}(\phi(a, F(q)).$$

Лемма 9. *Пусть задан булев оператор* $\phi(a, \alpha_0, \ldots, \alpha_{k-1}) = (\beta_0, \ldots, \beta_{k-1})$, *где* $a, \alpha_i, \beta_i \in E_2$, $k = \log_2 n$. *Оператор, порождаемый кодированием* F *и переходной системой* V_ϕ^F, *равен оператору* ϕ .

Доказательство. Согласно определению 10

$$\phi_{V_\phi^F}(a, \alpha_0, \ldots, \alpha_{k-1}) = F(\varphi(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))) \quad \forall a, \alpha_0, \ldots, \alpha_{k-1},$$

где $a \in E_2, \alpha_i \in E_2$. Согласно определению 13 переходной системы, определяемой по оператору,

$$F(\varphi(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))) = F(F^{-1}(\phi(a, F(F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))))) =$$

$$= \phi(a, \alpha_0, \ldots, \alpha_{k-1}).$$

Следовательно,

$$\phi^F_{V_\phi}(a, \alpha_0, \ldots, \alpha_{k-1}) = \phi(a, \alpha_0, \ldots, \alpha_{k-1}) \quad \forall a, \alpha_0, \ldots, \alpha_{k-1},$$

где $a \in E_2, \alpha_i \in E_2$. □

Лемма 10. *Число различных нумерованных переходных систем с $n = 2^k$ состояниями, линейно реализуемых посредством стандартного кодирования F_0, равно $n^{\log_2(n)+2} = 2^{k(k+2)}$.*

Доказательство. Пусть задана нумерованная переходная система с n состояниями, линейно реализуемая посредством стандартного кодирования F_0. Согласно условию леммы $k = \log_2(n)$. Данное кодирование порождает булев оператор ϕ: $E_2^{k+1} \to E_2^k$. Рассмотрим этот оператор как набор $\mathcal{F}_V(F_0)$. Поскольку переходная система линейно реализуема, элементы $\mathcal{F}_V(F_0)$ есть линейные булевы функции от $k+1$ переменных, а именно $\mathcal{F}_V(F_0) = \{f_0, \ldots, f_{k-1}\}$, где $k = \log_2 n$. Как известно, число различных линейных булевых функций, зависящих от $k+1$ переменных,й равно 2^{k+2} [10]. Значит, число различных наборов $\mathcal{F}_V(F_0)$ равно $\left(2^{k+2}\right)^k = n^{\log_2(n)+2}$.

Теперь покажем, что двум различным наборам соответствуют две различные переходные системы, линейно реализуемые посредством стандартного кодирования F_0. Каждый набор соответствует булеву оператору

$$\phi(a, \alpha_0, \ldots, \alpha_{k-1}) = (\beta_0, \ldots, \beta_{k-1}),$$

где $a, \alpha_i, \beta_i \in E_2$. Определим переходную систему следующим правилом: $V_\phi = (E_2, \{0, \ldots, n-1\}, \varphi_\phi)$, где $\varphi_\phi(a, q) = F_0^{-1}(\phi(a, F_0(q))$. Согласно лемме 9 линейный оператор, порождаемый кодированием F_0 и переходной системой V_ϕ, равен оператору ϕ.

Пусть заданы два различных набора $\mathcal{F}_1$ и $\mathcal{F}_2$. Поскольку они различны, найдутся две такие различные функции $f_i^1 \in \mathcal{F}_1$ и $f_i^2 \in \mathcal{F}_2$ и такой набор $a, \alpha_0, \ldots, \alpha_{k-1}$, где $a, \alpha_i \in E_2$, что $f_i^1(a, \alpha_0, \ldots, \alpha_{k-1}) \neq f_i^2(a, \alpha_0, \ldots, \alpha_{k-1})$. Следовательно, операторы, соответствующие первому и второму наборам,

не равны на наборе $a, \alpha_0, \ldots, \alpha_{k-1}$. Обозначим булев оператор, соответствующий первому набору, через ϕ_1, а второму — через ϕ_2;

$$\phi_1(a, \alpha_0, \ldots, \alpha_{k-1}) \neq \phi_2(a, \alpha_0, \ldots, \alpha_{k-1}).$$

Пусть $q = F_0(\alpha_0, \ldots, \alpha_{k-1})$. Тогда согласно построению переходной системы по булеву оператору

$$\varphi_{\phi_1}(a, q) = F_0^{-1}(\phi_1(a, \alpha_0, \ldots, \alpha_{k-1})),\ \varphi_{\phi_2}(a, q) = F_0^{-1}(\phi_2(a, \alpha_0, \ldots, \alpha_{k-1})).$$

□

Определение 14. Пусть заданы нумерованная переходная система $V = (E_2, Q, \varphi)$ и некоторое кодирование F. Обозначим через V_{s_F} переходную систему с входным алфавитом E_2, алфавитом состояний $Q = \{0, \ldots, n-1\}$ и функцией φ, определяемой правилом

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

Пример 11. Рассмотрим переходную систему V из примера 7 и кодирование F из примера 9

q	0	1	2	3	4	5	6	7
$F(q)$	001	010	100	011	110	111	101	000

Соответствующая ей есть подстановка есть

$$s_F = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 3 & 6 & 7 & 5 & 0 \end{pmatrix}.$$

На рисунке 2.2 изображена переходная система V_{S_F}

Порождающие ее внутренней полугруппы есть

$$p_0 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 2 & 4 & 6 & 3 & 1 & 7 & 5 \end{pmatrix},$$

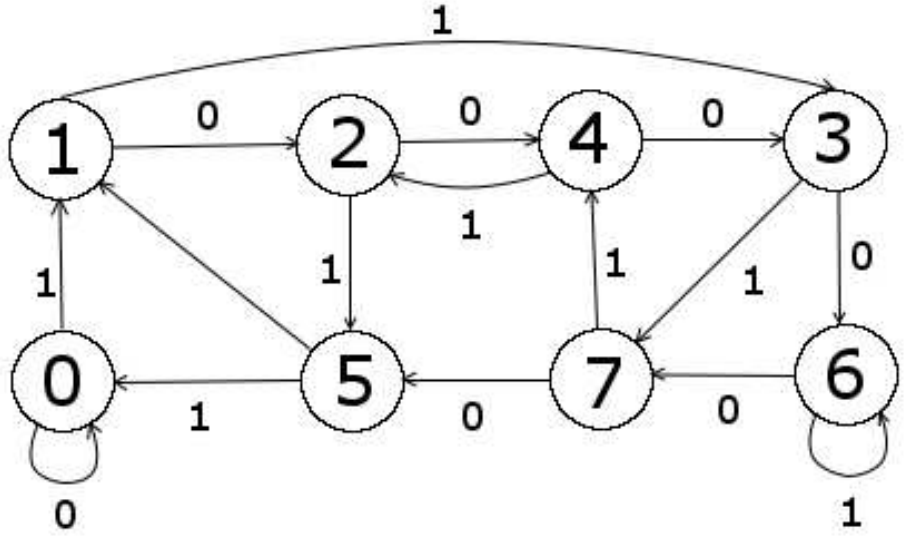

Рис. 2.2. Переходная система, полученная переобозначением состояний

$$p_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 7 & 2 & 0 & 6 & 4 \end{pmatrix}.$$

Лемма 11. *Пусть заданы нумерованная переходная система* $V = (E_2, Q, \varphi)$ *и некоторое кодирование* F*. Тогда булев оператор* ϕ_V*, порождаемый кодированием* F*, равен булеву оператору, порождаемому кодированием* F_0 *и переходной системой* V_{s_F}*.*

Доказательство. Пусть заданы нумерованная переходная система $V = (E_2, Q, \varphi)$ и кодирование $F : \{0, \ldots, n-1\} \to E_2^k$. Тогда соответствующий булев оператор определяется равенством

$$\phi_V(a, \alpha_0, \ldots, \alpha_{k-1}) = F(\varphi(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))),$$

где $a \in A, \alpha_i \in E_2$. Несложно видеть, что булев оператор, порождаемый кодированием F_0 и переходной системой V_{s_F}, определяется равенством

$$V_{s_F}(a, \alpha_0, \ldots, \alpha_{k-1}) = F_0(s_F(\varphi(a, s_F^{-1}(F_0^{-1}(\alpha_0, \ldots, \alpha_{k-1}))))).$$

Так как $s_F(i) = F_0^{-1}(F(i))$, то

$$V_{s_F}(a, \alpha_0, \ldots, \alpha_{k-1}) = F_0(F_0^{-1}(F(\varphi(a, F^{-1}(F_0(F_0^{-1}(\alpha_0, \ldots, \alpha_{k-1}))))))) =$$

$$= F(\varphi(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))).$$

Лемма доказана. □

Пример 12. Рассмотрим переходную систему V из примера 7 и кодирование F из примера 9

q	0	1	2	3	4	5	6	7
$F(q)$	001	010	100	011	110	111	101	000

Переходная система V_{S_F} изображена на рисунке 2.2. Стандартное кодирование и переходная система V_{S_F} порождают булев оператор

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$
0	0	0	0	0	0	0
0	0	0	1	0	1	0
0	0	1	0	1	0	0
0	0	1	1	1	1	0
0	1	0	0	0	1	1
0	1	0	1	0	0	1
0	1	1	0	1	1	1
0	1	1	1	1	0	1
1	0	0	0	0	0	1
1	0	0	1	0	1	1
1	0	1	0	1	0	1
1	0	1	1	1	1	1
1	1	0	0	0	1	0
1	1	0	1	0	0	0
1	1	1	0	1	1	0
1	1	1	1	1	0	0

.

Как видно из примера 9 данный оператор совпадает с оператором, порождаемым кодированием F и переходной системой V.

Лемма 12. *Число различных нумерованных переходных систем с вход-*

ным алфавитом E_2 и алфавитом состояний E_n равно n^{2n}.

Доказательство. Нумерованная переходная система полностью определяется порождающими внутренней полугруппы. Число отображений множества $Q = \{0, \ldots, n-1\}$ в себя равно n^n. Поскольку в нашем случае число порождающих равно 2, число всех возможных пар порождающих равно n^{2n}. □

Лемма 13. *Нумерованная переходная система $V = (E_2, Q, \varphi)$ линейно реализуема посредством кодирования F тогда и только тогда, когда существуют такое отображение p множества Q в себя и такие $h_1, h_2 \in s_F^{-1} \cdot H_+ \cdot s_F$, что*

- *p линейно реализуема посредством кодирования F,*
- *$p(s_F^{-1}(0)) = s_F^{-1}(0)$,*
- *$p_0 = p \cdot h_1$, $p_1 = p \cdot h_2$.*

Доказательство. Докажем необходимость условия линейной реализуемости. Пусть задана нумерованная переходная система $V = (E_2, Q, \varphi)$ линейно реализуемая посредством кодирования F_0. Обозначим число ее состояний через n. Рассмотрим множество $\mathcal{F}_V(F_0) = \{h_1, h_2, \ldots, h_k\}$, где $k = \log_2 n$. По определению булева оператора и множества $\mathcal{F}_V(F_0)$ имеем $h_i : E_2^{k+1} \to E_2^k$.

Поскольку h_i — линейная булева функция, из того, что первая переменная является существенной, следует:

$$h_i(0, \alpha_0, \ldots, \alpha_{k-1}) = h_i(1, \alpha_0, \ldots, \alpha_{k-1}) \oplus 1, \text{ где } \alpha_0, \ldots, \alpha_{k-1} \in E_2.$$

Если первая переменная является фиктивной, то по определению несущественной переменной $h_i(0, \alpha_0, \ldots, \alpha_{k-1}) = h_i(1, \alpha_0, \ldots, \alpha_{k-1})$, где $\alpha_0, \ldots, \alpha_{k-1} \in E_2$. Таким образом, для всех $\alpha_0, \ldots, \alpha_{k-1} \in E_2$

$$h_i(0, \alpha_0, \ldots, \alpha_{k-1}) = h_i(1, \alpha_0, \ldots, \alpha_{k-1}) \oplus c_i, \text{ где } c_i \in E_2.$$

По определениям булева оператора, порождаемого кодированием F и переходной системой V, множества $\mathcal{F}_V(F)$ и порождающих внутренней полугруппы верны следующие равенства:

$$p_0(q) = F_0^{-1}(h_0(0, F_0(q)), h_1(0, F_0(q)), \ldots, h_{k-1}(0, F_0(q))),$$

$$p_1(q) = F_0^{-1}(h_0(1, F_0(q)), h_1(1, F_0(q)), \ldots, h_{k-1}(1, F_0(q))) =$$

$$= F_0^{-1}(h_0(0, F_0(q)) \oplus c_0, h_1(0, F_0(q)) \oplus c_1, \ldots, h_{k-1}(1, F_0(q)) \oplus c_{k-1}) =$$

$$= p_0(q) + c,$$

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 подстановку, соответствующую многочлену $x + c$, через h_c. Тогда $p_1 = p_0 \cdot h_c$. Пусть $p_0(0) = a$. Обозначим подстановку, соответствующую многочлену $x + a$, через h_a. Тогда справедливо представление $p_0 = p_0 \cdot h_a^{-1} \cdot h_a$. Обозначим $p = p_0 \cdot h_a^{-1}$, тогда $p_0 = p \cdot h_a$, $p_1 = p \cdot h_a \cdot h_c$.

Пусть переходная система линейно реализуема посредством кодирования F. Согласно лемме 11 булев оператор, порождаемый кодированием F и переходной системой V, совпадает с булевым оператором, порождаемым кодированием F_0 и переходной системой 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 было только что показано, $p_0^{V_{s_F}} = p \cdot h_0$, $p_1^{V_{s_F}} = p \cdot h_1$, где $h_0, h_1 \in H_+$. Следовательно, $s_F^{-1} \cdot p_0 \cdot s_F = p \cdot h_0$, $s_F^{-1} \cdot p_1 \cdot s_F = p \cdot h_1$. Значит,

$$p_0 = s_F \cdot p \cdot h_0 \cdot s_F^{-1} = s_F \cdot p \cdot s_F^{-1} \cdot s_F \cdot h_0 \cdot s_F^{-1},$$

$$p_1 = s_F \cdot p \cdot h_1 \cdot s_F^{-1} = s_F \cdot p \cdot s_F^{-1} \cdot s_F \cdot h_1 \cdot s_F^{-1}.$$

Обозначим $p' = s_F \cdot p \cdot s_F^{-1}$, $h'_0 = s_F \cdot h_0 \cdot s_F^{-1}$, $h'_1 = s_F \cdot h_1 \cdot s_F^{-1}$. Тогда $p_0 = p' \cdot h'_0$, $p_1 = p' \cdot h'_1$, где $h'_0, h'_1 \in s_F \cdot H_+ \cdot s_F^{-1}$.

Докажем достаточность условия линейной реализуемости. Пусть существует такое отображение p, что оно линейно реализуемо посредством ко-

дирования F и

$$p(s_F^{-1}(0)) = s_F^{-1}(0),\ p_0 = p \cdot h_1,\ p_1 = p \cdot h_2,\ \text{где } h_1, h_2 \in s_F^{-1} \cdot H_+ \cdot s_F.$$

Следовательно, $\mathcal{F}_p(F) = \{f_0(x_0, x_1, \ldots, x_{k-1}), \ldots, f_{k-1}(x_0, x_1, \ldots, x_{k-1})\}$, где f_i — линейные булевы функции. Согласно лемме 3 булевы операторы подстановок h_0, h_1 совпадают с булевыми операторами, которые кодирование F_0 сопоставляет подстановкам $h_0' = s_F^{-1} \cdot h_0 \cdot s_F$ и $h_1' = s_F^{-1} \cdot h_1 \cdot s_F$. Можно заметить, что $h_0' \in H_+$ и $h_1' \in H_+$. Согласно следствию 1

$$\mathcal{F}_{h_0}(F) = \{x_0 + c_0^{h_0}, \ldots, x_{k-1} + c_{k-1}^{h_0}\},\ \mathcal{F}_{h_1}(F) = \{x_0 + c_0^{h_1}, \ldots, x_{k-1} + c_{k-1}^{h_1}\},$$

где $(c_0^{h_0}, \ldots, c_{k-1}^{h_0}) = F(h_0(s_{h_0}(0)))$, $(c_0^{h_1}, \ldots, c_{k-1}^{h_1}) = F(h_0(s_{h_1}(0)))$. Согласно следствию 2

$$\mathcal{F}_{p \cdot h_0}(F) = \{f_0(x_0, x_1, \ldots, x_{k-1}) + c_0^{h_0}, \ldots, f_{k-1}(x_0, x_1, \ldots, x_{k-1}) + c_{k-1}^{h_0}\},$$

$$\mathcal{F}_{p \cdot h_1}(F) = \{f_0(x_0, x_1, \ldots, x_{k-1}) + c_0^{h_1}, \ldots, f_{k-1}(x_0, x_1, \ldots, x_{k-1}) + c_{k-1}^{h_1}\}.$$

Заметим, что

$$f_i(x_0, x_1, \ldots, x_{k-1}) + c_i^{h_1} = f_i(x_0, x_1, \ldots, x_{k-1}) + c_i^{h_0} + c_i^{h_0} + c_i^{h_1},$$

где $0 \leq i \leq k-1$. Обозначим $f_i(x_0, x_1, \ldots, x_{k-1}) + c_i^{h_0}$ через $f_i^{p_0}(x_0, x_1, \ldots, x_{k-1})$. Тогда $f_i(x_0, x_1, \ldots, x_{k-1}) + c_i^{h_1} = f_i^{p_0}(x_0, x_1, \ldots, x_{k-1}) + c_i^{h_0} + c_i^{h_1}$. Следовательно, в новых обозначениях

$$\mathcal{F}_{p \cdot h_0}(F) = \{f_0^{p_0}(x_0, x_1, \ldots, x_{k-1}), \ldots, f_{k-1}^{p_0}(x_0, x_1, \ldots, x_{k-1})\},$$

$$\mathcal{F}_{p \cdot h_1}(F) = \{f_0^{p_0}(x_0, x_1, \ldots, x_{k-1}) + c_0^{h_0} + c_0^{h_1}, \ldots, f_{k-1}^{p_0}(x_0, x_1, \ldots, x_{k-1}) + c_{k-1}^{h_0} + c_{k-1}^{h_1}\}.$$

Согласно определению 10 оператора переходной системы V, порождаемого кодированием F,

$$\phi_V^F(a, \alpha_0, \ldots, \alpha_{k-1}) = F(\varphi(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))),$$

где $a \in E_2, \alpha_i \in E_2$ Заметим, что согласно определению порождающих внутренней полугруппы $\varphi(0,q) = p_0(q) = p{\cdot}h_0(q)$ и $\varphi(1,q) = p_1(q) = p{\cdot}h_1(q)$ для каждого $q \in Q$.

Разложим оператор ϕ по первой переменной:

$$\phi_V^F(a,\alpha_0,\ldots,\alpha_{k-1}) = \phi_V^F(0,\alpha_0,\ldots,\alpha_{k-1})\cdot\overline{a} \oplus \phi_V^F(1,\alpha_0,\ldots,\alpha_{k-1})\cdot a =$$

$$= \phi_V^F(0,\alpha_0,\ldots,\alpha_{k-1})\cdot(a\oplus 1) \oplus \phi_V^F(1,\alpha_0,\ldots,\alpha_{k-1})\cdot a =$$

$$= (\phi_V^F(0,\alpha_0,\ldots,\alpha_{k-1}) \oplus \phi_V^F(1,\alpha_0,\ldots,\alpha_{k-1}))\cdot a \oplus \phi_V^F(0,\alpha_0,\ldots,\alpha_{k-1}).$$

Так как

$$\phi_V^F(0,\alpha_0,\ldots,\alpha_{k-1}) = F(\varphi(0,F^{-1}(\alpha_0,\ldots,\alpha_{k-1}))) = F(p_0(F^{-1}(\alpha_0,\ldots,\alpha_{k-1}))) =$$

$$= F(p\cdot h_0(F^{-1}(\alpha_0,\ldots,\alpha_{k-1}))),$$

$$\phi_V^F(1,\alpha_0,\ldots,\alpha_{k-1}) = F(\varphi(1,F^{-1}(\alpha_0,\ldots,\alpha_{k-1}))) = F(p_1(F^{-1}(\alpha_0,\ldots,\alpha_{k-1}))) =$$

$$= F(p\cdot h_1(F^{-1}(\alpha_0,\ldots,\alpha_{k-1}))),$$

то множество $\mathcal{F}_V(F)$ имеет вид

$$\mathcal{F}_V(F) = \{(f_0^{p_0}(q_0,\ldots,q_{k-1}) \oplus f_0^{p_0}(q_0,\ldots,q_{k-1}) \oplus c_0^{h_0} \oplus c_0^{h_1})\cdot x \oplus f_0^{p_0}(q_0,\ldots,q_{k-1}),$$

$$\ldots$$

$$(f_{k-1}^{p_0}(q_0,\ldots,q_{k-1}) \oplus f_{k-1}^{p_0}(q_0,\ldots,q_{k-1}) \oplus c_{k-1}^{h_0} \oplus c_{k-1}^{h_1})\cdot x \oplus f_{k-1}^{p_0}(q_0,\ldots,q_{k-1})\} =$$

$$= \{(c_0^{h_0} \oplus c_0^{h_1})\cdot x \oplus f_0^{p_0}(q_0,\ldots,q_{k-1}),\ldots,(c_{k-1}^{h_0} \oplus c_{k-1}^{h_1})\cdot x \oplus f_{k-1}^{p_0}(q_0,\ldots,q_{k-1})\}.$$

Поскольку функции f_i — линейные, лемма доказана. □

Теорема 1. *Нумерованная переходная система $V = (E_2, Q, \varphi)$ линейно реализуема посредством кодирования F тогда и только тогда, когда порождающие внутренней полугруппы p_0 и p_1 линейно реализуемы посредством кодирования F и существует такая подстановка $h \in s_F^{-1}\cdot H_+ \cdot s_F$, что $p_1 = p_0\cdot h$.*

Доказательство. Если V линейно реализуема посредством кодирования F, то согласно лемме 13 существует такое отображение p множества Q в себя, что p линейно реализуема посредством кодирования F, $p(s_F^{-1}(0)) = s_F^{-1}(0)$, и существуют такие $h_0, h_1 \in s_F^{-1} \cdot H_+ \cdot s_F$, что $p_0 = p \cdot h_0$, $p_1 = p \cdot h_1$. Заметим, что $p_1 = p \cdot h_1 = p \cdot h_0 \cdot h_0^{-1} \cdot h_1 = p_0 \cdot h_0^{-1} \cdot h_1$. Так как $h_0^{-1} \cdot h_1 \in s_F^{-1} \cdot H_+ \cdot s_F$, то необходимость доказана.

Пусть порождающие p_0 и p_1 внутренней полугруппы V линейно реализуемы посредством кодирования F и существует такая подстановка $h \in s_F^{-1} \cdot H_+ \cdot s_F$, что $p_1 = p_0 \cdot h$. Согласно лемме 3 оператор, сопоставляемый отображению p_0 кодированием F, совпадает с оператором, сопоставляемым отображению $s_F^{-1} \cdot p_0 \cdot s_F$ кодированием F_0. Из леммы 7 следует, что $s_F^{-1} \cdot p_0 \cdot s_F = p \cdot h'$, где $h' \in H_+$, p линейно реализуема посредством кодирования F_0, причем $p(0) = 0$. Линейная реализуемость p следует из линейной релизуемости $s_F^{-1} \cdot p_0 \cdot s_F$ и h', а также леммы 5 о суперпозиции. Справедливо равенство $p_0 = s_F \cdot p \cdot s_F^{-1} \cdot s_F \cdot h' \cdot s_F^{-1} = p' \cdot h_0$, причем p' линейно реализуема посредством кодирования F.

Найдем значение p' на элементе $s_F^{-1}(0)$:

$$p'(s_F^{-1}(0)) = s_F \cdot p \cdot s_F^{-1}(s_F^{-1}(0)) = s_F^{-1}(p(s_F(s_F^{-1}(0)))) = s_F^{-1}(p(0)) = s_F^{-1}(0).$$

Заметим, что $h_0 \in s_F^{-1} \cdot H_+ \cdot s_F$. Согласно условию утверждения $p_1 = p_0 \cdot h$, следовательно, $p_1 = p_0 \cdot h = p' \cdot h_0 \cdot h$ и $h_0 \cdot h \in s_F^{-1} \cdot H_+ \cdot s_F$. А значит, согласно лемме 13 переходная система V линейно реализуема. □

Пример 13. Как видно, из формулировки теоремы 1 линейная реализуемость порождающих полугруппы не является достаточным условием линейно реализуемости переходной системы. Рассмотрим переходную систему, изображенную на рисунке 2.3

Порождающие её внутренней полугруппы есть

$$p_0 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 2 & 4 & 6 & 3 & 1 & 7 & 5 \end{pmatrix},$$

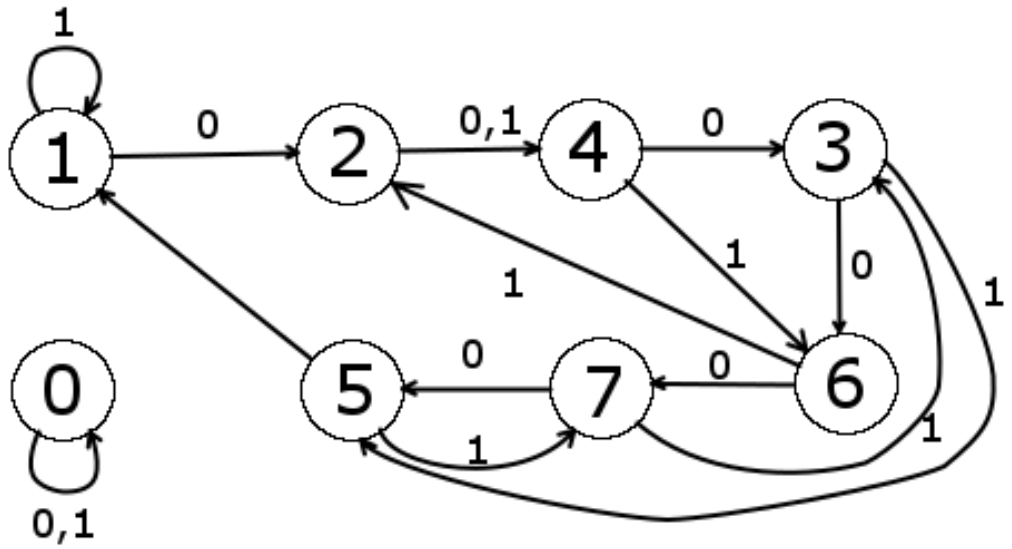

Рис. 2.3. Переходная система, не являющаяся линейно реализуемой

$$p_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 4 & 5 & 6 & 7 & 2 & 3 \end{pmatrix}.$$

Стандартное кодирование сопоставляет подстановке p_0 булев оператор

q_0	q_1	q_2	f_0	f_1	f_2
0	0	0	0	0	0
0	0	1	0	1	0
0	1	0	1	0	0
0	1	1	1	1	0
1	0	0	0	1	1
1	0	1	0	0	1
1	1	0	1	1	1
1	1	1	1	0	1

Множество $\mathcal{F}_{p_0}(F_0)$ есть

$$\mathcal{F}_{p_0}(F_0) = \{f_0(q_0, q_1, q_2) = q_1, f_1 = q_0 + q_2, f_2 = q_0\}.$$

Стандартное кодирование сопоставляет подстановке p_1 булев оператор

q_0	q_1	q_2	f_0	f_1	f_2
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	1	0	0
0	1	1	1	0	1
1	0	0	1	1	0
1	0	1	1	1	1
1	1	0	0	1	0
1	1	1	0	1	1

Множество $\mathcal{F}_{p_1}(F_0)$ есть

$$\mathcal{F}_{p_0}(F_0) = \{f_0 = q_0 + q_1, f_1 = q_0, f_2 = q_2\}.$$

Т.е. как видно, подстановки p_0 и p_1 линейно реализуемы. В тоже время стандартное кодирование и переходная система порождает булев оператор

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$
0	0	0	0	0	0	0
0	0	0	1	0	1	0
0	0	1	0	1	0	0
0	0	1	1	1	1	0
0	1	0	0	0	1	1
0	1	0	1	0	0	1
0	1	1	0	1	1	1
0	1	1	1	1	0	1
1	0	0	0	0	0	0
1	0	0	1	0	0	1
1	0	1	0	1	0	0
1	0	1	1	1	0	1
1	1	0	0	1	1	0
1	1	0	1	1	1	1
1	1	1	0	0	1	0
1	1	1	1	0	1	1

.

Канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = 0 \\ q_0(t+1) = q_1(t) + x(t)q_0(t) \\ q_1(t+1) = x(t)q_2(t) + q_0(t) + q_2(t) \\ q_2(t+1) = x(t)q_0(t) + x(t)q_2(t) + q_0(t) \end{cases}$$

Пример 14. Рассмотрим переходную систему V из примера 7 и кодирование F из примера 9

q	0	1	2	3	4	5	6	7
$F(q)$	001	010	100	011	110	111	101	000

Как было показано в примере 9 переходная система V линейно реализуема посредством кодирования F. Порождающие ее внутренней полугруппы есть

$$p_0 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 7 \end{pmatrix},$$

$$p_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 1 & 5 & 4 & 2 & 7 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 7 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 6 & 1 & 5 & 4 & 2 & 0 \end{pmatrix} =$$

$$= p_0 \cdot (07)(13)(26)(45).$$

Можно заметить, что подстановки p_0 и p_1 линейно реализуемы посредством кодирования F и $p_1 = p_0 \cdot (07)(13)(26)(45)$, где

$$(07)(13)(26)(45) = s_F^{-1} \cdot (01)(23)(45)(67) \cdot s_F =$$

$$= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 0 & 1 & 3 & 2 & 6 & 4 & 5 \end{pmatrix} \cdot (01)(23)(45)(67) \cdot \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 3 & 6 & 7 & 5 & 0 \end{pmatrix}$$

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

Доказательство. Согласно лемме 13 линейно реализуемая переходная система определяется линейно реализуемым отображением и подстановками, принадлежащими $s_F^{-1} \cdot H_+ \cdot s_F$. Число линейно реализуемых отображений не превосходит $n^{\log_2(n)+1} \cdot (n-2)!$. Подстановку $h \in s_F^{-1} \cdot H_+ \cdot s_F$ можно выбрать n способами. Следовательно, 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. □

Следствие 3. *Число линейно реализуемых нумерованных переходных систем с n состояниями есть $o(n^{2 \cdot n})$ при $n \to \infty$.*

Доказательство. Обозначим через $N_L(n)$ число линейно реализуемых нумерованных переходных систем с n состояниями. Согласно теореме 2

$$\frac{N_L(n)}{n^{2 \cdot n}} \leq \frac{n^{\log_2(n)+2} \cdot (n-2)!}{n^{2 \cdot n}},$$

$$\frac{n^{\log_2(n)+2} \cdot (n-2)!}{n^{2 \cdot n}} \leq \frac{n^{\log_2(n)} \cdot (n-2)^{n-2}}{n^{2 \cdot (n-1)}} \leq \frac{n^{\log_2(n)}}{n^{(n-1)}}.$$

Из полученного неравенства следует, что

$$lim_{n \to \infty} \frac{n^{\log_2(n)}}{n^{(n-1)}} = 0.$$

Отсюда следует, что $\lim_{n \to \infty} \frac{N_L(n)}{n^{2 \cdot n}} = 0$. Следствие доказано. □

2.3 Линейно реализуемые автоматы

В данном разделе изучается вопрос о линейной реализуемости автоматов.

Определение 15. *Нумерованным автоматом* назовем пятерку $\mathfrak{A} = (E_2, Q, E_2, \varphi, \psi)$, где $Q = \{0, \ldots, n-1\}$, φ — функция переходов, ψ — выходная функция [15].

Пример 15. На рисунке 2.4 изображен пример автомата

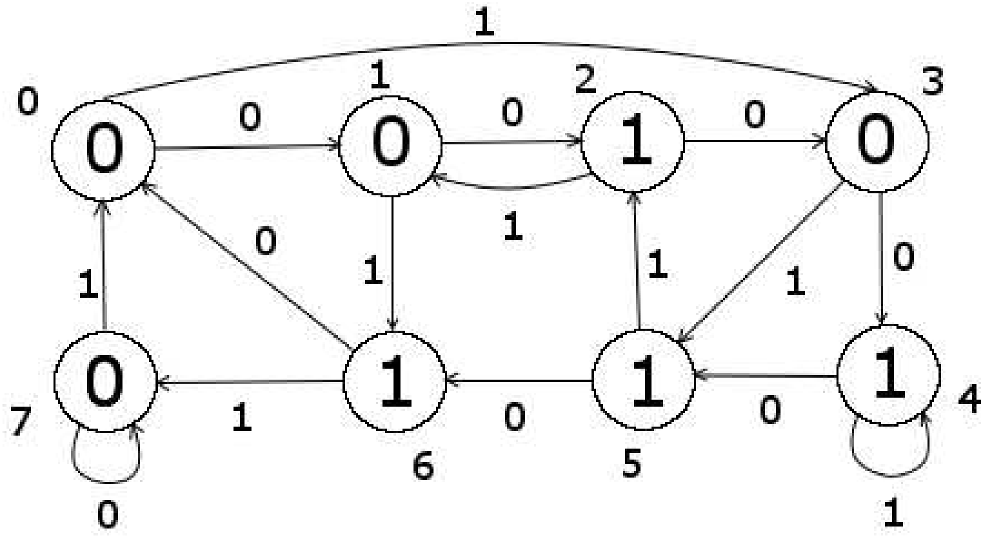

Рис. 2.4. Пример автомата

Определение 16. Для автомата $\mathfrak{A} = (E_2, Q, E_2, \varphi, \psi)$ каждое кодирование F множества Q порождает булев оператор $\phi^F_{\mathfrak{A}} : E_2^{k+1} \to E_2^{k+1}$, определяемый правилом

$$\phi(a, \alpha_0, \dots, \alpha_{k-1}) = (F(\varphi(a, F^{-1}(\alpha_0, \dots, \alpha_{k-1}))), \psi(a, F^{-1}(\alpha_0, \dots, \alpha_{k-1}))),$$

где $a \in E_2, \alpha_i \in E_2$. Этот оператор можно рассматривать как набор $k+1$ булевых функций, зависящих от $k+1$ переменных. Будем обозначать этот набор через $\mathcal{F}_{\mathfrak{A}}(F)$.

Пример 16. Для автомата из примера 15 стандартное кодирование порождает булев оператор

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$	$y(t)$
0	0	0	0	0	0	1	0
0	0	0	1	0	1	0	0
0	0	1	0	0	1	1	1
0	0	1	1	1	0	0	0
0	1	0	0	1	0	1	1
0	1	0	1	1	1	0	1
0	1	1	0	0	0	0	1
0	1	1	1	1	1	1	0
1	0	0	0	0	1	1	0
1	0	0	1	1	1	0	0
1	0	1	0	0	0	1	1
1	0	1	1	1	0	1	0
1	1	0	0	1	0	0	1
1	1	0	1	0	1	0	1
1	1	1	0	1	1	1	1
1	1	1	1	0	0	0	0

Канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = 0 \\ q_0(t+1) = q_1(t) \cdot q_2(t) + x(t) \cdot q_2(t) + q_0(t) + x(t) \cdot q_0(t) + x(t) \cdot q_1(t) \cdot q_2(t) \\ q_1(t+1) = q_2(t) + q_1(t) + q_0(t) \cdot q_1(t) + x(t) + x(t) \cdot q_3(t) + x(t) \cdot q_2(t) + \\ +x(t) \cdot q_1(t) \cdot q_2(t) + x \cdot q_0(t) + x \cdot q_0(t) \cdot q_2(t) \\ q_2(t+1) = 1 + q_2(t) + q_1(t) + q_0(t) \cdot q_2(t) + q_0(t) \cdot q_1(t) \cdot q_2(t) + \\ +x(t) \cdot q_1(t) \cdot q_2(t) + x(t) \cdot q_0(t) \cdot q_1(t) + x(t) \cdot q_0(t) \cdot q_1(t) \cdot q_2(t) \\ y(t) = q_0(t) + q_1(t) + q_1(t) \cdot q_2(t) + q_0(t) \cdot q_1(t) \end{cases}$$

Определение 17. Назовем нумерованный автомат $\mathfrak{A}$ *линейно реализуемым посредством кодирования* F, или просто *линейно реализуемым*, если для существует такое кодирование F, что все элементы $\mathcal{F}_{\mathfrak{A}}(F)$ являются линейными функциями алгебры логики.

Пример 17. Автомат $\mathcal{A}$ из примера 15 является линейно реализуемым посредством кодирования F

q	0	1	2	3	4	5	6	7
$F(q)$	001	010	100	011	110	111	101	000

Кодирование F и автомат $\mathcal{A}$ порождают булев оператор

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$	$y(t)$
0	0	0	0	0	0	0	0
0	0	0	1	0	1	0	0
0	0	1	0	1	0	0	0
0	0	1	1	1	1	0	0
0	1	0	0	0	1	1	1
0	1	0	1	0	0	1	1
0	1	1	0	1	1	1	1
0	1	1	1	1	0	1	1
1	0	0	0	0	0	1	0
1	0	0	1	0	1	1	0
1	0	1	0	1	0	1	0
1	0	1	1	1	1	1	0
1	1	0	0	0	1	0	1
1	1	0	1	0	0	0	1
1	1	1	0	1	1	0	1
1	1	1	1	1	0	0	1

.

Канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = 0 \\ q_0(t+1) = q_1(t) \\ q_1(t+1) = q_0(t) + q_2(t) \\ q_2(t+1) = q_0(t) + x(t) \\ y(t) = q_0(t) \end{cases}$$

Определение 18. Пусть заданы булев оператор $\phi(\alpha_0, \ldots, \alpha_k) = (\beta_0, \ldots, \beta_k)$, где $\alpha_i, \beta_i \in E_2$, $k = \log_2 n$, и кодирование F. Рассмотрим этот

оператор как множество функций $\mathcal{F}_\phi = \{f_0, f_1, \ldots, f_k\}$. Определим автомат $\mathfrak{A}_\phi^F = (E_2, E_n, E_2, \varphi, \psi)$ следующим правилом:

$$\varphi(a, q) = F^{-1}(f_0(a, F(q), f_1(a, F(q)), \ldots, f_{k-1}(a, F(q)))),$$

$$\psi(a, q) = f_k(a, F(q)).$$

Лемма 14. *Пусть задан булев оператор $\phi(\alpha_0, \ldots, \alpha_k) = (\beta_0, \ldots, \beta_k)$, где $\alpha_i, \beta_i \in E_2$, $k = \log_2 n$. Оператор, порождаемый кодированием F и автоматом $\mathfrak{A}_\phi^F$, равен оператору ϕ.*

Доказательство. Согласно определению 16 для всех $(\alpha_0, \ldots, \alpha_k)$

$$\phi_{\mathfrak{A}_\phi}(\alpha_0, \ldots, \alpha_k) = (F(\varphi(\alpha_0, F^{-1}(\alpha_1, \ldots, \alpha_k))), \psi(\alpha_0, F^{-1}(\alpha_1, \ldots, \alpha_k))),$$

где $\alpha_i \in \{0, 1\}$. Согласно определению 18 автомата, определяемого по оператору,

$$F(\varphi(\alpha_0, F^{-1}(\alpha_1, \ldots, \alpha_k))) = F(F^{-1}(f_0(\alpha_0, F(F^{-1}(\alpha_1, \ldots, \alpha_k)),$$

$$f_1(\alpha_0, F(F^{-1}(\alpha_1, \ldots, \alpha_k)), \ldots, f_k(\alpha_0, F(F^{-1}(\alpha_1, \ldots, \alpha_k)))) =$$

$$= (f_0(\alpha_0, \ldots, \alpha_k), f_1(\alpha_0, \alpha_1, \ldots, \alpha_k), \ldots, f_k(\alpha_0, \alpha_1, \ldots, \alpha_k)),$$

$$\psi(\alpha_0, F^{-1}(\alpha_1, \ldots, \alpha_k))) = f_k(\alpha_0, F(F^{-1}(\alpha_1, \ldots, \alpha_k)))) = f_k(\alpha_0, \ldots, \alpha_k).$$

Следовательно, для всех $(\alpha_0, \ldots, \alpha_k)$

$$\phi_{s_\phi}(\alpha_0, \ldots, \alpha_{k-1}) = \phi(\alpha_0, \ldots, \alpha_{k-1}),$$

где $\alpha_i \in \{0, 1\}$. □

Лемма 15. *Число различных нумерованных автоматов с n состояниями, линейно реализуемых посредством стандартного кодирования F_0, равно $(2n)^{\log_2(n)+2}$.*

Доказательство. Пусть задан нумерованный автомат с n состояниями,

линейно реализуемый посредством стандартного кодирования F_0. Обозначим $k = \log_2(n)$. Данное кодирование порождает булев оператор $\phi : E_2^{k+1} \to E_2^{k+1}$. Рассмотрим этот оператор как набор $\mathcal{F}_{\mathfrak{A}}(F_0)$. Поскольку автомат линейно реализуем, элементы $\mathcal{F}_{\mathfrak{A}}(F_0)$ есть линейные булевы функции от $k+1$ переменных, а именно $\mathcal{F}_{\mathfrak{A}}(F_0) = \{f_0, \ldots, f_k\}$, где $k = \log_2 n$. Как известно, число различных линейных булевых функций, зависящих от $k+1$ переменных, равно 2^{k+2} [10]. Значит, число различных наборов $\mathcal{F}_{\mathfrak{A}}(F_0)$ равно $\left(2^{k+2}\right)^{k+1}$, т. е. $(2n)^{\log_2(n)+2}$.

Теперь покажем, что двум различным наборам соответствуют два различных автомата, линейно реализуемых посредством стандартного кодирования F_0. Автомат, соответствующий набору $\mathcal{F} = \{f_0, f_1, \ldots, f_k\}$, определяется следующим правилом: $\mathfrak{A}_{\mathcal{F}} = (E_2, (0, \ldots, n-1), \varphi_{\mathcal{F}}, \psi_{\mathcal{F}})$, где

$$\varphi_{\mathcal{F}}(a, q) = F_0^{-1}(f_0(a, F_0(q)), f_1(a, F_0(q)), \ldots, f_{k-1}(a, F_0(q)),$$

а $\psi_{\mathcal{F}}(a, q) = f_k(a, F_0(q))$. Нетрудно проверить, что набор функций $\mathcal{F}_{\mathfrak{A}}$, порождаемых кодированинем F_0 и автоматом $\mathfrak{A}_{\mathcal{F}}$, равен набору $\mathcal{F}$.

Пусть заданы два различных набора $\mathcal{F}_1$ и $\mathcal{F}_2$. Поскольку они различны, найдутся две такие различные функции $f_i^1 \in \mathcal{F}_1$ и $f_i^2 \in \mathcal{F}_2$ и такой набор $a, \alpha_0, \ldots, \alpha_{k-1}$, где $a, \alpha_i \in E_2$, что $f_i^1(a, \alpha_0, \ldots, \alpha_{k-1}) \neq f_i^2(a, \alpha_0, \ldots, \alpha_{k-1})$. Если $i < k$, то согласно построению автомата по набору функций

$$\varphi_{\mathcal{F}_1}(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1})) =$$

$$= F_0^{-1}(f_0^1(a, \alpha_0, \ldots, \alpha_{k-1}), f_1^1(a, \alpha_0, \ldots, \alpha_{k-1}), \ldots, f_{k-1}^1(a, \alpha_0, \ldots, \alpha_{k-1})) \neq$$

$$\neq F_0^{-1}(f_0^2(a, \alpha_0, \ldots, \alpha_{k-1}), f_1^2(a, \alpha_0, \ldots, \alpha_{k-1}), \ldots, f_{k-1}^2(a, \alpha_0, \ldots, \alpha_{k-1})) =$$

$$= \varphi_{\mathcal{F}_2}(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1})).$$

Если $i = k$, то

$$\psi_{\mathcal{F}_1}(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1})) = f_k^1(a, (\alpha_0, \ldots, \alpha_{k-1})) \neq$$

$$\neq f_k^2(a, (\alpha_0, \ldots, \alpha_{k-1})) = \psi_{\mathcal{F}_1}(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1})).$$

□

Определение 19. Пусть задан автомат $\mathfrak{A} = (E_2, \{0, 1, \ldots, n-1\}, E_2, \varphi, \psi)$. Назовем тройку (E_2, Q, φ) *переходной системой* автомата $\mathfrak{A}$ и будем обозначать ее через $V_{\mathfrak{A}}$.

Переходная система автомата из примера 15 изображена на рисунке 2.1.

Пример 18. Рассмотрим автомат $\mathcal{A}$, изображенный на рисунке 2.5

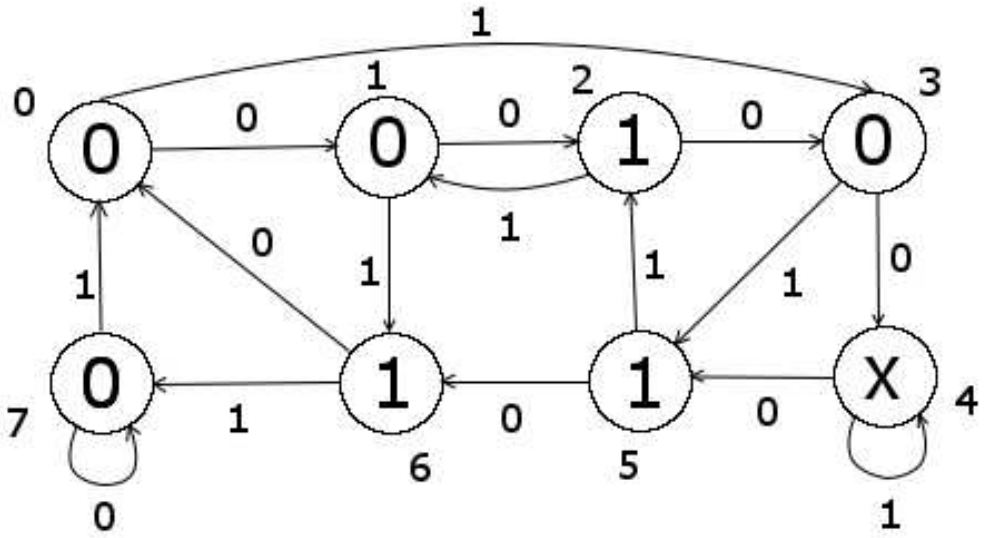

Рис. 2.5. Автомат, не являющийся линейно реализуемым.

Переходная система данного автомата изображена на рисунке 2.1. Как было показано данная переходная система линейно реализуема посредством кодирования F

q	0	1	2	3	4	5	6	7
$F(q)$	001	010	100	011	110	111	101	000

Данное кодирование и автомат $\mathcal{A}$ порождают булев оператор

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$	$y(t)$
0	0	0	0	0	0	0	0
0	0	0	1	0	1	0	0
0	0	1	0	1	0	0	0
0	0	1	1	1	1	0	0
0	1	0	0	0	1	1	1
0	1	0	1	0	0	1	1
0	1	1	0	1	1	1	0
0	1	1	1	1	0	1	1
1	0	0	0	0	0	1	0
1	0	0	1	0	1	1	0
1	0	1	0	1	0	1	0
1	0	1	1	1	1	1	0
1	1	0	0	0	1	0	1
1	1	0	1	0	0	0	1
1	1	1	0	1	1	0	1
1	1	1	1	1	0	0	1

.

Канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = 0 \\ q_0(t+1) = q_1(t) \\ q_1(t+1) = q_0(t) + q_2(t) \\ q_2(t+1) = q_0(t) + x(t) \\ y(t) = q_0(t) + q_0(t)q_1(t) + q_0(t)q_1(t)q_2(t) + x(t)q_0(t)q_1(t) + x(t)q_0(t)q_1(t)q_2(t) \end{cases}$$

Как видно из данного примера линейная реализуемость переходной системы автомата не является достаточным условием линейной реализуемости автомата. Далее изучается линейная реализуемость выходной функции.

Определение 20. Пусть задан автомат $\mathfrak{A} = (E_2, \{0, 1, \ldots, n-1\}, E_2, \varphi, \psi)$. Через ψ_q обозначим выходную функцию в состоянии q, т. е. $\psi_q(x) = \psi(x, q)$ для каждого $x \in E_2$.

Заметим, что функции $\{\psi_q\}$ есть булевы функции от одного аргумента. Следовательно, для каждого q функции $\psi_q \in \{0, 1, x, \overline{x}\}$. Введем следующие обозначения:

$$Q_0 = \{q \in \{0, 1, \ldots, n-1\} | \psi_q = 0\},$$

$$Q_1 = \{q \in \{0, 1, \ldots, n-1\} | \psi_q = 1\},$$

$$Q_x = \{q \in \{0, 1, \ldots, n-1\} | \psi_q = x\},$$

$$Q_{\overline{x}} = \{q \in \{0, 1, \ldots, n-1\} | \psi_q = \overline{x}\}.$$

Можно видеть, что для автомата из примера 15

$$Q_0 = \{0, 1, 3, 7\}$$

$$Q_1 = \{2, 4, 5, 6\},$$

$$Q_x = \varnothing,$$

$$Q_{\overline{x}} = \varnothing.$$

Лемма 16. *Пусть задан автомат* $\mathfrak{A} = (E_2, \{0, 1, \ldots, n-1\}, E_2, \varphi, \psi)$, *где* $n = 2^k$. *Если автомат линейно реализуем, то функции* $\{\psi_q\}$ *имеют одно и то же множество существенных переменных.*

Доказательство. Пусть автомат $\mathfrak{A} = (E_2, \{0, 1, \ldots, n-1\}, E_2, \varphi, \psi)$, где $n = 2^k$, линейно реализуем. Тогда существует такое кодирование F, что все элементы $\mathcal{F}_{\mathfrak{A}}(F)$ являются линейными функциями алгебры логики. В частности, линейна функция f_k, соответствующая выходной функции ψ. Значит, $f_k(a, q_0, q_1, \ldots, q_{k-1}) = c_0 + c_1 \cdot a + c_2 \cdot q_0 + c_3 \cdot q_1 + \ldots + c_{k+1} \cdot q_{k-1}$. Обозначим $c_q = c_2 \cdot q_0 + c_3 \cdot q_1 + \ldots + c_{k+1} \cdot q_{k-1}$, где $(q_0, q_1, \ldots, q_{k-1})$ — это код состояния q при кодировании F. Таким образом, $\psi_q(x) = c_1 \cdot x + c_0 + c_q$. Константа c_1 не зависит от состояния, следовательно, во всех состояниях реализуются либо функции $x, \overline{x}$, если $c_1 = 1$, либо функции $0, 1$, если $c_1 = 0$. □

Лемма 17. *Пусть задан линейно реализуемый автомат* $\mathfrak{A} =$

$(E_2, \{0, 1, \ldots, n-1\}, E_2, \varphi, \psi)$, *где* $n = 2^k$. *Если функция* ψ *не константа, то* $|Q_{\psi_0}| = |Q_{\overline{\psi_0}}|$.

Доказательство. Пусть автомат $\mathfrak{A} = (E_2, \{0, 1, \ldots, n-1\}, E_2, \varphi, \psi)$, где $n = 2^k$, линейно реализуем. Тогда существует такое кодирование F, что все элементы $\mathcal{F}_{\mathfrak{A}}(F)$ являются линейными функциями алгебры логики. В частности, линейна функция f_k, соответствующая выходной функции ψ. Следовательно, $f_k(x, q_0, q_1, \ldots, q_{k-1}) = c_0 + c_1 \cdot x + c_2 \cdot q_0 + c_3 \cdot q_1 + \ldots + c_{k+1} \cdot q_{k-1}$. Значит, $\psi_0(x) = c_0 + c_1 \cdot x + \beta$, где β — значение $c_2 \cdot q_0 + c_3 \cdot q_1 + \ldots + c_{k+1} \cdot q_{k-1}$ на коде состояния 0 при кодировании F. Функция, реализуемая в состоянии q, есть $\psi_q(x) = c_0 + c_1 \cdot x + c_0 + c_1 \cdot x + c_2 \cdot \alpha_0 + c_3 \cdot \alpha_1 + \ldots + c_{k+1} \cdot \alpha_{k-1}$, где $(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$ — код состояния q при кодировании F. Таким образом, в состояниях реализуется либо функция $c_0 + c_1 \cdot x$, либо $c_0 + c_1 \cdot x + 1$. Заметим, что $c_2 \cdot q_0 + c_3 \cdot q_1 + \ldots + c_{k+1} \cdot q_{k-1}$ принимает значение 1 на половине наборов $(\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$, где $\alpha_i \in E_2$, а на другой половине наборов принимает значение 0. Так как

$$c_0 + c_1 \cdot x + 1 = \overline{c_0 + c_1 \cdot x}, \text{ а } c_0 + c_1 \cdot x = \overline{c_0 + c_1 \cdot x + 1},$$

то $|Q_{\psi_0}| = |Q_{\overline{\psi_0}}|$. □

Определение 21. Пусть задан линейно реализуемый автомат $\mathfrak{A} = (E_2, \{0, 1, \ldots, n-1\}, E_2, \varphi, \psi)$. Определим выходной предикат $p^{out} : \{0, 1, \ldots, n-1\} \to E_2$ правилом $p^{out}(q) = \psi(0, q)$.

Пример 19. Выходной предикат автомата из примера 15 есть

q	0	1	2	3	4	5	6	7
$p^{out}(q)$	0	0	1	0	1	1	1	0

Определение 22. Пусть задан предикат $p : \{0, 1, \ldots, n-1\} \to E_2$. Каждое кодирование F множества Q сопоставляет предикату p булеву функцию $\phi_p^F : E_2^{k+1} \to E_2$ по правилу

$$\phi_p^F(\alpha_0, \ldots, \alpha_{k-1}) = p(F^{-1}(\alpha_0, \ldots, \alpha_{k-1})), \text{ где } \alpha_i \in E_2.$$

Пример 20. Стандартное кодирование сопоставляет предикату из примера

19 булеву функцию

q_0	q_1	q_2	$f(q_0, q_1, q_2)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

.

Функция $f(q_0, q_1, q_2) = q_0 + q_1 + q_1 \cdot q_2 + q_0 \cdot q_1$.

Определение 23. Назовем предикат $p^{out} : \{0, 1, \ldots, n-1\} \to E_2$ *линейно реализуемым посредством кодирования* F или просто *линейно реализуемым*, если существует такое кодирование F, что функция ϕ_p^F является линейной функцией алгебры логики.

Пример 21. Предикат p^{out} из примера 19 линейно реализуем посредством кодирования F

q	0	1	2	3	4	5	6	7
$F(q)$	001	010	100	011	110	111	101	000

Кодирование F сопоставляет предикату p^{out} булеву функцию

q_0	q_1	q_2	$f(q_0, q_1, q_2)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

.

Функция $f(q_0, q_1, q_2) = q_0$.

Лемма 18. *Пусть автомат* $\mathfrak{A} = (E_2, \{0, 1, \ldots, n-1\}, E_2, \varphi, \psi)$ *линейно реализуем. Пусть* $M_0 = \{q \in \{0, 1, \ldots, n-1\} | p^{out}(q) = 0\}$ *и* $M_1 = \{q \in$

$\{0,1,\ldots,n-1\}|p^{out}(q)=1\}$. *Если функция* ψ *не константа, то* $|M_0|=|M_1|=\frac{n}{2}$.

Доказательство. Пусть автомат $\mathfrak{A}=(E_2,\{0,1,\ldots,n-1\},E_2,\varphi,\psi)$, где $n=2^k$, линейно реализуем. Тогда существует такое кодирование F, что все элементы $\mathcal{F}_{\mathfrak{A}}(F)$ являются линейными функциями алгебры логики. В частности, линейна функция f_k, соответствующая выходной функции ψ. Значит, $f_k(x,q_0,q_1,\ldots,q_{k-1})=c_0+c_1\cdot x+c_2\cdot q_0+c_3\cdot q_1+\ldots+c_{k+1}\cdot q_{k-1}$. Заметим, что $\psi(x,q)=f_{k+1}(x,F(q))$. Тогда предикат $p^{out}(q)=f_{k+1}(0,F(q))=c_0+c_2\cdot q_0+c_3\cdot q_1+\ldots+c_{k+1}\cdot q_{k-1}$, где $(\alpha_0,\alpha_1,\ldots,\alpha_{k-1})$ — код состояния q при кодировании F. Заметим, что функция $p^{out}(q)=c_0+c_2\cdot q_0+c_3\cdot q_1+\ldots+c_{k+1}\cdot q_{k-1}$ принимает значение 1 на половине наборов $(\alpha_0,\alpha_1,\ldots,\alpha_{k-1})$, где $\alpha_i\in E_2$, а на другой половине наборов принимает значение 0. Отсюда следует утверждение леммы. □

Лемма 19. *Пусть автомат* $\mathfrak{A}=(E_2,\{0,1,\ldots,n-1\},E_2,\varphi,\psi)$ *линейно реализуем. Тогда существуют такие* $a,b\in E_2$, *что* $\psi(x,q)=p^{out}(q)+ax+b$ *для всех* $q\in\{0,1,\ldots,n-1\}$.

Доказательство. Пусть автомат $\mathfrak{A}=(E_2,\{0,1,\ldots,n-1\},E_2,\varphi,\psi)$, где $n=2^k$, линейно реализуем. Тогда существует такое кодирование F, что все элементы $\mathcal{F}_{\mathfrak{A}}(F)$ являются линейными функциями алгебры логики. В частности, линейна функция f_k, соответствующая выходной функции ψ. Значит, $f_k(x,q_0,q_1,\ldots,q_{k-1})=c_0+c_1\cdot x+c_2\cdot q_0+c_3\cdot q_1+\ldots+c_{k+1}\cdot q_{k-1}$. Заметим, что $\psi(x,q)=f_k(x,F(q))$. Тогда предикат $p^{out}(q)=f_{k+1}(0,F(q))=c_0+c_2\cdot q_0+c_3\cdot q_1+\ldots+c_{k+1}\cdot q_{k-1}$. Следовательно, $\psi(x,q)=p^{out}(q)+c_0+c_1\cdot x$. □

Теорема 3. *Пусть задан автомат* $\mathfrak{A}=(E_2,\{0,1,\ldots,n-1\},E_2,\varphi,\psi)$, *где* $n=2^k$. *Автомат линейно реализуем посредством кодирования* F *тогда и только тогда, когда*

- *переходная система* $V_{\mathfrak{A}}=(E_2,\{0,1,\ldots,n-1\},\varphi)$ *линейно реализуема посредством кодирования* F,
- *существуют такие* $\alpha,\beta\in E_2$ *и предикат* $p^{out}:Q\to E_2$, *что* $\psi(x,q)=p^{out}(q)+\alpha\cdot x+\beta$ *для каждого* $q\in\{0,1,\ldots,n-1\}$,

- *предикат p^{out} линейно реализуем посредством кодирования F.*

Доказательство. Пусть автомат линейно реализуем посредством кодирования F. Тогда элементы $\mathcal{F}_{\mathfrak{A}}(F)$ являются линейными функциями алгебры логики. Рассмотрим переходную систему $V_{\mathfrak{A}} = (E_2, \{0, 1, \ldots, n-1\}, \varphi)$. Несложно видеть, что $\mathcal{F}_{V_{\mathfrak{A}}}(F)$ является подмножеством множества $\mathcal{F}_{\mathfrak{A}}(F)$. Отсюда следует линейная реализуемость переходной системы $V_{\mathfrak{A}}$.

Существование констант α, β и предиката $p^{out} : Q \to E_2$ следует из теоремы 19, причем предикат $p^{out}(q) = f_k(0, F(q))$, где $f_k \in \mathcal{F}_{\mathfrak{A}}(F)$. А значит, $p^{out}(q)$ линейно реализуем посредством кодирования F.

Докажем теорему в обратную сторону. Пусть переходная система $V_{\mathfrak{A}} = (E_2, \{0, 1, \ldots, n-1\}, \varphi)$ линейно реализуема посредством кодирования F. Согласно определению 11 все элементы $\mathcal{F}_{V_{\mathfrak{A}}}(F)$ есть линейные функции. Согласно определению 17 функции $\mathcal{F}_{V_{\mathfrak{A}}}(F)$ являются первыми k функциями множества $\mathcal{F}_{\mathfrak{A}}(F)$. Покажем, что функция f_k, соответствующая выходной функции ψ, также является линейной функцией. Согласно условию теоремы существуют такие $\alpha, \beta \in E_2$ и предикат $p^{out} : Q \to E_2$, что $\psi(x, q) = p^{out}(q) + \alpha \cdot x + \beta$ для каждого $q \in \{0, 1, \ldots, n-1\}$ и предикат p^{out} линейно реализуем посредством кодирования F. Значит, функция $\phi^F_{p^{out}}(\alpha_0, \ldots, \alpha_{k-1}) = p^{out}(F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))$ — это линейная функция. $\psi(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1})) = p^{out}(F^{-1}(\alpha_0, \ldots, \alpha_{k-1})) + \alpha \cdot a + \beta$. А значит, $\psi(a, F^{-1}(\alpha_0, \ldots, \alpha_{k-1}))$ — это линейная функция. □

Пример 22. Рассмотрим автомат $\mathcal{A}$ из примера 15. Как было показано, он линейно реализуем посредством кодирования F

q	0	1	2	3	4	5	6	7
$F(q)$	001	010	100	011	110	111	101	000

С другой стороны в примере 9 было показано, что переходная система $V_{\mathcal{A}}$ линейно реализуема посредством кодирования F. Выходная функция автомата $\mathcal{A}$ имеет вид $\psi(x, q) = p^{out}(q)$, где

q	0	1	2	3	4	5	6	7
$p^{out}(q)$	0	0	1	0	1	1	1	0

,

т.е. $\alpha = 0$,$\beta = 0$ и предикат $p^{out}(q)$ линейно реализуем посредством кодирования F.

Следствие 4. *Пусть $\mathfrak{A}(n)$ — множество нумерованных автоматов с n состояниями с входным алфавитом E_2 и выходным алфавитом E_2. Число линейно реализуемых автоматов с $n = 2^k$ состояниями есть $o(|\mathfrak{A}(n)|)$.*

Доказательство. Пусть задан автомат $\mathfrak{A} = (E_2, \{0, 1, \ldots, n-1\}, E_2, \varphi, \psi)$. Автомат полностью определяется переходной системой $(E_2, \{0, 1, \ldots, n-1\}, \varphi)$ и функцией $\psi : E_2 \times E_n \to E_2$. Согласно лемме 12 число различных переходных систем есть n^{2n}. Число различных выходных функций есть 2^{2n}. Следовательно, число автоматов с n состояниями с входным алфавитом E_2 и выходным алфавитом E_2 равно $n^{2n} \cdot 2^{2n} = (2n)^{2n}$.

Как было показано в теореме 3, линейно реализуемый автомат определяется линейно реализуемой переходной системой, предикатом $p^{out} : Q \to E_2$ и константами $\alpha, \beta \in E_2$. Число линейно реализуемых переходных систем с входным алфавитом E_2 и алфавитом состояний E_n не превосходит $n^{\log_2(n)+2} \cdot (n-2)!$ Число предикатов $p^{out} : Q \to E_2$ не превосходит $C_n^{\frac{n}{2}}$. Число различных констант α, β равно 2^2. Следовательно, число линейно реализумых автоматов не превосходит $n^{\log_2(n)+2} \cdot (n-2)! \cdot \frac{n!}{\frac{n}{2}!\cdot\frac{n}{2}!} \cdot 2^2$. Далее,

$$\frac{n^{\log_2(n)+2} \cdot (n-2)! \cdot \frac{n!}{\frac{n}{2}!\cdot\frac{n}{2}!} \cdot 2^2}{(2n)^{2\cdot n}} \leq \frac{n^{\log_2(n)} \cdot (n-2)^{n-2} \cdot n^{\frac{n}{2}}}{(2n)^{2\cdot(n-1)}} \leq \frac{n^{\log_2(n)}}{2^{2n-2} \cdot n^{\frac{n}{2}}},$$

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

□

Глава 3

Избыточные кодирования

В данной главе будут изучены избыточные кодирования. В отличии от неизбыточных кодирований, где длина кода строго определена мощностью множества состояний автомата, избыточные кодирования сопоставляют состояниям вектора большей длины. За счет удлинения кода сложность автомата может уменьшиться.

3.1 Линейно реализуемые элементы полугруппы P_n

Определение 24. Пусть задано кодирование $F : \{0, \ldots, n-1\} \to E_2^k$, где $k \geq]\log_2 n[$. Кодирование $\hat{F} : \{0, \ldots, 2^k - 1\} \to E_2^k$ назовем *доопределением кодирования* F, если для каждого $q \in \{0, \ldots, n-1\}$

$$F(q) = \hat{F}(q).$$

Определение 25. Пусть $s : E_n \to E_n$ — отображение множества $E_n = \{0, \ldots, n-1\}$ в себя. Кодирование $F : Q \to E_2^k$ множества E_n сопоставляет отображению s булев оператор $\phi_s^F : R \to R$, где $R \subseteq E_2^k$, по правилу

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

где $\alpha_1, ..., \alpha_{k-1} \in E_2$.

Определение 26. Оператор $\widehat{\phi} : E_2^m \to E_2^k$, $m, k \in N$ назовем *доопределением оператора* $\phi : R \to {E_2}^k$, где $R \subseteq E_2^m$, если для каждого $(\alpha_1, \ldots, \alpha_m) \in R$ верно

$$\phi(\alpha_1, ..., \alpha_m) = \widehat{\phi}(\alpha_1, ..., \alpha_m).$$

Определение 27. Отображение $s : E_n \to E_n$ называется *линейно реализуемым посредством кодирования* F, если для оператора ϕ_s^F существует такое доопределение $\hat{\phi}_s^F$, что набор $\mathcal{F}_{\hat{\phi}_s^F}$ состоит из линейных булевых функций.

Определение 28. Кодирование $F : \{0, \ldots, n-1\} \to E_2^n$, опредеяемое равенством $F(i) = (0 \ldots \underset{i}{1} \ldots 0)$, где «1» стоит в i-м разряде, а в остальных разрядах «0», назовем простым позиционным кодированием. Будем обозначать такое кодирование через F_{pos}.

Пример 23. Приведем пример простого позиционного кодирования F_{pos} множества $E_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

q	0	1	2	3	4	5	6	7
$F_{pos}(q)$	00000001	00000010	00000100	00001000	00010000	00100000	01000000	10000000

Лемма 20. *Отображение $s : E_n \to E_n$ является линейно реализуемым посредством простого позиционного кодирования.*

Доказательство. Обозначим через $s(Q)$ полный образ множества Q отображения s, а через $s^{-1}(q)$ полный прообраз одно-элементного множества $\{q\}$ отображения s. Покажем, что множество

$$\mathcal{F} = \{f_j(\alpha_1, ..., \alpha_{k-1}) = \sum_{i \in s^{-1}(j)} \alpha_i, 0 \le j \le k-1\}$$

задает оператор ϕ, являющийся доопределением $\phi_s^{F_{pos}}$.

Рассмотрим значение оператора $\phi_s^{F_{pos}}$ на кодах элементов множества Q.

Пусть $s(i) = j$, тогда согласно определению 3

$$\phi_s^F(0,\ldots,\underset{i}{1},\ldots,0) = F_{pos}(s(F_{pos}^{-1}(0,\ldots,\underset{i}{1},\ldots,0))) =$$

$$= F_{pos}(s(i)) = F_{pos}(j) = (0,\ldots,\underset{j}{1},\ldots,0).$$

Заметим, что $f_j(0,\ldots,\underset{i}{1},\ldots,0) = \sum_{i\in s^{-1}(j)} \alpha_i = 1$, так как $i \in s^{-1}(j)$, и в наборе $(0,\ldots,\underset{i}{1},\ldots,0)$ ровно одна «1».

С другой стороны $f_l(0,\ldots,\underset{i}{1},\ldots,0) = \sum_{i\in s^{-1}(j)} \alpha_i = 0$, где $l \neq j$, т.е.

$$\phi(0,\ldots,\underset{i}{1},\ldots,0) = (0,\ldots,\underset{j}{1},\ldots,0).$$

□

Пример 24. Булев оператор, сопоставляемый простым позиционным кодированием подстановке

$$p = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \end{pmatrix}$$

есть

q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Можно увидеть, что данный частично определенный оператор доопре-

деляется до оператора, задаваемого функциями:

$$f_0(q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7) = q_1$$
$$f_1(q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7) = q_2$$
$$f_2(q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7) = q_3$$
$$f_3(q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7) = q_4$$
$$f_4(q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7) = q_5$$
$$f_5(q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7) = q_6$$
$$f_6(q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7) = q_7$$
$$f_7(q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7) = q_0$$

Заметим, что p не является линейно реализуемой посредством неизбыточного кодирования подстановкой.

3.2 Линейно реализуемые переходные системы

В этом разделе будут рассмотрены переходные системы.

Определение 29. Каждое кодирование F множества Q нумерованной переходной системы (A, Q, φ) порождает булев оператор $\phi_V^F : E_2 \times R \to R$, где $R \subseteq E_2^k$, по правилу

$$\phi_V^F(a, \alpha_1, ..., \alpha_k) = F(\varphi(a, F^{-1}(\alpha_1, ..., \alpha_k))),$$

где $a \in E_2, (\alpha_1, \ldots, \alpha_k) \in R$.

Определение 30. Назовем переходную систему *линейно реализуемой посредством кодирования* F, или просто *линейно реализуемой*, если для заданной нумерованной переходной системы V существует такое кодирование F, что для оператора ϕ_V^F существует доопределение $\widehat{\phi}_V^F$, у которого все элементы $\mathcal{F}_{\widehat{\phi}_V^F}$ являются линейными функциями алгебры логики.

Пример 25. Рассмотрим переходную систему V, изображенную на рисунке 3.1

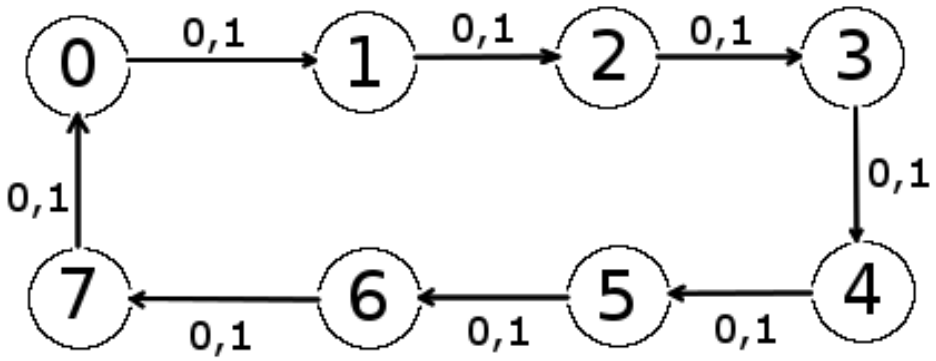

Рис. 3.1. Линейно реализуемая переходная система

Заметим,что переходная система V не является линейно реализуемой посредством неизбыточных кодирований. Данная переходная система и кодирование F_{pos}

q	0	1	2	3	4	5	6	7
$F_{pos}(q)$	00000001	00000010	00000100	00001000	00010000	00100000	01000000	10000000

порождают булев оператор

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_3(t)$	$q_4(t)$	$q_5(t)$	$q_6(t)$	$q_7(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$	$q_3(t+1)$	$q_4(t+1)$	$q_5(t+1)$	$q_6(t+1)$	$q_7(t+1)$
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
1	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
1	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

Можно видеть, что канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = q_3(0) = q_4(0) = q_5(0) = q_6(0) = q_7(0) = 0 \\ q_0(t+1) = q_1(t) \\ q_1(t+1) = q_2(t) \\ q_2(t+1) = q_3(t) \\ q_3(t+1) = q_4(t) \\ q_4(t+1) = q_5(t) \\ q_5(t+1) = q_6(t) \\ q_6(t+1) = q_7(t) \\ q_7(t+1) = q_0(t) \end{cases}$$

Определение 31. Пусть задана переходная система $V = (E_2, \{0, \ldots, n-1\}, \varphi)$. Переходную систему $\hat{V} = (E_2, \{0, \ldots, \hat{n}-1\}, \hat{\varphi})$, где $\hat{n} > n$ назовем *доопределением переходной системы* V, если для каждого $a \in E_2$ и $q \in \{0, \ldots, n-1\}$

$$\varphi(a, q) = \hat{\varphi}(a, q).$$

Лемма 21. *Пусть нумерованная переходная система* $V = (E_2, Q = \{0, \ldots, n-1\}, \varphi)$ *линейно реализуема посредством кодирования* $F : \{0, \ldots, n-1\} \to E_2^k$, *где* $k \geq]\log_2 n[$. *Обозначим* $R = F(Q)$. *Тогда существует такое доопределение* $\hat{V} = (E_2, \{0, \ldots, 2^k - 1\}, \hat{\varphi})$ *переходной системы* V, *что переходная система* $\hat{V}$ *является линейно реализуемой.*

Доказательство. Из определения линейной реализуемости следует, что для оператора ϕ_V^F существует такое доопределение $\hat{\phi}_V^F$, что все элементы $\mathcal{F}_{\hat{\phi}_V^F}$ являются линейными функциями. Рассмотрим произвольное доопределение $\hat{F} : \{0, \ldots, 2^k - 1\} \to E_2^k$ кодирования F. По оператору $\hat{\phi}_V^F$ и кодированию $\hat{F}$ построим переходную систему $V_{\hat{\phi}_V^F}^{\hat{F}}$ согласно определению 13. Покажем, что данная переходная система является доопределением V. Множество состояний переходной системы $V_{\hat{\phi}_V^F}^{\hat{F}}$ есть множество $\{0, \ldots, 2^k - 1\}$ и поскольку $k \geq]\log_2 n[$, то $2^k - 1 \geq n - 1$. Согласно определению 13 для

функции переходов $V^{\hat{F}}_{\hat{\phi}^F_V}$ верно равенство

$$\varphi^{\hat{F}}_{\hat{\phi}^F_V}(a,q) = \hat{F}^{-1}(\hat{\phi}^F_V(a,\hat{F}(q))).$$

Найдем значение этого оператора на элементах $q \in Q$. Поскольку $\hat{F}$ — доопределение кодирования F, для каждого $q \in Q$ верно равенсво $\hat{F}(q) = F(q)$. Следовательно для всех $q \in Q$

$$\varphi^{\hat{F}}_{\hat{\phi}^F_V}(a,q) = \hat{F}^{-1}(\hat{\phi}^F_V(a,F(q))).$$

Оператор $\hat{\phi}^F_V$ является доопределением оператора ϕ^F_V, значит для всех $q \in Q$ верно

$$\hat{\phi^F_V}(a,F(q)) = \phi^F_V(a,F(q)),$$

так как согласно определению 26 значения этих операторов совпадают на множестве определения оператора ϕ^F_V. Следовательно для всех $q \in Q$

$$\varphi^{\hat{F}}_{\hat{\phi}^F_V}(a,q) = \hat{F}^{-1}(\phi^F_V(a,F(q))).$$

Поскольку согласно определению 25 для любого $q \in Q$ его образ $\phi^F_V(a,F(q))$ принадлежит R, то для каждого $q \in Q$

$$\hat{F}^{-1}(\phi^F_V(a,F(q))) = F^{-1}(\phi^F_V(a,F(q))).$$

Значит для каждого $q \in Q$

$$\varphi^{\hat{F}}_{\hat{\phi}^F_V}(a,q) = F^{-1}(\phi^F_V(a,F(q))).$$

По построению оператора ϕ^F_V для всех $a \in E_2$ и $q \in Q$ верно равенство

$$\varphi^{\hat{F}}_{\hat{\phi}^F_V}(a,q) = F^{-1}(F(\varphi(a,F^{-1}(F(q))))) = \varphi(a,q).$$

Значит, переходная система $V^{\hat{F}}_{\hat{\phi}^F_V}$ является доопределением переходной системы V.

Согласно лемме 9 кодирование $\hat{F}$ по переходной системе $V^{\hat{F}}_{\hat{\phi}^F_V}$ порождает оператор $\hat{\phi}^F_V$. По условию леммы все элементы $\mathcal{F}_{\hat{\phi}^F_V}$ являются линейными функциями, значит переходная система $V^{\hat{F}}_{\hat{\phi}^F_V}$ является линейно реализуемой. □

Определение 32. Пусть задана нумерованная переходная система $V = (E_2, Q, \varphi)$, где $Q = \{0, \ldots, n-1\}$. *Сложностью переходной переходной системы* V назовем миннимальную сложность среди всех доопределений оператора ϕ^F_V, порождаемых всеми кодированиями F или $L_{deg}(V) = min_F L(\hat{\phi^F_V})$.

Теорема 4. *Пусть задана нумерованная переходная система* $V = (E_2, Q, \varphi)$, *где* $Q = \{0, \ldots, n-1\}$. *Тогда* $L_{deg}(V) \leq 2$.

Доказательство. Пусть задана нумерованная переходная система $V = (E_2, Q, \varphi)$. Обозначим ее порождающие через p_0 и p_1. Согласно лемме 20 они линейно реализуемы посредством простого позиционного кодирования F_{pos}. Рассмотрим линейные доопределения ϕ_{p_0} и ϕ_{p_1} булевых операторов, сопоставляемые подстановкам p_0 и p_1 кодированием F_{pos}. Рассмотрим множества функций

$$\mathcal{F}_{\phi_{p_0}} = \{f^0_0(q_0, q_1, \ldots, q_{n-1}), \ldots, f^0_{n-1}(q_0, q_1, \ldots, q_{n-1})\}$$

и

$$\mathcal{F}_{\phi_{p_1}} = \{f^1_0(q_0, q_1, \ldots, q_{n-1}), \ldots, f^1_{n-1}(q_0, q_1, \ldots, q_{n-1})\},$$

определяемых операторами ϕ_{p_0} и ϕ_{p_1}. Покажем, что функции

$$\mathcal{F} = \{x \cdot (f^0_0(q_0, q_1, \ldots, q_{n-1}) \oplus f^1_0(q_0, q_1, \ldots, q_{n-1})) \oplus f^0_0(q_0, q_1, \ldots, q_{n-1}),$$

$$\ldots$$

$$x \cdot (f^0_{n-1}(q_0, q_1, \ldots, q_{n-1}) \oplus f^1_{n-1}(q_0, q_1, \ldots, q_{n-1})) \oplus f^0_{n-1}(q_0, q_1, \ldots, q_{n-1})\}$$

задают оператор ϕ, являющийся доопределением оператора $\phi^{F_{pos}}_V$.

Согласно определению порождающих внутренней полугруппы переходной системы верны равенства $\varphi(0, q) = p_0(q), \varphi(1, q) = p_1(q)$. Пусть

$(\alpha_0, \ldots, \alpha_{n-1})$ код некоторого состояния $q \in Q$ при кодировании F_{pos}. Рассмотрим значение оператора $\phi_V^{F_{pos}}$ на наборах $(0, \alpha_0, \ldots, \alpha_{n-1})$.

$$\phi_V^{F_{pos}}(0, \alpha_0, \ldots, \alpha_{n-1}) = F_{pos}(\varphi(0, F_{pos}^{-1}(\alpha_0, \ldots, \alpha_{n-1}))) =$$

$$= F_{pos}(p_0(F_{pos}^{-1}(\alpha_0, \ldots, \alpha_{n-1}))) = \phi_{p_0}(\alpha_0, \ldots, \alpha_{n-1}) =$$

$$= (f_0^0(q_0, q_1, \ldots, q_{n-1}), \ldots, f_{n-1}^0(q_0, q_1, \ldots, q_{n-1})) = \phi(0, \alpha_0, \ldots, \alpha_{n-1}).$$

Рассмотрим значение оператора $\phi_V^{F_{pos}}$ на наборах $(1, \alpha_0, \ldots, \alpha_{n-1})$

$$\phi_V^{F_{pos}}(1, \alpha_0, \ldots, \alpha_{n-1}) = F_{pos}(\varphi(1, F_{pos}^{-1}(\alpha_0, \ldots, \alpha_{n-1}))) =$$

$$= F_{pos}(p_1(F_{pos}^{-1}(\alpha_0, \ldots, \alpha_{n-1}))) = \phi_{p_1}(\alpha_0, \ldots, \alpha_{n-1}) =$$

$$= (f_0^1(q_0, q_1, \ldots, q_{n-1}), \ldots, f_{n-1}^1(q_0, q_1, \ldots, q_{n-1})) = \phi(0, \alpha_0, \ldots, \alpha_{n-1}).$$

Из полученных равенств следует, что оператор ϕ совпадает с $\phi_V^{F_{pos}}$ на области определения оператора $\phi_V^{F_{pos}}$. Поскольку функции из наборов $\mathcal{F}_{\phi_{p_0}}$ и $\mathcal{F}_{\phi_{p_1}}$ линейные, функции из набора $\mathcal{F}$ задаются полиномами Жегалкина степени не выше 2. □

Следствие 5. *Нумерованная переходная система $V = (E_2, Q, \varphi)$, у которой функция переходов фиктивным образом зависит от входа является линейно реализуемой.*

Пример 26. Рассмотрим переходную систему V, изображенную на рисунке 3.2

Данная переходная система и кодирование

q	0	1	2	3	4	5	6	7
$F_{pos}(q)$	00000001	00000010	00000100	00001000	00010000	00100000	01000000	10000000

порождают булев оператор

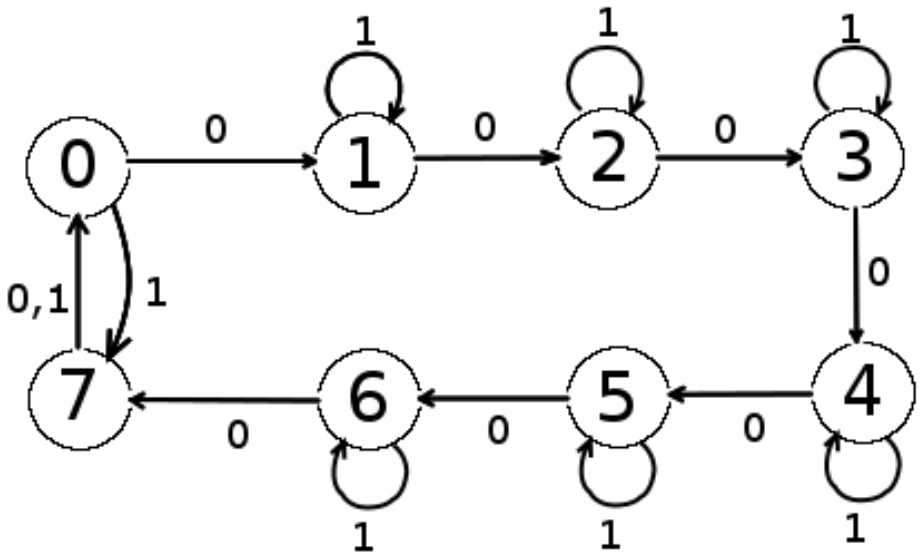

Рис. 3.2. Переходная система, не являющаяся линейно реализуемой

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_3(t)$	$q_4(t)$	$q_5(t)$	$q_6(t)$	$q_7(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$	$q_3(t+1)$	$q_4(t+1)$	$q_5(t+1)$	$q_6(t+1)$	$q_7(t+1)$
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0
1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0
1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
1	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Можно видеть, что канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = q_3(0) = q_4(0) = q_5(0) = q_6(0) = q_7(0) = 0 \\ q_0(t+1) = x(t) \cdot q_1(t) + x(t) \cdot q_7(t) + q_1(t) \\ q_1(t+1) = x(t) \cdot q_2(t) + x(t) \cdot q_1(t) + q_2(t) \\ q_2(t+1) = x(t) \cdot q_3(t) + x(t) \cdot q_2(t) + q_3(t) \\ q_3(t+1) = x(t) \cdot q_4(t) + x(t) \cdot q_3(t) + q_4(t) \\ q_4(t+1) = x(t) \cdot q_5(t) + x(t) \cdot q_4(t) + q_5(t) \\ q_5(t+1) = x(t) \cdot q_6(t) + x(t) \cdot q_5(t) + q_6(t) \\ q_6(t+1) = x(t) \cdot q_7(t) + x(t) \cdot q_6(t) + q_7(t) \\ q_7(t+1) = x(t) \cdot q_0(t) + x(t) \cdot q_0(t) + q_0(t) \end{cases}$$

Теорема 5. *Пусть задана линейно реализуемая нумерованная переходная система $V = (E_2, Q, \varphi)$, где $Q = \{0, \ldots, n-1\}$. Тогда существует такое кодирование $F : Q \to E_2^k$, где $k \leq 2^n$, что переходная система V линейно реализуема посредством F.*

Доказательство. Пусть задана нумерованная переходная система $V = (E_2, Q, \varphi)$, где $Q = \{0, \ldots, n-1\}$, линейно реализуемая посредством кодирования $F : Q \to E_2^k$, где $k > 2^n$. Рассмотрим матрицу кодов, задаваемых кодированием F,

$$T = \begin{pmatrix} F(0) \\ F(1) \\ \ldots \\ F(n-1) \end{pmatrix}.$$

Столбцы этой матрицы имеют длину n и состоят из 0 и 1. Число различных векторов длины n из 0 и 1 равно 2^n. Число столбцов в матрице равно k. Так как $k > 2^n$, то в данной матрице найдутся два равных столбца. Без ограничения общности считаем, что равны первый и второй столбцы, т.е. для любого $q \in Q$, из условия $(\alpha_0, \alpha_1, \ldots, \alpha k - 1 = F(q)$ следует, что $\alpha_0 = \alpha_1$.

Обозначим через ϕ_L линейное доопределение оператора ϕ_V^F. Согласно определению 26 доопределения оператора для всех $a \in E_2$ и $q \in Q$

$$\phi_L(a, F(q)) = \phi_V^F(a, F(q)).$$

Следовательно для всех $a \in E_2$ и $q \in Q$

$$f_i(a, F(q)) = g_i(a, F(q)),$$

где $f_i \in \mathcal{F}_{\phi_L}, g_i \in \mathcal{F}_{\phi_V^F}$. Причем f_i - линейные функции, где $0 \leq i \leq k-1$, т.е.

$$f_i(x, q_0, q_1, \ldots, q_{k-1}) = c \cdot x + \sum_{l=0}^{k-1} c_l \cdot q_l.$$

Согласно определению оператора 25 $\phi_V^F(a, F(q)) \in F(Q)$. Значит, для всех $a \in E_2$ и $q \in Q$

$$g_0(a, F(q)) = g_1(a, F(q)),$$

где $g_0, g_1 \in \mathcal{F}_{\phi_V^F}$. Поскольку для всех $a \in E_2$ и $q \in Q$

$$g_0(a, F(q)) = f_0(a, F(q)),$$

$$g_1(a, F(q)) = f_1(a, F(q)),$$

где $f_0 \in \mathcal{F}_{\phi_L}, g_0 \in \mathcal{F}_{\phi_V^F}, f_1 \in \mathcal{F}_{\phi_L}, g_1 \in \mathcal{F}_{\phi_V^F}$, верно, что для всех $a \in E_2$ и $q \in Q$

$$f_0(a, F(q)) = f_1(a, F(q)).$$

По кодированию $F : Q \to E_2^k$ построим кодирование $F' : Q \to E_2^{k-1}$ по следующему правилу: если $F(q) = (\alpha_0, \alpha_1, \ldots, \alpha_{k-1})$, то $F'(q) = (\alpha_1, \ldots, \alpha_{k-1})$. Заметим, что по определению кодирования, если $q \neq q'$, то $F(q) = (\alpha_0, \alpha_1, \ldots, \alpha_{k-1}) \neq (\alpha'_0, \alpha'_1, \ldots, \alpha'_{k-1}) = F(q')$. Значит существует такое i, что $\alpha_i = \alpha'_i$.

Если $i > 0$, то $(\alpha_1, \ldots, \alpha_{k-1}) \neq (\alpha'_1, \ldots, \alpha'_{k-1})$. Если $i = 0$, то заметим, что $\alpha_0 = \alpha_1$ и $\alpha'_0 = \alpha'_1$, и следовательно, $\alpha_1 \neq \alpha'_1$, что означает $(\alpha_1, \ldots, \alpha_{k-1}) \neq (\alpha'_1, \ldots, \alpha'_{k-1})$. Таким образом показано, что отображение

F' взаимоднозначно на Q.

Рассмотрим оператор переходной системы, построенный посредством кодирования F'.

$$\phi_V^{F'}(a, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}) = F'(\varphi(a, F'^{-1}(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}))) =$$

$$= F'(\varphi(a, F^{-1}(\alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}))) =$$

$$= (g_1(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), \ldots, g_{k-1}(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1})),$$

где $g_i \in \mathcal{F}_{\phi_V^F}$. Последнее равенство следует из построения кодирования F' и равенства

$$F(\varphi(a, F^{-1}(\alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}))) =$$

$$= (g_0(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), g_1(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), \ldots,$$

$$g_{k-1}(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1})).$$

Как было показано раннее, функции f_i и g_i равны для всех $a \in E_2$ и $q \in Q$. Следовательно, верно равенство

$$(g_1(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), \ldots, g_{k-1}(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1})) =$$

$$= (f_1(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}), \ldots, f_{k-1}(a, \alpha_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1})),$$

где $f_i \in \mathcal{F}_{\phi_L}$. То есть множество $\mathcal{F}_{\phi_V^{F'}}$ составляют функции, полученые из линейных операцией отождествления первого и второго аргументов. При такой операции функции остаются линейными[10].

Таким образом показано, что если переходная системы линейно реализуема посредством кодирования, которое кодирует состояния кодами длины k больше чем 2^n, то можно построить кодирование, которое кодирует состояния кодами длины $k-1$, посредством которого переходная система линейно реализуема. Повторяя данные построения, придем к кодированию, которое кодирует состояния кодами длины 2^n.

□

Глава 4

Максимальная вариативность относительно кодирования состояний

В данной главе изучаются «максимально реализуемые» переходные системы. Каждое кодирование множества состояний порождает по переходной системе булев оператор. Естественным является вопрос какое множество операторов возникает при всевозможных кодированиях множества состояний и, в частности, какова его мощность. В первую очередь представляет интерес вопрос существуют ли такие переходные системы, что для двух различных кодирований возникаемые операторы различны. В данной главе изучаются переходные системы с числом состояний $n = 2^k$.

4.1 Критерий свойства максимальности

Определение 33. Нумерованная переходная система $V = (E_2, Q, \varphi)$ с n состояниями обладает *свойством максимальности*, если все операторы, задаваемые всевозможными неизбыточными кодированиями множества Q,

различны.

Пример 27. На рисунке 4.1 изображена переходная система V, не обладающей свойством максимальности. Построим оператор $\phi_V(F_1)$ по переходной

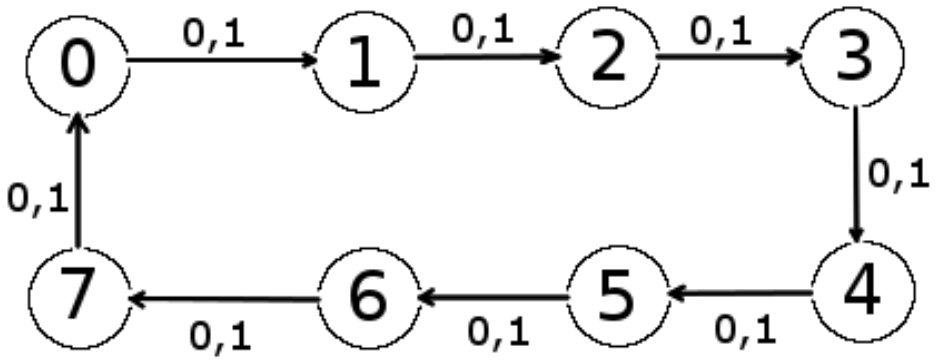

Рис. 4.1. Переходная система, не обладающая свойством максимальности.

системе V и кодированию F_1

q	0	1	2	3	4	5	6	7
$F_1(q)$	000	001	010	011	100	101	110	111

Оператор $\phi_V(F_1)$ имеет вид

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$
0	0	0	0	0	0	1
0	0	0	1	0	1	0
0	0	1	0	0	1	1
0	0	1	1	1	0	0
0	1	0	0	1	0	1
0	1	0	1	1	1	0
0	1	1	0	1	1	1
0	1	1	1	0	0	0
1	0	0	0	0	0	1
1	0	0	1	0	1	0
1	0	1	0	0	1	1
1	0	1	1	1	0	0
1	1	0	0	1	0	1
1	1	0	1	1	1	0
1	1	1	0	1	1	1
1	1	1	1	0	0	0

Теперь построим оператор $\phi_V(F_2)$ по переходной системе V и кодированию F_2

q	0	1	2	3	4	5	6	7
$F_2(q)$	001	010	011	100	101	110	111	000

Оператор $\phi_V(F_2)$ имеет вид

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$
0	0	0	0	0	0	1
0	0	0	1	0	1	0
0	0	1	0	0	1	1
0	0	1	1	1	0	0
0	1	0	0	1	0	1
0	1	0	1	1	1	0
0	1	1	0	1	1	1
0	1	1	1	0	0	0
1	0	0	0	0	0	1
1	0	0	1	0	1	0
1	0	1	0	0	1	1
1	0	1	1	1	0	0
1	1	0	0	1	0	1
1	1	0	1	1	1	0
1	1	1	0	1	1	1
1	1	1	1	0	0	0

Как видно, операторы $\phi_V(F_1)$ и $\phi_V(F_2)$ равны. Значит, переходная система V не обладает свойством максимальности.

Теорема 6. *Нумерованная переходная система $V = (E_2, Q, \varphi)$ не обладает свойством максимальности тогда и только тогда, когда существует такая нетривиальная подстановка s, что $s \cdot p_0 = p_0 \cdot s$ и $s \cdot p_1 = p_1 \cdot s$.*

Доказательство. Пусть нумерованная переходная система $V = (E_2, Q, \varphi)$ не обладает *свойством максимальности*. Следовательно найдутся два различных кодирования F_1 и F_2, порождающие один булев оператор ϕ. Рассмотрим операторы $\phi_V^{F_1}$ и $\phi_V^{F_2}$, порождаемый этими кодированиями. Для всех $a \in E_2, \alpha_i \in E_2$ верно

$$F_1(\varphi(a, F_1^{-1}(\alpha_0, \ldots, \alpha_{k-1}))) = \phi_V^{F_1}(a, \alpha_0, \ldots, \alpha_{k-1}) =$$

$$= \phi_V^{F_2}(a, \alpha_0, \ldots, \alpha_{k-1}) = F_2(\varphi(a, F_2^{-1}(\alpha_0, \ldots, \alpha_{k-1}))).$$

е Следовательно, для всех $a \in E_2, \alpha_i \in E_2$

$$F_2^{-1}(F_1(\varphi(a, F_1^{-1}(\alpha_0, \ldots, \alpha_{k-1})))) = (\varphi(a, F_2^{-1}(\alpha_0, \ldots, \alpha_{k-1}))). \qquad (4.1)$$

Заметим, что для всех $\alpha_i \in E_2$ верно

$$(F_1(F_1^{-1}(\alpha_0, \ldots, \alpha_{k-1}))) = (\alpha_1, \ldots, \alpha_{k-1}) = (F_2(F_2^{-1}(\alpha_0, \ldots, \alpha_{k-1}))).$$

Следовательно, для всех $\alpha_i \in E_2$

$$(F_1^{-1}(\alpha_0, \ldots, \alpha_{k-1})) = F_1^{-1}(F_2(F_2^{-1}(\alpha_0, \ldots, \alpha_{k-1}))).$$

Подставим полученное выражение в уравнение (4.1), для всех $a \in E_2, \alpha_i \in E_2$

$$F_2^{-1}(F_1(\varphi(a, F_1^{-1}(F_2(F_2^{-1}(\alpha_0, \ldots, \alpha_{k-1})))))) = \varphi(a, F_2^{-1}(\alpha_0, \ldots, \alpha_{k-1})).$$

Отметим, что поскольку кодирование это биективное отображение, следовательно образ F_2^{-1} есть все Q. Следовательно, для всех $a \in E_2, q \in Q$

$$F_2^{-1}(F_1(\varphi(a, F_1^{-1}(F_2(q))))) = \varphi(a, q).$$

Также отметим, что $F_2^{-1}(F_1(q))$ задает взаимно-однозначное отображение на множестве $Q = \{0, 1, \ldots, n-1\}$. Обозначим это отображение через s. Поскольку кодирования F_1 и F_2 различны, то подстановка s отлична от тождественной. Действительно, пусть $F_1(q) \neq F_2(q)$ для некоторого $q \in Q$. Так как F_2 — взаимно-однозначное отображение, то $F_2^{-1}(F_1(q)) \neq q$. Полученное равенство означает, что для всех $a \in E_2, q \in Q$

$$s(\varphi(a, s^{-1}(q)) = \varphi(a, q).$$

А следовательно, для всех $q \in Q$

$$s(\varphi(0, s^{-1}(q)) = \varphi(a, q),$$

$$s(\varphi(0, s^{-1}(q)) = \varphi(a, q).$$

Таким образом указана нетривиальная подстановка, коммутирующая с порождающими внутренней полугруппы переходной системы.

Теперь докажем теорему в обратную сторону. Пусть задана нумерованная переходная система $V = (E_2, Q, \varphi)$. Обозначим через p_0 отображение, задаваемое входным символом 0, через p_1 — отображение, задаваемое входным символом 1. Предположим, что существует такая нетривиальная подстановка s, что $s \cdot p_0 = p_0 \cdot s$ и $s \cdot p_1 = p_1 \cdot s$. Рассмотрим «стандартное» кодирование F_0 и кодирование F_s, определяемое по правилу

$$F_s(q) = F_0(s(q)),$$

где $q \in Q = \{0, \ldots, n-1\}$. Поскольку подстановка s нетривиальна, а отображение F_0 взаимно-однозначно, кодирования F_0 и F_s различны. Рассмотрим булевы операторы порождаемые этими кодированиями. Оператор, порождаемый кодированием F_0, определяется по правилу

$$\phi_V^{F_0}(a, \alpha_1, \ldots, \alpha_k) = F_0(\varphi(a, F_0^{-1}(\alpha_1, \ldots, \alpha_k))),$$

где $a \in E_2, \alpha_i \in E_2$.

Оператор, порождаемый кодированием F_s, определяется по правилу

$$\phi_V^{F_s}(a, \alpha_1, \ldots, \alpha_k) = F_s(\varphi(a, F_s^{-1}(\alpha_1, \ldots, \alpha_k))),$$

где $a \in E_2, \alpha_i \in E_2$.

Из определения F_s следует, что

$$\phi_V^{F_s}(a, \alpha_1, \ldots, \alpha_k) = F_0(s(\varphi(a, s^{-1}(F_0^{-1}(\alpha_1, \ldots, \alpha_k))))),$$

где $a \in E_2, \alpha_i \in E_2$.

Поскольку подстановка s коммутирует с порождающими внутренней полу-

группы переходной системы V, для всех $a \in E_2, q \in Q$

$$s(\varphi(a, s^{-1}(q))) = \varphi(a, q).$$

Следовательно, для всех $a \in E_2, \alpha_i \in Q$

$$\phi_V^{F_s}(a, \alpha_1, \ldots, \alpha_k) = F_0(s(\varphi(a, s^{-1}(F_0^{-1}(\alpha_1, \ldots, \alpha_k))))) =$$

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

Таким образом указаны два различных кодирования, порождающих один булев оператор. Переходная система не обладает *свойством максимальности* □

Следствие 6. *Нумерованная переходная система $V = (E_2, Q, \varphi)$ обладает свойством максимальности тогда и только тогда, когда не существует такой нетривиальной подстановки s, что $s \cdot p_0 = p_0 \cdot s$ и $s \cdot p_1 = p_1 \cdot s$.*

Замечание 2. Заметим, что если порождающие внутренней полугруппы переходной системы коммутируют с нетривиальной подстановкой s, то все элементы внутренней полугруппы коммутируют с s. Известно, что группы S_n при $n \geq 3$ и A_n при $n \geq 4$ имеют тривиальный центр [14]. Учитывая данный факт и следствие 6, верны утверждения:

- переходная система, чья внутренняя полугруппа есть S_n, где $n \geq 3$, обладает свойством максимальности;
- переходная система, чья внутренняя полугруппа есть A_n, где $n \geq 4$, обладает свойством максимальности;

Пример 28. На рисунке 4.2 изображена переходная система V, не обладающей свойством максимальности. Порождающие переходной системы V есть

$$p_0 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 2 & 3 & 4 & 5 & 6 & 0 \end{pmatrix} = (07),$$

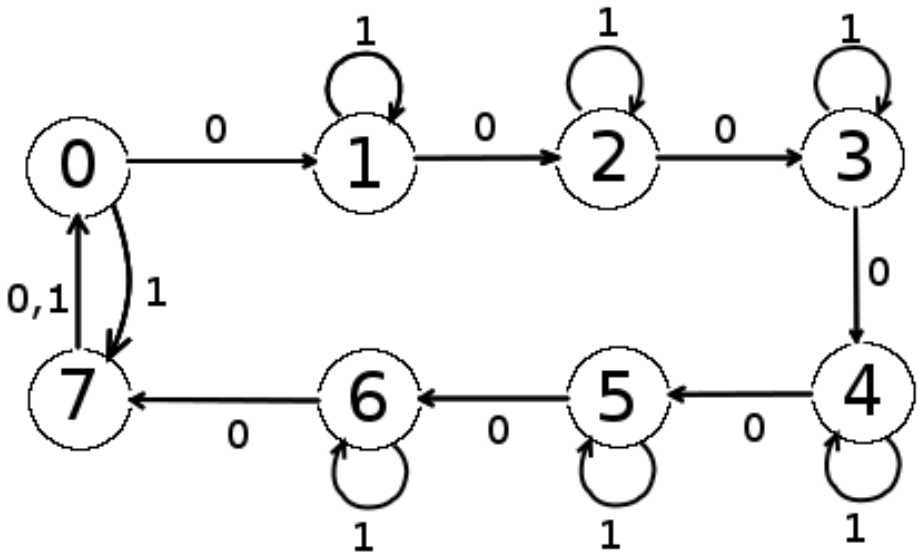

Рис. 4.2. Переходная система, обладающая свойством максимальности.

$$p_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \end{pmatrix} = (01234567).$$

Так как транспозция (07) и цикл (01234567) порождают симметрическую группу S_8 [14], то внутренняя полугруппа S_V переходной системы V есть S_8. Принимая во внимание замечание 2, можно утверждать, что данная переходная система обладает свойством максимальности.

Чтобы переходная система не обладала свойством максимальности необходимо и достаточно, чтобы порождающие внутренней полугруппы, индуцированные входными буквами, коммутировали с некоторой нетривиально подстановкой. Далее изучаются отображения множества E_n в себя, коммутирующие с некотрой подстановкой.

Определение 34. Подстановка s сохраняет множество $N \subseteq Q = \{0, \ldots, n-1\}$, если множества N и $s(N)$ равны.

Лемма 22. *Пусть подстановка $s : E_n \to E_n$ и отображение $p : Q \to Q$ коммутируют, т.е. $s \cdot p = p \cdot s$. Если подстановка s сохраняет множество $N \subseteq E_n = \{0, \ldots, n-1\}$, то:*

i) подстановка s сохраняет полный прообраз отображения p множе-

ства N;

ii) подстановка s сохраняет образ отображения p множества N;

Доказательство. Обозначим через N' — полный прообраз отображения p множества N, т.е. множество всех таких $q \in E_n$, что $p(q) \in N$. Предположим, что s не сохраняет N'.

Поскольку s — подстановка, найдется такое $q \in N'$, что $s(q) \notin N'$, т.е. $s(q)$ не лежит в прообразе отображения p множества N. Следовательно $p(s(q)) \notin N$. Поскольку p и s коммутируют, $p(s(q)) = s(p(q)) \notin N$.

Однако, так как $q \in N'$, то $p(q) \in N$. А так как s сохраняет множество N, то $s(p(q)) \in N$. Полученное противоречие доказывает утвержении i).

Докажем утверждение ii. Так как подстановка s сохраняет множество N, т.е. $s(N) = N$, то $p(s(N)) = p(N)$. Поскольку s и p коммутируют, то для всех $q \in N$

$$s(p(q)) = p(s(q)).$$

Следовательно $s(p(N)) = p(N)$, что доказывает утверждении ii).

□

Лемма 23. *Пусть задана подстановка $s = (i_1, \ldots, i_l)$, где $Q_1 = \{i_1, \ldots, i_l\}$. Обозначим через $Q_2 = E_n \setminus Q_1$. Тогда отображение p множества E_n в себя, с ней коммутирующее, имеет один следующих видов: либо*

$$p = \begin{pmatrix} \ldots i_1 \ldots i_l \ldots \\ \ldots s^m(i_1) \ldots s^m(i_l) \ldots \end{pmatrix},$$

где $0 \leq m \leq l-1$, и $p(j) \in Q_2$ для всех $j \in Q_2$, либо

$$p = \begin{pmatrix} \ldots i_1 \ldots i_l \ldots \\ \ldots i' \ldots i' \ldots \end{pmatrix},$$

где $i' \in Q_2$ и $p(i) \in Q_2$ для всех $i \in Q_2$.

Доказательство. Пусть отображение p коммутирует с s. Заметим, что $s(j) = j$ для всех $j \in Q_2$, т.е. s сохраняет одно-элементные множества $\{j\}$,

где $j \in Q_2$. Значит, согласно лемме 23, если отображение p коммутирует с s, то $s(p(j)) = p(j)$ для всех $j \in Q_2$. Следовательно $p(Q_2) \subseteq Q_2$.

Так как подстановка s сохраняет множество Q_1, то подстановка s сохраняет множество $p(Q_1)$. Если множество $p(Q_1)$ содержит i_p, то это множество содержит также $s(i_p)$, а также $s(s(i_p))$, $s^3(i_p)$,...,$s^l(i_p)$. То есть, если множество $p(Q_1)$ содержит элемент множества Q_1, то оно содержит и все множество Q_1. Отсюда следует, что либо $p(Q_1) = Q_1$, либо $p(Q_1) \subseteq Q_2$.

Пусть $p(Q_1) \subseteq Q_2$, то есть $p(i_1) = k_1, p(i_2) = k_2, \ldots, p(i_l) = k_l$, где $k_1, k_2, \ldots, k_l \in Q_2$. Подстановка s сохраняет одно-элементное множество $\{k_1\}$, значит, подстановка s сохраняет и полный прообраз отображения p этого множества. Следовательно $s(i_1)$ лежит в полном прообразе отображения p множества $\{k_1\}$, то есть $k1 = p(s(i_1)) = p(i_2) = k_2$. Продолжая рассуждения получаем, что $k_1 = k_2 = \ldots = k_l$. В этом случае подстановка имеет вид

$$p = \begin{pmatrix} \ldots i_1 \ldots i_l \ldots \\ \ldots k \ldots k \ldots \end{pmatrix},$$

где $k \in Q_2$ и $p(j) \in Q_2$ для всех $j \in Q_2$.

Рассмотрим второй случай. Пусть $p(i_1) = i_k = s^{k-1}(i_1)$. Поскольку p коммутирует с s, то

$$p(i_2) = p(s(i_1)) = s(p(i_1)) = s(s^{k-1}(i_p) = s^{k-1}(s(i_1)) = s^{p-1}(i_2).$$

Продолжая рассуждения получим, что для всех $i_m \in Q_1$

$$p(i_m) = s^{k-1}(i_m).$$

В этом случае подстановка имеет вид

$$p = \begin{pmatrix} \ldots i_1 \ldots i_l \ldots \\ \ldots s^{k-1}(i_1) \ldots s^{k-1}(i_l) \ldots \end{pmatrix},$$

где $0 \leq k-1 \leq l-1$ и $p(j) \in Q_2$ для всех $j \in Q_2$. □

Следствие 7. *Пусть задана подстановка* $s = c_1 \cdot \ldots \cdot c_k$, *где* $c_j =$

$(i_1^j \dots i_l^j), j = 1, \dots, k$. *Обозначим через* $Q_j = \{i_1^j, \dots, i_l^j\}, j = 1, \dots, k$. *Тогда отображение* p *множества* E_n, *коммутирующее с* s, *имеет следующий вид*

$$p = \begin{pmatrix} \dots i_1^1 \dots i_l^1 \dots i_1^2 \dots i_l^2 \dots i_1^k \dots i_l^k \dots \\ \dots i'^1_1 \dots i'^1_l \dots i'^2_1 \dots i'^2_l \dots i'^k_1 \dots i'^k_l \dots \end{pmatrix},$$

где для каждого j *множество* $\{i'^j_1, \dots, i'^j_l\}$ *либо совпадает с* Q_t *для некоторого* $t \in \{1, \dots, k\}$, *либо* $i'^j_1 = i'^j_2 = \dots = i'^j_l$ *и не существует такого* $t \in \{1, \dots, k\}$, *что* Q_t *содержит* $\{i'^j_1, \dots, i'^j_l\}$.

Доказательство. Пусть отображение p коммутирует с s. Заметим, что $s(j) = j$ для всех $j \in Q \setminus \bigcup_{1 \le t \le k} Q_t$, т.е. s сохраняет одно-элементные множества $\{j\}$, где $j \in Q \setminus \bigcup_{1 \le t \le k} Q_t$. Значит, согласно лемме 23, если отображение p коммутирует с s, то $s(p(j)) = p(j)$ для всех $j \in Q \setminus \bigcup_{1 \le t \le k} Q_t$. Следовательно $p(Q \setminus \bigcup_{1 \le t \le k} Q_t) \subseteq Q \setminus \bigcup_{1 \le t \le k} Q_t$.

Так как подстановка s сохраняет множества Q_t, где $1 \le t \le k$, то подстановка s сохраняет множество $p(Q_t)$, где $1 \le t \le k$. Если множество $p(Q_t)$ содержит $i_m^{t'}$, то это множество содержит также $s(i_m^{t'})$, а также $s(s(i_m^{t'}))$, $s^3(i_m^{t'}), \dots, s^l(i_m^{t'})$. То есть, если множество $p(Q_t)$ содержит элемент множества $Q_{t'}$, то оно содержит и все множество $Q_{t'}$. Отсюда следует, что либо $p(Q_t) = Q_{t'}$, либо $p(Q_t) \subseteq Q \setminus \bigcup_{1 \le t \le k} Q_t$.

Пусть $p(Q_t) \subseteq Q \setminus \bigcup_{1 \le t \le k} Q_t$, то есть $p(i_1^t) = i'_1, p(i_2^t) = i'_2, \dots, p(i_l^t) = i'_l$, где $i'_1, i'_2, \dots, i'_l \in Q \setminus \bigcup_{1 \le t \le k} Q_t$. Подстановка s сохраняет одно-элементное множество $\{i'_1\}$, значит, подстановка s сохраняет и полный прообраз отображения p этого множества. Следовательно $s(i_1^t)$ лежит в полном прообразе отображения p множества $\{i'_1\}$, то есть $i'_1 = p(s(i_1^t)) = p(i_2^t) = i'_2$. Продолжая рассуждения получаем, что $i'_1 = i'_2 = \dots = i'_l$. □

Лемма 24. *Пусть задана подстановка* $s = (i_1, \dots, i_l)$ *на множестве* $E_n = \{0, \dots, n-1\}$. *Тогда число отображений с ней коммутирующих равно либо* $n(n-l)^{n-l}$, *если* $2 \le l < n$, *либо* n, *если* $l = n$.

Доказательство. Посчитаем количество подстановок первого и второго

вида коммутирующих с подстановкой $s = (i_1, \ldots, i_l)$, если $2 \leq l < n$. В этом случае множество $Q_2 = Q \setminus \{i_1, \ldots, i_l\}$ не пусто. Заметим, что число отображений множества Q_2 в себя равно $(n-l)^{n-l}$. Число отображений множества $Q_1 = \{i_1, \ldots, i_l\}$ в себя образом задаваемым подстановкой типа (1) равно l. Следовательно число подстановок, коммутируюших с s, первого типа равно $l(n-l)^{n-l}$. Отметим, что число отображений множества Q_1 в себя образом, задаваемым подстановкой типа (2) равно $(n-l)$. Следовательно число подстановок, коммутируюших с s, второго типа равно $(n-l)(n-l)^{n-l}$. Таким образом общее число подстановок, коммутирующих с s, если $2 \leq l < n$, равно $n(n-l)^{n-l}$. Если $l = n$, то множество Q_2 пусто. При этом число коммутирующих подстановок первого типа равно n. А подстановок второго типа, коммутирующих с подстановкой s, не существует. □

Лемма 25. *Пусть задана подстановка $s = c_1 \cdot \ldots \cdot c_k$, где $c_j = (i_1^j \ldots i_m^j), j = 1, \ldots, k$. Обозначим через $Q_j = \{i_1^j, \ldots, i_m^j\}, j = 1, \ldots, k$. Обозначим через $l = m \cdot k$. Тогда число подстановок с ней коммутирующих равно $n^k(n-l)^{n-l}$, если $\bigcup_{1 \leq j \leq k} Q_j \subset Q$, и равно n^k, если $\bigcup_{1 \leq j \leq k} Q_j = Q$.*

Доказательство. Пусть $\bigcup_{1 \leq j \leq k} Q_j \subset Q$. Обозначим $Q_0 = Q \setminus \bigcup_{1 \leq j \leq k} Q_j$. Согласно следствию 3 образ множества $(i_1^j \ldots i_m^j)$ есть либо элемент k множества Q_0, таких элементов l, либо множество Q_t, таких множеств k, а способов отображения m, то есть $m \cdot k$ отображений. Суммируя получаем $|Q_0| + k \cdot m = n - l + l = n$. Поскольку число множеств Q_j равно k, получаем что число отображений элементов из $\bigcup_{1 \leq j \leq k} Q_j$ равно n^k. Согласно следствию 3 образами элементов Q_0 являются элементы Q_0. Таких отображений $(n-l)^{n-l}$. Следовательно всего отображений $n^k(n-l)^{n-l}$. Пусть $\bigcup_{1 \leq j \leq k} Q_j = Q$. Тогда множество Q_0 пусто. Значит образ множества $(i_1^j \ldots i_m^j)$ есть одно из множеств Q_t, таких множеств k, а способов отображения m, то есть $m \cdot k$ отображений. Суммируя получаем $k \cdot m = l = n$. Число подстановок, коммутирующих с s, равно n^k □

4.2 Линейная реализуемость и свойство максимальности

4.2.1 $M(n) \setminus L(n)$

Для произвольного $n = 2^k$ приведем пример переходной системы, обладающей *свойством максимальности*, но не являющейся линейно реализуемой. Рассмотрим нумерованную переходную систему
$V = (E_2, \{0, 1, \ldots, n-1\}, \varphi)$, чья функция переходов определяется как:

$$\varphi(0,0) = 1$$

$$\varphi(0,1) = 0$$

$$\varphi(0,q) = q, 3 \leq q \leq n-1$$

$$\varphi(1,q) = q + 1 \,(mod\, n)$$

Порождающие внутренней полугруппы имеют вид:

$$p_0 = (0\,1),$$

$$p_1 = (0\,1\,\ldots\,n-1).$$

На рисунке 4.3 изображена диаграмма переходов данной переходной системы.

Заметим, что внутренняя полугруппа переходной системы V есть S_n, как транспозиция $(0\,1)$ и цикл $(0\,1\,\ldots\,n-1)$ порождают S_n [14]. Согласно замечанию 2, переходная система V обладает свойством максимальности. Теперь покажем, что данная переходная система не является линейно реализуемой. Согласно теореме 1, если переходная система V линейно реализуема, то найдется такие подстановки s и $h \in s^{-1}H_+s$, что $p_1 = p_0 \cdot h$. Так как для данной переходной системы порождающие p_0 и p_1 — подстановки, то найдется такая подстановка s, что $p_0^{-1} \cdot p_1 \in s^{-1}H_+s$. Найдем указанное

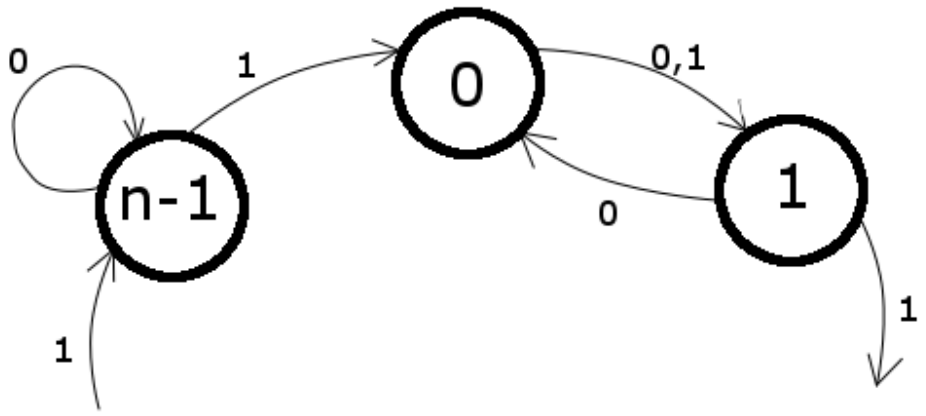

Рис. 4.3. Переходная система, обладающая свойством максимальности, но не являющаяся линейно реализуемой

произведение порождающих

$$p_0^{-1} \cdot p_1 = (0\,1)(0\,\ldots\,n-1) = (0\,2\,\ldots\,n-1),$$

т.е. $p_0^{-1} \cdot p_1$ — это цикл длины $n-1$. Подстановки, принадлежащие H_+, представляют произведение $n/2$ транспозиций. Поскольку при сопряжении цикловая структура подстановок сохраняется [14], то не существует таких подстановок s и $h \in H_+$, что $p_0^{-1} \cdot p_1 = s^{-1} \cdot h \cdot s$. Следовательно, построенная переходная система не является линейно реализуемой.

4.2.2 $L(n) \setminus M(n)$

Для произвольного $n = 2^k$ приведем пример линейно реализуемой переходной системы, но не обладающей *свойством максимальности*. Обозначим через s_{x^2} подстановку, соответствующую многочлену x^2 над полем Га-

луа F_n. Обозначим через h_{x+c} подстановку, соответствующую многочлену $x+c$ над полем Галуа F_n, где $c \neq 0$. Рассмотрим нумерованную переходную систему
$V = (E_2, \{0, 1, \ldots, n-1\}, \varphi)$, чья функция переходов определяется как:

$$\varphi(0, q) = s_{x^2}(q)$$

$$\varphi(1, q) = h_{x+c}(s_{x^2}(q))$$

Согласно построению переходной системой для ее порождающих верно равенство $p_1 = s_{x^2} \cdot h_{x+3} = p_0 \cdot h_{x+c}$, причем $h_{x+c} \in H_+$. Согласно лемме 4 отображение линейно реализуемо 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 $i = 0, .., k-1$ и константы $c \in F_{2^k}$. Следовательно, набор

$$\mathcal{F}_{p_0}(F_0) = \{f_i^{s_{x^2}}(q_0, q_1, \ldots, q_{n-1}), 0 \leq i \leq k-1\},$$

где $(q_0, q_1, \ldots q_{n-1})$ — код состояния при «стандартном» кодировании F_0, состоит из линейных функций, т.е. подстановка p_0 линейно реализуема.

Согласно следствию 1

$$\mathcal{F}_{h_{x+c}}(F_0) = \{f_i^{h_{x+c}}(q_0, q_1, \ldots, q_{n-1}) = q_i + h_i, 0 \leq i \leq k-1\},$$

где $(h_0, h_1, ...h_k) = F_0(c)$. Так как $p_1 = h_{x+c}(s_{x^2}(q))$, то согласно следствию 2

$$\mathcal{F}_{p_1}(F_0) = \{f_i^{s_x^2}(q_0, q_1, \ldots, q_{n-1}) + h_i, 0 \leq i \leq k-1\},$$

где $(h_0, h_1, ...h_k) = F_0(3)$. Следовательно, набор $\mathcal{F}_{p_1}(F_0)$ состоит из линейных функций, т.е. подстановка p_1 линейно реализуема. Согласно теореме 1 переходная система V линейно реализуема.

Теперь покажем, что подстановка, соответствующая многочлену $x+1$, коммутирует с p_0 и p_1. Обозначим ее через h_{x+1}. Для каждого $q \in F_n$ верно

равенство

$$h_{x+1}(p_0(q)) = p_0(q) + 1 = q^2 + 1.$$

С другой стороны для каждого $q \in F_n$ верно

$$p_0(h_{x+1}(q)) = p_0(q+1) = (q+1)^2.$$

Так как для элементов a, b поля Галуа F_n верно равенство $(a+b)^{2^j} = a^{2^j} + b^{2^j}$ [13], то

$$p_0(h_{x+1}(q)) = q^2 + 1.$$

Отсюда следует, что $h_{x+1}(p_0(q)) = q^2 + 1 = p_0(h_{x+1}(q))$ для всех $q \in F_n$, т.е. h_{x+1} коммутирует с p_0.

Теперь покажем, что h_{x+1} коммутирует с p_1.

$$h_{x+1}(p_1(q)) = p_1(q) + 1 = h_{x+c}(p_0(q)) + 1 = p_0(q) + c + 1 = q^2 + c + 1.$$

С другой стороны для каждого $q \in F_n$ верно

$$p_1(h_{x+1}(q)) = p_1(q+1) = h_{x+c}(p_0(q+1)) = p_0(q+1) + c = (q+1)^2 + c + 1.$$

Так как для элементов a, b поля Галуа F_n верно равенство $(a+b)^{2^j} = a^{2^j} + b^{2^j}$ [13], то

$$p_1(h_{x+1}(q)) = q^2 + 1 + c = q^2 + c + 1.$$

Отсюда следует, что $h_{x+1}(p_1(q)) = q^2 + 2 = p_1(h_{x+1}(q))$ для всех $q \in F_n$, т.е. h_{x+1} коммутирует с p_1. Следовательно согласно теореме 6 построенная переходная система не обладает *свойством максимальности.*

Пример 29. На рисунке 4.4 изображена переходная система $V_{L\setminus M}$, построенная описанным выше способом для $n = 8$ и $c = 3$.

Функция переходов $V_{L\setminus M}$ определяется как:

$\varphi(a,q)$	0	1	2	3	4	5	6	7
0	0	1	4	5	6	7	2	3
1	3	2	7	6	5	4	1	0

Порождающие внутренней полугруппы переходной системы $V_{L\setminus M}$ имеют

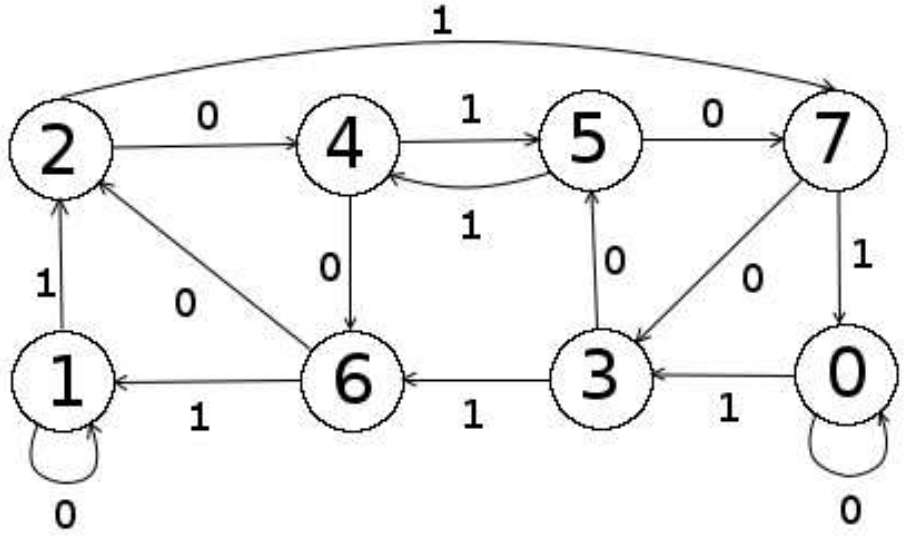

Рис. 4.4. Линейно реализуемая переходная система, не обладающая *свойством максимальности*

вид:

$$p_0 = (0)(1)(2\,4\,6)(3\,5\,7),$$

$$p_1 = (0\,3\,6\,1\,2\,7)(4\,5).$$

Построим оператор $\phi_V^{F_0}$, порождаемый переходной системой V и стандартным кодированием F_0

q	0	1	2	3	4	5	6	7
$F_0(q)$	000	001	010	011	100	101	110	111

Оператор $\phi_V^{F_0}$ имеет вид

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$
0	0	0	0	0	0	0
0	0	0	1	0	0	1
0	0	1	0	1	0	0
0	0	1	1	1	0	1
0	1	0	0	1	1	0
0	1	0	1	1	1	1
0	1	1	0	0	1	0
0	1	1	1	0	1	1
1	0	0	0	0	1	1
1	0	0	1	0	1	0
1	0	1	0	1	1	1
1	0	1	1	1	1	0
1	1	0	0	1	0	1
1	1	0	1	1	0	0
1	1	1	0	0	0	1
1	1	1	1	0	0	0

Канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = 0 \\ q_0(t+1) = q_0(t) + q_1(t) \\ q_1(t+1) = q_0(t) + x(t) \\ q_2(t+1) = q_2(t) + x(t) \end{cases}$$

Построим оператор $\phi_V^{F_1}$, порождаемый переходной системой V и кодированием $F_{h_{x+1}}$

q	0	1	2	3	4	5	6	7
$F_1(q)$	001	000	011	010	101	100	111	110

Оператор $\phi_V^{F_1}$ имеет вид

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$
0	0	0	0	0	0	0
0	0	0	1	0	0	1
0	0	1	0	1	0	0
0	0	1	1	1	0	1
0	1	0	0	1	1	0
0	1	0	1	1	1	1
0	1	1	0	0	1	0
0	1	1	1	0	1	1
1	0	0	0	0	1	1
1	0	0	1	0	1	0
1	0	1	0	1	1	1
1	0	1	1	1	1	0
1	1	0	0	1	0	1
1	1	0	1	1	0	0
1	1	1	0	0	0	1
1	1	1	1	0	0	0

Канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = 0 \\ q_0(t+1) = q_0(t) + q_1(t) \\ q_1(t+1) = q_0(t) + x(t) \\ q_2(t+1) = q_2(t) + x(t) \end{cases}$$

Как видно, операторы $\phi_V(F_0)$ и $\phi_V(F_{h_{x+1}})$ равны.

4.2.3 $M(n) \bigcap L(n)$

Для произвольного $n = 2^k$ приведем пример линейно реализуемой переходной системы, обладающей *свойством максимальности*. Мультипликативная группа $F*_n$ поля F_n циклическая. Обозначим через a образующий элемент. Обозначим через $s_{a \cdot x}$ подстановку, соответствующую многочлену

$a \cdot x$ над полем Галуа F_n. Обозначим через h_{x+1} подстановку, соответствующую многочлену $x+1$ над полем Галуа F_n. Данная подстановка имеет следующий вид $(0\,1)(2\,3)\ldots(n-2\,n-1)$. Рассмотрим нумерованную переходную систему $V = (E_2, \{0,1,\ldots,n-1\}, \varphi)$, чья функция переходов определяется как:

$$\varphi(0,q) = s_{a\cdot x}(q)$$

$$\varphi(1,q) = h_{x+1}(s_{a\cdot x}(q))$$

Согласно построению переходной системой для ее порождающих верно равенство $p_1 = s_{a\cdot x} \cdot h_{x+1} = p_0 \cdot h_{x+1}$, причем $h_{x+1} \in H_+$. Согласно лемме 4 отображение линейно реализуемо 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 $i = 0,..,k-1$ и константы $c \in F_{2^k}$. Следовательно, набор

$$\mathcal{F}_{p_0}(F_0) = \{f_i^{s_{a\cdot x}}(q_0,q_1,\ldots,q_{n-1}), 0 \le i \le k-1\},$$

где $(q_0,q_1,\ldots q_{n-1})$ — код состояния при «стандартном» кодировании F_0, состоит из линейных функций, т.е. подстановка p_0 линейно реализуема.

Согласно следствию 1

$$\mathcal{F}_{h_{x+1}}(F_0) = \{f_i^{h_{x+1}}(q_0,q_1,\ldots,q_{n-1}) = q_i + h_i, 0 \le i \le k-1\},$$

где $(h_0,h_1,...h_k) = F_0(1)$. Так как $p_1 = h_{x+1}(s_{a\cdot x}(q))$, то согласно следствию 2

$$\mathcal{F}_{p_1}(F_0) = \{f_i^{s_{a\cdot x}}(q_0,q_1,\ldots,q_{n-1}) + h_i, 0 \le i \le k-1\},$$

где $(h_0,h_1,...h_k) = F_0(1)$. Следовательно, набор $\mathcal{F}_{p_1}(F_0)$ состоит из линейных функций, т.е. подстановка p_1 линейно реализуема. По теореме 1 переходная система V линейно реализуема.

Пусть подстановка s коммутирует с p_0 и p_1. Согласно построению p_0 соответствует многочлену $a \cdot x$, p_1 соответствует многочлену $a \cdot x + 1$, т.е.

для любого $q \in E_n$

$$p_0(q) = a \cdot q,$$

$$p_1(q) = a \cdot q + 1.$$

Обозначим через f_s многочлен над полем Галуа F_n, соответствующий подстановке s, а через f_s^{-1} многочлен над полем Галуа F_n, соответствующий подстановке s^{-1}. Обозначим через q_0 прообраз «0» при отображении s, т.е. $s(q_0) = f_s(q_0) = 0$. Поскольку s коммутирует с $p_0 = s_{a \cdot x}$, то верно

$$s \cdot p_0 \cdot s^{-1} = p_0. \tag{4.2}$$

Рассмотрим правую и левую часть равенства (4.2) на элементе q_0 и перепишем его в виде многочленов:

$$f_s^{-1}(a \cdot (f_s(q_0))) = f_s^{-1}(a \cdot 0) = f_s^{-1}(0) = q_0,$$

$$p_0(q_0) = a \cdot q_0.$$

Следовательно, $q_0 = a \cdot q_0$, где $a \neq 0$. Отсюда следует, что $q_0 = 0$ и $f_s(0) = s(0) = 0$. Поскольку s коммутирует с $p_1 = s_{a \cdot x + 1}$, то верно

$$s \cdot p_1 \cdot s^{-1} = p_1. \tag{4.3}$$

Рассмотрим правую и левую часть равенства (4.3) на элементе 0 и перепишем его в виде многочленов:

$$f_s^{-1}(a \cdot (f_s(0)) + 1) = f_s^{-1}(a \cdot 0 + 1) = f_s^{-1}(1),$$

$$p_1(0) = a \cdot 0 + 1 = 1.$$

Следовательно, $f_s^{-1}(1) = 1$. Отсюда следует, что $f_s(1) = s(1) = 1$. Рассмотрим правую и левую часть равенства (4.2) на элементе 1 и перепишем его в виде многочленов

$$f_s^{-1}(a \cdot (f_s(1))) = f_s^{-1}(a \cdot 1) = f_s^{-1}(a) = a \cdot 1 = a.$$

Отсюда следует, что $f_s(a) = s(a) = a$. Заметим, что $a = p_0(1)$. Рассмотрим правую и левую часть равенства (4.2) на элементе $p_0^l(a)$

$$s^{-1}(p_0^l(s(a))) = s^{-1}(p_0^l(a)) = p_0^l(a).$$

Следовательно, $f_s(p_0^l(a)) = s(p_0^l(a)) = p_0^l(a)$ для любого $l \in N$. Так как $p_0(q) = a \cdot q$, то $p_0^l(a) = a^{l-1}$. Значит, для любого $l \in N$ верно, что $f_s(p_0^l(a)) = s(p_0^l(a)) = a^l$. Принимая во внимание, что a — порождающий элемент мультипликативной группы, $s(q) = q$ для всех $q \in F*_n$. Отсюда следует, что переходная система обладает *свойством максимальности.*

На рисунке 4.5 изображена переходная система V, построенная описанным выше способом для $n = 16$. Поле Галуа F_{16} построим как расширение F_2 с помощью многочлена $x^4 + x + 1$. Приведем множества H_+ и H_* для поля F_{16}. Обозначим подстановку, соответствующую многочлену f над полем Галуа, через h_f.

$$H_+ = \{h_{x+0} = e, h_{x+1} = (0\,1)(2\,3)(4\,5)(6\,7)(8\,9)(10\,11)(12\,13)(14\,15),$$

$$h_{x+2} = (0\,2)(1\,3)(4\,6)(5\,7)(8\,10)(9\,11)(12\,14)(13\,15),$$

$$h_{x+3} = (0\,3)(1\,2)(4\,7)(5\,6)(8\,13)(9\,10)(12\,15)(13\,14),$$

$$h_{x+4} = (0\,4)(1\,5)(2\,6)(3\,7)(8\,12)(9\,13)(10\,14)(11\,15),$$

$$h_{x+5} = (0\,5)(1\,4)(2\,7)(3\,6)(8\,13)(9\,12)(10\,15)(11\,14),$$

$$h_{x+6} = (0\,6)(1\,7)(2\,4)(3\,5)(8\,14)(9\,15)(10\,12)(11\,13),$$

$$h_{x+7} = (0\,7)(1\,6)(2\,5)(3\,4)(8\,15)(9\,14)(10\,13)(11\,12)$$

$$h_{x+8} = (0\,8)(1\,9)(2\,10)(3\,11)(4\,12)(5\,13)(6\,14)(7\,15),$$

$$h_{x+9} = (0\,9)(1\,8)(2\,11)(3\,10)(4\,13)(5\,12)(6\,15)(7\,14),$$

$$h_{x+10} = (0\,10)(1\,11)(2\,8)(3\,9)(4\,14)(5\,15)(6\,12)(7\,13),$$

$$h_{x+11} = (0\,11)(1\,10)(2\,9)(3\,8)(4\,15)(5\,14)(6\,13)(7\,12)$$

$$h_{x+12} = (0\,12)(1\,13)(2\,14)(3\,15)(4\,8)(5\,9)(6\,10)(7\,11),$$

$$h_{x+13} = (0\,13)(1\,12)(2\,15)(3\,14)(4\,9)(5\,8)(6\,11)(7\,10),$$

$$h_{x+14} = (0\,14)(1\,15)(2\,12)(3\,11)(4\,10)(5\,11)(6\,8)(7\,9),$$

$$h_{x+15} = (0\,15)(1\,14)(2\,13)(3\,12)(4\,11)(5\,10)(6\,9)(7\,8)\},$$

$$H_* = \left\{ h_{0\cdot x} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, h_{1\cdot x} = e,\right.$$

$$h_{2\cdot x} = (1\,2\,4\,8\,3\,6\,12\,11\,5\,10\,7\,14\,15\,13\,9),$$

$$h_{3\cdot x} = (1\,3\,5\,15\,2\,6\,10\,13\,4\,12\,7\,9\,8\,11\,14),$$

$$h_{4\cdot x} = (1\,4\,3\,12\,5\,7\,15\,9\,2\,8\,6\,11\,10\,14\,13),$$

$$h_{5\cdot x} = (1\,5\,2\,10\,4\,7\,8\,14\,3\,15\,6\,13\,12\,9\,11),$$

$$h_{6\cdot x} = (1\,6\,7)(2\,12\,14)(3\,10\,9)(4\,11\,15)(5\,13\,8),$$

$$h_{7\cdot x} = (1\,7\,6)(2\,14\,12)(3\,9\,10)(4\,15\,11)(5\,8\,13),$$

$$h_{8\cdot x} = (1\,8\,12\,10\,15)(2\,3\,11\,7\,13)(4\,6\,5\,14\,9),$$

$$h_{9\cdot x} = (1\,9\,13\,15\,14\,7\,10\,5\,11\,12\,6\,3\,8\,4\,2),$$

$$h_{10\cdot x} = (1\,10\,8\,15\,12)(2\,7\,3\,13\,11)(4\,14\,6\,9\,5),$$

$$h_{11\cdot x} = (1\,11\,9\,12\,13\,6\,15\,3\,14\,8\,7\,4\,10\,2\,5),$$

$$h_{12\cdot x} = (1\,12\,15\,8\,10)(2\,11\,13\,3\,7)(4\,5\,9\,6\,14),$$

$$h_{13\cdot x} = (1\,13\,14\,10\,11\,6\,8\,2\,9\,15\,7\,5\,12\,3\,4),$$

$$h_{14\cdot x} = (1\,14\,11\,8\,9\,7\,12\,4\,13\,10\,6\,2\,15\,5\,3),$$

$$\left. h_{15\cdot x} = (1\,15\,10\,12\,8)(2\,13\,7\,11\,3)(4\,9\,14\,5\,6) \right\}.$$

Порождающие переходной системы V имеют вид

$$p_0 = (1\,2\,4\,8\,3\,6\,12\,11\,5\,10\,7\,14\,15\,13\,9),$$

$$p_1 = (0\,1\,3\,7\,15\,12\,10\,6\,13\,8\,2\,5\,11\,4\,9).$$

Построим оператор $\phi_V^{F_0}$, порождаемый переходной системой V и стандартным кодированием F_0

q	0	1	2	3	4	5	6	7
$F_0(q)$	000	001	010	011	100	101	110	111

Оператор $\phi_V^{F_0}$ имеет вид

$x(t)$	$q_0(t)$	$q_1(t)$	$q_2(t)$	$q_3(t)$	$q_0(t+1)$	$q_1(t+1)$	$q_2(t+1)$	$q_3(t+1)$
0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	0	1	0
0	0	0	1	0	0	1	0	0
0	0	0	1	1	0	1	1	0
0	0	1	0	0	1	0	0	0
0	0	1	0	1	1	0	1	0
0	0	1	1	0	1	1	0	0
0	0	1	1	1	1	1	1	0
0	1	0	0	0	0	0	1	1
0	1	0	0	1	0	0	0	1
0	1	0	1	0	0	1	1	1
0	1	0	1	1	0	1	0	1
0	1	1	0	0	1	0	1	1
0	1	1	0	1	1	0	0	1
0	1	1	1	0	1	1	1	1
0	1	1	1	1	1	1	0	1
1	0	0	0	0	0	0	0	1
1	0	0	0	1	0	0	1	1
1	0	0	1	0	0	1	0	1
1	0	0	1	1	0	1	1	1
1	0	1	0	0	1	0	0	1
1	0	1	0	1	1	0	1	1
1	0	1	1	0	1	1	0	1
1	0	1	1	1	1	1	1	1
1	1	0	0	0	0	0	1	0
1	1	0	0	1	0	0	0	0
1	1	0	1	0	0	1	1	0
1	1	0	1	1	0	1	0	0
1	1	1	0	0	1	0	1	0
1	1	1	0	1	1	0	0	0
1	1	1	1	0	1	1	1	0
1	1	1	1	1	1	1	0	0

Канонические уравнения имеют вид

$$\begin{cases} q_0(0) = q_1(0) = q_2(0) = 0 \\ q_0(t+1) = q_1(t) \\ q_1(t+1) = q_2(t) \\ q_2(t+1) = q_0(t) + q_3(t) \\ q_3(t+1) = q_0(t) + x(t) \end{cases}$$

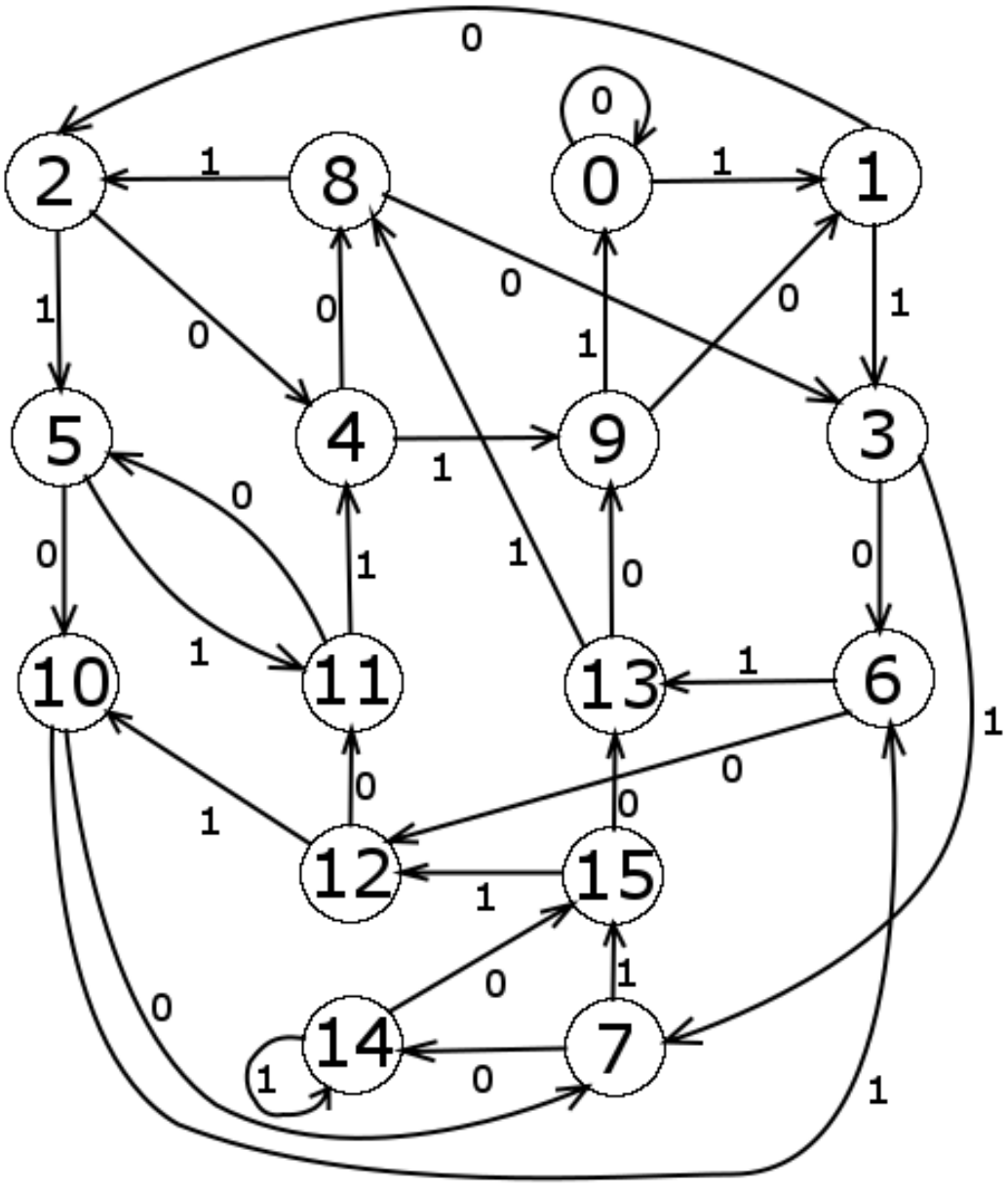

Рис. 4.5. Линейно реализуемая переходная система, обладающая *свойством максимальности*

Заключение

Настоящая работа содержит результаты решения задачи сложности реализации автомата посредством кодирований состояний автоматов. Основные результаты состоят в следующем:

- Сформулирован критерий линейной реализуемости автомата посредством неизбыточных кодирований в терминах порождающих внутренней полугруппы.
- Получена оценка сложности реализации переходных систем посредством всевозможных однородных кодирований состояний, не обязательно неизбыточных.
- Доказана алгоритмическая разрешимость задачи распознавания свойства линейной реализуемости переходной системы посредством всевозможных однородных кодирований состояний автомата, не обязательно неизбыточных.
- Сформулирован критерий максимальной реализуемости автомата в терминах порождающих внутренней полугруппы.
- С помощью полученных критериев установлено как взаимосвязаны классы линейно реализуемых автоматов и максимально реализуемых автоматов. Было показано, что данные классы имеют непустое пересечение, и ни один из классов не лежит в другом.

Список литературы

1. *Ashar P.*, *Devadas S.*, *Newton R. A.* Sequential Logic Synthesis. — Kluwer Academic Publishers Norwell, MA, USA, 1992.
2. *Hartmanis J.*, *Stearns R. E.* A study of feedback and errors in sequential machines // IRE Transactions on Electronic Computers. — 1963. — Т. EC—12, № 3. — С. 223—232.
3. *Хартманис Ю.*, *Стирнс Р. Э.* Алгебра пар и ее применение к теории автоматов // Кибернетический сборник. — 1969. — Т. 6. — С. 89—111.
4. *Гилл А.* Линейные последовательностные машины. — 4-е изд. — Москва «Наука», 1974.
5. *Арбиб М.* Декомпозиция автоматов и расширение полугрупп // Алгебраическая теория автоматов, языков и полугрупп. — 1975. — С. 46—64.
6. *Ecker K.* On the semigroup of a linear nonsingular automaton // Mathematical Systems Theory. — 1973. — Т. 6. — С. 353—358.
7. *Hartmanis J.*, *Walter H.* Group theoretic characterization of linear permutation automata // Journal of Computer and System Sciences. — 1973. — Т. 7, № 2. — С. 168—188.
8. *Hartfiel D.*, *Maxson C.* A Semigroup Characterization of a linearly realizable automaton over GF(p) // Journal of Computer and System Sciences. — 1977. — Т. 14, № 1. — С. 150—155.
9. *Hartmanis J.*, *Davis W. A.* Homomorphic images of linear sequential machines // Journal of Computer and System Sciences. — 1967. — Т. 1, № 2. — С. 155—165.

10. *Яблонский С. В.* Введение в дискретную математику. — Москва «Наука», 1979.

11. *Лупанов О. Б.* Асимптотические оценки сложности управляющих систем. — Москва «Изд-во Московского университета», 1984. — 134 с.

12. *Клиффорд А.*, *Престон Г.* Алгебраическая теория полугрупп. Том 1. — Москва «Мир», 1972.

13. *Лидл Р.*, *Нидеррайтер Г.* Конечные поля. — Москва «Мир», 1988.

14. *Каргаполов М. И.*, *Мерзляков Ю. И.* Основы теории групп. — Москва «Наука», 1982.

15. *Кудрявцев В. Б.*, *Алешин С. В.*, *Подколзин А. С.* Введение в теорию автоматов. — Москва «Наука», 1985.

16. *Hartmanis J.*, *Stearns R. E.* Pair algebra and its application to automata theory // Information and control. — 1964. — Т. 7. — С. 485—507.

17. *Hartmanis J.*, *Stearns R. E.* Symbolic analysis of a decomposition of information processing machines // Information and control. — 1960. — Т. 3. — С. 154—178.

18. *Hartmanis J.* Loop-free structures of sequential machines // Information and control. — 1962. — Т. 5. — С. 25—43.

19. *Hartmanis J.*, *Stearns R. E.* Some dangers in state reduction of sequential machines // Information and control. — 1962. — Т. 5. — С. 252—260.

20. *Hartmanis J.* On the state assignment problem for sequential machines. I // IRE Transactions on Electronic Computers. — 1961. — Т. EC—10, № 2. — С. 157—165.

21. *Hartmanis J.*, *Stearns R. E.* On the state assignment problem for sequential machines. II // IRE Transactions on Electronic Computers. — 1963. — Т. EC—10, № 4. — С. 593—603.

22. *Клиффорд А.*, *Престон Г.* Алгебраическая теория полугрупп. Том 2. — Москва «Мир», 1972.

23. *Алешин С. В.* Алгебраические системы автоматов. — Москва «МАКС пресс», 2016.

24. *Глушков В. М.* Синтез цифровых автоматов. — Москва «Физматгиз», 1962.

25. *Кобринский Н. Е.*, *Трахтенброт Б. А.* Введение в теорию конечных автоматов. — Москва «Физматгиз», 1962.

26. *Баркалов А. А.*, *Бабаков Р. М.* Переходные системы с максимальной вариантностью относительно кодирования состояний // Кибернетика и системный анализ. — 2011. — Т. 1. — С. 21—26.

27. *Капитонова Ю. В.* Кодирование абстрактных автоматов С-кодами. // Кибернетика и системный анализ. — 1965. — Т. 1. — С. 40—44.

Работы автора то теме диссертации

28. *Родин С. Б.* О связи линейно реализуемых автоматов и автоматов с максимальной вариативностью относительно кодирования состояний // Интеллектуальные системы. — 2016. — Т. 20, № 2. — С. 337—347.

29. *Родин С. Б.* Линейно реализуемые автоматы // Дискретная математика. — 2017. — Т. 29, № 1. — С. 59—79. — DOI: `https://doi.org/10.4213/dm1406`.

30. *Родин С. Б.* О свойствах кодирований состояний автомата. // Интеллектуальные системы. — 2017. — Т. 21, № 1.

31. *Родин С. Б.* Переходные системы с максимальной вариантностью относительно кодирования состояний // Интеллектуальные системы. — 1999. — Т. 4, № 3/4. — С. 335—352.