В. Г. Скобелев

Анализ Дискретных Систем

ИПММ НАНУ

НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК УКРАИНЫ

ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ И МЕХАНИКИ

В.Г. Скобелев

АНАЛИЗ ДИСКРЕТНЫХ СИСТЕМ

Донецк

2002

УДК 510.5 + 681.142

Рецензенты:

Д.т.н., профессор, декан факультета компьютерных наук и информационных технологий Саратовского государственного университета им. Н.Г. Чернышевского *Д.В. Сперанский*

К.ф.-м.н., с.н.с., старший научный сотрудник отдела теории управляющих систем ИПММ НАНУ *И.С. Грунский*

Анализ дискретных систем.

В.Г. Скобелев. ИПММ НАН Украины, Донецк, 2002. – 172с.

Монография посвящена разработке комбинаторно-алгебраических основ анализа дискретных систем. Решены проблемы поиска безусловных и адаптивных решений на частично упорядоченных структурах. С единых позиций исследованы поиск всех неприводимых множеств представителей семейства множеств, идентификация внутренних состояний конечного автомата, построение простых импликант и состоящих из них ДНФ, анализ управляемости/наблюдаемости булевых функций. Исследовано представление автоматов группами. Решена проблема идентификации булевой вектор-функции методами теории линейных пространств над конечными полями. Созданы основы анализа систем, подверженных дестабилизирующим воздействиям внешней среды.

Для специалистов в областях дискретной математики и computer science, студентов и аспирантов, специализирующихся в этих областях, а также для специалистов, занимающихся анализом дискретных систем как в теоретическом, так и прикладном аспекте.

Утверждено к печати Ученым советом Института прикладной математики и механики НАН Украины

Аналіз дискретних систем.

В.Г. Скобелєв. ІПММ НАН України, Донецьк, 2002. – 172с. (На російській мові).

Монографія присв'ячена розробці комбінаторно-алгебраїчних основ аналізу дискретних систем. Отримано розв'язки проблем пошуку безумовних та адаптивних розв'язків на частково впорядкованих структурах. З спільних позицій досліджено пошук усіх множин представників для родини множин, які не є надлишковими, ідентифікацію внутрішніх станів скінченого автомата, побудову простих імпликант та ДНФ, які складаються з них, аналіз керуємості/співстережності булевих функцій. Досліджено представлення автоматів групами. Отримано розв'язок проблеми ідентифікації булевої вектор-функції методами теорії лінейних просторів над скінченими полями. Створено основи аналізу систем, які є підвладними до дестабілізуючого впливу зовнішнього середовища.

Для спеціалістів в галузях дискретної математики та computer science, студентів та аспірантів, які спеціалізуються у цих галузях, а також для спеціалістів, які займаються аналізом дискретних систем як у теоретичному, так і прикладному аспекті.

ISBN 966-02-2356-0

ПРЕДИСЛОВИЕ

Предмет исследования монографии – анализ дискретных систем. Основными характеристиками теории дискретных систем являются широкий спектр существенно отличающихся друг от друга *моделей систем* и *поиск* (того или иного типа), как основной метод построения решений. В то же время, *дискретная система* может рассматриваться как *алгебраическая система* того или иного типа. Именно это обстоятельство делает возможным привлечение мощного арсенала современной алгебры для решения проблем анализа дискретных систем. Поэтому, основной целью монографии и является

разработка основ комбинаторно-алгебраической теории, предназначенной для анализа дискретных систем.

Актуальность решения этой проблемы обусловлена тем, что дискретная система – одно из фундаментальных понятий дискретной математики, computer science и их многочисленных приложений в технике, экономике, социальных науках.

Монография состоит из пяти разделов.

Раздел 1 представляет собой развернутое введение. В нем изложен необходимый математический аппарат, проведен ретроспективный анализ предмета исследования, сформулированы основные проблемы.

В разделе 2 впервые систематически изложена разработанная автором общая теория поиска на частично упорядоченных структурах, включающая в себя в качестве специальных случаев классические теоретико-множественный и основанный на оценивании подходы. В рамках этой теории получено решение общей проблемы поиска безусловных решений, определяемых характеристической функцией. Определены и исследованы базовые математические модели для поиска безусловных и адаптивных решений, соответственно, M-источник и AM-источник. Получено исчерпывающее решение проблем поиска как всех основных типов безусловных решений (минимальных, неприводимых и кооперативных), так и адаптивных решений. Решена фундаментальная проблема поиска множества всех неприводимых множеств представителей заданного семейства множеств.

Раздел 3 посвящен анализу конечных автоматов – фундаментальному классу дискретных систем как в теоретическом, так и прикладном аспектах. На основе методов поиска, разработанных в разделе 2, получено исчерпывающее решение проблем идентификации внутренних состояний слабоинициального конечного автомата. Разработан общий метод построения нижних экспоненциальных оценок для функции Шеннона. Исследована проблема представления функций переходов и выходов конечного автомата конечными группами. На основе полученных результатов решена проблема построения нестационарных секретных замков сколь угодно большой сложности.

Раздел 4 посвящен анализу булевых функций – другому фундаментальному классу дискретных систем как в теоретическом, так и прикладном аспектах. На основе методов поиска, разработанных в разделе 2, решены проблемы поиска всех и одной простых импликант, покрывающих заданную точку, а так же ДНФ, состоящих из простых импликант. На основе этих результатов получено полное решение проблем анализа управляемости/наблюдаемости для булевых функций. Решена проблема идентификации булевых вектор-функций методами теории линейных пространств над конечными полями.

В разделе 5 на основе аксиоматического подхода разработана теория ДДФ-систем – фрагмент общей теории систем, предназначенный для исследования систем, находящихся под действием дестабилизирующих факторов внешней среды. Решена проблема адаптивного управления ДДФ-системой.

Монография написана в замкнутой форме, т.е. определяются все понятия, кроме общепринятых.

Полученные результаты - оригинальные результаты автора – старшего научного сотрудника отдела теории управляющих систем ИПММ НАНУ и отражают тематику исследований этого отдела. Многие результаты были опубликованы ранее в том или ином виде (см. список литературы). Однако настоящая монография – это первая попытка систематически представить все эти результаты с единых позиций.

Монография предназначена для специалистов в областях дискретной математики и computer science, студентов и аспирантов, специализирующихся в этих областях и специалистов, занимающихся анализом дискретных систем как в теоретическом, так и прикладном аспекте. Она также может быть использована преподавателями при разработке спецкурсов для специальностей прикладная математика и computer science (часть материала из разделов 2-4 использовалась автором при чтении курса лекций *Дискретная математика* для специальности 0106 *Прикладная математика* в Донецком государственном университете).

Благодарности. Прежде всего, автор считает своим долгом выразить искреннюю благодарность научным руководителям на стадии кандидатской диссертации, профессорам **А.М. Богомолову** и *В.Б. Кудрявцеву*, чьи усилия и терпение, во многом, сформировали сегодняшние позиции и точки зрения автора на исследуемые проблемы. Многие результаты были доложены в различное время на семинарах и конференциях. Автор благодарен их участникам, особенно, профессорам *Ю.В. Капитоновой*, *А.А. Летичевскому* и *В.Н. Редько* за полезные обсуждения, а иногда, и подсказки, способствовавшие усилению результатов и обобщению постановок проблем. Раздел 4 своим появлением на свет во многом обязан профессору *Д.В. Сперанскому*, выложившему перед автором изумительные постановки проблем и принимавшему активное участие в обсуждении и шлифовке полученных результатов, за что автор ему искренне благодарен. За возможность обсуждать проблемы в процессе их постановки и решения автор благодарит своих коллег по отделу *В.А. Козловского*, *Ю.А. Скобцова* и особенно *И.С. Грунского*, который на протяжении более тридцати лет добровольно и бескорыстно является для автора самым терпеливым слушателем и самым мудрым советчиком.

Автор выражает искреннюю благодарность администрации ИПММ НАНУ – директору, академику *И.В. Скрыпнику* и зам. директора, профессору *А.М. Ковалеву* за обеспечение идеальных условий для работы над монографией.

Написание любой книги требует больших затрат сил и времени. Автор выражает глубокую и искреннюю благодарность своим близким – жене *Галине* и сыну *Владимиру* за их терпение и постоянную поддержку в процессе работы над монографией.

Безусловно, что за все недостатки ответственность несет только автор.

Автор будет благодарен за любые конструктивные замечания, касающиеся содержания книги.

АВТОР

Декабрь, 2001, Донецк

СОДЕРЖАНИЕ

СПИСОК ОБОЗНАЧЕНИЙ ……………………………………………………………7

1. Модели и методы теории систем ……………………………………………..9

1.1. Основы математической теории систем ……………………………………9

1.2. Проблемы идентификации систем ………………………………………..16

1.3. Конечные автоматы ………………………………………………………19

1.4. Булевы функции …………………………………………………………23

1.5. Поиск …………………………………………………………………..27

1.6. Выводы ………………………………………………………………...38

2. Поиск на частично упорядоченных структурах ……………………………39

2.1. Общие схемы поиска безусловных решений ……………………………..39

2.2. M*-источник* ……………………………………………………………49

2.3. Поиск безусловных решений для M*-источников* ……………………….52

2.4. AM*-источник* …………………………………………………………..65

2.5. Поиск адаптивных решений для AM*-источников* ………………………..70

2.6. Неприводимые множества представителей семейства множеств ………………75

2.7. Выводы …………………………………………………………………..86

3. Анализ конечных автоматов …………………………………………………87

3.1. Поиск идентифицирующих слов …………………………………………..87

3.2. Построение нижних экспоненциальных оценок ……………………………101

3.3. Сложность поиска минимальных идентифицирующих слов ………………107

3.4. Построение автоматов-экспериментаторов ……………………………...112

3.5. Представление автоматов группами ……………………………………..114

3.6. Рекурсивная модель секретного замка ……………………………………127

3.7. Выводы …………………………………………………………………..129

4. Анализ булевых функций …………………………………………………………….131

4.1. Комбинаторные алгоритмы построения ДНФ ……………………………….…131

4.2. Управляемость/наблюдаемость булевых функций ……………………………....140

4.3. Идентификация булевых вектор-функций ………………………………………..145

4.4. Выводы ……………………………………………………………………...…..152

5. ДДФ-системы ……………………………………………………….……………….153

5.1. Основные понятия и определения …………………………………………………153

5.2. Композиции ДДФ-систем ………………………………………………………….157

5.3. Адаптивное управление ДДФ-системой ……………………………………….159

5.4. Выводы ……………………………………………………………………………163

Заключение ……………………………………………………………………………165

СПИСОК ЛИТЕРАТУРЫ ……………………………………………………………….167

СПИСОК ОБОЗНАЧЕНИЙ

Логические:

$A \Rightarrow B$ - если A, то B;

$A \Leftrightarrow B$ - A тогда и только тогда, когда B;

$\overline{a}$ - отрицание a, т.е. $\overline{a} = 1$ тогда и только тогда, когда $a = 0$;

$a \wedge b$ - конъюнкция a и b, т.е. $a \wedge b = 1$ тогда и только тогда, когда $a = b = 1$;

$a \vee b$ - дизъюнкция a и b, т.е. $a \vee b = 0$ тогда и только тогда, когда $a = b = 0$;

$(\forall x)P(x)$ - для всех x утверждение $P(x)$ - истинное;

$(\exists x)P(x)$ - существует такое x, что утверждение $P(x)$ - истинное.

Теоретико-множественные:

$\varnothing$ - пустое множество, т.е. не содержащее ни одного элемента;

$x \in X$ - x является элементом множества X;

$x \notin X$ - x не является элементом множества X;

$X = Y$ - множества X и Y равны, т.е. состоят из одних и тех же элементов;

$X \subseteq Y$ - множество X является подмножеством множества Y, т.е. каждый элемент множества X является элементом множества Y;

$X \not\subseteq Y$ - множество X не является подмножеством множества Y,

$X \subset Y$ - $X \subseteq Y$ и существует такой элемент $x \in X$, что $x \notin X$;

$X \not\subset Y$ - утверждение $X \subset Y$ - ложное;

$\{x \mid P(x)\}$ - множество всех таких x, что утверждение $P(x)$ - истинное;

$\mathbf{B}(X)$ - булеан множества X, т.е. множество всех подмножеств множества X;

$|X|$ - мощность множества X;

$\aleph_0$ - мощность счетного множества;

$X \cap Y$ - пересечение множеств X и Y, т.е. $x \in X \cap Y$ тогда и только тогда, когда $x \in X$ и $x \in Y$;

$X \cup Y$ - объединение множеств X и Y, т.е. $x \in X \cap Y$ тогда и только тогда, когда $x \in X$ или $x \in Y$;

$X \setminus Y$ - разность множеств X и Y, т.е. $x \in X \setminus Y$ тогда и только тогда, когда $x \in X$ и $x \notin Y$;

$X \times Y$ - декартово произведение множеств X и Y, т.е. $(x, y) \in X \times Y$ тогда и только тогда, когда $x \in X$ и $y \in Y$;

X / ε - фактор-множество множества X по отношению эквивалентности ε;

$\mathbf{N}$ - множество всех натуральных чисел;

$\mathbf{Z}$ - множество всех целых чисел;

$\mathbf{Z}_+$ - множество всех неотрицательных целых чисел;

$\mathbf{Z}_k$ $(k \in \mathbf{N})$ - множество, состоящее из чисел $0,1,\ldots,k-1$;

$\mathbf{R}$ - множество всех действительных чисел;

$\mathbf{R}_+$ - множество всех неотрицательных действительных чисел;

$\mathbf{E}$ - множество, состоящее из двух элементов 0 и 1;

$P_2(n)$ - множество всех булевых функций от переменных $x_1,\ldots,x_n$.

Функциональные:

$f : X \to Y$ - (возможно частичное) отображение множества X в множество Y;

$\mathrm{Dom}\, f$ - область определения отображения f;

$\mathrm{Val}\, f$ - множество значений отображения f;

A^B - множество всех (возможно частичных) отображений множества B в множество A;

$\ker f$ - ядерная эквивалентность отображения f.

Лингвистические:

Λ - пустое слово, т.е. не содержащее ни одного символа;

X^n $(n \in \mathbf{N})$ - множество всех слов длины n в алфавите X;

X^+ - множество всех непустых слов в алфавите X;

X^* - множество всех, включая и пустое, слов в алфавите X;

$erase(p)$ $(p \in X^+)$ - множество всех непустых слов, полученных в результате вычеркивания (т.е. удаления) хотя бы одной буквы в слове p.

1. МОДЕЛИ И МЕТОДЫ ТЕОРИИ СИСТЕМ

Теория систем существует более полувека. За этот период времени появилось большое число публикаций, посвященных как общей теории систем, исследующей фундаментальные понятия и аспекты систем, так и теориям, исследующим системы более конкретных типов. Списки таких публикаций приведены, практически, в каждой монографии, посвященной теории систем, а также в многочисленных обзорах, посвященных различным аспектам теории систем. При этом, в связи с интенсивным развитием технических, экономических и организационных систем, постоянно возникают новые направления теории систем.

В данном разделе проведен систематический анализ состояния теории систем, отражающий предмет настоящего исследования. С этой целью изложен математический аппарат, необходимый для решения проблем анализа дискретных систем. Дан ретроспективный анализ моделей и методов, лежащих в основе решения этих проблем. В п.1.1 кратко изложен аксиоматический подход к построению математической теории систем, приведена иерархия математических моделей систем. В п.1.2 сформулированы проблемы идентификации дискретных систем и исследованы их особенности, связанные с уровнем абстракции при выборе математической модели исследуемой системы. В п.1.3 дан ретроспективный анализ проблем идентификации внутренних состояний конечных автоматов. В п.1.4 изложены основы минимизации дизъюнктивных нормальных форм (ДНФ). В п.1.5 дан ретроспективный анализ проблем поиска. В терминах базовой математической модели для представления проблем поиска – источника – формально определены основные типы решений.

1.1. Основы математической теории систем.

В результате интенсивного развития теории систем появилось значительное число публикаций, излагающих на аксиоматической основе различные ее решения и аспекты с использованием логико-лингвистических, теоретико-множественных, алгебраических и топологических методов (см., напр., [21,29-31,95-97]). Это направление - *математическая теория систем* - характеризуется тем, что для него до сих пор не выработана единая общепризнанная аксиоматика. Для представленных в монографии исследований удобным и адекватным является теоретико-множественный подход, систематически изложенный в [31]. Рассмотрим его кратко. В основе этого подхода лежит выделение ряда уровней абстракции при определении понятия *система*.

На высшем уровне абстракции система определяется как отношение

$$\boldsymbol{S} \subseteq \prod_{i \in I} V_i \,, \tag{1.1}$$

где $\boldsymbol{V} = \{V_i \mid i \in I\}$ - *семейство объектов*. Отметим, что запись (1.1) автоматически предполагает, что множество индексов I - *линейно упорядоченное*. При фиксированном семействе объектов $\boldsymbol{V}$ все многообразие систем определяется комплексами условий, накладываемых на отношение $\boldsymbol{S}$, а так же с помощью математических структур, определенных на множестве $\bigcup_{i \in I} V_i$. Так как

$$\prod_{i \in I} V_i = \{f : I \to \bigcup_{i \in I} V_i \mid f(i) \in V_i \ (i \in I)\} = \boldsymbol{F} \tag{1.2}$$

и переименованием элементов множества I всегда можно добиться выполнения равенства $I \cap (\bigcup_{i \in I} V_i) = \varnothing$, то любой элемент множества $\prod_{i \in I} V_i$ можно рассматривать как частичную унарную операцию, определенную на множестве $I \cup (\bigcup_{i \in I} V_i)$. Следовательно, система (1.1) является алгеброй

$$\boldsymbol{A} = (I \cup (\bigcup_{i \in I} V_i), \boldsymbol{F_S}), \tag{1.3}$$

где

$$\boldsymbol{F_S} = \{ f \in \boldsymbol{F} \mid \{f(i)\}_{i \in I} \in \boldsymbol{S} \}. \tag{1.4}$$

Представление (1.3) дает возможность непосредственно перенести в *теорию систем* все основные понятия теории алгебраических систем [29], в том числе такие, как *подсистема*, *гомоморфизм* и *изоморфизм*. Действительно, пусть система $\boldsymbol{T} \subseteq \boldsymbol{G} (= \prod_{j \in J} U_j)$ представлена алгеброй

$$\boldsymbol{B} = (J \cup (\bigcup_{j \in J} U_j), \boldsymbol{G_T}),$$

где

$$\boldsymbol{G_T} = \{ g \in \boldsymbol{G} \mid \{g(j)\}_{j \in J} \} \in \boldsymbol{T} .$$

Определение 1.1. Система $\boldsymbol{T}$ называется *подсистемой* системы $\boldsymbol{S}$, если выполнены следующие три условия: 1) $J \subseteq I$; 2) $U_j \subseteq V_j$ для всех $j \in J$; 3) для любого $g \in \boldsymbol{G_T}$ существует такое $f \in \boldsymbol{F_S}$, что $g(j) = f(j)$ для всех $j \in J$.

Определение 1.2. Система $\boldsymbol{T}$ называется *гомоморфным образом* системы $\boldsymbol{S}$, если существуют такие сюръективные отображения

$$\alpha : I \to J, \quad \beta_i : V_i \to U_{\alpha(i)} \ (i \in I), \quad \gamma : \boldsymbol{F_S} \to \boldsymbol{G_T}, \tag{1.5}$$

что равенство

$$\beta_i(f(i)) = (\gamma(f))(\alpha(i)) \tag{1.6}$$

справедливо для всех $i \in I$ и $f \in \boldsymbol{F_S}$.

Определение 1.3. Системы $\boldsymbol{S}$ и $\boldsymbol{T}$ называются *изоморфными*, если биективными являются отображения (1.5), удовлетворяющие условию (1.6).

Отметим, что при определении изоморфизма систем равенство (1.5) может быть записано в следующей эквивалентной форме

$$\beta^{-1}_{\alpha^{-1}(j)}(g(j)) = (\gamma^{-1}(g))(\alpha^{-1}(i))$$

для всех $j \in J$ и $g \in \boldsymbol{G}$.

Значение определения 1.3 состоит в следующем. Представление системы в виде (1.1) предполагает *упорядочение* множества объектов. Этот порядок фиксируется с помощью линейно упорядоченного множества индексов I. Упорядочение множества объектов влияет на *внешнюю форму* системы, но не затрагивает *комплекс абстрактных характеристик* отношения $\boldsymbol{S}$. При определении математических структур на системе (1.1) для упрощения изложения удобно изменять предписанный порядок объектов соответствующим образом, т.е. переходить к изоморфной системе. Такой переход, если он не вызывает недоразумений, как правило, не оговаривается в явном виде.

Определение тех или иных отношений на множествах индексов и объектов системы (1.1) дает возможность выделить различные типы систем. Каждая из них представляется уже не алгеброй вида (1.3), а *алгебраической системой* общего вида [29], т.е. упорядоченной тройкой

$$(A, \Omega_F, \Omega_P), \tag{1.7}$$

где A - *основное множество*, а Ω_F и Ω_P - *множества основных*, соответственно, *операций* и *предикатов* (т.е. характеристических функций отношений, определенных на множествах индексов и объектов системы). Определения *гомоморфизма* и *изоморфизма* для алгебраических систем типа (1.7) требуют сохранения свойств как основных операций, так и основных предикатов. Именно по этой причине определения *гомоморфизма* и *изоморфизма* - различные для различных типов систем.

Рассмотрим детализации, применяемые для понижения уровня абстракции при определении понятия *система*.

Пусть зафиксирована упорядоченная пара $\pi = (I_{in}, I_{out})$, где

$$I_{in} \cap I_{out} = \varnothing,\ I_{in} \cup I_{out} = I\ . \tag{1.8}$$

Формула (1.1) может быть преобразована к виду *абсолютного черного ящика* (т.е. *системы вход-выходного типа*)

$$\boldsymbol{S} \subseteq X \times Y\ , \tag{1.9}$$

где $X = \prod\limits_{i \in I_{in}} V_i$ и $Y = \prod\limits_{i \in I_{out}} V_i$ называются, соответственно, *входным* и *выходным* объектом системы $\boldsymbol{S}$. Ясно, что существует взаимно-однозначное соответствие между множеством всевозможных представлений системы (1.1) в виде абсолютного черного ящика и множеством всех упорядоченных пар $\pi = (I_{in}, I_{out})$, удовлетворяющих условиям (1.8). Среди этих представлений особую роль играют следующие два, соответствующие случаям, когда одно из множеств I_{in} или I_{out} - пустое. Представления, определяемые парами $\pi_1 = (\varnothing, I)$ и $\pi_2 = (I, \varnothing)$, называются системами, соответственно, *без входа* и *без выхода*. К этим типам систем относятся, в частности, соответственно, *автономные системы* и *акцепторы*.

Отметим, что, несмотря на высокий уровень абстракции, представления (1.1) и (1.9) могут быть успешно использованы при решении конкретных прикладных проблем. Проиллюстрируем сказанное следующими тремя примерами.

Пример 1.1. Текущее состояние любой организации естественно представляется упорядоченным набором показателей $\mathbf{v} = (v_1, \ldots, v_n)$. Это означает, что концептуальной математической моделью организации является система $\boldsymbol{S} \subseteq \mathbf{R}^n$, определяемая как n-арное отношение (т.е. представление (1.1)). На множестве $\boldsymbol{S}$ обычным образом можно определить отношение предпочтения $\leq_{\boldsymbol{S}}$, а, следовательно, и определяемую им *функцию полезности* $u : \boldsymbol{S} \to \mathbf{R}$. Последняя дает возможность строить кривые безразличия

$$\Gamma_{\mathbf{v}} = \{\mathbf{w} \in \boldsymbol{S} \mid u(\mathbf{w}) = u(\mathbf{v})\} (\mathbf{v} \in \boldsymbol{S}),$$

а также представить систему $\boldsymbol{S}$ в виде

$$\boldsymbol{S} = (\boldsymbol{S}_{крит}, \boldsymbol{S}_{пер}, \boldsymbol{S}_{благ}),$$

где $\boldsymbol{S}_{крит}$, $\boldsymbol{S}_{пер}$ и $\boldsymbol{S}_{благ}$ - подмножества, соответственно, критических, переходных и благоприятных состояний исследуемой организации.

Пример 1.2. Разработка стратегии планирования для организации основана на выделении упорядоченных наборов ресурсов $\mathbf{v} = (v_1, \ldots, v_k)$, внешних факторов $\mathbf{w} = (w_1, \ldots, w_l)$ и производимой продукции $\mathbf{y} = (y_1, \ldots, y_n)$. Таким образом, концептуальной математической моделью организации является система $\boldsymbol{S} \subseteq X \times Y$ (т.е. представление (1.9)), где $X \subseteq \mathbf{V} \times \mathbf{W}$ $(\mathbf{V} \subseteq \mathbf{R}_+^k, \mathbf{W} \subseteq \mathbf{R}^l)$ и $Y \subseteq \mathbf{R}_+^n$. Оценка взаимодействия организации с внешней средой осуществляется с помощью функции полезности $u(\mathbf{x}, \mathbf{y})$. В качестве последней, в соответствии с основной аксиомой производителя, может быть выбрана *прибыль*.

Пример 1.3. Комбинационная микросхема реализует заданную булеву вектор-функцию $f:\{0,1\}^m \to \{0,1\}^n$. Это означает, что как при проектировании, так и при контроле комбинационных микросхем, в качестве концептуальной математической модели может быть выбран график булевой вектор-функции f или, иными словами, система $\mathbf{S} \subseteq X \times Y$ (т.е. представление (1.9)), где $X = \{0,1\}^m$ и $Y \subseteq \{0,1\}^n$.

Переход от (1.1) к (1.9) дает возможность задать *систему* в виде *бинарного отношения*. Последнее может быть представлено в виде

$$\mathbf{S} = \bigcup_{c \in C} \mathbf{S}_c\,, \tag{1.10}$$

где каждое бинарное отношение

$$\mathbf{S}_c \subseteq X \times Y \;\; (c \in C) \tag{1.11}$$

функционально, т.е. $\mathbf{S}_c \; (c \in C)$ является *графиком* такой (возможно частичной) функции $f_c : X \to Y$, что

$$f_c(x) = y \Leftrightarrow (x, y) \in \mathbf{S}_c \;\; (x \in X, y \in Y). \tag{1.12}$$

Отсюда вытекает, что существует (возможно, частичная) функция

$$f : C \times X \to Y\,, \tag{1.13}$$

определяемая формулой

$$f(c, x) = y \Leftrightarrow f_c(x) = y\,. \tag{1.14}$$

Итак, осуществлен переход от системы (1.9) к *относительному черному ящику*

$$\mathbf{S} = (C, X, Y, f)\,, \tag{1.15}$$

где C - *множество глобальных состояний*, X и Y - соответственно, *входной* и *выходной* объекты, а f - *глобальная реакция*. Переход от (1.9) к (1.15) осуществляется не единственным образом, т.к. могут быть построены различные множества глобальных состояний (и, соответственно, различные глобальные реакции). Отметим, что формулы (1.13) и (1.14) отражают только *функциональную зависимость* между входными и выходными объектами системы, представленной в виде *черного ящика*. Для отражения причинно-следственной зависимости необходим тщательный анализ исследуемой проблемы.

Для исследования динамических аспектов поведения системы вводится понятие *временна́я функция.* Она определяется как элемент множества U^T всех (возможно, частичных) отображений *множества моментов времени* (т.е. линейно упорядоченного множества, содержащего наименьший элемент) в *алфавит* (т.е. произвольное непустое множество) U.

Абсолютный черный ящик (1.9) называется *общей временно́й системой*, если входной и выходной объекты – множества временных функций, т.е. $X \subseteq A^T$ и $Y \subseteq B^T$, где A и B - *входной* и *выходной* алфавиты. *Сужением* общей временно́й системы $\mathbf{S}$ на промежуток времени $\{t' \in T \mid t' \geq t\}$ называется система

$$\mathbf{S}\big|_t = \{(x|_{\{t' \in T \mid t' \geq t\}}, y|_{\{t' \in T \mid t' \geq t\}}) \mid (x, y) \in \mathbf{S}\} \;\; (t \in T)$$

Для системы $\mathbf{S}\big|_t \; (t \in T)$ в соответствии с формулами (1.10)-(1.14) может быть построено множество глобальных состояний C_t и глобальная реакция $f_t : C_t \times X_t \to Y_t$ в момент времени t, где

$$X_t = \{x|_{\{t'\in T\,|\,t'\geq t\}} \mid x\in X\}\ \ (t\in T)$$

и

$$Y_t = \{y|_{\{t'\in T\,|\,t'\geq t\}} \mid y\in Y\}\ \ t\in T\,.$$

Следовательно, система $\mathbf{S}|_t\ \ (t\in T)$ может быть представлена в виде

$$\mathbf{S}|_t = (C_t, X_t, Y_t, f_t)\,(t\in T).$$

Итак, с каждой общей временно́й системой $\boldsymbol{S}$ ассоциируется семейство сужений

$$\{\mathbf{S}|_t \mid t\in T\} = \{(C_t, X_t, Y_t, f_t) \mid t\in T\}. \qquad (1.16)$$

Формула (1.16) часто записывается в виде

$$\boldsymbol{S} = (\mathbf{C}, X, Y, \mathbf{f}), \qquad (1.17)$$

где $\mathbf{C} = \{C_t \mid t\in T\}$ и $\mathbf{f} = \{f_t \mid t\in T\}$ называются, соответственно*, семейством объектов состояний* и *семейством глобальных реакций* общей временно́й системы $\boldsymbol{S}$.

Система (1.17) преобразует множество входных функций $X\,(X\subseteq A^T)$ в множество выходных функций $Y\,(Y\subseteq B^T)$. Фиксация начального состояния $c\in C_0$ интерпретируется как *внешняя настройка* для реализации конкретного оператора $(f_0)_c$. Кроме того, возможно вычисление образов сужений входных функций $x|_{\{t'\in T\,|\,t'\geq t\}}\,(t\in T)$. Для этого, в дополнение к указанной внешней настройке, требуется также и *внутренняя настройка*. Она состоит в вычислении состояния $c'\,(c'\in C_t)$ системы $\boldsymbol{S}$ в момент времени t, выборе глобальной реакции f_t и ее настройке на реализацию оператора $(f_t)_{c'}$.

Для системы (1.17) отсутствует механизм вычисления ее состояния в момент времени $t\,(t\in T)$. Такой механизм может быть определен следующим образом. Пусть

$$X_{tt'} = \{x|_{\{\tau\in T\,|\,t\leq\tau<t'\}} \mid x\in X\}\ \ (t,t'\in T, t<t').$$

Общая временна́я система $\boldsymbol{S}\subseteq X\times Y\,(X\subseteq A^T, Y\subseteq B^T)$ называется *динамической* (или, говорят также, что $\boldsymbol{S}$ допускает *динамическое представление*), если хотя бы при одном выборе семейства объектов состояний $\mathbf{C} = \{C_t \mid t\in T\}$ и соответствующего ему семейства глобальных реакций $\mathbf{f} = \{f_t \mid t\in T\}$ существует такое семейство (возможно, частичных) отображений

$$\Phi = \{\varphi_{tt'} : C_t\times X_{tt'} \to C_{t'} \mid t,t'\in T, t\leq t'\}, \qquad (1.18)$$

что при любых $t,t',t''\,(t\leq t'<t'')$ равенства

$$f_t(c, x|_{\{\tau\in T\,|\,\tau\geq t\}})\big|_{\{\tau\in T\,|\,\tau\geq t'\}} = f_{t'}(\varphi_{tt'}(c, x|_{\{\tau\in T\,|\,t\leq\tau<t'\}}), x|_{\{\tau\in T\,|\,\tau\geq t'\}}), \qquad (1.19)$$

$$\varphi_{tt}(c, x|_{\{\tau\in T\,|\,\tau=t\}}) = c \qquad (1.20)$$

и

$$\varphi_{tt''}(c, x|_{\{\tau\in T\,|\,t\leq\tau<t''\}}) = \varphi_{t't''}(\varphi_{tt'}(c, x|_{\{\tau\in T\,|\,t\leq\tau<t'\}}), x|_{\{\tau\in T\,|\,t'\leq\tau<t''\}}) \qquad (1.21)$$

справедливы для всех $c\in C_t$ и $x\in X$. Отображения $\varphi_{tt'}$ называются *функциями перехода состояний* (на промежутке $\{\tau\in T \mid t\leq\tau<t'\}$), а Φ - *семейством функций перехода состояний*. Равенства (1.19)-(1.21) определяют правила, в соответствии с которыми для системы $\boldsymbol{S}$ и ее сужений должны быть построены представления (1.10)-(1.15) с тем, чтобы сконструированные относительные черные ящики могли сформировать динамическую систему. Свойства, определяемые равенствами (1.19) и (1.21), называются, соответственно, *согласованностью* семейства Φ с семейством $\mathbf{f}$ и *полугрупповым* для семейства Φ.

Семейство функций перехода состояний дает возможность выделить среди представлений (1.17) *общие динамические системы*

$$\boldsymbol{S} = (\mathbf{C}, X, Y, \mathbf{\Phi}, \mathbf{f}). \tag{1.22}$$

Для (1.22) (в отличие от (1.17)) в явном виде задана схема вычисления состояния в любой момент времени $t \in T$, определяемая равенствами (1.20) и (1.21). Эта схема обеспечивает вычисление выходных функций (а также их сужений) в терминах преобразования состояний системы.

Важный специальный случай имеет место, когда существует такое множество C, что равенство $C_t = C$ справедливо для всех $t \in T$. Это множество C называется *пространством* (или *множеством*) *состояний*. Таким образом, среди систем (1.22) выделены *общие динамические системы в пространстве состояний*

$$\boldsymbol{S} = (C, X, Y, \mathbf{\Phi}, \mathbf{f}). \tag{1.23}$$

Все рассмотренные выше временные системы преобразуют входные функции в выходные функции. Такой уровень абстракции приемлем, когда исследуются общие свойства системы. Однако, он является слишком общим, а описание системы – слишком сложным, при исследовании конкретных проблем, связанных с изучением поведения системы. Основной недостаток представлений (1.17), (1.22) и (1.23) состоит в отсутствии механизма вычисления значений выходной функции в конкретные моменты времени. Этот недостаток можно устранить следующим образом. Пусть

$$Y(t) = \{y(t) \mid y \in Y, t \in \mathrm{Dom}\, y\} \ \left(t \in T\right)$$

и

$$\overline{X}_{tt'} = \{x|_{\{\tau\in T \mid t\le\tau\le t'\}} \mid x \in X\} \ \left(t, t' \in T, t \le t'\right).$$

Определим тернарные отношения

$$\kappa_{tt'} \subseteq C_t \times \overline{X}_{tt'} \times Y(t') \ \left(t, t' \in T, t \le t'\right)$$

соотношением

$$(c_t, x|_{\{\tau\in T \mid t\le\tau\le t'\}}, \alpha) \in \kappa_{tt'} \Leftrightarrow (f_t(c_t, x|_{\{\tau\in T \mid \tau\ge t\}}))(t') = \alpha .$$

Если тернарное отношение $\kappa_{tt'}$ $\left(t, t' \in T, t \le t'\right)$ - функциональное, то функция

$$\mu_{tt'} : C_t \times \overline{X}_{tt'} \to Y\left(t'\right),$$

определяемая соотношением

$$\mu_{tt'}(c_t, x|_{\{\tau\in T \mid t\le\tau\le t'\}}) = \alpha \Leftrightarrow (c_t, x|_{\{\tau\in T \mid t\le\tau\le t'\}}, \alpha) \in \kappa_{tt'}$$

(т.е. отношение $\kappa_{tt'}$ - график функции $\mu_{tt'}$) называется *производящей функцией выхода на промежутке* $\left\{\tau \in T \mid t \le \tau \le t'\right\}$. В том случае, когда все отношения $\kappa_{tt'}$ $\left(t, t' \in T, t \le t'\right)$ - функциональные, семейство функций

$$\Psi = \{\mu_{tt'} \mid t, t' \in T, t \le t'\}$$

называется *производящим семейством выхода*. Таким образом, среди систем (1.17), (1.22) и (1.23) выделены, соответственно, представления

$$\boldsymbol{S} = (\mathbf{C}, X, Y, \Psi), \tag{1.24}$$

$$\boldsymbol{S} = (\mathbf{C}, X, Y, \mathbf{\Phi}, \Psi) \tag{1.25}$$

и

$$\boldsymbol{S} = (C, X, Y, \mathbf{\Phi}, \Psi). \tag{1.26}$$

В них механизм вычисления значений выходной функции заложен в явном виде. Отметим, что существование производящего семейства выхода Ψ эквивалентно требованию о том, что *вся информация о предыстории системы до момента t содержится в состоянии системы в момент t*.

Системы (1.24)-(1.26) преобразуют сужения входной функции в значение выходной функции на правом конце промежутка. Такое понижение уровня преобразования (по сравнению с (1.17), (1.22) и (1.23)) существенно расширяет класс проблем анализа, допускающих эффективное решение.

Сложность описания производящего семейства выхода Ψ, в свою очередь, обосновывает переход к *семейству выходных функций*

$$\Omega = \{\omega_t = \mu_{tt} \mid t \in T\}.$$

Таким образом, среди систем (1.24)-(1.26) выделены, соответственно, представления

$$\boldsymbol{S} = (\mathbf{C}, X, Y, \Omega), \tag{1.27}$$

$$\boldsymbol{S} = (\mathbf{C}, X, Y, \Phi, \Omega) \tag{1.28}$$

и

$$\boldsymbol{S} = (C, X, Y, \Phi, \Omega). \tag{1.29}$$

Дальнейшее понижение уровня абстракции можно осуществить за счет выделения среди (1.27)-(1.29) систем, допускающих переход от семейства функций перехода состояний Φ к полугруппе его образующих. Именно такой переход, в частности, дает возможность выделить среди (1.29) класс систем, известных под именем *автоматы*.

В заключение, выделим некоторые фундаментальные классы систем.

Все многообразие временных систем естественно делится на *стационарные* и *не стационарные*. Пусть U - множество временных функций, определенных на множестве моментов времени T. Оператор сдвига

$$F^{\Delta t} : U\big|_{\{\tau \in T \mid \tau \geq t\}} \to U\big|_{\{\tau \in T \mid \tau \geq t + \Delta t\}} \ (\Delta t \in T)$$

определяется равенством

$$F^{\Delta t}(u)(t) = u(t + \Delta t) \ (\Delta t \in T, u \in U).$$

В наиболее общем случае *стационарная система* может быть определена следующим образом.

Определение 1.4. Общая временнáя система $\boldsymbol{S}$ называется *стационарной*, если при всех $t \in T$ оператор сдвига $F^{\Delta t}$ $(\Delta t \in T)$ переводит сужение $\boldsymbol{S}\big|_t$ в сужение $\boldsymbol{S}\big|_{t+\Delta t}$.

Систему, не являющуюся стационарной, часто называют *системой с переменной структурой*. Отличительной особенностью таких систем является наличие параметра $t\,(t \in T)$ в качестве существенной переменной в функциях, определяющих переходы состояний и/или выход системы.

С помощью спецификации множества моментов времени T можно выделить *непрерывные* и *дискретные* системы.

Для *непрерывных* систем, как правило, $T = \mathbf{R}_+$, $A \subseteq \mathbf{R}^m$, $B \subseteq \mathbf{R}^n$, X и Y - компактные множества (по крайней мере) кусочно-непрерывных функций, замкнутые относительно операций сужения и сочленения, семейство $\mathbf{f}$ состоит из непрерывных отображений, а элементы семейств Φ и Ω определяются с помощью систем дифференциальных уравнений.

Для *дискретных* систем, как правило, $T = \mathbf{N}$ или $T = \mathbf{Z}_+$, $A \subseteq \mathbf{Z}_{k_1}^m$ и $B \subseteq \mathbf{Z}_{k_2}^n$. Отличительной особенностью дискретных систем является большое разнообразие математических моделей, используемых для их описания. Именно это обстоятельство и определяет большое разнообразие методов, применяемых для анализа и синтеза дискретных систем.

1.2. Проблемы идентификации систем.

Широкий класс как фундаментальных, так и прикладных *проблем анализа дискретных систем* допускает их естественное сведение к *проблемам идентификации*. По этой причине в настоящем пункте изложим новую интерпретацию некоторых результатов из [11,28,90], на основе которой будут проводиться исследования в последующих разделах.

Говоря неформально, *процесс идентификации* реального объекта, процесса или явления состоит из ряда последовательно выполняемых этапов. Поскольку на эти этапы будут иногда ссылки, сведем их в один процесс.

Процесс 1.1. (Идентификация реального объекта, процесса или явления).

Этап 1.1. Сбор данных.

Этап 1.2. Выбор типа математической модели для описания анализируемого объекта (соответственно, процесса или явления).

Этап 1.3. Определение подкласса моделей выбранного типа в качестве возможных кандидатов.

Этап 1.4. Выбор метода идентификации в терминах определенного подкласса моделей.

Этап 1.5. Осуществление (т.е. реализация) процесса идентификации.

Этап 1.6. Анализ полученных результатов в терминах выбранной модели.

Этап 1.7. Интерпретация полученных результатов в терминах исходного объекта (соответственно, процесса или явления).

Процесс 1.1 является, по своей сути, *итеративным*. Выделим следующие два существенно различных типа итеративности.

Тип 1.1. Итеративность, непосредственно связанная с начальной стадией процесса идентификации, т.е. с выбором и анализом математической модели (этапы 1.2-1.4).

Тип 1.2. Итеративность, непосредственно связанная со стадией доработки выбранных средств (этапы 1.3-1.7) и предназначенная для повышения качества (и/или точности) идентификации.

Процесс 1.1 связан как с *реальным объектом*, так и с *математическими моделями*. Это означает, что он с необходимостью должен использовать как инженерные, так и математические методы (в том числе *компьютерное моделирование*). При таком широком понимании проблемы идентификации ее весьма сложно исследовать в общем случае. Поэтому, как правило, термин *идентификация* используется только применительно к *уровню математических моделей*, т.е. в узком смысле этого слова. Выбранные математические модели принято называть *системами*. По этой причине и используется термин *идентификация систем*. Этот термин отражает очень важную характеристику, а именно: *идентификация систем* представляет собой *направление в теории систем*. В настоящее время имеется значительное число публикаций, посвященных как различным разделам этого направления, так и идентификации систем в целом. Обширную библиографию работ по идентификации систем можно найти, практически, в каждом учебнике или монографии, посвященным этим проблемам (см., напр., [28]).

При решении проблем идентификации среди всего многообразия систем, как правило, выделяют *непрерывные* и *дискретные*. Для этих классов существенно различаются как модели, используемые для описания систем, так и допустимые методы анализа.

Отличительной особенностью теории дискретных систем является чрезвычайно широкий спектр существенно различающихся между собой математических моделей *нечисловой природы*, т.е. теоретико-множественных, логических, лингвистических и т.д. Это означает, что основным методом построения решений является *поиск*.

При решении проблем идентификации дискретных систем выделим следующие три уровня абстракции.

Уровень 1.1. Исследуемая система рассматривается как *абсолютный черный ящик*, т.е. вообще ничего не известно ни о ее структуре, ни о ее параметрах.

Единственно возможным подходом к решению проблемы идентификации в таких условиях является синтез той или иной системы, преобразующей заданное множество вход-выходных пар точно также, как и исследуемая система. Очевидно, что такое решение является, по своей сути, приближенным.

Уровень 1.2. Исследуемая система рассматривается как *относительный черный ящик*, т.е. практически ничего не известно о ее структуре, но заданы верхние границы ее параметров.

В этом случае класс возможных кандидатов на модель – *конечный*. Это означает, что проблема идентификации системы, по крайней мере, теоретически, может быть решена с той или иной степенью точности тем или иным методом поиска.

Уровень 1.3. Структуры возможных кандидатов на модель описаны (как правило, в неявной форме).

Анализ этих структур представляет собой основу для разработки оптимальных процедур идентификации дискретных систем. Такая ситуация является типичной для абсолютного большинства прикладных проблем. Поэтому, в дальнейшем проблемы идентификации дискретных систем будем рассматривать именно на этом уровне абстракции.

Как правило, исследуемая проблема идентификации дискретной системы будет сформулирована в одной из следующих двух форм.

Проблема 1.1. Для заданной системы $\boldsymbol{S}$ и для заданного конечного множества систем $\boldsymbol{U} = \{\boldsymbol{S}_i \mid i \in I\}$ требуется проверить выполнено ли условие $\boldsymbol{S} \in \boldsymbol{U}$. В случае положительного ответа необходимо найти такую систему $\boldsymbol{S}_j \in \boldsymbol{U}$, что справедливо равенство $\boldsymbol{S} = \boldsymbol{S}_j$.

Проблема 1.2. Задана система $\boldsymbol{S}_0$ и конечное множество систем $\boldsymbol{U}\ (\boldsymbol{S}_0 \notin \boldsymbol{U})$. Для заданной системы $\boldsymbol{S} \in \{\boldsymbol{S}_0\} \cup \boldsymbol{U}$ необходимо проверить, выполнено ли равенство $\boldsymbol{S} = \boldsymbol{S}_0$.

Следует особо отметить, что при решении проблем 1.1 и 1.2, как правило, имеют место следующие два обстоятельства:

1) множество $\boldsymbol{U}$ задано в неявной форме, т.е. имеется то или иное описание того, что является элементом множества $\boldsymbol{U}$;
2) мощность множества $\boldsymbol{U}$ достаточно велика.

Класс методов, применяемых при решении проблем 1.1 и 1.2, в значительной мере определяется как типом выбранной модели системы, так и методами, допустимыми непосредственно в процессе идентификации. Последние, обычно, определяются с помощью *специального комплекса условий*.

Рассмотрим кратко основные особенности решения проблем идентификации дискретных систем, связанные с выбором уровня абстракции при определении понятия *система*.

На уровне 1.1 выбранная модель *системы* является *системой типа отношение* (т.е. имеет вид (1.1) или (1.9)). Это означает, что проблемы 1.1 и 1.2 представляют собой *проблему идентификации отношения*, т.е. подмножества заданного множества. Возможны следующие два случая.

Случай 1.1. Заданное множество рассматривается как *абстрактное множество*.

Случай 1.2. На заданном множестве определена та или иная *алгебраическая структура*.

В случае 1.1 единственно возможным методом решения проблем идентификации дискретной системы является *исчерпывающий поиск*, организованный тем или иным образом. В случае 1.2 *кроме* или *вместо* поиска могут быть применены *методы современной алгебры*. Одним из наиболее успешных примеров такого подхода является использование алгебраических методов в теории кодирования, т.е. методов, основанных на *теории конечных полей*.

Отметим, что идентификация подмножества часто может быть сведена к *проблеме поиска множества представителей заданного семейства множеств*. Поэтому, исчерпывающее решение этой проблемы имеет исключительное значение.

На уровне 1.2 выбранная модель *системы* является *относительным черным ящиком* (т.е. имеет вид (1.15)). В этом случае заданное конечное множество систем $\boldsymbol{U}$ часто может быть представлено в виде множества $\boldsymbol{F}$ возможных глобальных реакций. Это означает, что проблемы идентификации дискретной системы сводятся к идентификации отображения, определенного на заданном множестве. При этом, возникают те же ситуации, что и в рассмотренных выше случаях 1.1 и 1.2.

На уровне 1.3 выбранная модель *системы* является *динамической системой*. В этом случае заданное конечное множество систем $\boldsymbol{U}$ часто может быть представлено в виде декартового произведения множеств допустимых функций перехода состояний и функций выхода. Это означает, что проблемы идентификации дискретной системы сводятся к *проблемам идентификации состояний* специальным образом построенной системы.

Выше было отмечено, что при решении проблем идентификации дискретных систем мощность множества $\boldsymbol{U}$ заданных систем, как правило, велика. Поэтому, естественно возникает следующая проблема.

Проблема 1.3. Выделить такое достаточно малое по мощности подмножество $\boldsymbol{U}'$ множества $\boldsymbol{U}$, что решение проблемы идентификации системы для множества $\boldsymbol{U}'$ однозначно определяет решение проблемы идентификации системы для множества $\boldsymbol{U}$.

Для решения проблемы 1.3 достаточно разработать эффективный механизм представления реакции любой системы $\boldsymbol{S} \in \boldsymbol{U}$ в виде композиции реакций систем, принадлежащих множеству $\boldsymbol{U}'$.

Так как множество $\boldsymbol{U}$ задается, как правило, в неявном виде, то сложность решения проблемы 1.3 достаточно велика. Поэтому, при решении прикладных проблем часто используется следующий *инверсный* подход. Определяется достаточно малое по мощности подмножество $\boldsymbol{U}_{\mathrm{ker}}$ множества $\boldsymbol{U}$. Это подмножество называется *ядром*. Решается проблема идентификации системы, принадлежащей ядру $\boldsymbol{U}_{\ker}$. После этого решается проблема поиска как можно более широкого класса $[\boldsymbol{U}_{\ker}]$ систем, *совместимых с найденным решением*. Множество $[\boldsymbol{U}_{\ker}]$ называется замыканием ядра $\boldsymbol{U}_{\ker}$. Отметим, что именно этот подход часто используется при построении тестов для дискретных устройств.

1.3. Конечные автоматы.

Стационарные дискретные системы вида (1.29) с конечными пространством состояний, входным и выходным алфавитами называются *конечными автоматами*. Для краткости, в словосочетании *конечный автомат*, слово *конечный*, в дальнейшем, будет опускаться. Для автоматов семейство выходных функций – одноэлементное, а семейство функций перехода состояний может быть компактно представлено конечным числом образующих. Ниже используются стандартные определения, термины и обозначения *теории автоматов* (см., напр., [11,25,90,110,114]).

Автомат – это пятерка объектов $M = (Q, X, Y, \delta, \lambda)$, где Q, X и Y - непустые конечные *множество состояний*, *входной* и *выходной алфавиты*, а $\delta : Q \times X \to Q$ и $\lambda : Q \times X \to Y$ - *функции переходов* и *выходов*. Если представляют интерес только переходы состояний, то автомат определяется как тройка объектов $M = (Q, X, \delta)$, т.е. выходной алфавит и функция выходов опускаются.

Обозначим через A^+ множество всех непустых слов в алфавите A (т.е. $A^+ = \bigcup_{i=1}^{\infty} A^i$), а через A^* - множество всех слов в алфавите A, включая и *пустое слово* Λ (т.е. $A^* = \{\Lambda\} \cup A^+$).

Функции δ и λ расширим до функций $\widetilde{\delta} : Q \times X^* \to Q$ и $\widetilde{\lambda} : Q \times X^* \to Y^*$ следующим образом:

$$\widetilde{\delta}(q, \Lambda) = q, \qquad \widetilde{\delta}(q, px) = \delta(\widetilde{\delta}(q, p), x),$$
$$\widetilde{\lambda}(q, \Lambda) = \Lambda, \qquad \widetilde{\lambda}(q, px) = \widetilde{\lambda}(q, p)\lambda(\widetilde{\delta}(q, p), x)$$

для всех $q \in Q$, $p \in X^*$ и $x \in X$.

Пусть Q_0 $(\varnothing \neq Q_0 \subseteq Q)$ - *множество допустимых начальных состояний* т.е. перед подачей любого входного слова автомат M находится в некотором состоянии $q \in Q_0$. Упорядоченная пара (M, Q_0) называется *слабоинициальным автоматом*. В специальном случае, когда $|Q_0| = 1$, слабоинициальнвй автомат называется *инициальным*.

Проблемы, возникающие при экспериментальном анализе поведения автомата, впервые исследованы в [32]. Систематически *теория экспериментов с автоматами* впервые изложена в [11]. Эксперимент с автоматом состоит в подаче входных слов и анализе соответствующих реакций. Многообразие экспериментов с автоматом определяется:

1) *объектом идентификации*, т.е. состояние слабоинициального автомата, автомат, принадлежащий заданному классу автоматов, автомат с неисправностями (т.е. обнаружение или локализация неисправностей в автомате) и т.д.;
2) *числом экземпляров* (*копий*) *автомата*, используемых в процессе эксперимента, т.е. *простой эксперимент*, если используется единственный экземпляр автомата и *кратный эксперимент*, если используется не менее двух копий автомата;

3) *способом исполнения эксперимента*, т.е. *безусловный эксперимент*, если при каждой реализации эксперимента подаются одни и те же входные слова и *адаптивный* (или *условный*) *эксперимент*, если каждый входной символ, начиная со второго, формируется в зависимости от реакции на предыдущие символы.

В [11] показано, что почти все типы экспериментов с автоматами могут быть сведены к экспериментам по идентификации состояний автомата. При этом, были выделены три основных типа экспериментов по идентификации состояний автомата:

1) *диагностические*, т.е. по идентификации начального состояния заданного слабоинициального автомата;
2) *установочные*, т.е. по идентификации финального состояния заданного слабоинициального автомата;
3) *синхронизирующие*, т.е. по переводу всех начальных состояний заданного слабоинициального автомата в одно и то же состояние.

Слова, подаваемые на автомат в процессе этих экспериментов, получили название, соответственно, *диагностических*, *установочных* и *синхронизирующих*. Именно синтез этих слов является основным фактором для эксперимента с автоматом. Формально указанные слова определяются следующим образом.

Для заданного слабоинициального автомата (M,Q_0) $(|Q_0|\ge 2)$ входное слово $p\in X^+$ называется:

1) *диагностическим*, если

$$\widetilde{\lambda}(q',p)=\widetilde{\lambda}(q'',p)\Rightarrow q'=q''$$

для всех $q',q''\in Q_0$;

2) *установочным*, если

$$\widetilde{\lambda}(q',p)=\widetilde{\lambda}(q'',p)\Rightarrow \widetilde{\delta}(q',p)=\widetilde{\delta}(q'',p)$$

для всех $q',q''\in Q_0$;

3) *синхронизирующим*, если

$$\widetilde{\delta}(q',p)=\widetilde{\delta}(q'',p)$$

для всех $q',q''\in Q_0$.

Таким образом, реакции на диагностические и установочные слова идентифицируют, соответственно, начальное и финальное состояние слабоинициального автомата (M,Q_0). Синхронизирующее слово переводит все начальные состояния автомата в одно и то же финальное состояние. Следовательно, синхронизирующее слово идентифицирует финальное состояние слабоинициального автомата. Так как в определении синхронизирующих слов вообще не задействована функция выходов, то при их построении и анализе рассматривают, как правило, автоматы без выхода. Для краткости, диагностические, установочные и синхронизирующие слова будем называть *идентифицирующими*.

Среди идентифицирующих слов естественно выделяются *минимальные* (по длине) и *неприводимые* (или *не избыточные*). Последние характеризуются тем, что при вычеркивании в них хотя бы одной буквы теряется свойство ‘быть идентифицирующим’. Для минимизации сложности исполнения эксперимента предпочтительно подавать на автомат минимальные слова, т.к. именно эти слова характеризуют *внутреннюю сложность* экспериментов по идентификации состояний автомата.

Диагностические слова используются при исследовании *наблюдаемости*, а установочные и синхронизирующие слова – при исследовании *управляемости* дискретных систем, представленных моделями с конечным числом состояний (см., напр., [14]). Таким образом, разработка и исследование сложности методов построения минимальных и неприводимых идентифицирующих слов, оценка длин минимальных таких слов являются актуальными для решения *проблем анализа контроллепригодности дискретных систем*, а также при решении проблем анализа и синтеза *систем дискретных событий*, интерес к которым резко возрос за последнее время (см., напр., [113,118,137]).

В [11] предложены методы поиска всех минимальных диагностических и установочных слов, основанные на *восстановлении начальных отрезков*. Основная конструкция – *дерево преемников* для заданного слабоинициального автомата (M,Q_0). Оно представляет собой размеченное корневое ориентированное ранжированное дерево, уровни которого занумерованы неотрицательными целыми числами. Вершины отмечены A-*группами* (т.е. мультимножествами мультимножеств множества Q), а дуги – элементами множества X в соответствии со следующими двумя правилами.

Правило 1.1. Единственная вершина 0-го уровня – корень дерева – отмечена A-группой $\{Q_0\}$.

Правило 1.2. Пусть вершина v i-го уровня отмечена A-группой $S=\{\sigma_1,\ldots,\sigma_j\}$. Из вершины v выходят $|X|$ дуг, ведущих в вершины $(i+1)$-го уровня. Эти дуги отмечены элементами множества X, причем отметки различных дуг – различные. Дуга, выходящая из вершины v и отмеченная символом x $(x\in X)$ ведет в вершину, отмеченную следующей A-группой: каждое мультимножество $\sigma\in S$ разбивается на мультимножества состояний с одной и той же реакцией на символ x и каждое состояние q заменяется его x-преемником, т.е. состоянием $\delta(q,x)$.

При поиске минимальных диагностических и установочных слов *правила обрыва путей* в дереве преемников основаны на отношении равенства A-групп и выделении A-групп, определяющих завершение процесса восстановления начальных отрезков.

В [136] предложен метод построения акцептора, представляющего множество всех диагностических слов. Состояниями этого акцептора являются разбиения множества Q. В этом методе, фактически, обоснована возможность использование техники *восстановления финальных отрезков* при построении идентифицирующих слов для заданного слабоинициального автомата.

Большая сложность подхода, предложенного в [11], во многом обусловлена организацией поиска. Таким образом, естественно возникают проблемы исследования структуры множеств идентифицирующих слов и разработки математических основ для унифицированной генерации методов поиска минимальных и неприводимых идентифицирующих слов. Этим проблемам посвящены работы [53,56,60,61].

Исследование сложности поиска минимальных идентифицирующих слов играет важную роль в теории автоматов и ее приложениях. Эта сложность характеризуется оценками длин указанных слов, а так же перечислением автоматов в соответствии со свойствами, формулируемыми в терминах длин этих слов. Проблемы перечисления автоматов систематически исследованы в [25]. Ряд проблем перечисления, связанных с *теорией экспериментов с автоматами*, решен в [54,57].

Множество всех диагностических, установочных и синхронизирующих слов для слабоинициального автомата (M,Q_0) обозначим, соответственно, через $D(M,Q_0)$, $H(M,Q_0)$ и $S(M,Q_0)$. Очевидно, что имеют место следующие включения

$$D(M,Q_0)\subseteq H(M,Q_0),\qquad S(M,Q_0)\subseteq H(M,Q_0).$$

Пусть $U(M,Q_0) \in \{D(M,Q_0), H(M,Q_0), S(M,Q_0)\}$. Обозначим через $U^{\min}(M,Q_0)$ и $U^{ir}(M,Q_0)$ множество всех, соответственно, минимальных и неприводимых слов, принадлежащих множеству $U(M,Q_0)$. Очевидно, что имеют место следующие включения

$$U^{\min}(M,Q_0) \subseteq U^{ir}(M,Q_0) \quad (U \in \{D,H,S\}).$$

Длину минимального диагностического, установочного и синхронизирующего слова для слабоинициального автомата (M,Q_0) обозначим, соответственно, через $L^d(M,Q_0)$, $L^h(M,Q_0)$ и $L^s(M,Q_0)$. Если для слабоинициального автомата (M,Q_0) диагностическое (соответственно, установочное или синхронизирующее) слово не существует, то считаем, что $L^d(M,Q_0)=0$ (соответственно, $L^h(M,Q_0)=0$ или $L^s(M,Q_0)=0$).

Обозначим через $\mathbf{A}_{kmn}$ множество всех автоматов $M=(Q,X,Y,\delta,\lambda)$, имеющих фиксированные множество состояний $Q=\{q_1,\ldots,q_k\}$, входной алфавит $X=\{x_1,\ldots,x_m\}$ и выходной алфавит $Y=\{y_1,\ldots,y_n\}$. Определим отображения

$$L^u_{kmn}:\{2,\ldots,k\} \to \mathbf{Z}_+ \quad (u \in \{d,h,s\})$$

равенством

$$L^u_{kmn}(r) = \max L^u(M,Q_0) \quad (r \in \{2,\ldots,k\}),$$

где максимум берется по всем $M \in \mathbf{A}_{kmn}$ и всем таким $Q_0 \subseteq Q$, что $|Q_0|=r$ и положим

$$L^u_{kmn} = \max_{r\in\{2,\ldots,k\}} L^u_{kmn}(r).$$

Отметим, что $L^d_{kmn}(r)$, $L^h_{kmn}(r)$, $L^s_{kmn}(r)$, L^d_{kmn}, L^d_{kmn} и L^d_{kmn} представляют собой *функции Шеннона*, характеризующие сложность построения минимальных идентифицирующих слов.

Исследованию длин минимальных идентифицирующих слов для слабоинициального автомата посвящен ряд работ. В [111] установлена точная оценка максимальной длины минимального установочного слова

$$L^h_{kmn}(r) = 0.5(2k-r)(r-1) \quad (r \in \{2,\ldots,k\}).$$

В [114] доказано, что в специальном случае, когда $Q_0=Q$, справедлива следующая верхняя оценка длины минимального синхронизирующего слова

$$L^s_{kmn}(k) \le 0.5k(k-1)^2.$$

Имеется много невыясненных моментов, связанных с оценками длин минимальных диагностических слов. Верхние оценки

$$L^d_{kmn}(r) \le (r-1)k^r \quad (r \in \{2,\ldots,k\})$$

и

$$L^d_{kmn}(r) \le k! \quad (r \in \{2,\ldots,k\})$$

установлены, соответственно, в [11] и в [136]. В [88,89] доказано, что справедливы верхняя оценка

$$L^d_{kmn}(r) \le \begin{cases} (r-1)k^{0.5k(1+\varepsilon)}, & \text{если } r \in \{2,\ldots,k-1\}, \\ \dbinom{k}{0.5k}, & \text{если } r=k, \end{cases}$$

где $\varepsilon \to 0$ при $r \to \infty$, а также нижняя оценка

$$L^d_{kmn}(r) \ge \begin{cases} \dbinom{k-1}{r-1}, & \text{если } r \in \{2,\ldots,\lfloor 0.5k \rfloor\}, \\ \dbinom{\mathrm{k-2}}{\lfloor 0.5(\mathrm{k-2}) \rfloor}, & \text{если } r \in \{\lfloor 0.5k \rfloor + 1,\ldots,k-1\}, \\ 3^{\left\lfloor \frac{1}{6}k \right\rfloor}, & \text{если } r = k. \end{cases}$$

В [45,46] доказано, что в специальном случае, когда $Q_0 = Q$, справедлива следующая асимптотически точная оценка

$$\log_3 L^d_{kmn}(k) \sim \frac{k}{6} \quad (k \to \infty).$$

Работы [45,46,88,89] объединяет то, что используемые в них автоматы имеют входной алфавит, мощность которого, фактически, совпадает с длиной минимального идентифицирующего слова. Это означает, что установленная в этих работах длина минимального идентифицирующего слова не превосходит память, необходимую для хранения таблицы переходов-выходов, определяющей автомат.

Исследованию нижних оценок длин минимальных диагностических и синхронизирующих слов посвящена также работа [63]. Существенным ее отличием от работ [45,46,88,89] является то, что в ней используются только автоматы с двухбуквенным входным алфавитом. Именно это обстоятельство позволило установить, что нижняя оценка длин минимальных диагностических и синхронизирующих слов является *экспонентой* от размера памяти, необходимой для хранения таблицы переходов-выходов, определяющей автомат.

1.4. Булевы функции.

Пусть $\mathbf{E} = \{0,1\}$ и $\mathbf{E}^n = \underbrace{\mathbf{E} \times \ldots \times \mathbf{E}}_{n \text{ раз}}$ $(n \in \mathbf{N})$. Переменная x называется *булевой*, если $x \in \mathbf{E}$. *Булевой функцией* называется любое отображение $f : \mathbf{E}^n \to \mathbf{E}$ $(n \in \mathbf{N})$. Булеву функцию $f(x_1,\ldots,x_n)$ $(n \in \mathbf{N})$ можно задать таблицей, содержащей 2^n строк и $n+1$ столбец. В каждой строке таблицы первые n столбцов содержат комбинацию значений переменных, а последний столбец – соответствующее значение функции f. Как правило, комбинация значений переменных, записанная в i-й строке $(i = 1,\ldots,2^n)$, является двоичным кодом десятичного числа $i-1$.

Зафиксируем бесконечную последовательность булевых переменных

$$x_1, x_2, \ldots, x_n, \ldots.$$

Обозначим через $P_2(n)$ $(n \in \mathbf{N})$ множество всех булевых функций от переменных $x_1,\ldots,x_n$. Булевы функции $f, g \in P_2(n)$ $(n \in \mathbf{N})$ *равны* друг другу (обозначается $f = g$), если они определяют одно и тоже отображение. Для функции $f \in P_2(n)$ $(n \in \mathbf{N})$ положим

$$\boldsymbol{N}_f = \{\mathbf{e} \in \mathbf{E}^n \mid f(\mathbf{e}) = 1\}.$$

Если a - булева переменная или булева функция и $\sigma \in \mathbf{E}$, то

$$a^\sigma = \begin{cases} a, \text{ если } \sigma = 1, \\ \bar{a}, \text{ если } \sigma = 0 \end{cases}. \tag{1.30}$$

Из (1.30) вытекает, что справедливы равенства

$$\sigma^{\sigma}=1,\quad \sigma^{\bar\sigma}=0,\quad \bar\sigma^{\sigma}=0\quad (\sigma\in\mathbf{E}).$$

В дальнейшем выражение x^{σ} $(\sigma\in\mathbf{E})$, где x - булева переменная (т.е булеву переменную или ее отрицание), будем называть *литералом*.

Известно, что для любой булевой функции $f\in P_2(n)$ $(n\in\mathbf{N})$ справедливы равенства

$$f(x_1,\ldots,x_n)=\bigvee_{(\sigma_1,\ldots,\sigma_n)\in \boldsymbol{N}_f} x_1^{\sigma_1}\ldots x_n^{\sigma_n} \tag{1.31}$$

и

$$f(x_1,\ldots,x_n)=\bigwedge_{(\sigma_1,\ldots,\sigma_n)\in \mathbf{E}^n\setminus \boldsymbol{N}_f} (x_1^{\bar\sigma_1}\vee\ldots\vee x_n^{\bar\sigma_n}). \tag{1.32}$$

Отметим, что по определению $\bigvee_{a\in\varnothing} a=0$ и $\bigwedge_{a\in\varnothing} a=1$. Представление булевой функции $f\in P_2(n)$ $(n\in\mathbf{N})$, определяемое равенством (1.31), называется *совершенной дизъюнктивной нормальной формой* (СДНФ) и обозначается $D_f^{сов}$. Аналогичным образом, представление булевой функции $f\in P_2(n)$ $(n\in\mathbf{N})$, определяемое равенством (1.32), называется *совершенной конъюнктивной нормальной формой* (СКНФ) и обозначается $K_f^{сов}$.

Выражения

$$x_{i_1}^{\beta_1}\ldots x_{i_r}^{\beta_r}\qquad (1\le i_1<\ldots<i_r,\ r\ge 1) \tag{1.33}$$

и

$$x_{i_1}^{\beta_1}\vee\ldots\vee x_{i_r}^{\beta_r}\qquad (1\le i_1<\ldots<i_r,\ r\ge 1), \tag{1.34}$$

где $\beta_j\in\mathbf{E}$ $(j=1,\ldots,r)$, называются, соответственно, *элементарной конъюнкцией и элементарной дизъюнкцией* ранга r. Ранг элементарной конъюнкции K обозначим через $Rank\ K$. Элементарная конъюнкция (1.33) и элементарная дизъюнкция (1.34) могут рассматриваться как булева функция $f\in P_2(n)$ при любом $n\in\mathbf{N}$, удовлетворяющем неравенству

$$n\ge i_r. \tag{1.35}$$

Пусть неравенство (1.35) выполнено. Булевы функции $g,h\in P_2(n)$ $(n\in\mathbf{N})$ определим равенствами

$$g(x_1,\ldots,x_n)=x_{i_1}^{\beta_1}\ldots x_{i_r}^{\beta_r} \tag{1.36}$$

и

$$h(x_1,\ldots,x_n)=x_{i_1}^{\beta_1}\vee\ldots\vee x_{i_r}^{\beta_r}, \tag{1.37}$$

где $\beta_j\in\mathbf{E}$ $(j=1,\ldots,r)$. Тогда

$$\boldsymbol{N}_g=\{\mathbf{e}=(\alpha_1,\ldots,\alpha_n)\in\mathbf{E}^n\mid \alpha_{i_j}=\beta_j\ (j=1,\ldots,r)\} \tag{1.38}$$

и

$$\mathbf{E}^n\setminus\boldsymbol{N}_h=\{\mathbf{e}=(\alpha_1,\ldots,\alpha_n)\in\mathbf{E}^n\mid \alpha_{i_j}=\bar\beta_j\ (j=1,\ldots,r)\}. \tag{1.39}$$

При интерпретации множества $\mathbf{E}^n$ как *n-мерного единичного куба* множества (1.38) и (1.39) являются *$(n-r)$-мерными гранями*. Размерность грани, определяемой элементарной конъюнкцией K, обозначим через $Dim\ K$. Отметим, что для любой элементарной конъюнкции $K\in P_2(n)$ справедливо равенство

$$Rank\ K+Dim\ K=n.$$

Элементарная конъюнкция g, определяемая равенством (1.36), *называется импликантой* булевой функции $f\in P_2(n)$ $(n\in\mathbf{N})$ тогда и только тогда, когда справедливо включение $\boldsymbol{N}_g \subseteq \boldsymbol{N}_f$. Булева функция $f \in P_2(n)$ $(n \in \mathbf{N})$ представлена в *дизъюнктивной нормальной форме* (ДНФ), если

$$f(x_1,\ldots,x_n) = \bigvee_{j=1}^{h} K_j,$$

где $K_1,\ldots,K_h$ - импликанты функции f. Аналогичным образом, булева функция $f \in P_2(n)$ $(n \in \mathbf{N})$ представлена в *конъюнктивной нормальной форме* (КНФ), если

$$f(x_1,\ldots,x_n) = \bigwedge_{j=1}^{h} D_j,$$

где $D_1,\ldots,D_h$ - элементарные дизъюнкции. В дальнейшем будут рассматриваться только ДНФ, т.к., в соответствии с *принципом двойственности*, любая конструкция или утверждение, полученные для ДНФ, легко могут быть переформулированы в терминах КНФ (см., напр., [18]).

Для булевой функции $f \in P_2(n)$ $(n \in \mathbf{N})$ могут существовать различные ДНФ. При этом, имеется взаимно-однозначное соответствие между множеством всех ДНФ булевой функции $f \in P_2(n)$ и множеством всех покрытий множества $\boldsymbol{N}_f$ содержащимися в нем гранями. ДНФ

$$D = \bigvee_{j=1}^{h} K_j \tag{1.40}$$

булевой функции $f \in P_2(n)$ $(n \in \mathbf{N})$ называется:

1) *минимальной*, если она содержит наименьшее число вхождений *литералов*;
2) *тупиковой*, если, при удалении хотя бы одной импликанты, оставшиеся импликанты не образуют ДНФ функции f.

Импликанта g булевой функции $f \in P_2(n)$ $(n \in \mathbf{N})$ называется *простой*, если каждая элементарная конъюнкция, получаемая из g в результате вычеркивания хотя бы одного литерала, не является импликантой функции f. Отметим, что имеется взаимно-однозначное соответствие между множеством всех простых импликант булевой функции $f \in P_2(n)$ и множеством всех граней максимальных размерностей, содержащихся в множестве $\boldsymbol{N}_f$. Среди ДНФ булевой функции $f \in P_2(n)$ $(n \in \mathbf{N})$ выделяются те, которые состоят из простых импликант. Они соответствуют покрытиям множества $\boldsymbol{N}_f$ содержащимися в нем гранями максимальных размерностей. Только такие ДНФ и рассматриваются в дальнейшем, т.к. именно они важны как при теоретических исследованиях, так и для многочисленных приложений.

ДНФ булевой функции $f \in P_2(n)$ $(n \in \mathbf{N})$, состоящая из всех простых импликант, называется *сокращенной* ДНФ и обозначается $D_f^{сокр}$. Эта ДНФ играет важную роль для исследования как минимальных, так и тупиковых ДНФ. Рассмотрим кратко основные методы построения сокращенной ДНФ $D_f^{сокр}$ $(f \in P_2(n)$ $(n \in \mathbf{N}))$.

Метод Квайна. Исходные данные - СДНФ $D_f^{сов}$. Применяются преобразования следующих двух типов (K - элементарная конъюнкция, x - булева переменная и $\sigma \in \mathbf{E}$):

1) *неполное склеивание*, т.е.

$$Kx \vee K\overline{x} = K \vee Kx \vee K\overline{x}; \tag{1.41}$$

2) *элементарное поглощение*, т.е.

$$Kx^{\sigma} \vee K = K. \tag{1.42}$$

Построение ДНФ $D_f^{сокр}$ осуществляется в соответствии со следующим алгоритмом.

Алгоритм 1.1.

Шаг 1. $i := 0$, $D_0 := D_f^{сов}$.

Шаг 2. Строим ДНФ D_i' в соответствии со следующим правилом: выполняем всевозможные преобразования (1.41) над всеми парами элементарных конъюнкций ранга $n-i$, принадлежащих D_i.

Шаг 3. Строим ДНФ D_{i+1} в соответствии со следующим правилом: удаляем из D_i' все элементарные конъюнкции ранга $n-i$, которые можно исключить в результате преобразования (1.42).

Шаг 4. Если D_i и D_{i+1} состоят из одних и тех же элементарных конъюнкций, то переход к шагу 6, иначе переход к шагу 5.

Шаг 5. $i := i+1$ и переход к шагу 2.

Шаг 6. $D_f^{сокр} := D_i$ и конец.

Метод Блейка. Исходные данные – любая ДНФ D булевой функции f. Применяются преобразования следующих двух типов (K_1, K_2 - элементарные конъюнкции, x - булева переменная):

1) *обобщенное склеивание*, т.е.

$$xK_1 \vee \bar{x}K_2 = xK_1 \vee \bar{x}K_2 \vee K_1K_2; \quad (1.43)$$

2) *поглощение*, т.е.

$$K_1 \vee K_1K_2 = K_1. \quad (1.44)$$

Построение ДНФ $D_f^{сокр}$ осуществляется в соответствии со следующим алгоритмом.

Алгоритм 1.2.

Шаг 1. $i := 0$, $D_0 := D$.

Шаг 2. Строим ДНФ D_i' в соответствии со следующим правилом: выполняем всевозможные преобразования (1.43) над всеми парами элементарных конъюнкций, принадлежащих D_i (при этом в D_i' не включаем ни одно из произведений K_1K_2 *ортогональных* конъюнкций, т.е в одну из которых входит некоторая переменная, а в другую конъюнкцию – отрицание этой переменной).

Шаг 3. Строим ДНФ D_{i+1} в соответствии со следующим правилом: удаляем из D_i' все элементарные конъюнкции, которые можно исключить в результате преобразования (1.44).

Шаг 4. Если D_i и D_{i+1} состоят из одних и тех же элементарных конъюнкций, то переход к шагу 6, иначе переход к шагу 5.

Шаг 5. $i := i+1$ и переход к шагу 2.

Шаг 6. $D_f^{сокр} := D_i$ и конец.

Метод Нельсона. Исходные данные – любая КНФ K булевой функции f. Применяются преобразования следующих трех типов (K_1, K_2, K_3 - элементарные конъюнкции, x - булева переменная):

1) *дистрибутивный закон*, т.е.

$$K_1(K_2 \vee K_3) = K_1K_2 \vee K_1K_3; \quad (1.45)$$

2) *правила дополнения*, т.е.

$$x\bar{x} = 0, \quad x \vee \bar{x} = 1; \tag{1.46}$$

3) *поглощение*, т.е. преобразование (1.44).

Алгоритм построения ДНФ $D_f^{сокр}$ состоит в последовательном раскрытии в КНФ K скобок в соответствии с (1.45). После каждого раскрытия скобок выполняются все возможные упрощения в соответствии с (1.44) и (1.46).

В заключение отметим следующие три особенности рассмотренных выше методов построения сокращенной ДНФ:

1. В каждом из рассмотренных выше методов построения сокращенной ДНФ, на промежуточных этапах возможен значительный рост объема памяти, необходимой для хранения результатов. Причем этот объем может совпадать с объемом памяти, необходимым для хранения сокращенной ДНФ, только на завершающих этапах алгоритма.
2. Ни один из рассмотренных выше методов построения сокращенной ДНФ не дает возможности строить простые импликанты, покрывающие заданную точку, со сложностью, существенно меньшей, чем сложность построения сокращенной ДНФ.
3. Метод Нельсона, в отличие от методов Квайна и Блейка, допускает *параллелизм* при построении сокращенной ДНФ (за счет независимого перемножения и обработки пар дизъюнкций).

1.5. Поиск.

Известно, что *поиск* является универсальным, и, часто, единственным, методом решения многих комбинаторных задач. Именно это обстоятельство и послужило основной причиной создания *теории поиска* – раздела дискретной математики, имеющего исключительное значение как в ней самой, так и в ее многочисленных приложениях. Стимулом к возникновению этой теории явились следующие два направления исследований.

Первое направление состоит в непосредственной разработке алгоритмов для решения конкретных задач (см., напр., [102.120]). Отметим некоторые из таких задач. По видимому, наиболее значимой из них является *задача построения кратчайших путей на графах*. Ее непосредственному исследованию посвящено большое число публикаций (см., напр., [6,103,108,112,123,133]). Было показано, что этой задаче эквивалентен ряд важных задач дискретной математики [23,122]. *Задача построения остовных деревьев для графа* также оказалась в центре внимания (см., напр., [104,115,134]). Обзоры, библиографии, а также основные результаты, связанные с двумя указанными задачами, представлены в работах [1,43,100,112,126,127,135]. Следует упомянуть, также, *целочисленное линейное программирование* [116] и *задачу коммивояжера* [99,101,115,121,124,135].

Второе направление связано с распространением *динамического программирования* на дискретный случай [3,4,98,128]. В этой связи следует особо отметить *анализ критических путей* в методе PERT (т.е. в *сетевом планировании*) [109].

В результате этих и дальнейших исследований для решения конкретных задач были предложены различные варианты поиска: *в глубину*, *в ширину*, *с возвращением*, *ветвей и границ*, *направленный*, *поэтапный*, *локальный* и т.д. Их анализ, совершенствование и детальная проработка позволили построить *общие методы поиска*, т.е. схемы, формулируемые в терминах теории множеств [1,5,34,35,38,43,117]. Теоретико-множественный (и, по существу, лингвистический) подход дал возможность формально доказать корректность общих методов поиска и выделить *классы выигрышных стратегий поиска* [5,34,35]. Все это привело к формированию единого подхода к решению конкретных задач методом поиска. Рассмотрим основные этапы, характерные для этого подхода.

Этап 1.8. Конкретная задача формулируется следующим образом.

Задача 1.1. Заданы допустимые *конфигурации*. Среди них выделены *исходные* и *целевые* конфигурации. Задано множество *воздействий*, переводящих одни конфигурации в другие.

Найти воздействия, обладающие требуемыми свойствами и переводящие исходные конфигурации в целевые конфигурации.

Для приведенной выше формулировки исследуемой задачи типичны следующие особенности.

Во-первых, чаще всего требуется найти воздействия, которые переводят в целевую конфигурацию либо фиксированную исходную конфигурацию, либо каждую из исходных конфигураций. Ясно, что в последнем случае искомые воздействия могут быть существенно различными для различных исходных конфигураций. Более того, такие воздействия могут существовать для одних исходных конфигураций и не существовать для других.

Во-вторых, допустимые, исходные и целевые конфигурации, как правило, *заданы в неявном виде*, т.е. дано описание того, что является соответствующей конфигурацией. Однако в тех случаях, когда количество исходных или целевых конфигураций невелико, они могут быть перечислены в явном виде.

В третьих, воздействия, обычно, представляют собой *наборы инструкций*. Каждый такой набор описывает последовательность операций, которую, если это осуществимо, необходимо выполнить над конфигурацией для того, чтобы получить новую конфигурацию.

Этап 1.9. Строится соответствующая *математическая модель*, которая называется *представлением* задачи 1.1. Построение математической модели осуществляется следующим образом. Конфигурациям ставятся в соответствие элементы некоторого абстрактного множества, быть может наделенного той или иной структурой. Это множество называется *множеством* (или *пространством*) *ситуаций*, а его элементы – *ситуациями*. Воздействиям ставятся в соответствие *операторы*, т.е. (возможно, частичные) отображения пространства ситуаций в себя. Указанные соответствия дают возможность выделить *начальную* и *финальные* ситуации. Ими являются именно те ситуации, которые соответствуют исходным и целевым конфигурациям. Определяется множество *решений*. Оно состоит из всех операторов, переводящих начальную ситуацию в множество финальных (такие операторы называются *выигрышными*) и удовлетворяющих *заданному комплексу условий*, сформулированных в терминах ситуаций и операторов. Отметим, что само множество всех выигрышных операторов является множеством всех решений при пустом комплексе условий. Формулируется следующая задача поиска.

Задача 1.2. Найти заданное множество решений (для выбранного представления задачи 1.1).

Построение математической модели является весьма сложным и трудоемким процессом. Причина этого состоит в следующем. Для любой задачи можно выбрать различные представления. От этого выбора, во многом, зависит сложность поиска искомых воздействий. Эвристические способы последовательного улучшения представлений ряда конкретных задач рассмотрены в [34,35,43]. Однако общие закономерности выбора *хороших представлений* до сих пор не изучены. Поэтому, как правило, приходится действовать по следующей схеме. Строятся различные представления задачи 1.1. Производится их сравнительный анализ. На основании результата этого анализа выбирается наилучшее или наиболее приемлемое представление.

Этап 1.10. Решается задача 1.2. Возможны следующие два случая.

Первый случай имеет место, если представление задачи 1.1 полностью укладывается в рамки известной теоретико-множественной схемы поиска. В качестве метода решения может быть выбрана любая выигрышная для этой схемы стратегия поиска. Часто удается существенно повысить ее эффективность за счет дополнительного учета конкретных особенностей выбранного представления.

Второй случай имеет место, когда представление задачи 1.1 не укладывается в рамки ни одной из известных схем поиска. В этом случае решение задачи 1.2 осуществляется, как правило, следующим образом. Исследуется строение выигрышных операторов. Устанавливаются свойства тех из них, которые удовлетворяют заданному комплексу условий. Исходя из этих свойств, строится соответствующая стратегия поиска. Доказывается ее корректность и оценивается сложность.

Этап 1.11. Найденные на предыдущем этапе *решения* интерпретируются в терминах *конфигураций* и *воздействий*.

Общие методы поиска являются теоретико-множественными схемами, предназначенными для решения задачи 1.2 в предположении, что зафиксирован тот или иной класс представлений. Этот класс определяется набором ограничений, наложенных на структуры пространства ситуаций и множества операторов. Любой общий метод поиска реализует итеративный процесс, в результате которого строится последовательность множеств операторов

$$\Omega_0, \Omega_1, \ldots, \Omega_l, \tag{1.47}$$

удовлетворяющая следующим трем условиям.

Условие 1.1. Множество Ω_0 состоит из всех операторов.

Условие 1.2. Включение

$$\Omega_i \subset \Omega_{i+1}$$

справедливо для всех $i \in \mathbf{Z}_l$.

Условие 1.3. Множество Ω_l состоит из всех решений.

Переход от множества Ω_i $(i \in \mathbf{Z}_l)$ к множеству Ω_{i+1} осуществляется с помощью *правил отсечения*. Эти правила предназначены для принятия решений о том, какие из принадлежащих множеству Ω_i операторов заведомо не являются искомыми. Множество Ω_{i+1} получается из множества Ω_i в результате удаления указанных операторов. Принятие решений, определяемое правилами отсечения, осуществляется только на основании заданного комплекса условий и свойств, характеризующих строение множества выигрышных операторов для выбранного класса представлений. Именно это обстоятельство и лежит в основе построения формальных методов доказательства корректности общих методов поиска. Следует отметить, что, как правило, множество всех операторов Ω_0 задано *неявно*, а множество Ω_l решений конструируется в *явном виде*. В процессе построения последовательности (1.47) как раз и происходит постепенный переход от неявного задания операторов к их представлению в явном виде.

Пустой набор ограничений при выборе представления задачи 1.1 определяет универсальный класс, которому принадлежат все представления. В этом случае пространство ситуаций рассматривается как абстрактное множество, состоящее из некоторых элементов, а операторы - как отображения, к которым применимы только теоретико-множественные понятия. Общие методы поиска, разработанные при таких предположениях, получили название *исчерпывающий поиск*. Их безусловным достоинством является *универсальность*, т.е. возможность решения задачи 1.2 для любого представления при любом комплексе условий. При исчерпывающем поиске осуществляется полный перебор вариантов. Ресурсы, требуемые для организации такого перебора, и определяют сложность исчерпывающего поиска. Эти ресурсы, как правило, весьма велики и никак не характеризуют затраты, действительно необходимые для построения решения конкретной задачи.

Большая сложность исчерпывающего поиска стимулировала изучение тех особенностей представлений конкретных задач, которые существенно влияют на строение множества выигрышных операторов. На этой основе был выделен достаточно общий класс представлений, определяемых следующим условием.

Условие 1.4. В пространстве ситуаций можно ввести *легко вычисляемую* меру, оценивающую *расстояние* от любой ситуации до множества финальных ситуаций.

Такие меры были названы *оценочными функциями*. Они дали возможность разработать правила отсечения, основанные на следующем принципе.

Принцип 1.1. В процессе построения последовательности (1.47) предпочтение отдается операторам, переводящим начальную ситуацию в ситуации, для которых значения оценочной функции экстремальны.

Исследования показали, что такие правила отсечения являются более сильными, чем правила отсечения, применяемые при исчерпывающем поиске. Поэтому, общие методы поиска, использующие оценочные функции, оказались более эффективными, чем исчерпывающий поиск. Следует отметить, что именно для методов, основанных на оценивании, и были получены наиболее сильные результаты теории поиска [5,34,43].

Однако для подавляющего большинства задач все попытки использования оценочных функций оказались безрезультатными. В числе таких задач оказался и ряд фундаментальных проблем самой дискретной математики, включая некоторые задачи теории экспериментов с автоматами и задачи минимизации ДНФ. Исследования показали, что правила отсечения, созданные на основе оценочных функций, используемые в теории экспериментов с автоматами, приводят к обычному поиску с возвращением. Последний, как известно, является вариантом исчерпывающего поиска. Более того, в настоящее время не известно, существуют ли вообще оценочные функции, которые дают возможность решать ряд задач теории экспериментов с автоматами более эффективным методом, чем исчерпывающий поиск. Для задач минимизации ДНФ картина совсем иная. В [19,20] доказано отсутствие локального критерия вхождения конъюнкции в объединение $D_{\cup M}$ всех минимальных ДНФ булевой функции. Таким образом, понятие оценочной функции вообще является бесполезным при решении задач минимизации ДНФ.

Подход, основанный на оценивании, сыграл важную роль для развития методологии поиска. В то же время, его значение как средства разработки конкретных алгоритмов поиска невелико. Это обусловлено следующими обстоятельствами. Для оценочных функций отсутствует конструктивное строгое математическое определение. Поэтому не может быть четко очерчен класс представлений, для которых такие функции существуют. Это означает, что не существует алгоритм, обеспечивающий конструктивное построение оценочной функции по представлению. Невозможно, также разработать средства, позволяющие с единых позиций сравнивать методы поиска, основанные на оценивании. И, наконец, класс представлений, для которых удалось построить оценочные функции, оказался достаточно узким.

Из сказанного выше вытекает, что одной из наиболее актуальных проблем теории поиска является разработка математического аппарата, обладающего следующими двумя особенностями. Во-первых, он дает возможность четко определить достаточно широкий класс представлений, заведомо включающий в себя представления, обладающие оценочными функциями. Во-вторых, он позволяет выработать для указанного класса представлений единый подход к разработке методов поиска, более эффективный, чем исчерпывающий поиск и естественно включающий в себя методы, основанные на оценивании. Именно таким подходом и является *поиск на частично упорядоченных структурах* [56,71,81,85,86].

Рассмотрим математическую модель, в рамки которой укладывается исследование проблем поиска.

Как было отмечено выше (см. этап 1.9), операторами являются (возможно, частичные) отображения множества ситуаций в себя. Всюду в дальнейшем будем считать, что выполнено следующее предположение.

Предположение 1.1. Множество операторов является конечно порожденной полугруппой по отношению к операции суперпозиции.

Предположение 1.1 дает возможность исследовать представление задачи 1.1 в рамках математической модели, определенной в терминах *акцептора* (или, иными словами, *распознавателя*) с конечным числом состояний [7,110,114] или, что то же самое, источника [90]. Рассмотрим соответствующие понятия и определения.

Определение 1.5. *Источником* назовем систему объектов

$$\mathbf{S} = (S, \mathsf{F}, s_{in}, S_{fin}),$$

где S - конечное *множество ситуаций*, F - конечное множество (возможно, частичных) отображений множества S в себя, s_{in} $(s_{in} \in S)$ - *начальная ситуация*, а S_{fin} $(\varnothing \neq S_{fin} \subseteq S \setminus \{s_{in}\})$ - *множество финальных ситуаций*.

Множество $\mathsf{F}^+ = \bigcup_{m=1}^{\infty} \mathsf{F}^m$, где $\mathsf{F}^m = \{f_1 \dots f_m \mid f_i \in \mathsf{F}\,(i = 1, \dots, m)\}$, представляет собой *свободную полугруппу*, порожденную множеством F. Термин *свободная полугруппа* означает, что *композиция* определена следующим образом: если $F = f_1 \dots f_m$ и $G = g_1 \dots g_n$ - элементы множества F^+, то $FG = f_1 \dots f_m g_1 \dots g_n$.

Будем называть F - *множеством элементарных операторов*, а F^+ - *множеством операторов*. Для операторов будем использовать *правую запись*, т.е. действие оператора $f_1 f_2 \dots f_m \in \mathsf{F}^+$ на ситуацию $s \in S$ определим равенством

$$s(f_1 f_2 \dots f_m) = (\dots((s f_1) f_2) \dots) f_m .$$

Обозначим через F_s^+ $(s \in S)$ множество всех таких операторов $f_1 \dots f_m \in \mathsf{F}^+$, что $s \in \mathrm{Dom}\, f_1$ и $sf_1 \dots f_{i-1} \in \mathrm{Dom}\, f_i$ для всех $i = 2, \dots, m-1$. Таким образом, если $F \in \mathsf{F}_s^+$ $(s \in S)$, то sF - ситуация, в которую оператор F переводит ситуацию s, а если $F \in \mathsf{F}^+ \setminus \mathsf{F}_s^+$, то sF не определено. Всюду в дальнейшем будем считать, что выполнено следующее условие.

Условие 1.5. $s_{in} \in \mathrm{Dom}\, f$ хотя бы для одного элементарного оператора $f \in \mathsf{F}$.

Отметим, что условие 1.5 – это критерий не пустоты множества $\mathsf{F}_{s_{in}}^+$.

Множество всех выигрышных операторов $\boldsymbol{L}(\mathbf{S})$ для источника $\mathbf{S}$ определим равенством

$$\boldsymbol{L}(\mathbf{S}) = \{F \in \mathsf{F}_{s_{in}}^+ \mid s_{in} \in S_{fin}\},$$

а длину $d(F)$ $(F \in \mathsf{F}^+)$ оператора F - формулой

$$d(F) = m \Leftrightarrow F \in \mathsf{F}^m.$$

Проиллюстрируем применение источника для решения конкретной задачи.

Пример 1.4. Рассмотрим следующий фрагмент *задачи о раскрое* – модельной задачи линейного программирования.

Для пошива ателье использует m видов заготовок ткани, имеющих длины $l_1, \dots, l_m$. Эти заготовки получаются при разрезании рулонов ткани длины L. Величина отходов при разрезании каждого рулона должна быть меньшей, чем $\min\{l_1, \dots l_m\}$. Вариант раскроя – это инструкция, указывающая, сколько заготовок каждого вида необходимо вырезать из рулона ткани.

Требуется найти все возможные варианты раскроя.

Пусть $\mathbf{S} = (S, \mathsf{F}, s_{in}, S_{fin})$ - такой источник, что

$$S = \{L - \sum_{i=1}^{m} \alpha_i l_i \geq 0 \mid \alpha_1, \dots, \alpha_m \in \mathbf{Z}_+\}, \quad s_{in} = L,$$

$$S_{fin} = \{0 \leq L - \sum_{i=1}^{m} \alpha_i l_i < \min\{l_1, \dots, l_m\} \mid \alpha_1, \dots, \alpha_m \in \mathbf{Z}_+\}$$

и

$$\mathsf{F} = \{f_{ij} \mid i = 1, \dots, m; \quad j = 0, 1, \dots, \lfloor L \cdot l_i^{-1} \rfloor\},$$

где

$$f_{ij}(s) = \begin{cases} s - l_i j, & \text{если } s - l_i j \geq 0 \\ \text{не определено}, & \text{если } s - l_i j < 0 \end{cases}.$$

Таким образом, каждая ситуация $s \in S$ соответствует возможному остатку рулона, а элементарный оператор f_{ij} - операции вырезания j заготовок длины l_i.

Так как

$$f_{ij} f_{rh} = f_{rh} f_{ij} \quad (f_{ij}, f_{rh} \in \mathsf{F}),$$

то F^+ - *коммутативная полугруппа*. Следовательно, любой оператор $F \in \mathsf{F}^+$ может быть преобразован к виду $f_{1j_1}^{k_1} \dots f_{mj_m}^{k_m}$ $(k_1, \dots, k_m \in \mathbf{Z}_+)$. Кроме того

$$f_{ij}^k = f_{i,jk}$$

для всех $i = 1,\ldots,m$; $j = 0,1,\ldots,\lfloor L \cdot l_i^{-1} \rfloor$ и $k \in \mathbf{Z}_+$. Следовательно, существует взаимно-однозначное соответствие между вариантами раскроя и выигрышными операторами вида $f_{1n_1}\ldots f_{mn_m}$ (соответствующий этому оператору вариант раскроя имеет вид: из рулона ткани вырезается n_1 заготовок длины l_1, …, n_m заготовок длины l_m).

Следует отметить, что любой источник $\boldsymbol{S} = (S, \mathsf{F}, s_{in}, S_{fin})$ единственным образом определяет такую алгебраическую систему

$$\boldsymbol{A_S} = (A, \Omega_F, \Omega_P),$$

что $A = S$, $\Omega_F = \mathsf{F}^+_{s_{in}} \cup \{\varsigma_{s_{in}}\} \cup \{\varsigma_s \mid s \in S_{fin}\}$, где ς_{s_1} $(s_1 \in \{s_{in}\} \cup S_{fin})$ - 0-арная операция, выделяющая элемент s_1, а $\Omega_P = \varnothing$. Следовательно, все модели и методы *теории алгебраических систем* [29] непосредственно могут быть использованы при решении проблем поиска.

В процессе анализа этапа 1.9 было отмечено, что *решения* – это выигрышные операторы, удовлетворяющие заданному комплексу условий. Определим основные типы решений.

Минимальными решениями называются кратчайшие по длине выигрышные операторы. *Множество всех минимальных решений* для источника $\boldsymbol{S}$ обозначим через $\boldsymbol{L}^{\min}(\boldsymbol{S})$, т.е.

$$\boldsymbol{L}^{\min}(\boldsymbol{S}) = \{F \in \boldsymbol{L}(\boldsymbol{S}) \mid d(F) = \min_{F_1 \in \boldsymbol{L}(\boldsymbol{S})} d(F_1)\}.$$

Неприводимыми (или *не избыточными*) *решениями* называются выигрышные операторы, для которых удаление (или, иными словами, вычеркивание) хотя бы одного элементарного оператора приводит к потере свойства ‘*быть выигрышным оператором*’. Обозначим через $erase(F)$ $(F \in \mathsf{F}^+)$ множество всех операторов, полученных из оператора F в результате удаления хотя бы одного элементарного оператора. Таким образом, оператор $F \in \boldsymbol{L}(\boldsymbol{S})$ является неприводимым решением (для источника $\boldsymbol{S}$) тогда и только тогда, когда

$$erase(F) \cap \boldsymbol{L}(\boldsymbol{S}) = \varnothing.$$

Множество всех неприводимых решений для источника $\boldsymbol{S}$ обозначим через $\boldsymbol{L}^{ir}(\boldsymbol{S})$, т.е.

$$\boldsymbol{L}^{ir}(\boldsymbol{S}) = \{F \in \boldsymbol{L}(\boldsymbol{S}) \mid erase(F) \cap \boldsymbol{L}(\boldsymbol{S}) = \varnothing\}.$$

Ясно, что для любого источника $\boldsymbol{S}$ справедливо включение

$$\boldsymbol{L}^{\min}(\boldsymbol{S}) \subseteq \boldsymbol{L}^{ir}(\boldsymbol{S}), \tag{1.48}$$

т.е. любое минимальное решение всегда является неприводимым. Более того, для любого источника $\boldsymbol{S}$ справедливо равенство

$$\boldsymbol{L}^{\min}(\boldsymbol{S}) = \{F \in \boldsymbol{L}^{ir}(\boldsymbol{S}) \mid d(F) = \min_{F_1 \in \boldsymbol{L}^{ir}(\boldsymbol{S})} d(F_1)\}.$$

Отметим, что обратное к (1.48) включение часто оказывается ложным. Это означает, что во многих случаях (1.48) может быть усилено до строгого включения

$$\boldsymbol{L}^{\min}(\boldsymbol{S}) \subset \boldsymbol{L}^{ir}(\boldsymbol{S}). \tag{1.49}$$

Распространение свойства ‘*быть решением*’ на множества операторов приводит к понятию *кооперативное решение*. Такое распространение можно осуществить следующим образом. Пусть $\omega_i : \underbrace{S \times \ldots \times S}_{i \text{ раз}} \to S$ $(i = 2,\ldots,r)$ - фиксированные операции, каждая из которых - *симметрическое отображение*, т.е.

$$\omega_i(x_1,\ldots,x_i) = \omega_i(x_{\alpha(1)},\ldots,x_{\alpha(i)}) \ (i = 2,\ldots,r)$$

для любой перестановки α множества $\{1,\ldots,i\}$.

Определение 1.6. j*-кооперативным решением* $(j = 2,\dots,r)$ для источника $\boldsymbol{S}$ назовем множество операторов

$$\{F_1,\dots,F_j\}, \qquad (1.50)$$

удовлетворяющее следующим трем условиям:

Условие 1.6. $\omega_j(s_{in}F_1,\dots,s_{in}F_j) \in S_{fin}$.

Условие 1.7. Для каждого $i = 2,\dots, j-1$

$$\omega_i(s_{in}F_{h_1},\dots,s_{in}F_{h_i}) \notin S_{fin}$$

при всех таких $h_i,\dots,h_i$, что $1 \le h_1 < \dots < h_i \le j$.

Условие 1.8. Если $\boldsymbol{L}(\boldsymbol{S}) \ne \varnothing$, то

$$d(F_i) < \min_{F \in \boldsymbol{L}(\boldsymbol{S})} d(F)$$

для всех $i = 1,\dots, j$.

Отметим, что из условия 1.7 вытекает, что множество операторов (1.50) является *не избыточным* (в обычном понимании этого слова). *Множество* $\boldsymbol{L}^{cprtv}(\boldsymbol{S})$ *всех кооперативных решений* для источника $\boldsymbol{S}$ определим равенством

$$\boldsymbol{L}^{cprtv}(\boldsymbol{S}) = \bigcup_{j=2}^{r} \boldsymbol{L}_{\boldsymbol{j}}^{cprtv}(\boldsymbol{S}),$$

где $\boldsymbol{L}_j^{cprtv}(\boldsymbol{S})$ $(j = 2,\dots,r)$ - множество всех j*-кооперативных решений* для источника $\boldsymbol{S}$.

Общей характеристикой всех рассмотренных до сих пор типов решений (т.е. минимальных, неприводимых и кооперативных) является то, что при каждой их реализации выполняется одна и та же последовательность элементарных операторов. Это означает, что при решении любой конкретной задачи вначале осуществляются все воздействия и только после этого анализируются полученные результаты. Такие решения принято называть *безусловными*. В отличии от них *адаптивные решения* характеризуются тем, что результат осуществления каждого воздействия немедленно анализируется и следующее воздействие определяется, исходя из результатов этого анализа. Для обеспечения такой возможности достаточно рассматривать каждую ситуацию как множество некоторых попарно несовместных случаев (т.е. конфигураций), которые находятся во взаимно-однозначном соответствии с различными воздействиями, осуществляемыми в этой ситуации. Анализ результатов воздействия и предназначен для идентификации того, какой случай, в действительности, имеет место. Таким образом, в процессе реализации адаптивного решения последовательность воздействий формируется на основании идентификации тех случаев, которые имеют место в каждый момент времени. Это означает, что каждое (начиная со второго) воздействие является функцией от некоторых предыдущих воздействий и от того случая, который имеет место перед осуществлением этого воздействия. Определим адаптивное решение в терминах источника.

Пусть $\boldsymbol{S} = (S, \mathsf{H}, s_{in}, S_{fin})$ - такой источник, что $\mathsf{H} \subseteq \mathsf{F} \times \mathsf{G}$. Элементарный оператор $(f,g) \in \mathsf{H}$ интерпретируем следующим образом: f $(f \in \mathsf{F})$ - элементарный оператор в обычном смысле этого слова, а g $(g \in \mathsf{G})$ - имя случая, идентифицированного в результате дополнительного анализа ситуации, к которой применяется f. Положим $\mathsf{G}^* = \{\Lambda\} \cup \mathsf{G}^+$ (где Λ - пустое слово) и

$$\mathsf{G}_{s,f} = \{g \in \mathsf{G} \mid (f,g) \in \mathsf{H}, s \in \mathrm{Dom}\,(f,g)\} \quad (s \in S).$$

Определение 1.7. *Адаптивным решением* для источника $\boldsymbol{S}$ назовем частичное отображение $B: \mathsf{G}^* \to \mathsf{F}$, удовлетворяющее следующим четырем условиям:

Условие 1.9. $\Lambda \in \mathrm{Dom}\, B$.

Условие 1.10. $g_1 \dots g_r \in \mathrm{Dom}\, B$ $(r \in \mathbf{N})$ тогда и только тогда, когда справедливы следующие три утверждения:

1) $g_1 \dots g_{r-1} \in \mathrm{Dom}\, B$;
2) $s_{in} \in \mathrm{Dom}\,(B(\Lambda), g_1)(B(g_1), g_2)\dots(B(g_1 \dots g_{r-1}), g_r)$;
3) $s_{in}(B(\Lambda), g_1)(B(g_1), g_2)\dots(B(g_1 \dots g_{r-1}), g_r) \notin S_{fin}$.

Условие 1.11. Если $g_1 \dots g_r \in \mathrm{Dom}\, B$ $(r \in \mathbf{N})$ и $g_1 \dots g_r g \notin \mathrm{Dom}\, B$ для всех $g \in \mathsf{G}$, то

$$\mathsf{G}_{s_{in}(B(\Lambda),g_1)(B(g_1),g_2)\dots(B(g_1\dots g_{r-1}),g_r),B(g_1\dots g_r)} \neq \varnothing$$

и

$$s_{in}(B(\Lambda), g_1)(B(g_1), g_2)\dots(B(g_1 \dots g_{r-1}), g_r)(B(g_1 \dots g_r), g') \in S_{fin}$$

для всех $g' \in \mathsf{G}_{s_{in}(B(\Lambda),g_1)(B(g_1),g_2)\dots(B(g_1\dots g_{r-1}),g_r),B(g_1\dots g_r)}$.

Условие 1.12. Существует такое число $l_{\mathbf{S}}$, что $d(G) \le l_{\mathbf{S}}$ для всех $G \in \mathrm{Dom}\, B$.

Множество всех адаптивных решений для источника $\boldsymbol{S}$ обозначим через $\boldsymbol{L}^{adptv}(\boldsymbol{S})$.

Многочисленные детализации задачи 1.2, как правило, укладываются в рамки одной из следующих пяти проблем.

Проблема 1.4. Для заданного источника $\boldsymbol{S}$ построить множество всех минимальных решений $\boldsymbol{L}^{\min}(\boldsymbol{S})$.

Проблема 1.5. Для заданного источника $\boldsymbol{S}$ построить один, безразлично какой именно, элемент множества $\boldsymbol{L}^{\min}(\boldsymbol{S})$.

Проблема 1.6. Для заданного источника $\boldsymbol{S}$ построить множество всех неприводимых решений $\boldsymbol{L}^{ir}(\boldsymbol{S})$.

Проблема 1.7. Для заданного источника $\boldsymbol{S}$ построить один, безразлично какой именно, элемент множества $\boldsymbol{L}^{cprtv}(\boldsymbol{S})$.

Проблема 1.8. Для заданного источника $\boldsymbol{S}$ построить множество всех адаптивных решений $\boldsymbol{L}^{adptv}(\boldsymbol{S})$.

Проблемы поиска, как правило, исследуются в терминах теории графов (см., напр., [1,34,35,38,43]). В соответствии с этой традицией сопоставим с источником $\boldsymbol{S} = (S, \mathsf{F}, s_{in}, S_{fin})$ следующее дерево.

Определение 1.8. Деревом $\mathsf{D}_{\mathbf{S}}$ для источника $\boldsymbol{S} = (S, \mathsf{F}, s_{in}, S_{fin})$ назовем корневое ориентированное ранжированное дерево, вершины которого отмечены элементами множества S, а дуги – элементами множества F в соответствии со следующими тремя правилами:

Правило 1.3. Единственная вершина 0-го уровня – корень дерева - отмечена элементом s_{in}.

Правило 1.4. Из вершины i-го уровня $(i = 0,1,2,\ldots)$, отмеченной элементом s $(s \in S)$ выходит дуга с отметкой f $(f \in \mathsf{F})$ тогда и только тогда, когда $s \in \mathrm{Dom}\, f$. Эта дуга ведет в вершину $(i+1)$-го уровня, отмеченную элементом sf.

Правило 1.5. Различные дуги, выходящие из одной и той же вершины, отмечены различными элементами множества F.

Дерево может содержать как конечное, так и бесконечное число вершин. В тех случаях, когда число уровней дерева – конечное, номер последнего из уровней называется *высотой дерева*.

Если, расположенные в порядке их прохождения, отметки дуг пути, идущего из корня дерева $\mathsf{D}_{\boldsymbol{S}}$ в некоторую некорневую вершину, образуют последовательность $f_1,\ldots,f_r$, то будем говорить, что вдоль этого пути *считывается оператор* $F = f_1 \ldots f_r$.

Из определения 1.8 вытекает справедливость следующих двух утверждений (доказательство – индукцией по длине оператора).

Утверждение 1.1. Множество операторов, считываемых в дереве $\mathsf{D}_{\boldsymbol{S}}$ вдоль всех путей, идущих из корня в некорневые вершины, совпадает с множеством $\mathsf{F}^{+}_{s_{in}}$.

Утверждение 1.2. Вдоль различных путей, идущих в дереве $\mathsf{D}_{\boldsymbol{S}}$ из корня в некорневые вершины, считываются различные операторы.

Утверждения 1.1 и 1.2 обосновывают корректность следующего обозначения вершин дерева $\mathsf{D}_{\boldsymbol{S}}$.

Правило 1.6. Корень дерева $\mathsf{D}_{\boldsymbol{S}}$ обозначим через v_{Λ} (Λ - пустой оператор, причем, по определению, $d(\Lambda) = 0$ и $s\Lambda = s$ для всех $s \in S$, т.е. Λ действует как *тождественный* оператор).

Правило 1.7. Если вдоль пути, идущего из корня дерева $\mathsf{D}_{\boldsymbol{S}}$ в некорневую вершину, считывается оператор F, то обозначим эту вершину через v_F.

Таким образом, установлено взаимно-однозначное соответствие между множеством всех вершин дерева $\mathsf{D}_{\boldsymbol{S}}$ и множеством $\mathsf{F}^{*}_{s_{in}} = \{\Lambda\} \cup \mathsf{F}^{+}_{s_{in}}$. Индукцией по длине оператора доказывается справедливость следующих двух утверждений.

Утверждение 1.3. Вершина v_F $(F \in \mathsf{F}^{*}_{s_{in}})$ дерева $\mathsf{D}_{\boldsymbol{S}}$ отмечена элементом $s_{in}F$.

Следствие 1.1. Множество $\boldsymbol{L}(\boldsymbol{S})$ всех выигрышных операторов для источника $\boldsymbol{S}$ совпадает с множеством всех операторов, считываемых в дереве $\mathsf{D}_{\boldsymbol{S}}$ вдоль всех путей, идущих из корня в вершины, отмеченные элементами множества S_{fin}.

Утверждение 1.4. Множество всех вершин i-го уровня $(i = 0,1,\dots)$ дерева $\mathsf{D}_{\mathbf{S}}$ совпадает с множеством $\{v_F \mid F \in \mathsf{F}^*_{s_{in}}, d(F) = i\}$.

Аналогичным образом, сопоставим с источником $\boldsymbol{S} = (S, \mathsf{H}, s_{in}, S_{fin})$ $(\mathsf{H} \subseteq \mathsf{F} \times \mathsf{G})$ следующее дерево.

Определение 1.9. Деревом $\mathsf{D}_{\mathbf{S}}$ для источника $\boldsymbol{S} = (S, \mathsf{H}, s_{in}, S_{fin})$ $(\mathsf{H} \subseteq \mathsf{F} \times \mathsf{G})$ назовем корневое ориентированное ранжированное дерево, размеченное в соответствии со следующими двумя правилами:

Правило 1.8. Единственная вершина 0-го уровня – корень дерева - отмечена элементом s_{in}.

Правило 1.9. Пусть вершина v $2i$-го уровня $(i = 0,1,\dots)$ отмечена элементом s $(s \in S)$. Из вершины v выходит дуга с отметкой f $(f \in \mathsf{F})$ тогда и только тогда, когда $\mathsf{G}_{s,f} \neq \varnothing$. Эта дуга ведет в неотмеченную вершину $v'_{v,f}$ $(2i+1)$-го уровня. Различные дуги, выходящие из вершины v имеют различные отметки.

Из вершины $v'_{v,f}$ выходит дуга с отметкой g $(g \in \mathsf{G})$ тогда и только тогда, когда $g \in \mathsf{G}_{s,f}$. Эта дуга ведет в вершину v'' $2(i+1)$-го уровня, отмеченную элементом $s(f, g)$. Различные дуги, выходящие из вершины $v'_{v,f}$ имеют различные отметки.

Индукцией по длине оператора доказывается справедливость следующих двух утверждений.

Утверждение 1.5. Множество всех последовательностей отметок дуг, считываемых в дереве $\mathsf{D}_{\mathbf{S}}$ источника $\boldsymbol{S} = (S, \mathsf{H}, s_{in}, S_{fin})$ $(\mathsf{H} \subseteq \mathsf{F} \times \mathsf{G})$ вдоль всех путей, идущих из корня в вершины, расположенные в уровнях с четными номерами, совпадает с множеством $\mathsf{H}^*_{s_{in}}$.

Утверждение 1.6. Последовательности отметок дуг, считываемых в дереве $\mathsf{D}_{\mathbf{S}}$ источника $\boldsymbol{S} = (S, \mathsf{H}, s_{in}, S_{fin})$ $(\mathsf{H} \subseteq \mathsf{F} \times \mathsf{G})$ вдоль различных путей, идущих из корня, различны между собой.

Утверждение 1.6 обосновывает корректность следующего обозначения вершин дерева дереве $\mathsf{D}_{\mathbf{S}}$ источника $\boldsymbol{S} = (S, \mathsf{H}, s_{in}, S_{fin})$ $(\mathsf{H} \subseteq \mathsf{F} \times \mathsf{G})$.

Правило 1.10. Если W - последовательность отметок дуг, считываемых вдоль пути, идущего из корня дерева $\mathsf{D}_{\mathbf{S}}$, то финальная вершина этого пути обозначается через v_W.

В заключение отметим, что безусловное решение допускает интерпретацию *как игра одного игрока*, а адаптивное решение – как *игра двух лиц*. Таким образом, для построения адаптивных решений могут быть использованы методы поиска на дереве игры [34,35].

1.6. Выводы.

В разделе 1 дан ретроспективный анализ моделей и методов, лежащих в основе решения проблем анализа дискретных систем. Основные результаты состоят в следующем.

1. Предложена новая интерпретация результатов из [28,31,34,35,90]. Сформулированы общие проблемы идентификации дискретных систем (проблемы 1.1-1.3). Выделена структура решения этих проблем, связанная с уровнем абстракции при выборе математической модели исследуемой системы.

2. В терминах базовой модели для представления проблем поиска – источника – определены основные типы решений: *безусловные* (минимальные, неприводимые и кооперативные) и *адаптивные*. Сформулированы основные проблемы поиска (проблемы 1.4-1.8). Решению этих проблем посвящен раздел 2.

3. Показана актуальность решения следующих двух проблем идентификации внутренних состояний конечных автоматов

Проблема 1.9. Детализировать общие решения проблем 1.4-1.8 для идентификации внутренних состояний конечных автоматов.

Проблема 1.10. Исследовать сложность поиска минимальных диагностических и синхронизирующих слов для слабоинициальных автоматов.

Проблемы 1.9 и 1.10 решены в разделе 3.

4. Проведен анализ аналитических методов построения дизъюнктивных нормальных форм (ДНФ), из которого вытекает актуальность решения следующей проблемы

Проблема 1.11. Детализировать общие решения проблем 1.4-1.7 для построения простых импликант и состоящих из них ДНФ.

Проблема 1.11 решена в разделе 4.

5. Анализ моделей и методов теории систем показывает, что отсутствуют унифицированные средства представления систем в условиях действий нестабильной среды. Поэтому, актуальной является следующая проблема

Проблема 1.12. Разработать унифицированные методы анализа и управления для систем в условиях действий нестабильной среды.

Решению проблемы 1.12 посвящен раздел 5.

Таким образом, в разделе 1 очерчен новый фрагмент общей теории систем, позволяющий явно выделить ряд задач, актуальных как в теоретическом, так и в прикладном аспекте.

2. ПОИСК НА ЧАСТИЧНО УПОРЯДОЧЕННЫХ СТРУКТУРАХ

В настоящем разделе впервые систематически изложена общая теория поиска на частично упорядоченных структурах, включающая в себя в качестве специальных случаев классические теоретико-множественный и основанный на оценивании подходы. Именно эта теория является математической основой исследований, представленных в разделах 3 и 4.

В п.2.1 исследуется общая проблема поиска множества безусловных решений, определяемого характеристической функцией. Разработан унифицированный подход к созданию общих схем поиска, основанный на выделении в дереве поиска множеств бесперспективных, финальных и порождающих вершин. В п.2.2 определяется базовая математическая модель для поиска безусловных решений - M-источник и исследуются его свойства. В п.2.3 получено исчерпывающее решение проблем 1.4-1.7 для M-источника. Выделены прямые и обратные M-источники. Построена общая схема двустороннего поиска минимальных решений для M-источников. В п.2.4 определяется базовая математическая модель для поиска адаптивных решений - AM-источник и исследуются его свойства. Исследованы общие соотношения между моделями, предназначенными для поиска адаптивных и безусловных решений. В п.2.5 получено исчерпывающее решение проблемы 1.8 для AM-источника. В п.2.6 получено исчерпывающее решение фундаментальной проблемы дискретной математики – поиска всех неприводимых множеств представителей семейства множеств.

2.1. Общие схемы поиска безусловных решений.

Основные проблемы поиска решений - проблемы 1.4-1.8 - сформулированы в п.1.5 в терминах базовой модели – источника. Четыре из них (проблемы 1.4-1.7) - это поиск *безусловных решений*. Поэтому актуальной является разработка *метатеории поиска безусловных решений*, т.е. средств, позволяющих единым образом представить все многообразие проблем и методов поиска безусловных решений и выделить факторы, определяющие внутреннюю сложность решения конкретных проблем. Основной целью настоящего пункта как раз и является исследование общей проблемы поиска множества безусловных решений для источника.

В соответствии с подходом, развитым в п.1.5, *множество безусловных решений для источника* - это *множество выигрышных операторов* (т.е. переводящих начальную ситуацию в множество финальных ситуаций), *удовлетворяющих заданному комплексу условий*. Унифицированное средство представления множества - его *характеристическая функция*. Следовательно, для заданного источника $\boldsymbol{S} = (S, \mathsf{F}, s_{in}, S_{fin})$ определение *множества безусловных решений* эквивалентно построению *характеристической функции* χ_Ω некоторого подмножества Ω множества F^*, удовлетворяющего условию $\Omega \subseteq \boldsymbol{L}(\boldsymbol{S})$. Итак, характеристическая функция множества безусловных решений Ω для источника $\boldsymbol{S}$ всегда представляет собой такое отображение

$$\chi_\Omega : \mathsf{F}^* \to \{0,1\},$$

что

$$(\forall F \in \mathsf{F}^*)(\chi_\Omega(F) = 1 \Leftrightarrow F \in \Omega),$$

где равенство $\chi_\Omega(F) = 1$ *с необходимостью включает в себя выполнение условия* $F \in \boldsymbol{L}(\boldsymbol{S})$. Напомним, что, по определению множества выигрышных операторов, условия $F \in \boldsymbol{L}(\boldsymbol{S})$ и $s_{in}F \in S_{fin}$ эквивалентны.

Пример 2.1. Пусть $\chi^{\min}$ и χ^{ir} - характеристические функции множеств $\boldsymbol{L}^{\min}(\boldsymbol{S})$ и $\boldsymbol{L}^{ir}(\boldsymbol{S})$ всех, соответственно, минимальных и неприводимых решений для источника $\boldsymbol{S}$. Из определений, сформулированных в п.1.5, вытекает, что

$$\chi^{\min}(F)=1 \Leftrightarrow (F \in \boldsymbol{L}(\boldsymbol{S}) \wedge (\forall F_1 \in \mathsf{F}^*)(d(F_1)<d(F) \vee d(F_1)>d(F) \Rightarrow \chi^{\min}(F_1)=0)$$

и

$$\chi^{ir}(F)=1 \Leftrightarrow (F \in \boldsymbol{L}(\boldsymbol{S}) \wedge (\forall F_1 \in erase(F))(\chi^{ir}(F_1)=0),$$

где $d(F)$ - длина оператора F (т.е. число вхождений в F элементарных операторов), а $erase(F)$ - множество всех операторов, полученных из оператора F в результате вычеркивания, по крайней мере, одной буквы.

Зафиксируем источник $\boldsymbol{S}=(S,\mathsf{F},s_{in},S_{fin})$ и множество безусловных решений Ω. Обозначим через χ характеристическую функцию, определяющую множество Ω. Положим

$$\boldsymbol{L}_\chi(\boldsymbol{S})=\Omega .$$

Отметим, что

$$\boldsymbol{L}_\chi(\boldsymbol{S}) \subseteq \boldsymbol{L}(\boldsymbol{S}) .$$

Общая проблема поиска безусловных решений имеет следующий вид

Проблема 2.1. Для заданных источника $\boldsymbol{S}$ и характеристической функции χ построить множество безусловных решений $\boldsymbol{L}_\chi(\boldsymbol{S})$.

Рассмотрим решение проблемы 2.1.

Обозначим через $\mathsf{D}(\chi,\boldsymbol{S})$ минимальное поддерево дерева $\mathsf{D}_{\boldsymbol{S}}$ (см. определение 1.8), содержащее корень и множество вершин

$$V_{fin}=\{v_F \mid F \in \boldsymbol{L}_\chi(\boldsymbol{S})\} .$$

Отметим, что:

1) дерево $\mathsf{D}(\chi,\boldsymbol{S})$ состоит из единственной вершины – корня v_Λ тогда и только тогда, когда $\boldsymbol{L}_\chi(\boldsymbol{S})=\varnothing$;
2) дерево $\mathsf{D}(\chi,\boldsymbol{S})$ содержит конечное множество вершин тогда и только тогда, когда $\boldsymbol{L}_\chi(\boldsymbol{S})$ - конечное множество.

Будем интерпретировать вершины дерева $\mathsf{D}_{\boldsymbol{S}}$ как *состояния*, корень v_Λ - как *начальное состояние*, а множество вершин V_{fin} - как *множество финальных состояний*. Тогда множество $\boldsymbol{L}_\chi(\boldsymbol{S})$ - это язык, представленным настроенным автоматом $(\mathsf{D}(\chi,\boldsymbol{S}),v_\Lambda,V_{fin})$.

Все многообразие методов решения проблемы 2.1 сводится, по своей сути, к различным способам построения некоторой последовательности деревьев

$$\mathsf{D}(0),\mathsf{D}(1),\mathsf{D}(2),\ldots , \qquad (2.1)$$

удовлетворяющей следующим шести условиям:

Условие 2.1. $\mathsf{D}(i)$ $(i=0,1,\ldots)$ - поддерево дерева $\mathsf{D}_{\boldsymbol{S}}$, содержащее корень v_Λ.

Условие 2.2. $D(\chi,\boldsymbol{S}) \subseteq D(0) \cup D(1) \cup \ldots \cup (\subseteq \mathsf{D}_{\boldsymbol{S}})$.

Условие 2.3. Дерево $D(i)$ $(i=1,2,\ldots)$ полностью определяется последовательностью деревьев $D(0),\ldots,D(i-1)$.

Условие 2.4. Дерево $D(i)$ $(i=0,1,\ldots)$ содержит как можно меньше вершин.

Условие 2.5. Если $D(\chi,\boldsymbol{S})$ - конечное дерево, то (2.1) – конечная последовательность.

Условие 2.6. Если (2.1) – бесконечная последовательность, то $\boldsymbol{L}_\chi(\boldsymbol{S})$ - бесконечное множество и

$$\lim_{h\to\infty}\frac{|V((\bigcup_{i=0}^{\infty}D(i))[h])|}{|V(D(\chi,\boldsymbol{S})[h])|}=1,$$

где $D[h]$ $(h=0,1,\ldots)$ - максимальное поддерево дерева D, имеющее высоту h, а $V(D)$ - множество вершин дерева D.

Отметим, что условие 2.2 обеспечивает *корректность*, а условия 2.4-2.6 – *максимальное снижение сложности* поиска.

Если $D(\chi,\boldsymbol{S})$ - бесконечное дерево, то естественно возникает *проблема остановки*. Последняя алгоритмически разрешима, если $\boldsymbol{L}_\chi(\boldsymbol{S})$ - регулярное множество. Более того, в этом случае существует конечное поддерево $D_{\boldsymbol{S}}^{\chi}$ дерева $D(\chi,\boldsymbol{S})$, которое, посредством отождествления некоторых его вершин, может быть свернуто в (возможно, частичный) конечный настроенный автомат, представляющий множество $\boldsymbol{L}_\chi(\boldsymbol{S})$. Высота $L_{D_{\boldsymbol{S}}^{\chi}}$ дерева $D_{\boldsymbol{S}}^{\chi}$, как правило, заранее не известна и определяется только в процессе построения дерева $D_{\boldsymbol{S}}^{\chi}$ в явном виде. Отметим, что $\boldsymbol{L}^{\min}(\boldsymbol{S})$ и $\boldsymbol{L}^{ir}(\boldsymbol{S})$ - регулярные множества, т.к. они – конечные. Более того, в силу последнего обстоятельства, в случае проблем 1.4 и 1.6 имеет место равенство

$$D_{\boldsymbol{S}}^{\chi}=D(\chi,\boldsymbol{S}).$$

Всюду в дальнейшем будем считать, что $\boldsymbol{L}_\chi(\boldsymbol{S})$ - это регулярное множество. Такое предположение дает возможность, не ограничивая общности изложения, перейти от дерева $D(\chi,\boldsymbol{S})$ к дереву $D_{\boldsymbol{S}}^{\chi}$ и считать, что $\boldsymbol{L}_\chi(\boldsymbol{S})$ - это конечное множество, представляемое конечным настроенным автоматом $(D_{\boldsymbol{S}}^{\chi},v_\Lambda,V_{fin})$. Таким образом, всюду в дальнейшем предполагается, что (2.1) – это конечная последовательность деревьев.

$$D(0),D(1),\ldots,D(k)\quad(k\in\mathbf{N}),\qquad(2.2)$$

удовлетворяющих условиям 2.1-2.4.

Исследуем общие схемы решения проблемы 2.1.

Поиск в ширину. Основан на последовательном, поуровневом (один за другим), восстановлении дерева $D_{\boldsymbol{S}}^{\chi}$. Таким образом, строится такая последовательность деревьев (2.2), что условия 2.1-2.4 имеют следующий вид

Условие 2.7. $D(i)$ $(i=0,1,\ldots,k-1)$ - поддерево дерева $D_{\boldsymbol{S}}$, имеющее высоту i и $D(k)$ - поддерево дерева $D_{\boldsymbol{S}}$, имеющее высоту $L_{D_{\boldsymbol{S}}^{\chi}}$.

Условие 2.8. $D^{\chi}_{\mathbf{S}}[i] \subseteq D(i) (\subseteq D_{\mathbf{S}}[i])$ $(i = 0,1,\ldots,k)$.

Условие 2.9. Дерево $D(i)$ $(i = 1,\ldots,k)$ полностью определяется последовательностью деревьев $D(0),\ldots,D(i-1)$.

Условие 2.10. Дерево $D(i)$ $(i = 0,1,\ldots,k)$ содержит как можно меньше вершин.

Отметим, что из условия 2.8 вытекает, что

$$D^{\chi}_{\mathbf{S}} \subseteq \bigcup_{i=0}^{k} D(i).$$

Обозначим через V_i $(i = 1,\ldots,k)$ множество всех вершин последнего (т.е. i-го) уровня дерева $D(i)$.

Определение 2.1. Вершину $v \in V_i$ $(i = 0,1,\ldots,k)$ назовем:

1) *финальной*, если оператор, считываемый вдоль пути, идущего из корня в вершину v, является элементом множества $\boldsymbol{L}_{\chi}(\mathbf{S})$;
2) *бесперспективной*, если оператор, считываемый вдоль пути, идущего из корня в вершину v, заведомо не является начальным отрезком ни для одного элемента множества $\boldsymbol{L}_{\chi}(\mathbf{S})$;
3) *порождающей*, если вершина v используется для построения хотя бы одной вершины $(i+1)$-го уровня дерева $D(i+1)$.

Обозначим множества всех финальных, бесперспективных и порождающих вершин дерева $D(i)$ $(i = 0,1,\ldots,k)$ через, соответственно, $fnl(i)$, $nprsp(i)$ и $gnrt(i)$. Свойство '*быть начальным отрезком*' – рефлексивное, т.е. любой оператор - начальный отрезок самого себя. Следовательно, оператор, считываемый вдоль пути, идущего из корня дерева $D(i)$ $(i = 0,1,\ldots,k)$ в бесперспективную вершину, *не является* элементом множества $\boldsymbol{L}_{\chi}(\mathbf{S})$. Таким образом, из определения 2.1 вытекает, что:

1) $gnrt(0) = \{v_{\Lambda}\}$, $fnl(0) = \varnothing$, $nprsp(0) = \varnothing$;
2) $gnrt(i) \neq \varnothing$ $(i = 0,1,\ldots,k-1)$;
3) $gnrt(k) = \varnothing$;
4) $\bigcup_{i=0}^{k} fnl(i) \neq \varnothing \Leftrightarrow \boldsymbol{L}_{\chi}(\mathbf{S}) \neq \varnothing$;
5) $fnl(i) \cup gnrt(i) \cup nprsp(i) \subseteq V_i$ $(i = 0,1,\ldots k-1)$;
6) $fnl(k) \cup nprsp(k) = V_k$;
7) $\{v_F \in V_i \setminus fnl(i) \,|\, (\forall f \in \mathsf{F})(s_{in}F \notin \mathrm{Dom}\, f)\} \subseteq nprsp(i)$ $(i = 0,1,\ldots,k)$;
8) $nprsp(i) \cap (gnrt(i) \cup fnl(i)\} = \varnothing$ $(i = 0,1,\ldots,k)$.

Конструктивное определение множеств $fnl(i)$, $nprsp(i)$ и $gnrt(i)$ $(i = 1,2,\ldots)$ является результатом исследования структуры множества $\boldsymbol{L}_{\chi}(\mathbf{S})$, осуществляется в терминах дерева $D_{\mathbf{S}}[i]$ и строится следующим образом.

Вначале формулируются и доказываются утверждения, определяющие множества $fnl(i)$ и $nprsp(i)$ $(i = 1,2,\ldots)$. Эти утверждения, как правило, имеют следующий вид (символом ### обозначена фраза: '*выполнен заданный комплекс условий*')

Утверждение 2.1. Вершина v_F i-го уровня $(i = 1,2,\ldots)$ дерева $D_{\mathbf{S}}$ является финальной тогда и только тогда, когда $s_{in}F \in S_{fin}$ и ни один из операторов, считываемых в дереве $D_{\mathbf{S}}[i]$, вдоль такого пути, что ### не ведет в такую вершину, что ###.

Утверждение 2.2. Вершина v_F i-го уровня $(i = 1,2,\ldots)$ дерева $D_{\mathbf{S}}$ является бесперспективной тогда и только тогда, когда $s_{in}F \notin S_{fin}$ и либо $s_{in}F \notin \mathrm{Dom}\, f$ для всех $f \in \mathsf{F}$, либо ни один из операторов, считываемых в дереве $D_{\mathbf{S}}[i]$, вдоль такого пути, что ### не ведет в такую вершину, что ###.

Далее определяются множества $gnrt(i)$ $(i = 1,2,\ldots)$. Возможны следующие два принципиально различных случая.

Первый случай имеет место, когда множества $gnrt(i)$ $(i = 1,2,\ldots)$ определяются однозначно. Это означает, что справедливы равенства

$$gnrt(i) = V_i \setminus nprsp(i) \quad (i = 1,2,\ldots),$$

или равенства

$$gnrt(i) = V_i \setminus (nprsp(i) \cup fnl(i)) \quad (i = 1,2,\ldots).$$

Второй случай имеет место, если существуют такие $i = 1,2,\ldots$, что

$$V_i \setminus (nprsp(i) \cup fnl(i)) \subset gnrt(i) \subset V_i \setminus nprsp(i) \tag{2.3}$$

или

$$gnrt(i) \subset V_i \setminus (nprsp(i) \cup fnl(i)). \tag{2.4}$$

Это означает, что возникает *проблема поиска множеств* $gnrt(i)$ $(i = 1,2,\ldots)$. Сложность этого поиска характеризуется следующим образом: для (2.3) нижняя и верхняя границы сложности - это мощности множеств, соответственно, $V_i \setminus (nprsp(i) \cup fnl(i))$ и $V_i \setminus nprsp(i)$, а для (2.4) верхняя граница сложности – это мощность множества $V_i \setminus (nprsp(i) \cup fnl(i))$.

Во втором случае формулируются и доказываются утверждения следующего вида, определяющие множества $gnrt(i)$ $(i = 1,2,\ldots)$ (символом ### обозначена фраза: '*выполнен заданный комплекс условий*')

Утверждение 2.3. Множество $gnrt(i)$ $(i = 1,2,\ldots)$ является таким минимальным по мощности множеством вершин $v \notin nprsp(i)$ i-го уровня дерева $D_{\mathbf{S}}[i]$, что ###.

Утверждение 2.4. Каждое множество $gnrt(i)$ $(i = 1,2,\ldots)$ порождает некоторое множество $gnrt(i+1)$.

Отметим, что именно утверждение 2.4 обеспечивает корректность поиска в ширину.

Значение множеств $fnl(i)$, $nprsp(i)$ и $gnrt(i)$ $(i = 0,1,\ldots,k)$ состоит в том, что именно они дают возможность обеспечить выполнение условий 2.9 и 2.10. Действительно, для того, чтобы получить дерево $D(i)$ $(i = 1,\ldots,k)$ достаточно достроить в дереве $D(i-1)$ ту часть i-го уровня дерева $D_{\mathbf{S}}$, которая определяется вершинами, принадлежащими множеству $gnrt(i-1)$. Выполнение условия 2.10 осуществляется за счет применения к дереву $D(i)$ $(i = 1,\ldots,k)$ следующей процедуры *сборки мусора*.

Procedure $GRBG(D(i))$.

Шаг 1. Отметить каждую вершину $v \in V_i \setminus (gnrt(i) \cup fnl(i))$ символом ♠, $j := i-1$.

Шаг 2. Если $j = 0$, то переход к шагу 5, иначе переход к шагу 3.

Шаг 3. Отметить символом ♠ каждую такую вершину v j-го уровня, что $v \notin V_{fin}$ и из вершины v идут дуги только в вершины $(j+1)$-го уровня, отмеченные символом ♠.

Шаг 4. Если хотя бы одна вершина j-го уровня отмечена символом ♠, то $j := i-1$ и переход к шагу 2, иначе переход к шагу 5.

Шаг 5. Удалить все вершины (и инцидентные им дуги), отмеченные символом ♠ и конец.

С учетом этой процедуры решение проблемы 2.1 *поиском в ширину* имеет следующий вид.

Алгоритм 2.1.

Шаг 1. $D(0) := D_{\mathbf{S}}[0]$, $D := D_{\mathbf{S}}[1]$, $i := 1$.

Шаг 2. $D := GRBG(D)$, $D(i) := D$.

Шаг 3. Если $gnrt(i) = \varnothing$, то конец, иначе переход к шагу 4.

Шаг 4. $D :=$ дерево, полученное из дерева $D(i)$ в результате достройки той части $(i+1)$-го уровня дерева $D_{\mathbf{S}}$, которая порождается элементами множества $gnrt(i)$.

Шаг 5. $i := i+1$ и переход к шагу 2.

Корректность алгоритма 2.1 обосновывается следующей теоремой.

Теорема 2.1. Если последовательность деревьев

$$D(0), D(1), \ldots, D(k)$$

построена в результате работы алгоритма 2.2, то $D(k) = D_{\mathbf{S}}^{\chi}$.

Доказательство. При выполнении процедуры $GRBG$ не удаляется ни одна из вершин, принадлежащих множеству V_{fin}. Поэтому, для доказательства теоремы достаточно показать, что любая висячая вершина (или, иными словами, лист) i-го уровня $(i = 1, \ldots, k)$ дерева $D(k)$ принадлежит множеству V_{fin}.

Остановка работы алгоритма 2.1 может произойти только на шаге 3. Переход на шаг 3 осуществляется только из шага 2, после выполнения процедуры $GRBG$. Так как $gnrt(k) = \varnothing$, то в результате последнего выполнения процедуры $GRBG$ любая вершина $v \in V_k \setminus fnl(k)$ отмечается символом ♠ и, следовательно, удаляется. Таким образом, $V_k \subseteq V_{fin}$.

Предположим, что в i-м уровне $(i = 1, \ldots, k-1)$ дерева $D(k)$ расположена висячая вершина v_F, не принадлежащая множеству V_{fin}. При i-м выполнении процедуры $GRBG$ удаляются все вершины, принадлежащие множеству $nprsp(i)$. Следовательно, $s_{in}F \in \mathrm{Dom}\, f$ хотя бы для одного $f \in F$. Это означает, что существует такое j $(i \le j \le k)$, что при j-ом выполнении процедуры $GRBG$ символом ♠ отмечены все вершины, в которые ведут дуги из вершины v_F. Но тогда, при j-ом выполнении процедуры $GRBG$ вершина v_F также отмечается символом ♠ и, следовательно, удаляется. Это противоречит тому, что вершина v_F принадлежит дереву $D(k)$. Полученное противоречие показывает, что предположение – ложное. Следовательно, любая висячая вершина i-го уровня $(i = 1,\ldots,k)$ дерева $D(k)$ принадлежит множеству V_{fin}.

Теорема доказана.

Поиск с возвращением. Говоря неформально, этот метод основан на действиях, осуществляемых в соответствии со следующими двумя правилами.

Правило 2.1 (*прямой ход*)**.** Выполнять допустимые действия до тех пор, пока это возможно.

Правило 2.2 (*обратный ход*)**.** Если дальнейшие действия недопустимы, то аннулировать последнее действие, вернуться к предыдущей конфигурации и перейти к правилу 2.1.

Применительно к проблеме 2.1, *поиск с возвращением* состоит в построении конечной последовательности (2.2) поддеревьев дерева $D_{\mathbf{S}}$, осуществляемом за счет детализации правил 2.1 и 2.2 для организации обхода некоторого такого минимального дерева D, что

$$D_{\mathbf{S}}^{\chi} \subseteq D \subseteq D_{\mathbf{S}}[k]. \tag{2.5}$$

Отметим, что любой обход дерева $D_{\mathbf{S}}$ автоматически предполагает, что множество элементарных операторов F (а именно они являются отметками дуг) является *линейно упорядоченным*. В дальнейшем считаем, что это условие выполнено.

Для того, чтобы для дерева D обеспечить свойство '*быть минимальным*', достаточно воспользоваться множествами $fnl(i)$, $nprsp(i)$ и $gnrt(i)$ $(i = 0,1,\ldots,k)$. Таким образом, решение проблемы 2.1 *поиском с возвращением* имеет следующий вид (через $lbl(v)$ обозначена метка вершины v дерева $D_{\mathbf{S}}$, через $lvl(v)$ - уровень дерева $D_{\mathbf{S}}$, которому принадлежит вершина v, а через $strng(v_{\Lambda}, v)$ - оператор, считываемый вдоль пути, идущего из корня v_{Λ} дерева $D_{\mathbf{S}}$ в вершину v).

Алгоритм 2.2.

Шаг 1. $v^{anlsd} := v_{\Lambda}$, $\boldsymbol{L} := \varnothing$.

Шаг 2. $vrnts(v^{anlsd}) := \{f \in F \mid lbl(v^{anlsd}) \in \mathrm{Dom}\, f\}$.

Шаг 3. Если $vrnts(v^{anlsd}) \neq \varnothing$, то переход к шагу 4, иначе переход к шагу 11.

Шаг 4. $f :=$ первый элемент множества $vrnts(v^{anlsd})$,

$$vrnts(v^{anlsd}) := vrnts(v^{anlsd}) \setminus \{f\}.$$

Шаг 5. Построить дугу, выходящую из вершины v^{anlsd} и вершину v $(lvl(v^{anlsd})+1)$-го уровня, являющуюся концом этой дуги. Отметить построенную дугу элементарным оператором f, а вершину v - ситуацией $lbl(v^{anlsd})f$.

Шаг 6. Если $v \notin gnrt(lvl(v^{anlsd})+1) \cup fnl(lvl(v^{anlsd})+1)$, то переход к шагу 7, иначе переход к шагу 8.

Шаг 7. Удалить вершину v и инцидентную ей дугу и переход к шагу 3.

Шаг 8. $v^{anlsd} := v$ и переход к шагу 9.

Шаг 9. Если $v^{anlsd} \in fnl(lvl(v^{anlsd})+1)$, то

$$\boldsymbol{L} := \boldsymbol{L} \cup \{strng(v_{\Lambda}, v^{anlsd})\}.$$

Шаг 10. Переход к шагу 2.

Шаг 11. Если $v^{anlsd} = v_\Lambda$, то конец, иначе переход к шагу 12.

Шаг 12. Если $v^{anlsd} = v_{Ff}$ $(F \in \mathsf{F}^*, f \in \mathsf{F})$, то $vrnts(v_F) := vrnts(v_F) \setminus \{f\}$, $v^{anlsd} := v_F$, удалить вершину v_{Ff} и инцидентную ей дугу и переход к шагу 3.

Отметим, что при работе алгоритма 2.2 шаги 1-10 реализуют *прямой ход*, а шаг 12 – *обратный ход*.

Корректность алгоритма 2.2 обосновывается следующей теоремой.

Теорема 2.2. Если множество $\boldsymbol{L}$ построено в результате работы алгоритма 2.2, то

$$\boldsymbol{L} = \boldsymbol{L}_\chi(\boldsymbol{S}).$$

Доказательство. Из шагов 1 и 9 вытекает, что $\boldsymbol{L} \subseteq \boldsymbol{L}_\chi(\boldsymbol{S})$. Из шагов 1-8,11,12 вытекает, что в результате работы алгоритма 2.2 осуществляется обход некоторого поддерева D дерева $D_{\boldsymbol{S}}$, порождаемого вершинами, принадлежащими множеству $\bigcup_{i=0}^{k} gnrt(i)$. Следовательно, поддерево D удовлетворяет включениям (2.5). Это означает, что любой оператор $F \in \boldsymbol{L}_\chi(\boldsymbol{S})$ считывается в дереве D вдоль некоторого пути, идущего из корня. Из этого факта, с учетом шагов 1 и 9, вытекает, что $\boldsymbol{L} \supseteq \boldsymbol{L}_\chi(\boldsymbol{S})$. Из включений $\boldsymbol{L} \subseteq \boldsymbol{L}_\chi(\boldsymbol{S})$ и $\boldsymbol{L} \supseteq \boldsymbol{L}_\chi(\boldsymbol{S})$ вытекает, что имеет место равенство $\boldsymbol{L} = \boldsymbol{L}_\chi(\boldsymbol{S})$.

Теорема доказана.

Минимальность дерева D, обход которого осуществляется в результате работы алгоритма 2.2, обеспечивается следующим образом. Дерево D порождается вершинами, принадлежащими множеству $\bigcup_{i=0}^{k} gnrt(i)$. Из шагов 6 и 7 вытекает, что в процессе обхода дерева D все вершины дерева $D_{\boldsymbol{S}}$, принадлежащие множеству $\bigcup_{i=1}^{k} nprsr(i)$, удаляются сразу же, по мере их появления. Кроме того, из шагов 4,6,7 и 12 вытекает, что в процессе работы алгоритма 2.2 *сборка мусора* осуществляется сразу же, как только установлено его наличие. Именно эти обстоятельства и обеспечивают минимальность восстанавливаемого дерева D.

Метод ветвей и границ. Этот метод предназначен для поиска решений *наименьшей стоимости* и организован в соответствии с условием 1.4 и принципом 1.1. Таким образом, предполагается, что построена *оценочная функция*, т.е. некоторая такая функция

$$cst : \mathsf{F}^*_{s_{in}} \to \mathbf{R}_+,$$

что

$$(\forall F \in \mathsf{F}^*_{s_{in}})(\forall f \in \mathsf{F})(s_{in}F \in \mathrm{Dom}\, f \Rightarrow cst(Ff) \geq cst(F)),$$

и

$$\boldsymbol{L}_\chi(\boldsymbol{S}) = \{F \in \boldsymbol{L}_{\chi_1}(\boldsymbol{S}) \mid cst(F) = \min_{F_1 \in \boldsymbol{L}_{\chi_1}(\boldsymbol{S})} cst(F_1)\}, \tag{2.6}$$

где χ_1 - заданная характеристическая функция. Принимая во внимание взаимнооднозначное соответствие между множеством $\mathsf{F}^*_{s_{in}}$ и множеством вершин дерева $D_{\boldsymbol{S}}$, положим

$$cst(v_F) = cst(F) \quad (F \in \mathsf{F}^*_{s_{in}}).$$

Применительно к проблеме 2.1, *метод ветвей и границ* состоит в построении конечной последовательности (2.2) поддеревьев дерева $D_{\mathbf{S}}$, осуществляемом за счет организации восстановления некоторого минимального дерева D, удовлетворяющего включениям (2.5), в соответствии со следующим правилом.

Правило 2.3. На очередном шаге раскрывается некоторая висячая вершина, стоимость которой – наименьшая.

Для того, чтобы для дерева D обеспечить свойство '*быть минимальным*', достаточно воспользоваться множествами $fnl_{\chi_1}(i)$, $nprsp_{\chi_1}(i)$ и $gnrt_{\chi_1}(i)$ $(i=1,\ldots,k)$ (индекс, в данном случае χ_1, означает, что множества построены для характеристической функции χ_1).

Таким образом, решение проблемы 2.1 *методом ветвей и границ* имеет следующий вид (через LST обозначен список висячих вершин, элементы которого расположены в порядке не убывания значений функции cst, а через lub - нижняя граница вычисленных значений функции cst для элементов множества $\boldsymbol{L}_{\chi_1}(\boldsymbol{S})$).

Алгоритм 2.3.

Шаг 1. $\mathrm{lub} := \infty$, $LST := \{v_\Lambda\}$, $\boldsymbol{L} := \varnothing$.

Шаг 2. Если $LST = \varnothing$, то конец, иначе переход к шагу 3.

Шаг 3. $v^{anlsd} :=$ первый элемент списка LST, $LST := LST \setminus \{v^{anlsd}\}$.

Шаг 4. $vrnts(v^{anlsd}) := \{f \in \mathsf{F} \mid lbl(v^{anlsd}) \in \mathrm{Dom}\, f\}$.

Шаг 5. Если $vrnts(v^{anlsd}) \neq \varnothing$, то переход к шагу 6, иначе переход к шагу 2.

Шаг 6. $f :=$ первый элемент множества $vrnts(v^{anlsd})$,

$$vrnts(v^{anlsd}) := vrnts(v^{anlsd}) \setminus \{f\}.$$

Шаг 7. Построить дугу, выходящую из вершины v^{anlsd} и вершину v $(lvl(v^{anlsd})+1)$-го уровня, являющуюся концом этой дуги. Отметить построенную дугу элементарным оператором f, а вершину v - ситуацией $lbl(v^{anlsd})f$.

*Шаг 8.*Если $v \notin gnrt_{\chi_1}(lvl(v^{anlsd})+1) \cup fnl_{\chi_1}(lvl(v^{anlsd})+1)$, то переход к шагу 13, иначе переход к шагу 9.

Шаг 9. Если $cst(v) \leq \mathrm{lub}$, то переход к шагу 10, иначе переход к шагу 13.

Шаг 10. Если $v \in V_{fin}$, то переход к шагу 11, иначе переход к шагу 12.

Шаг 11. Если $cst(v) = \mathrm{lub}$, то

$$\boldsymbol{L} := \boldsymbol{L} \cup \{str(v_\Lambda, v)\},$$

иначе $\mathrm{lub} := cst(v)$ и

$$\boldsymbol{L} := \{str(v_\Lambda, v)\}.$$

Шаг 12. $LST := LST \cup \{v\}$ и переход к шагу 5.

Шаг 13. Удалить вершину v и инцидентную ей дугу и переход к шагу 5.

Корректность алгоритма 2.3 обосновывается следующей теоремой.

Теорема 2.3. Если множество $\boldsymbol{L}$ построено в результате работы алгоритма 2.3, то

$$\boldsymbol{L} = \boldsymbol{L}_\chi(\boldsymbol{S}).$$

Доказательство. Алгоритм 2.3 использует более сильное правило обрыва путей, чем алгоритм 2.2. Это усиление состоит в том, что удаляется также любая вершина v (а, следовательно, и все инцидентные ей дуги), *стоимость* которой превосходит *стоимость* уже построенных элементов множества $\boldsymbol{L}_{\chi_1}(\boldsymbol{S})$. При этом, после каждого выполнения шагов 9-11, множество $\boldsymbol{L}$ состоит из всех тех уже построенных элементов множества $\boldsymbol{L}_{\chi_1}(\boldsymbol{S})$, *стоимость* которых – наименьшая. Оценочная функция cst - монотонно неубывающая. Следовательно, любой оператор, считываемый в дереве $D_{\boldsymbol{S}}$ вдоль пути, идущего из корня v_Λ и проходящего через вершину v, удаляемую в результате выполнения шагов 9 и 13, не принадлежит множеству $\boldsymbol{L}_\chi(\boldsymbol{S})$. Из этого факта и из корректности алгоритма 2.2 вытекает, что все элементы множества $\boldsymbol{L}_\chi(\boldsymbol{S})$ присутствуют в дереве D, восстановление которого осуществляется в результате работы алгоритма 2.3. Следовательно, $\boldsymbol{L} = \boldsymbol{L}_\chi(\boldsymbol{S})$.

Теорема доказана.

Оценим сложность алгоритмов 2.1-2.3. Для упрощения изложения считаем, что выбран *равномерный вес* (см., напр., [1]). Такое предположение не ограничивает общность рассуждений. Кроме того, не будем учитывать сложность хранения тех уже построенных элементов множества $\boldsymbol{L}_\chi(\boldsymbol{S})$, которые заведомо не используются при дальнейших вычислениях.

В результате работы каждого из алгоритмов 2.1-2.3 восстанавливается поддерево

$$D = \bigcup_{i=0}^{k} D(i)$$

дерева $D_{\boldsymbol{S}}$, определяемое последовательностью деревьев (2.2). Обозначим через L_D высоту дерева D. Верхняя граница числа вершин дерева D равна $O(|F|^{L_D})$ $(L_D \to \infty)$. Следовательно, каждый из алгоритмов 2.1-2.3 имеет *экспоненциальную временную сложность*. Возможность хранения дерева D в явном виде гарантирует только *экспоненциальная память*. Явный вид дерева D необходим при работе алгоритмов 2.1 и 2.3. Однако при работе алгоритма 2.2 не требуется явный вид дерева D. Действительно, отличительная особенность поиска с возвращением состоит в том, что процесс восстановления дерева D является *локальным*, т.е. постоянно необходим только фрагмент, содержащий единственный путь, идущий из корня дерева D, или, иными словами, последовательность вида

$$s_{in} f_1 s_1 f_2 s_2 \ldots s_{i-1} f_i s_i \quad (i = 0,1,\ldots,L_D),$$

где $s_j f = s_{j+1}$ $(j = 0,1,\ldots,i-1)$, причем $s_0 = s_{in}$. Таким образом, справедливы следующие утверждения.

Утверждение 2.5. Алгоритмы 2.1-2.3 имеют экспоненциальную временную сложность.

Утверждение 2.6. Алгоритмы 2.1 и 2.3 имеют экспоненциальную емкостную сложность.

Утверждение 2.7. Емкостная сложность алгоритма 2.2 равна

$$V = O(L_D) \quad (L_D \to \infty), \tag{2.7}$$

где D - дерево, восстанавливаемое в результате работы алгоритма 2.2.

Ниже показано, что оценку (2.7) можно улучшить для важного специального случая.

Теорема 2.4. Если F - порождающее множество коммутативной полугруппы, то емкостная сложность алгоритма 2.2 равна
$$V = O(|\mathsf{F}|) \quad (L_{\mathsf{D}} \to \infty), \tag{2.8}$$
где D - дерево, восстанавливаемое в результате работы алгоритма 2.2.

Доказательство. Пусть $\mathsf{F} = \{f_1, \ldots, f_m\}$. Упорядочим элементарные операторы в соответствии с их индексами, т.е.
$$(\forall i, j \in \{1, \ldots, m\})(f_i \prec f_j \Leftrightarrow i < j).$$
Равенства
$$f_i f_j = f_j f_i \quad (f_i, f_j \in \mathsf{F}) \tag{2.9}$$
дают возможность представить каждый оператор $F \in \mathsf{F}^*$ в *стандартной форме*
$$F = f_1^{\alpha_1} \ldots f_m^{\alpha_m},$$
где $\alpha_i \in \mathbf{Z}_+$ $(i = 1, \ldots, m)$. Из (2.9) вытекает, что любые два оператора с одной и той же стандартной формой равны друг другу, как отображения. Следовательно, множество $\boldsymbol{L}_\chi(\boldsymbol{S})$ однозначно определяется множеством стандартных форм операторов. Для того, чтобы построить множество стандартных форм операторов, достаточно хранить последовательность *показателей*
$$\alpha_1, \ldots, \alpha_m \tag{2.10}$$
и последовательность *флагов* (т.е. булевых переменных)
$$\xi_1, \ldots, \xi_m, \tag{2.11}$$
где $\xi_i = 1$ $(i = 1, \ldots, m)$ тогда и только тогда, когда оператор $f_i^{\alpha_i}$ проанализирован в качестве возможного кандидата. Объем памяти, необходимой для хранения последовательностей (2.10) и (2.11) определяется формулой (2.8).

Теорема доказана.

Пример 2.2. Множество элементарных операторов F источника $\boldsymbol{S}$, построенного в примере 1.4 для решения фрагмента *задачи о раскрое* является порождающим множеством коммутативной полугруппы. Следовательно, в процессе построения множества всех вариантов раскроя достаточно хранить последовательность
$$\alpha_1, \ldots, \alpha_m,$$
где α_i $(i = 1, \ldots, m)$ - число вырезанных из рулона заготовок длины i и последовательность флагов
$$\xi_1, \ldots, \xi_m.$$
Отметим, что восстанавливаемое дерево будет минимальным, если выкраивать заготовки в соответствии с таким порядком $j_1, \ldots, j_m$, что $l_{j_1} < \ldots < l_{j_m}$.

2.2. M- источник.

Основной целью настоящего пункта является определение и исследование математической модели, предназначенной для представления задач поиска безусловных решений, свободной от указанных п.1.5 недостатков классического теоретико-множественного подхода, а также подхода, основанного на оценивании.

Одной из наиболее общих теоретико-множественных структур *является частичный порядок*. Наделение множества структурой частичного порядка не накладывает больших ограничений на само множество. Поэтому, в основе предлагаемого подхода и лежит предположение о возможности наделения пространства ситуаций структурой *частичного порядка*, позволяющего *сравнивать* между собой *расстояния* от двух ситуаций до множества финальных ситуаций. Возможность сравнения расстояний не требует знания истинных значений самих расстояний, т.е. последние могут быть вообще не известны. В [5] показано, что строение выигрышных операторов описывается в терминах ситуаций, *равноотстоящих* от множества финальных ситуаций. Следовательно, естественным является требование о том, чтобы определяемый на пространстве ситуаций частичный порядок был *согласован* с множествами равноотстоящих ситуаций. Отметим, что в подавляющем большинстве конкретных задач поиска такой частичный порядок можно определить. Кроме этого, предполагается, что элементарные операторы являются *монотонными отображениями* относительно этого частичного порядка. Последнее предположение выглядит вполне естественным, если действие элементарного оператора на ситуацию интерпретировать, как *снятие неопределенности*. Именно такой подход и дает возможность определить один из наиболее общих классов структурированных источников.

Определение 2.2. Источник $\mathbf{S} = (S, \mathsf{F}, s_{in}, S_{fin})$ назовем M-источником, если на множестве ситуаций S задано отношение частичного порядка $\leq_S$, удовлетворяющее следующим трем условиям:

Условие 2.11. Если $s_1 \in S_{fin}$ и $s_2 \leq_S s_1$, то $s_2 \in S_{fin}$.

Условие 2.12. Если $s_1 \in \mathrm{Dom}\, f$ $(f \in \mathsf{F})$ и $s_2 \leq_S s_1$, то $s_2 \in \mathrm{Dom}\, f$.

Условие 2.13. Если $s_2 \leq_S s_1$ $(s_1, s_2 \in S)$, то $s_2 f \leq_S s_1 f$ для любого такого $f \in \mathsf{F}$, что $s_1 \in \mathrm{Dom}\, f$.

Определенная выше математическая модель – M-источник – имеет следующее соотношение с классическими моделями, используемыми при построении безусловных решений. Обычный источник является M-источником, для которого отношение частичного порядка $\leq_S$ является *отношением равенства* на множестве ситуаций, а источник, построенный при использовании подхода, основанного на оценивании является M-источником, для которого отношение частичного порядка $\leq_S$ удовлетворяет условию

$$s_2 \leq_S s_1 \Rightarrow cst(s_2) \leq cst(s_1) \quad (s_1, s_2 \in S).$$

Отметим, что M-источник $\mathbf{S} = (S, \mathsf{F}, s_{in}, S_{fin})$ (как и обычный источник (см. п.1.5)) единственным образом определяет такую алгебраическую систему

$$\mathbf{A_S} = (A, \Omega_F, \Omega_P),$$

что $A = S$, $\Omega_F = \mathsf{F}^+_{s_{in}} \cup \{\varsigma_{s_{in}}\} \cup \{\varsigma_s \mid s \in S_{fin}\}$, где ς_{s_1} $(s_1 \in \{s_{in}\} \cup S_{fin})$ - 0-арная операция, выделяющая элемент s_1, а $\Omega_P = \{\leq_S\}$ (для обычного источника $\Omega_P = \varnothing$), где отношение частичного порядка $\leq_S$ удовлетворяет условиям 2.11-2.13.

Ограничения на отношение частичного порядка $\leq_S$ сформулированы выше в терминах элементарных операторов. Как показывает следующая теорема, эти ограничения естественно распространяются на множество F^*.

Теорема 2.5. Для любого $\mathcal{M}$-источника $\mathbf{S} = (S, \mathcal{F}, s_{in}, S_{fin})$, если $s_2 \le_S s_1$ $(s_1, s_2 \in S)$, то:

1) $\mathcal{F}^*_{s_2} \supseteq \mathcal{F}^*_{s_1}$;

2) $s_2 F \le_S s_1 F$ для любого $F \in \mathcal{F}^*_{s_1}$.

Доказательство. Так как $\mathcal{F}^*_s = \{\Lambda\} \cup \mathcal{F}^+_s$, где пустое слово Λ интерпретируется как тождественный оператор, определенный на всем множестве S, то для доказательства теоремы достаточно показать, что:

если $s_2 \le_S s_1$ $(s_1, s_2 \in S)$, *то* $\mathcal{F}^+_{s_2} \supseteq \mathcal{F}^+_{s_1}$ *и* $s_2 F \le_S s_1 F$ *для любого* $F \in \mathcal{F}^+_{s_1}$. (*)

Из равенства

$$\mathcal{F}^+_s = \bigcup_{r=1}^{\infty} (\mathcal{F}^+_s \cap \mathcal{F}^r) \ (s \in S)$$

вытекает, что для доказательства утверждения (*) достаточно показать, что:

если $s_2 \le_S s_1$ $(s_1, s_2 \in S)$, *то при всех* $n \in \mathbf{N}$
из $F \in \mathcal{F}^+_{s_1}$ *и* $d(F) = n$, *следует, что* $F \in \mathcal{F}^+_{s_2}$ *и* $s_2 F \le_S s_1 F$.

Докажем это утверждение индукцией по длине оператора.

1. Пусть $F \in \mathcal{F}^+_{s_1}$ и $d(F) = 1$. Тогда $F = f \in \mathcal{F}$. Так как $f \in \mathcal{F}^+_{s_1}$, то $s_1 \in \mathrm{Dom}\, f$. А так как $s_2 \le_S s_1$, то (см. условие 2.12) $s_2 \in \mathrm{Dom}\, f$, т.е. $f \in \mathcal{F}^+_{s_2}$ и (см. условие 2.13) $s_2 f \le_S s_1 f$, что и требовалось доказать.

2. Предположим, что утверждение справедливо для всех таких операторов $F \in \mathcal{F}^+_{s_1}$, что $d(F) \le r$.

3. Пусть $F \in \mathcal{F}^+_{s_1}$ и $d(F) = r + 1$. Тогда $F = F_1 f$, где $F_1 \in \mathcal{F}^r$ и $f \in \mathcal{F}$. Так как $F \in \mathcal{F}^+_{s_1}$, то $F_1 \in \mathcal{F}^+_{s_1}$ и $s_1 F_1 \in \mathrm{Dom}\, f$. Поскольку $F_1 \in \mathcal{F}^+_{s_1}$ и $d(F_1) = r$, то по предположению индукции из $s_2 \le_S s_1$ следует, что $F_1 \in \mathcal{F}^+_{s_2}$ и $s_2 F_1 \le_S s_1 F_1$. Так как $s_2 F_1 \le_S s_1 F_1$ и $s_1 F_1 \in \mathrm{Dom}\, f$, то (см. условия 2.12 и 2.13) $s_2 F_1 \in \mathrm{Dom}\, f$ и $(s_2 F_1) f \le_S (s_1 F_1) f$. Соотношение $s_2 F_1 \in \mathrm{Dom}\, f$ означает, что $F = F_1 f \in \mathcal{F}^+_{s_2}$. А из соотношения $(s_2 F_1) f \le_S (s_1 F_1) f$ вытекает, что $s_2 (F_1 f) \le_S s_1 (F_1 f)$, т.е. $s_2 F \le_S s_1 F$, что и требовалось доказать.

Теорема доказана.

Следствие 2.1. Для любого $\mathcal{M}$-источника $\mathbf{S} = (S, \mathcal{F}, s_{in}, S_{fin})$, если $s_2 \le_S s_1$ $(s_1, s_2 \in S)$ и

$$\mathcal{F}^*(s_2, S_{fin}) = \{F \in \mathcal{F}^*_{s_2} \mid s_2 F \in S_{fin}\} = \varnothing,$$

то

$$\mathcal{F}^*(s_1, S_{fin}) = \{F \in \mathcal{F}^*_{s_1} \mid s_1 F \in S_{fin}\} = \varnothing.$$

Доказательство. Предположим противное, т.е. что

$$\mathcal{F}^*(s_1, S_{fin}) \ne \varnothing.$$

Пусть $F \in \mathsf{F}^*(s_1, S_{fin})$. Тогда $F \in \mathsf{F}^+_{s_1}$. Так как $s_2 \le_S s_1$ и $F \in \mathsf{F}^+_{s_1}$, то (см. теорему 2.5) $F \in \mathsf{F}^+_{s_2}$ и $s_2 F \le_S s_1 F$. Так как $s_2 F \le_S s_1 F$ и $s_1 F \in S_{fin}$, то (см. условие 2.11) $s_2 F \in S_{fin}$. Из соотношений $F \in \mathsf{F}^+_{s_2}$ и $s_2 F \in S_{fin}$ вытекает, что $F \in \mathsf{F}^*(s_2, S_{fin})$, т.е.

$$\mathsf{F}^*(s_2, S_{fin}) \ne \varnothing .$$

Полученное противоречие показывает, что предположение – ложное. Следовательно,

$$\mathsf{F}^*(s_1, S_{fin}) = \varnothing ,$$

что и требовалось доказать.

Следствие доказано.

Теорема 2.5 характеризует структуру множества F^*_s $(s \in S)$ для M-источника $\boldsymbol{S}$ в терминах определенного на множестве ситуаций S отношения частичного порядка $\le_S$. Следствие 2.1 дает возможность выявить не пустоту множества выигрышных операторов в терминах *финальных отрезков* операторов и определенного на множестве ситуаций S отношения частичного порядка $\le_S$. Именно эти обстоятельства и дают возможность строить множества решений для M-источников более эффективно, чем при классических подходах.

2.3. Поиск безусловных решений для M-источников.

Основная цель настоящего пункта – это решение проблем 1.4-1.7 в предположении, что источник

$$\boldsymbol{S} = (S, \mathsf{F}, s_{in}, S_{fin})$$

является M-источником.

Общие методы поиска безусловных решений построены и исследованы в п.1.1. Следовательно, для решения проблем 1.4-1.6 достаточно построить множества *финальных*, *бесперспективных* и *порождающих вершин*, а затем детализировать соответствующим образом алгоритм 2.1.

Поиск минимальных решений. Исследуем вначале строение множества $\boldsymbol{L}^{\min}(\boldsymbol{S})$ для M-источника $\boldsymbol{S}$.

Теорема 2.6. Для любого M-источника $\boldsymbol{S} = (S, \mathsf{F}, s_{in}, S_{fin})$, если

$$s_{in} F_1 \le_S s_{in} F_2 \quad (F_1, F_2 \in \mathsf{F}^+_{s_{in}})$$

и

$$d(F_1) < d(F_2) ,$$

то

$$F_2 F \notin \boldsymbol{L}^{\min}(\boldsymbol{S})$$

для всех $F \in \mathsf{F}^+_{s_{in} F_2}$.

Доказательство. Предположим противное, т.е. что существует такой оператор $F \in \mathsf{F}^+_{s_{in} F_2}$, что

$$F_2 F \in \boldsymbol{L}^{\min}(\boldsymbol{S}) .$$

Оператор F_2F является выигрышным. Следовательно, $s_{in}(F_2F) \in S_{fin}$. В силу теоремы 2.5 из соотношений $s_{in}F_1 \leq_S s_{in}F_2$ и $F \in \mathsf{F}^+_{s_{in}F_2}$ вытекает, что $F \in \mathsf{F}^+_{s_{in}F_1}$ и $(s_{in}F_1)F \leq_S (s_{in}F_2)F$, т.е. $s_{in}(F_1F) \leq_S s_{in}(F_2F)$. Так как $s_{in}(F_1F) \leq_S s_{in}(F_2F)$ и $s_{in}(F_2F) \in S_{fin}$, то (см. условие 2.11) $s_{in}(F_1F) \in S_{fin}$, т.е. оператор F_1F является выигрышным. По условию $d(F_1) < d(F_2)$. Поэтому,

$$d(F_1F) = d(F_1) + d(F) < d(F_1) + d(F) = d(F_2F).$$

А так как F_1F и F_2F - выигрышные операторы и $d(F_1F) < d(F_2F)$, то

$$F_2F \notin \boldsymbol{L}^{\min}(\boldsymbol{S}).$$

Полученное противоречие показывает, что предположение – ложное. Следовательно,

$$F_2F \notin \boldsymbol{L}^{\min}(\boldsymbol{S})$$

для всех $F \in \mathsf{F}^+_{s_{in}F_2}$.

Теорема доказана.

Рассмотрим решение проблемы 1.4.

Переформулируем полученные выше результаты в терминах деревьев. Из теоремы 2.6 непосредственно вытекает справедливость следующей леммы.

Лемма 2.1. Пусть v_{F_1} и v_{F_2} - такие вершины соответственно $d(F_1)$-го и $d(F_2)$-го уровней $(d(F_1) < d(F_2))$ дерева $D_{\boldsymbol{S}}$ M-источника $\boldsymbol{S}$, что $s_{in}F_1 \leq_S s_{in}F_2$. Тогда любой оператор, считываемый в дереве $D_{\boldsymbol{S}}$ вдоль пути, идущего из корня и проходящего через вершину v_{F_2}, не принадлежит множеству $\boldsymbol{L}^{\min}(\boldsymbol{S})$.

Эта лемма дает возможность выделить поддерево дерева $D_{\boldsymbol{S}}$, представляющее множество $\boldsymbol{L}^{\min}(\boldsymbol{S})$ для M-источника $\boldsymbol{S}$.

Определение 2.3. Деревом $D^{\min}_{\boldsymbol{S}}$ для M-источника $\boldsymbol{S}$ назовем поддерево дерева $D_{\boldsymbol{S}}$, определяемое по правилу обрыва путей, в соответствии с которым вершина v_F - *оконечная* (т.е. удаляются все достижимые из нее вершины, расположенные в последующих уровнях и инцидентные им дуги), если выполнено хотя бы одно из следующих двух условий

Условие 2.14. В каком-либо из предшествующих $d(F)$-му уровней находится такая вершина v_{F_1}, что $s_{in}F_1 \leq_S s_{in}F$.

Условие 2.15. В $d(F)$-м уровне находится вершина, отмеченная элементом, принадлежащим множеству S_{fin}.

Пути в дереве $D_{\boldsymbol{S}}$, идущие из корня в вершины, отсутствующие в дереве $D^{\min}_{\boldsymbol{S}}$ назовем *усеченными*, а пути в дереве $D^{\min}_{\boldsymbol{S}}$, идущие из корня в вершины, отмеченные элементами, принадлежащими множеству S_{fin} - *выигрышными*.

Лемма 2.2. Если оператор $F \in \mathsf{F}^+_{s_{in}}$ считывается вдоль пути, усеченного при построении дерева $D^{\min}_{\boldsymbol{S}}$ для M-источника $\boldsymbol{S}$, то $F \notin \boldsymbol{L}^{\min}(\boldsymbol{S})$.

Доказательство. Пусть оператор $F \in F^{+}_{s_{in}}$ считывается вдоль пути, усеченного при построении дерева $D^{\min}_{\mathbf{S}}$ M-источника $\mathbf{S}$. Если путь усечен в соответствии с условием 2.14, то $F \notin \mathbf{L}^{\min}(\mathbf{S})$ в силу леммы 2.1. Предположим, что путь усечен в соответствии с условием 2.15. Тогда в дереве $D^{\min}_{\mathbf{S}}$ имеется такая вершина v_{F_1}, что $d(F_1) < d(F)$ и $s_{in}F \in S_{fin}$. Так как F_1 - выигрышный оператор и $d(F_1) < d(F)$, то $F \notin \mathbf{L}^{\min}(\mathbf{S})$.

Лемма доказана.

Теорема 2.7. Для любого M-источника $\mathbf{S}$ множество $\mathbf{L}^{\min}(\mathbf{S})$ - это множество всех операторов, считываемых вдоль выигрышных путей.

Доказательство. Возможны следующие два случая.

1. Пусть $\mathbf{L}^{\min}(\mathbf{S}) = \varnothing$. Тогда ни один оператор не является выигрышным для M-источника $\mathbf{S}$. Поэтому, ни одна вершина дерева $D_{\mathbf{S}}$, а, следовательно, и дерева $D^{\min}_{\mathbf{S}}$, не отмечена элементом множества S_{fin}. Это означает, что множество выигрышных путей пусто, что и требовалось доказать.

2. Пусть $\mathbf{L}^{\min}(\mathbf{S}) \neq \varnothing$. В силу утверждения 1.1, множество операторов, считываемых в дереве $D_{\mathbf{S}}$ вдоль всех путей, идущих из корня в некорневые вершины совпадает с множеством $F^{+}_{s_{in}}$. В силу леммы 2.2 операторы, считываемые вдоль усеченных путей, не являются минимальными выигрышными операторами. Следовательно, любой оператор $F \in \mathbf{L}^{\min}(\mathbf{S})$ считывается в дереве $D^{\min}_{\mathbf{S}}$ вдоль некоторого пути, идущего из корня. Из условия 2.15 вытекает, что все вершины, расположенные в первом из уровней, содержащих вершину, отмеченную элементом множества S_{fin} - оконечные. Поэтому, высота дерева $D^{\min}_{\mathbf{S}}$ равна наименьшей из длин выигрышных операторов. А это и означает, что $\mathbf{L}^{\min}(\mathbf{S})$ является множеством операторов, считываемых в дереве $D^{\min}_{\mathbf{S}}$ вдоль всех путей, идущих из корня в вершины, отмеченные элементами множества S_{fin}, т.е. вдоль выигрышных путей, что и требовалось доказать.

Теорема доказана.

Таким образом, в процессе решения проблемы 1.4 для M-источника $\mathbf{S}$ множества финальных, бесперспективных и порождающих вершин для всех $i = 0,1,\ldots$ определяются следующим образом (через V_i обозначено множество всех вершин i-го уровня восстанавливаемого дерева)

$$fnl_{\min}(i) = \{v_F \in V_i \mid s_{in}F \in S_{fin}\},$$

$$nprsp_{\min}(i) = \begin{cases} \{v_F \in V_i \mid (\exists v_{F_1} \in \bigcup_{j=0}^{i-1} V_j)(s_{in}F_1 \leq_S s_{in}F)\}, & \text{если } fnl_{\min}(i) = \varnothing \\ V_i \setminus fnl_{\min}(i), & \text{если } fnl_{\min}(i) \neq \varnothing \end{cases},$$

$$gnrt_{\min}(i) = V_i \setminus (fnl_{\min}(i) \cup nprsp_{\min}(i)).$$

Определенные выше множества финальных, бесперспективных и порождающих вершин приводят к следующей детализации алгоритма 2.1 для решения проблемы 1.4 для M-источника $\mathbf{S}$.

Алгоритм 2.4.

Шаг 1. Построить 0-й и 1-й уровни дерева $D_{\boldsymbol{S}}$, $i := 1$.

Шаг 2. Все оконечные вершины i-го уровня, отметки которых не принадлежат множеству S_{fin}, отметить символом ♠, $j := i - 1$.

Шаг 3. Если $j = 0$, то переход к шагу 6, иначе переход к шагу 4.

Шаг 4. Отметить символом ♠ каждую вершину j-го уровня, из которой достижимы только вершины $(j+1)$-го уровня, отмеченные символом ♠.

Шаг 5. Если хотя бы одна вершина j-го уровня отмечена символом ♠, то $j := j - 1$ и переход к шагу 3, иначе переход к шагу 6.

Шаг 6. Удалить все вершины (и инцидентные им дуги), отмеченные символом ♠.

Шаг 7. Если в i-м уровне имеются вершины, не являющиеся оконечными, то переход к шагу 8, иначе конец.

Шаг 8. Для каждой вершины i-го уровня построить все достижимые из нее вершины дерева $D_{\boldsymbol{S}}$, расположенные в $(i+1)$-м уровне, $i := i + 1$ и переход к шагу 2.

Корректность алгоритма 2.4 обеспечивается корректностью алгоритма 2.1. Отметим, что шаги 2-6 представляют собой детализацию процедуры $GRBG$.

Рассмотрим решение проблемы 1.5.

Очевидно, что решение проблемы 1.4 влечет и решение проблемы 1.5:

строим множество $\boldsymbol{L}^{\min}(\boldsymbol{S})$ и выбираем из него произвольный элемент.

Однако, при таком подходе решение проблемы 1.5 существенно усложняется за счет *не являющегося необходимым* построения всего множества $\boldsymbol{L}^{\min}(\boldsymbol{S})$. Поэтому принципиальное значение имеет выделение ядра $\boldsymbol{L}^{\min}_{\ker}(\boldsymbol{S})$ множества $\boldsymbol{L}^{\min}(\boldsymbol{S})$, удовлетворяющего следующим трем условиям

Условие 2.16. $\boldsymbol{L}^{\min}_{\ker}(\boldsymbol{S}) \subseteq \boldsymbol{L}^{\min}(\boldsymbol{S})$.

Условие 2.17. Построение множества $\boldsymbol{L}^{\min}_{\ker}(\boldsymbol{S})$ осуществляется наименее сложным образом.

Условие 2.18. $\boldsymbol{L}^{\min}_{\ker}(\boldsymbol{S}) \neq \varnothing$ тогда и только тогда, когда $\boldsymbol{L}^{\min}(\boldsymbol{S}) \neq \varnothing$.

Таким образом, проблема 1.5 естественно сводится к следующей проблеме.

Проблема 2.2. Для заданного M-источника $\boldsymbol{S}$ построить множество $\boldsymbol{L}^{\min}_{\ker}(\boldsymbol{S})$.

Рассмотрим решение проблемы 2.2.

Определение 2.4. i-характеристическим $(i = 0,1,\ldots)$ множеством для M-источника $\boldsymbol{S}$ назовем любое минимальное по мощности подмножество $V_i^{\ker}$ множества вершин V_i i-го уровня дерева $D^{\min}_{\boldsymbol{S}}$, что для каждой вершины $v_F \in V_i$ существует такая вершина $v_{F_1} \in V_i^{\ker}$, что $s_{in}F_1 \leq_S s_{in}F$.

Таким образом, $V_i^{\ker}$ $(i = 0,1,\ldots)$ - это *любое минимальное по мощности* подмножество вершин, принадлежащих множеству V_i, отметки которых – *все минимальные элементы* множества отметок вершин, принадлежащих множеству V_i.

Лемма 2.3. Каждое i-характеристическое $(i = 0,1,\ldots)$ множество $V_i^{\ker}$ порождает некоторое $(i+1)$-характеристическое множество $V_{i+1}^{\ker}$.

Доказательство. Докажем утверждение индукцией по высоте i $(i \in \mathbf{Z}_+)$ восстанавливаемого поддерева дерева $D_{\mathbf{S}}^{\min}$.

1. Пусть $i = 0$. Так как $V_0 = V_0^{\ker} = \{v_\Lambda\}$, то утверждение справедливо.
2. Предположим, что утверждение справедливо для всех $i = 0,1,\ldots,r$.
3. Докажем утверждение для $i = r+1$. Из предположения индукции вытекает, что

существует такая последовательность i-характеристических множеств

$$V_0^{\ker}, V_1^{\ker}, \ldots, V_r^{\ker},$$

что каждое i-характеристическое $(i = 0,1,\ldots,r-1)$ множество $V_i^{\ker}$ порождает $(i+1)$-характеристическое множество $V_{i+1}^{\ker}$. Так как $V_r^{\ker}$ - r-характеристическое множество, то для каждой вершины $v_F \in V_r$ существует такая вершина $v_{F_1} \in V_r^{\ker}$, что $s_{in}F_1 \le_S s_{in}F$ (см. определение 2.4). Из определения 2.2 (см. условие 2.13) вытекает, что $(s_{in}F_1)f \le_S (s_{in}F)f$ для каждого элементарного оператора $f \in \mathrm{Dom}\, s_{in}F$. Следовательно, множество вершин $(r+1)$-го уровня дерева $D_{\mathbf{S}}^{\min}$, порождаемых вершинами, принадлежащими множеству $V_r^{\ker}$ содержит некоторое подмножество вершин, принадлежащих множеству V_{r+1}, отметки которых – *все минимальные элементы* множества отметок вершин, принадлежащих множеству V_{r+1}. А это и означает, что r-характеристическое множество вершин $V_r^{\ker}$ порождает некоторое $(r+1)$-характеристическое множество вершин $V_{r+1}^{\ker}$, что и требовалось доказать.

Лемма доказана.

Таким образом, в процессе решения проблемы 2.2 для M-источника $\mathbf{S}$ множества финальных, бесперспективных и порождающих вершин определяются для всех $i = 0,1,\ldots$ следующим образом

$$fnl_{\ker}(i) = \{v_F \in V_i^{\ker} \mid s_{in}F \in S_{fin}\},$$

$$nprsp_{\ker}(i) = \begin{cases} \{v_F \in V_i^{\ker} \mid (\exists v_{F_1} \in \bigcup_{j=0}^{i-1} V_j^{\ker})(s_{in}F_1 \le_S s_{in}F)\}, & \text{если } fnl_{\ker}(i) = \varnothing \\ V_i^{\ker} \setminus fnl_{\ker}(i), & \text{если } fnl_{\ker}(i) \ne \varnothing \end{cases},$$

$$gnrt_{\ker}(i) = V_i^{\ker} \setminus (fnl_{\ker}(i) \cup nprsp_{\ker}(i)).$$

Определенные выше множества финальных, бесперспективных и порождающих вершин приводят к следующей детализации алгоритма 2.1 для решения проблемы 2.2.

Алгоритм 2.5.

Шаг 1. Построить 0-й и 1-й уровни дерева $D_{\mathbf{S}}^{\min}$. Найти 1-характеристическое множество $V_1^{\ker}$, $i := 1$.

Шаг 2. Отметить символом ♠ все вершины i-го уровня, не принадлежащие множеству $V_i^{\ker}$, а также все оконечные вершины, принадлежащие множеству $V_i^{\ker}$, отметки которых не принадлежат множеству S_{fin}, $j := i-1$.

Шаг 3. Если $j = 0$, то переход к шагу 6, иначе переход к шагу 4.

Шаг 4. Отметить символом ♠ каждую вершину j-го уровня, из которой достижимы только вершины $(j+1)$-го уровня, отмеченные символом ♠.

Шаг 5. Если хотя бы одна вершина j-го уровня отмечена символом ♠, то $j := j-1$ и переход к шагу 3, иначе переход к шагу 6.

Шаг 6. Удалить все вершины (и инцидентные им дуги), отмеченные символом ♠.

Шаг 7. Если в i-м уровне имеются вершины, не являющиеся оконечными, то переход к шагу 8, иначе конец.

Шаг 8. Для каждой вершины i-го уровня построить все достижимые из нее вершины дерева $D_{\mathbf{S}}$, расположенные в $(i+1)$-м уровне. Построить множество $V_{i+1}^{\ker}$, $i := i+1$ и переход к шагу 2.

Корректность алгоритма 2.5 обеспечивается корректностью алгоритма 2.1. Отметим, что шаги 2-6 представляют собой детализацию процедуры $GRBG$.

Подчеркнем, что в отличие от множества $\boldsymbol{L}^{\min}(\boldsymbol{S})$ *ядро* $\boldsymbol{L}_{\ker}^{\min}(\boldsymbol{S})$ *определяется не единственным образом*. Все многообразие ядер можно получить за счет варьирования i-характеристических множеств, конструируемых в результате работы алгоритма 2.5.

Поиск минимальных решений относится к классу тех проблем, для которых выполняется следующее условие.

Условие 2.19. Очередной *фрагмент* решения строится только на основе анализа *начальных отрезков* уже восстановленных операторов.

Именно это условие и является основой для снижения *сложности* решения проблем поиска за счет организации *параллельных вычислений*.

В [35] показано, как можно организовать параллельные вычисления в процессе поиска для специального случая. Исследуем общие принципы такой организации. Отметим, что актуальность этой проблемы резко возрастает в связи с интенсивным развитием новых парадигм вычислений - ДНК-вычислений и квантовых вычислений (см., напр., [125]).

Для представления каждой конкретной задачи поиска можно построить различные M-источники. Выбор того или иного M-источника определяется выбором множества ситуаций S и множества элементарных операторов F. Однако с точки зрения интерпретации модельных решений в терминах рассматриваемой задачи поиска (см. этапы 1.8-1.11), т.е. в терминах *конфигураций* и *воздействий*, а также способа построения последовательностей *воздействий*, все многообразие допустимых для рассматриваемой задачи поиска M-источников можно разбить на следующие два класса моделей.

Прямой M-источник. Элементы множества S представляют *конфигурации*, причем s_{in} - исходную *конфигурацию*, а S_{fin} - множество целевых *конфигураций*. Множество элементарных операторов F выбирается как множество *имен воздействий*, а именно: каждому *воздействию* ставится в соответствие такой $f \in \mathsf{F}$, что $s_1 f = s_2$ $(s_1, s_2 \in S)$ тогда и только тогда, когда рассматриваемое *воздействие* переводит *конфигурацию*, представленную ситуацией s_1 в *конфигурацию*, представленную ситуацией s_2. Выигрышное решение $F = f_1 \ldots f_r$ интерпретируется следующим образом: последовательное применение *воздействий*, представленных элементарными операторами $f_1, \ldots, f_r$ переводит исходную *конфигурацию* в некоторую целевую *конфигурацию*.

Обратный M-источник. Элементы множества S представляют подмножества *конфигураций*, причем s_{in} - множество целевых *конфигураций*, а S_{fin} - состоит из ситуаций, представляющих исходную *конфигурацию*. Множество элементарных операторов F выбирается следующим образом: каждому *воздействию* ставится в соответствие такой $f \in \mathsf{F}$, что $s_1 f = s_2$ $(s_1, s_2 \in S)$ тогда и только тогда, когда рассматриваемое *воздействие* переводит множество *конфигураций*, представленное ситуацией s_2 в множество *конфигураций*, представленное ситуацией s_1. Выигрышное решение $F = f_1 \ldots f_r$ интерпретируется следующим образом: последовательное применение *воздействий*, представленных элементарными операторами $f_r, \ldots, f_1$ переводит исходную *конфигурацию* в некоторую целевую *конфигурацию*.

Такая классификация M-источников дает возможность следующим образом произвести классификацию способов построения минимальных последовательностей *воздействий* для конкретных проблем поиска, в зависимости от типа выбранного M-источника:

1) *поиск минимальных последовательностей воздействий* осуществляется *восстановлением* их *начальных отрезков*, если для представления задачи поиска выбран *прямой* M*-источник* $\boldsymbol{S}$;
2) *поиск минимальных последовательностей воздействий* осуществляется *восстановлением* их *финальных отрезков*, если для представления задачи поиска выбран *обратный* M*-источник* $\boldsymbol{S}$.

Организацию *параллельных вычислений* при поиске минимальных последовательностей *воздействий* можно осуществить за счет одновременного построения отрезков минимальных последовательностей *воздействий* для прямого и обратного M-источников. Рассмотрим указанный процесс более подробно.

Пусть $\boldsymbol{S} = (S, \mathsf{F}^{(1)}, s_{in}, S_{fin})$ и $\boldsymbol{T} = (T, \mathsf{F}^{(2)}, t_{in}, T_{fin})$ есть, соответственно, *прямой и обратный* для рассматриваемой задачи поиска M-источник. Определим отображение

$$\theta : S \times T \to \{0,1\}$$

следующим образом:

$\theta(s,t) = 1$ $(s \in S, t \in T)$ тогда и только тогда, когда *конфигурация*, представленная в M-источнике $\boldsymbol{S}$ ситуацией s принадлежит множеству *конфигураций*, представленных в M-источнике $\boldsymbol{T}$ ситуацией t.

Из определения отображения θ непосредственно вытекает справедливость следующего утверждения (верхний индекс ‘ $^{(1)}$ ’ означает, что объект построен для прямого M-источника $\boldsymbol{S}$, а верхний индекс ‘ $^{(2)}$ ’ – что для обратного M-источника $\boldsymbol{T}$)

Утверждение 2.8. Предположим, что $v^{(1)}_{F^{(1)}_1}$ и $v^{(2)}_{F^{(2)}_2}$ - это такие вершины деревьев, соответственно, $D_{\boldsymbol{S}}$ и $D_{\boldsymbol{T}}$, что

$$\theta(s_{in}F_1^{(1)}, t_{in}F_2^{(2)}) = 1.$$

Если

$$F_1^{(1)} = f_1^{(1)} \dots f_i^{(1)}$$

и

$$F_2^{(2)} = f_1^{(2)} \dots f_j^{(2)},$$

то последовательное применение воздействий, определяемых последовательностью элементарных операторов

$$f_1^{(1)}, \dots, f_i^{(1)}, f_j^{(2)}, \dots, f_1^{(2)},$$

переводит исходную *конфигурацию* в множество целевых *конфигураций*.

Утверждение 2.8 обосновывает корректность следующего алгоритма поиска минимальных последовательностей *воздействий*, переводящих исходную *конфигурацию* в множество целевых *конфигураций*.

Алгоритм 2.6.

Шаг 1. $i := 0$, $j := 0$.

Шаг 2. Если $V_i^{(1)} = \varnothing$ или $V_j^{(2)} = \varnothing$, то конец, иначе переход к шагу 3.

Шаг 3. Если существуют такие вершины $v^{(1)}_{F^{(1)}_1} \in V_i^{(1)}$ и $v^{(2)}_{F^{(2)}_2} \in V_j^{(2)}$, что

$$\theta(s_{in}F_1^{(1)}, t_{in}F_2^{(2)}) = 1,$$

то конец, иначе переход к шагу 4.

Шаг 4. Если $|V_i^{(1)}| < |V_j^{(2)}|$, то $i := i+1$, иначе $j := j+1$.

Шаг 5. Переход к шагу 2.

Если остановка работы алгоритма 2.6 произойдет в процессе выполнения шага 2, то для рассматриваемой задачи поиска вообще не существует последовательностей *воздействий*, переводящих исходную *конфигурацию* в множество целевых *конфигураций*. Если же остановка работы алгоритма 2.6 произойдет в процессе выполнения шага 3, то для рассматриваемой задачи поиска множество всех минимальных последовательностей *воздействий*, переводящих исходную *конфигурацию* в множество целевых *конфигураций*, определяется всеми такими парами вершин $v^{(1)}_{F^{(1)}_1} \in V_i^{(1)}$ и $v^{(2)}_{F^{(2)}_2} \in V_j^{(2)}$, что $\theta(s_{in}F_1^{(1)}, t_{in}F_2^{(2)}) = 1$.

Покажем, что сложность алгоритма 2.6 может быть существенно ниже, чем сложность одностороннего поиска минимальных последовательностей воздействий, переводящих исходную *конфигурацию* в множество целевых *конфигураций*.

Пусть $|F^{(1)}| = |F^{(2)}| = m$ и l - длина минимальной последовательности воздействий, переводящих исходную *конфигурацию* в множество целевых *конфигураций*. Очевидно, что наихудший случай имеет место, если в процессе восстановления представляющего дерева вообще не произойдет ни одного обрыва путей. В этом случае при одностороннем поиске восстанавливается полное дерево в m-буквенном алфавите, имеющее высоту l. Число вершин этого дерева равно

$$1 + m + \ldots + m^l = \frac{m^{l+1} - 1}{m - 1}.$$

В то же время, при вычислениях в соответствии с алгоритмом 2.6 восстанавливается одно полное дерево в m-буквенном алфавите, имеющее высоту $\lfloor 0{,}5\cdot(l+1)\rfloor$ и одно полное дерево в m-буквенном алфавите, имеющее высоту $\lfloor 0{,}5\cdot l\rfloor$. Общее число вершин в восстановленных деревьях равно

$$1+m+\ldots+m^{\lfloor 0{,}5\cdot(l+1)\rfloor}+1+m+\ldots+m^{\lfloor 0{,}5\cdot l\rfloor}=\frac{m^{\lfloor 0{,}5\cdot(l+1)\rfloor+1}+m^{\lfloor 0{,}5\cdot l\rfloor+1}-2}{m-1}.$$

Поиск кооперативных решений. Рассмотрим решение проблемы 1.7.

В процессе решения этой проблемы будем считать, что заданный M-источник

$$\mathbf{S}=(S,\mathsf{F},s_{in},S_{fin})$$

удовлетворяет следующему дополнительному условию:

Условие 2.20. Частично упорядоченное множество $(S,\le_S)$ является *нижней полуструктурой*.

Условие 2.20 означает, что для каждой неупорядоченной пары ситуаций $\{s_1,s_2\}$ $(s_1,s_2\in S)$ существует единственная ситуация s $(s\in S)$, удовлетворяющая следующим двум условиям:

Условие 2.21. $s\le_S s_1$ и $s\le_S s_2$.

Условие 2.22. Для любой ситуации $\tilde{s}\in S$, если $\tilde{s}\le_S s_1$ и $\tilde{s}\le_S s_2$, то $\tilde{s}\le_S s$.

Ситуацию s, удовлетворяющую условиям 2.21 и 2.22, принято обозначать через $\mathrm{glb}\{s_1,s_2\}$. Таким образом, на множестве ситуаций S определена такая *коммутативная бинарная операция*

$$\mathrm{glb}: S\times S\to S,$$

что $s_1\le_S s_2$ $(s_1,s_2\in S)$ тогда и только тогда, когда $\mathrm{glb}\{s_1,s_2\}=s_1$.

Известно, что бинарная операция glb - *ассоциативная* (см., напр., [7]). Следовательно, запись

$$\mathrm{glb}\{s_1,\ldots,s_i\}$$

корректна для всех $i=2,3,\ldots$. Следовательно, для каждого $i=2,3,\ldots$ операция glb может рассматриваться как такая *коммутативная i-арная операция*

$$\mathrm{glb}:\underbrace{S\times\ldots\times S}_{i\ раз}\to S,$$

что $s=\mathrm{glb}\{s_1,\ldots,s_i\}$ тогда и только тогда, когда выполнены следующие два условия:

Условие 2.23. $s\le_S s_j$ для всех $j=1,\ldots,i$.

Условие 2.24. Если $\tilde{s}\le_S s_j$ для всех $j=1,\ldots,i$, то $\tilde{s}\le_S s$.

Так как множество ситуаций M-источника – *конечное*, то предположение, что $(S,\leq_S)$ - *нижняя полуструктура* влечет, что $\mathrm{glb}\,S_1$ существует для любого непустого подмножества S_1 множества S. В частности, существует наименьший элемент $\mathrm{glb}\,S$ множества S, причем (см. условие 2.11)

$$\mathrm{glb}\,S \in S_{fin}.$$

Отметим, что для любых двух непустых подмножеств S_1 и S_2 множества ситуаций S справедливо включение

$$S_1 \subseteq S_2 \Rightarrow \mathrm{glb}\,S_1 \leq_S \mathrm{glb}\,S_2.$$

Рассмотрим поиск *кооперативного решения* (см. п.1.5) в предположении, что в качестве j-арной операции ω_j $(j = 2,3,\ldots)$ выбрана j-арная операция glb. Таким образом, множество операторов $\{F_1,\ldots,F_j\}$ является j-*кооперативным решением* $(j = 2,3,\ldots)$, если выполнены следующие три условия (см. условия 1.6-1.8):

Условие 2.25. $\mathrm{glb}\{s_{in}F_1,\ldots,s_{in}F_j\} \in S_{fin}$.

Условие 2.26. Для каждого $i = 2,\ldots,j-1$

$$\mathrm{glb}(s_{in}F_{h_1},\ldots,s_{in}F_{h_i}) \notin S_{fin}$$

при всех таких $h_i,\ldots,h_i$, что $1 \leq h_1 < \ldots < h_i \leq j$.

Условие 2.27. Если $\boldsymbol{L}(\mathbf{S}) \neq \varnothing$, то

$$d(F_i) < \min_{F\in \boldsymbol{L}(\mathbf{S})} d(F)$$

для всех $i = 1,\ldots,j$.

Из определения i-характеристического множества $(i = 0,1,\ldots)$ и условий 2.25-2.27 вытекает, что поиск кооперативного решения осуществим с помощью следующей модификации алгоритма 2.5 (через X обозначено искомое кооперативное решение).

Алгоритм 2.7.

Шаг 1. $X := \varnothing$. Построить 0-й и 1-й уровни дерева $D_{\mathbf{S}}^{\min}$. Найти 1-характеристическое множество $V_1^{\ker}$, $i := 1$.

Шаг 2. Отметить символом ♠ все вершины i-го уровня, не принадлежащие множеству $V_i^{\ker}$, а также все оконечные вершины, принадлежащие множеству $V_i^{\ker}$, отметки которых не принадлежат множеству S_{fin}, $j := i-1$.

Шаг 3. Если $j = 0$, то переход к шагу 6, иначе переход к шагу 4.

Шаг 4. Отметить символом ♠ каждую вершину j-го уровня, из которой достижимы только вершины $(j+1)$-го уровня, отмеченные символом ♠.

Шаг 5. Если хотя бы одна вершина j-го уровня отмечена символом ♠, то $j := j-1$ и переход к шагу 3, иначе переход к шагу 6.

Шаг 6. Удалить все вершины (и инцидентные им дуги), отмеченные символом ♠.

Шаг 7. Если в i-м уровне имеются вершины, не являющиеся оконечными, то переход к шагу 8, иначе конец.

Шаг 8. Если

$$\mathrm{glb}\{s_{in}F \mid v_F \in \bigcup_{j=0}^{i} V_i\} \in S_{fin},$$

то переход к шагу 9, иначе переход к шагу 10.

Шаг 9. Выбрать в качестве U любое такое минимальное по мощности подмножество множества $\bigcup_{j=0}^{i} V_j$, что $\mathrm{glb}U \in S_{fin}$. $X := \{F \mid v_F \in U\}$ и конец.

Шаг10. Для каждой вершины i-го уровня построить все достижимые из нее вершины дерева $D_{\mathbf{S}}$, расположенные в $(i+1)$-м уровне. Построить множество $V_i^{\ker}$, $i := i+1$ и переход к шагу 2.

Корректность алгоритма 2.7 обеспечивается корректностью алгоритма 2.5.

Поиск неприводимых решений. Исследуем вначале строение множества $\boldsymbol{L}^{ir}(\boldsymbol{S})$ для M-источника $\boldsymbol{S}$.

Теорема 2.8. Для любого M-источника $\boldsymbol{S} = (S, \mathsf{F}, s_{in}, S_{fin})$ если для оператора $F \in \mathsf{F}^{+}_{s_{in}}$ существует такое представление

$$F = F_1F_2 \ \ (F_1, F_2 \in \mathsf{F}^{+}),$$

что

$$s_{in}F_1 \leq_S s_{in}F,$$

то

$$FF_3 \notin \boldsymbol{L}^{ir}(\boldsymbol{S})$$

для всех $F_3 \in \mathsf{F}^{+}_{s_{in}F}$.

Доказательство. Предположим противное, т.е. что существует такой оператор $F_3 \in \mathsf{F}^{+}_{s_{in}F}$, что

$$FF_3 \in \boldsymbol{L}^{ir}(\boldsymbol{S}).$$

Из соотношений $s_{in}F_1 \leq_S s_{in}F$ и $F_3 \in \mathsf{F}^{+}_{s_{in}F}$ вытекает (см. теорему 2.5), что $F_3 \in \mathsf{F}^{+}_{s_{in}F_1}$ и $(s_{in}F_1)F_3 \leq_S (s_{in}F)F_3$, т.е. $s_{in}(F_1F_3) \leq_S s_{in}(FF_3)$. Так как $FF_3 \in \boldsymbol{L}^{ir}(\boldsymbol{S})$, то FF_3 - выигрышный оператор. Следовательно, $s_{in}(FF_3) \in S_{fin}$. Из соотношений $s_{in}(F_1F_3) \leq_S s_{in}(FF_3)$ и $s_{in}(FF_3) \in S_{fin}$ вытекает (см. условие 2.11), что $s_{in}(F_1F_3) \in S_{fin}$, т.е. что F_1F_3 - выигрышный оператор. Итак, в результате удаления из выигрышного оператора $FF_3 = F_1F_2F_3$ непустого оператора F_2 получен выигрышный оператор F_1F_3. Это означает, что

$$FF_3 \notin \boldsymbol{L}^{ir}(\boldsymbol{S}).$$

Полученное противоречие показывает, что предположение – ложное. Следовательно,

$$FF_3 \notin \boldsymbol{L}^{ir}(\boldsymbol{S})$$

для всех $F_3 \in \mathsf{F}^{+}_{s_{in}F}$.

Теорема доказана.

Рассмотрим решение проблемы 1.6.

Переформулируем полученные результаты в терминах деревьев. Из теоремы 2.8 непосредственно вытекает справедливость следующей леммы.

Лемма 2.4. Пусть v_{F_1} и v_{F_2} $(d(F_1) < d(F_2))$ - такие вершины дерева $D_{\boldsymbol{S}}$ M-источника $\boldsymbol{S}$, что вершина v_{F_1} лежит на пути, идущем из корня v_Λ в вершину v_{F_2}. Если $s_{in}F_1 \le_S s_{in}F_2$, то любой оператор, считываемый в дереве $D_{\boldsymbol{S}}$ вдоль пути, идущего из корня и проходящего через вершину v_{F_2} не принадлежит множеству $\boldsymbol{L}^{ir}(\boldsymbol{S})$.

Эта лемма дает возможность выделить следующее поддерево дерева $D_{\boldsymbol{S}}$.

Определение 2.5. Деревом $D^{ir}_{\boldsymbol{S}}$ для M-источника $\boldsymbol{S}$ назовем поддерево дерева $D_{\boldsymbol{S}}$, определяемое по правилу обрыва путей, в соответствии с которым вершина v_F - *оконечная* (т.е. удаляются все достижимые из нее вершины, расположенные в последующих уровнях и инцидентные им дуги), если выполнено хотя бы одно из следующих двух условий:

Условие 2.28. На пути, идущем из корня дерева $D_{\boldsymbol{S}}$ в вершину v_F, расположена такая вершина v_{F_1} $(d(F_1) < d(F))$, что $s_{in}F_1 \le_S s_{in}F$.

Условие 2.29. Отметка вершины v_F - элемент множества S_{fin}.

Пути в дереве $D_{\boldsymbol{S}}$, идущие из корня в вершины, отсутствующие в дереве $D^{ir}_{\boldsymbol{S}}$ назовем *усеченными*, а пути в дереве $D^{ir}_{\boldsymbol{S}}$, идущие из корня в вершины, отмеченные элементами, принадлежащими множеству S_{fin} - *выигрышными*.

Лемма 2.5. Если оператор $F \in \mathsf{F}^+_{s_{in}}$ считывается вдоль пути, усеченного при построении дерева $D^{ir}_{\boldsymbol{S}}$ для M-источника $\boldsymbol{S}$, то $F \notin \boldsymbol{L}^{ir}(\boldsymbol{S})$.

Доказательство. Пусть оператор $F \in \mathsf{F}^+_{s_{in}}$ считывается вдоль пути, усеченного при построении дерева $D^{ir}_{\boldsymbol{S}}$.

Если путь усечен в соответствии с условием 2.28, то $F \notin \boldsymbol{L}^{ir}(\boldsymbol{S})$ в силу леммы 2.4.

Предположим, что путь усечен в соответствии с условием 2.29. Тогда для оператора F существует такое представление $F = F_1F_2$ $(F_1, F_2 \in \mathsf{F}^+)$, что $s_{in}F_1 \in S_{fin}$. Итак, в результате удаления из оператора F непустого оператора F_2 получен выигрышный оператор F_1. Это означает, что $F \notin \boldsymbol{L}^{ir}(\boldsymbol{S})$.

Лемма доказана.

Из леммы 2.5 вытекает, что множество операторов $\boldsymbol{L}$, считываемых в дереве $D^{ir}_{\boldsymbol{S}}$ вдоль выигрышных путей, *содержит* множество $\boldsymbol{L}^{ir}(\boldsymbol{S})$, т.е. справедливо включение

$$\boldsymbol{L}^{ir}(\boldsymbol{S}) \subseteq \boldsymbol{L}.$$

К сожалению, в этом случае не имеет места аналог теоремы 2.7. Поэтому процесс поиска множества $\boldsymbol{L}^{ir}(\boldsymbol{S})$ состоит из следующих двух этапов:

Этап 2.1. Осуществляется поиск множества операторов $\boldsymbol{L}$.

Этап 2.2. Выделяется подмножество $\boldsymbol{L}^{ir}(\boldsymbol{S})$ множества $\boldsymbol{L}$.

Рассмотрим каждый из этих этапов по отдельности.

Рассмотрим этап 2.1. Из лемм 2.4, 2.5 и определения 2.5 вытекает, что для $\mathcal{M}$-источника $\boldsymbol{S}$ множества финальных, бесперспективных и порождающих вершин для всех $i = 0,1,\ldots$ определяются следующим образом (через V_i обозначено множество всех вершин i-го уровня восстанавливаемого дерева)

$$fnl_{ir}(i) = \{v_F \in V_i \mid s_{in}F \in S_{fin}\} ,$$

$$nprsp_{ir}(i) = \{v_F \in V_i \mid (\exists F_1, F_2 \in \mathsf{F}^+)((F = F_1F_2) \wedge (s_{in}F_1 \leq_{\boldsymbol{S}} s_{in}F))\} ,$$

$$gnrt_{ir}(i) = V_i \setminus (nprsp_{ir}(i) \cup fnl_{ir}(i)) .$$

Определенные выше множества финальных, бесперспективных и порождающих вершин приводят к следующей детализации алгоритма 2.1 для поиска множества $\boldsymbol{L}$ для $\mathcal{M}$-источника $\boldsymbol{S}$.

Алгоритм 2.8.

Шаг 1. Построить 0-й и 1-й уровни дерева $D_{\boldsymbol{S}}$, $i := 1$.

Шаг 2. Все оконечные вершины i-го уровня, отметки которых не принадлежат множеству S_{fin}, отметить символом ♠, $j := i - 1$.

Шаг 3. Если $j = 0$, то переход к шагу 6, иначе переход к шагу 4.

Шаг 4. Отметить символом ♠ каждую вершину j-го уровня, из которой достижимы только вершины $(j+1)$-го уровня, отмеченные символом ♠.

Шаг 5. Если существует вершина j-го уровня, отмеченная символом ♠, то $j := j - 1$ и переход к шагу 3, иначе переход к шагу 6.

Шаг 6. Удалить все вершины (и инцидентные им дуги), отмеченные символом ♠.

Шаг 7. Если в i-м уровне имеются вершины, не являющиеся оконечными, то переход к шагу 8, иначе конец.

Шаг 8. Для каждой вершины i-го уровня построить все достижимые из нее вершины дерева $D_{\boldsymbol{S}}$, расположенные в $(i+1)$-м уровне, $i := i + 1$ и переход к шагу 2.

Корректность алгоритма 2.8 обеспечивается корректностью алгоритма 2.1. Отметим, что шаги 2-6 представляют собой детализацию процедуры $GRBG$.

Чисто внешне алгоритм 2.8 идентичен алгоритму 2.4. Различие в действиях этих алгоритмов происходит за счет различного определения множеств финальных, бесперспективных и порождающих вершин.

Рассмотрим этап 2.2. Свойство ‘*быть не избыточным*’, заложенное в *определении неприводимого решения*, проявляет себя тем, что без дополнительных ограничений на структуру $\mathcal{M}$-источника $\boldsymbol{S}$ выделить подмножество $\boldsymbol{L}^{ir}(\boldsymbol{S})$ множества $\boldsymbol{L}$ можно только *методом решета*. Отличительной особенностью конструируемого решета является *нечисловая природа* просеиваемых объектов.

Упорядочим множество $\boldsymbol{L}$, расположив принадлежащие ему операторы в порядке не убывания их длин. Процесс просеивания осуществляется в соответствии со следующим алгоритмом.

Алгоритм 2.9.
Шаг 1. $\boldsymbol{L}^{ir}(\boldsymbol{S}) := \boldsymbol{L}^{\min}(\boldsymbol{S})$, $\boldsymbol{L} := \boldsymbol{L} \setminus \boldsymbol{L}^{\min}(\boldsymbol{S})$.
Шаг 2. Если $\boldsymbol{L} \neq \varnothing$, то переход к шагу 3, иначе конец.
Шаг 3. Выбрать первый оператор $F \in \boldsymbol{L}$, $\boldsymbol{L} := \boldsymbol{L} \setminus \{F\}$.
Шаг 4. $\mathbf{L}_F := erase(F) \cap \mathbf{L}(\boldsymbol{S})$.
Шаг 5. Если $\mathbf{L}_F \cap \boldsymbol{L}^{ir}(\mathbf{S}) = \varnothing$, то переход к шагу 6, иначе переход к шагу 2.
Шаг 6. $\boldsymbol{L}^{ir}(\boldsymbol{S}) := \boldsymbol{L}^{ir}(\mathbf{S}) \cup \{F\}$ и переход к шагу 2.

Корректность алгоритма 2.9 непосредственно вытекает из определения неприводимого решения и из включений

$$\boldsymbol{L}^{\min}(\mathbf{S}) \subseteq \boldsymbol{L}^{ir}(\mathbf{S}) \subseteq \boldsymbol{L}.$$

Таким образом, построены исчерпывающие решения каждой из проблем 1.4-1.7 для M-источника.

2.4. AM-источник.

Основной целью настоящего пункта является определение и исследование математической модели - AM-источника, предназначенной для представления задач поиска адаптивных решений. Предложенная модель (как и M-источник, определенный в п.2.3) базируется на *частичной упорядоченности* множества ситуаций и предположении о том, что элементарные операторы – *монотонные* (возможно, частичные) *отображения*. Такая унификация дает возможность обеспечить выполнение следующих трех целей. Во-первых, определить один из наиболее общих классов структурированных источников, предназначенных для поиска адаптивных решений. Во-вторых, сохранить основные свойства операторов, справедливые для M-источников. В третьих, исследовать общие соотношения между моделями, предназначенными для поиска безусловных и адаптивных решений.

Определение 2.6. Источник $\boldsymbol{S} = (S, \mathsf{H}, s_{in}, S_{fin})$ ($\mathsf{H} \subseteq \mathsf{F} \times \mathsf{G}$) назовем AM-источником, если на множестве ситуаций S задано отношение частичного порядка $\leq_S$, удовлетворяющее следующим трем условиям:

Условие 2.30. Если $s_1 \in S_{fin}$ и $s_2 \leq_S s_1$, то $s_1 \in S_{fin}$.

Условие 2.31. Если $s_1 \in \mathrm{Dom}(f, g)$ ($(f, g) \in \mathsf{H}$) и $s_2 \leq_S s_1$, то $\varnothing \neq \mathsf{G}_{s_2, f} \subseteq \mathsf{G}_{s_1, f}$.

Условие 2.32. Если $s_2 \leq_S s_1$, то $s_2(f, g) \leq_S s_1(f, g)$ для любого такого $s_1 \in \mathrm{Dom}(f, g)$, что $g \in \mathsf{G}_{s_2, f}$.

Из определения 2.6 вытекает справедливость следующей леммы.

Лемма 2.6. Если существует такой $(f, g) \in \mathsf{H}$, что $s_2 \in \mathrm{Dom}(f, g)$ и $s_1 \notin \mathrm{Dom}(f, g)$, то $\mathsf{G}_{s_1, f} = \varnothing$.

Доказательство. Предположим противное, т.е. что $\mathsf{G}_{s_1, f} \neq \varnothing$. Тогда существует такой $(f, g_1) \in \mathsf{H}$, что $s_1 \in \mathrm{Dom}(f, g_1)$. Следовательно (см. условие 2.31) $\varnothing \neq \mathsf{G}_{s_2, f} \subseteq \mathsf{G}_{s_1, f}$. Так как $s_2 \in \mathrm{Dom}(f, g)$, то $g \in \mathsf{G}_{s_2, f}$. Из соотношений $g \in \mathsf{G}_{s_2, f}$ и

$G_{s_2,f} \subseteq G_{s_1,f}$ вытекает, что $g \in G_{s_1,f}$, т.е. $s_1 \in \mathrm{Dom}\,(f,g)$. Получено противоречие. Следовательно, предположение – ложное. Таким образом, $G_{s_1,f} = \varnothing$.

Лемма доказана.

Ограничения на отношение частичного порядка $\leq_S$ сформулированы выше в терминах элементарных операторов. Следующая теорема устанавливает, что эти ограничения естественно распространяются на множество H^*.

Теорема 2.9. Для любого AM-источника $\boldsymbol{S} = (S, H, s_{in}, S_{fin})$ $(H \subseteq F \times G)$, если $s_2 \leq_S s_1$ $(s_1, s_2 \in S)$, то $s_2 H \leq_S s_1 H$ для любого такого $H \in H^*$, что $s_1, s_2 \in \mathrm{Dom}\, H$.

Доказательство теоремы 2.9 аналогично доказательству теоремы 2.5 и *осуществляется индукцией по длине оператора*.

Из сравнения между собой определений 2.2 и 2.6 непосредственно вытекает справедливость следующего утверждения.

Утверждение 2.9. Если $|G| = 1$, то AM-источник $\boldsymbol{S} = (S, H, s_{in}, S_{fin})$ $(H \subseteq F \times G)$ является M-источником.

Исследуем соотношение между AM-источниками и M-источниками в общем случае. Пусть зафиксирован AM-источник

$$\boldsymbol{S} = (S, H, s_{in}, S_{fin}) \ (H \subseteq F \times G).$$

Положим

$$\Sigma = \{\sigma \in \mathbf{B}(S) \mid s_1 \not\leq_S s_2 \text{ и } s_2 \not\leq_S s_1 \text{ для всех таких } s_1, s_2 \in \sigma, \text{что } s_1 \neq s_2\},$$

где $\mathbf{B}(S)$ - булеан множества S. Отметим, что $\varnothing \in \Sigma$ для любого AM-источника $\boldsymbol{S}$.

Определим на множестве Σ отношение частичного порядка $\leq_\Sigma$ следующим образом:

$$\sigma_1 \leq_\Sigma \sigma_2 \Leftrightarrow (\forall s_1 \in \sigma_1)(\exists s_2 \in \sigma_2)(s_1 \leq_S s_2)$$

для любых $\sigma_1, \sigma_2 \in \Sigma$. Отметим, что для любого AM-источника $\boldsymbol{S}$

$$\varnothing \leq_\Sigma \sigma$$

для всех $\sigma \in \Sigma$.

Элементы множества F будем рассматривать как (возможно, частичные) отображения

$$f : \Sigma \to \Sigma \ (f \in F),$$

для которых значения σf $(\sigma \in \Sigma, f \in F)$ вычисляются в соответствии со следующим алгоритмом.

Алгоритм 2.10.

Шаг 1. Если существует такое $s \in \sigma$, что $G_{s,f} = \varnothing$, то σf не определено и конец, иначе переход к шагу 2.

Шаг 2. $\sigma' := \bigcup_{s \in \sigma} \{s(f,g) \mid g \in G_{s,f}\}$.

Шаг 3. $\sigma'' := \{s \mid s$ - максимальный по отношению $\leq_S$ элемент множества $\sigma'\}$.

Шаг 4. $\sigma f := \sigma'' \setminus S_{fin}$ и конец.

Сопоставим с AM-источником $\boldsymbol{S}$ источник

$$\boldsymbol{C}(\boldsymbol{S}) = (\Sigma, F, \{s_{in}\}, \{\varnothing\}).$$

Теорема 2.10. Для любого AM-источника

$$\boldsymbol{S} = (S, H, s_{in}, S_{fin}) \ (H \subseteq F \times G)$$

источник

$$\boldsymbol{C}(\boldsymbol{S}) = (\Sigma, F, \{s_{in}\}, \{\varnothing\})$$

является M-источником.

Доказательство. Для доказательства теоремы достаточно показать, что для источника $\boldsymbol{C}(\boldsymbol{S})$ выполнены условия 2.11-2.13.

Условие 2.11 для источника $\boldsymbol{C}(\boldsymbol{S})$ выполняется автоматически, так как множество финальных ситуаций $\{\varnothing\}$ источника $\boldsymbol{C}(\boldsymbol{S})$ содержит единственный элемент.

Покажем, что для источника $\boldsymbol{C}(\boldsymbol{S})$ выполнено условие 2.12. Пусть

$$\sigma_2 \leq_\Sigma \sigma_1 \ (\sigma_1, \sigma_2 \in \Sigma) \tag{2.12}$$

и

$$\sigma_1 \in \mathrm{Dom}\, f \ (f \in F). \tag{2.13}$$

Из (2.12) вытекает, что для каждого $s_2 \in \sigma_2$ существует такое $s_1 \in \sigma_1$, что

$$s_2 \leq_S s_1. \tag{2.14}$$

Из (2.13) и шага 1 алгоритма 2.10 вытекает, что $G_{s_1,f} \neq \varnothing$ для всех $s_1 \in \sigma_1$. Следовательно, для каждого $s_1 \in \sigma_1$ существует такое $g \in G$, что

$$s_1 \in \mathrm{Dom}\,(f, g). \tag{2.15}$$

Из (2.14), (2.15) вытекает (см. условие 2.31), что $G_{s_2,f} \neq \varnothing$ для всех $s_2 \in \sigma_2$. Поэтому, в соответствии с шагом 1 алгоритма 2.10,

$$\sigma_2 \in \mathrm{Dom}\, f,$$

т.е. для источника $\boldsymbol{C}(\boldsymbol{S})$ условие 2.12 выполнено.

Покажем, что для источника $\boldsymbol{C}(\boldsymbol{S})$ выполнено условие 2.13. Предположим, что справедливы формулы (2.12) и (2.13). Для источника $\boldsymbol{C}(\boldsymbol{S})$ выполнено условие 2.12. Следовательно, $\sigma_2 \in \mathrm{Dom}\, f$. Возможны следующие два случая.

Случай 1. Пусть $\sigma_2 f = \varnothing$. Тогда $\sigma_2 f \leq_\Sigma \sigma_1 f$, так как $\varnothing \leq_\Sigma \sigma$ для всех $\sigma \in \Sigma$. Следовательно, условие 2.13 выполнено в рассматриваемом случае.

Случай 2. Пусть $\sigma_2 f \neq \varnothing$. Выберем произвольный элемент $s_2 \in \sigma_2 f$. Из шага 4 алгоритма 2.10 вытекает, что $s_2 \notin S_{fin}$. В соответствии с шагами 2-4 алгоритма 2.10 существуют такие $s_2' \in \sigma_2$ и $g \in G$, что

$$s_2'(f, g) = s_2. \tag{2.16}$$

Из (2.12) вытекает, что существует такое $s_1' \in \sigma_1$, что

$$s_2' \leq_S s_1'. \tag{2.17}$$

Из (2.16) и (2.17) вытекает (см. условие 2.32), что

$$s_2'(f, g) \leq_S s_1'(f, g). \tag{2.18}$$

В соответствии с шагом 3 алгоритма 2.10 существует такое $s_1 \in \sigma_1 f$, что

$$s_1'(f, g) \leq_S s_1. \tag{2.19}$$

Из (2.16), (2.18) и (2.19) вытекает, что

$$s_2 \le_S s_1 . \tag{2.20}$$

Таким образом, показано, что для каждого $s_2 \in \sigma_2 f$ существует такое $s_1 \in \sigma_1 f$, что справедлива формула (2.20). Это и означает, что $\sigma_2 f \le_\Sigma \sigma_1 f$, т.е. условие 2.13 выполнено в рассматриваемом случае.

Теорема доказана.

Установим связь между безусловными решениями, построенными для M-источника $\boldsymbol{C}(\boldsymbol{S})$ и адаптивными решениями, построенными для AM-источника $\boldsymbol{S}$.

Предположим, что

$$\boldsymbol{L}(\boldsymbol{C}(\boldsymbol{S})) \ne \varnothing .$$

Из условий 1.10 и 1.11 вытекает, что, в первую очередь, интерес представляют именно неприводимые решения, построенные для M-источника $\boldsymbol{C}(\boldsymbol{S})$. С каждым неприводимым решением

$$F = f_1 \dots f_l \in \boldsymbol{L}^{ir}(\boldsymbol{C}(\boldsymbol{S}))$$

сопоставим частичное отображение

$$B_F : \mathsf{G}^* \to \mathsf{F},$$

удовлетворяющее следующим четырем условиям:

Условие 2.33. $\Lambda \in \mathrm{Dom}\, B_F$.

Условие 2.34. $g_1 \dots g_r \in \mathrm{Dom}\, B_F \ \ (r = 1, \dots, l)$ тогда и только тогда, когда справедливы следующие три соотношения:

$$g_1 \dots g_{r-1} \in \mathrm{Dom}\, B_F ,$$
$$s_{in} \in \mathrm{Dom}\,(f_1, g_1) \dots (f_r, g_r)$$

и

$$s_{in}(f_1, g_1) \dots (f_r, g_r) \notin S_{fin} .$$

Условие 2.35. Равенство

$$B_F(g_1, \dots, g_r) = f_{r+1}$$

справедливо для всех $g_1 \dots g_r \in \mathrm{Dom}\, B_F \ \ (r = 0, 1, \dots, l-1)$.

Условие 2.36. Если $G \notin \mathrm{Dom}\, B_F \ \ (G \in \mathsf{G}^+)$, то $GG_1 \notin \mathrm{Dom}\, B_F$ для всех $G_1 \in \mathsf{G}^+$.

Теорема 2.11. Частичное отображение

$$B_F : \mathsf{G}^* \to \mathsf{F} \ \ (F = f_1 \dots f_l \in \boldsymbol{L}^{ir}(\boldsymbol{C}(\boldsymbol{S}))), \tag{2.21}$$

удовлетворяющее условиям 2.33-2.36, является адаптивным решением для AM-источника $\boldsymbol{S}$.

Доказательство. Для доказательства теоремы достаточно показать, что для отображения (2.21) выполнены условия 1.9-1.12.

Условие 1.9 выполнено, так как оно совпадает с условием 2.33.

Покажем, что выполнено условие 1.11. Возможны следующие два случая.

Случай 1. Пусть $l = 1$. Тогда $\{s_{in}\}f_1 = \varnothing$. Следовательно (см. алгоритм 2.10), $\mathsf{G}_{s_{in},f_1} \neq \varnothing$ и $\{s_{in}\}(f_1, g) \in S_{fin}$ для всех $g \in \mathsf{G}_{s_{in}f_1}$. Так как $\{s_{in}\}(f_1, g) \in S_{fin}$ для всех $g \in \mathsf{G}_{s_{in}f_1}$, то (см. условие 2.34)

$$g \notin \mathrm{Dom}\, B_F$$

для всех $g \in \mathsf{G}$. Это означает, что условие 1.11 автоматически выполнено.

Случай 2. Пусть $l \geq 2$. Предположим, что $g_1 \ldots g_r \in \mathrm{Dom}\, B_F$ $(r = 1, \ldots, l-1)$ и $g_1 \ldots g_r g \notin \mathrm{Dom}\, B_F$ для всех $g \in \mathsf{G}$. Так как $g_1 \ldots g_r \in \mathrm{Dom}\, B_F$, то (см. условие 2.34)

$$s_{in} \in \mathrm{Dom}\,(f_1, g_1) \ldots (f_i, g_i)$$

и

$$s_{in}(f_1, g_1) \ldots (f_i, g_i) \notin S_{fin}$$

для всех $i = 1, \ldots, r$. А так как $g_1 \ldots g_r g \notin \mathrm{Dom}\, B_F$ для всех $g \in \mathsf{G}$, то (см. условие 2.34) для всех $g \in \mathsf{G}$

$$s_{in} \notin \mathrm{Dom}\,(f_1, g_1) \ldots (f_r, g_r)(f_{r+1}, g),$$

или

$$s_{in}(f_1, g_1) \ldots (f_r, g_r)(f_{r+1}, g) \in S_{fin}.$$

Предположим, что $s_{in} \notin \mathrm{Dom}\,(f_1, g_1) \ldots (f_r, g_r)(f_{r+1}, g)$ для всех $g \in \mathsf{G}$. Так как

$$s_{in}(f_1, g_1) \ldots (f_i, g_i) \notin S_{fin}$$

для всех $i = 1, \ldots, r$, то (см. алгоритм 2.10) существует такое $s \in \{s_{in}\}f_1 \ldots f_r$, что

$$s_{in}(f_1, g_1) \ldots (f_r, g_r) \leq_S s, \tag{2.22}$$

причем $s \notin S_{fin}$. Следовательно (см. алгоритм 2.10), $\mathsf{G}_{s,f_{r+1}} \neq \varnothing$, т.е. существует такое $g \in \mathsf{G}$, что

$$s \in \mathrm{Dom}\,(f_{r+1}, g) \tag{2.23}$$

Из (2.22) и (2.23) вытекает (см. условие 2.31), что существует такое $g \in \mathsf{G}$, что

$$s_{in}(f_1, g_1) \ldots (f_r, g_r) \in \mathrm{Dom}\,(f_{r+1}, g),$$

т.е. существует такое $g \in \mathsf{G}$, что

$$s_{in} \in \mathrm{Dom}\,(f_1, g_1) \ldots (f_r, g_r)(f_{r+1}, g).$$

Полученное противоречие показывает, что предположение – ложное.

Следовательно (см. условие 2.35),

$$\mathsf{G}_{s_{in}(B(\Lambda), g_1)(B(g_1), g_2) \ldots (B(g_1 \ldots g_{r-1}), g_r), B(g_1 \ldots g_r)} \neq \varnothing$$

и

$$s_{in}(B(\Lambda), g_1)(B(g_1), g_2) \ldots (B(g_1 \ldots g_{r-1}), g_r)(B(g_1 \ldots g_r), g) \in S_{fin}$$

для всех $g \in \mathsf{G}_{s_{in}(B(\Lambda), g_1)(B(g_1), g_2) \ldots (B(g_1 \ldots g_{r-1}), g_r), B(g_1 \ldots g_r)}$, т.е. условие 1.11 выполнено.

Покажем, что выполнено условие 1.12. Предположим, что $g_1 \ldots g_l \in \mathrm{Dom}\, B_F$. Тогда (см. условие 2.34)

$$s_{in} \in \mathrm{Dom}\,(f_1, g_1) \ldots (f_i, g_i)$$

и

$$s_{in}(f_1, g_1) \ldots (f_i, g_i) \notin S_{fin}$$

для всех $i = 1,\dots,l$. Это означает, что (см. алгоритм 2.10)

$$\{s_{in}\}f_1 \dots f_l \neq \varnothing. \qquad (2.24)$$

Соотношение (2.24) противоречит тому, что $F = f_1 \dots f_l \in \boldsymbol{L}(\boldsymbol{C}(\boldsymbol{S}))$ и, следовательно, что $F \in \boldsymbol{L}^{ir}(\boldsymbol{C}(\boldsymbol{S}))$. Таким образом, предположение – ложное, т.е. $g_1 \dots g_l \notin \mathrm{Dom}\, B_F$ для всех $g_1 \dots g_l \in \mathsf{G}^l$. Следовательно (см. условие 2.36)

$$d(G) \leq l - 1 \qquad (2.25)$$

для всех $G \in \mathrm{Dom}\, B_F$. А это и означает, что выполнено условие 1.12.

Покажем, что выполнено условие 1.10. Условие 2.35 и неравенство (2.25) дают возможность переформулировать условие 2.34 в следующем виде:

$g_1 \dots g_r \in \mathrm{Dom}\, B_F$ $(r \in \mathbf{N})$ тогда и только тогда, когда справедливы следующие три соотношения

$$g_1 \dots g_{r-1} \in \mathrm{Dom}\, B_F\,,$$

$$s_{in} \in \mathrm{Dom}\,(B_F(\Lambda), g_1)\dots(B_F(g_1 \dots g_{r-1}), g_r)$$

и

$$s_{in}(B_F(\Lambda), g_1)\dots(B_F(g_1 \dots g_{r-1}), g_r) \notin S_{fin}.$$

А это и означает, что выполнено условие 1.10.

Теорема доказана.

Значение теоремы 2.11 состоит в том, что она обосновывает общий метод конструирования, для любой конкретной задачи поиска, математической модели – M-источника, предназначенной для поиска безусловных решений по построенной раннее математической модели - AM-источнику, предназначенной для поиска адаптивных решений. Отметим, что известны случаи, когда в процессе решения конкретных задач поиска поступали наоборот. А именно, для построенного источника, предназначенного для поиска безусловных решений, (представленного, как правило, в виде дерева) исследовали множество ситуаций с целью выявления правил более раннего обрыва путей. Именно такой подход был применен в [11] при построении регулярных экспериментов по идентификации внутренних состояний конечного автомата.

2.5. Поиск адаптивных решений для AM- источников.

Основная цель настоящего пункта – это решение проблемы 1.8 в предположении, что источник

$$\boldsymbol{S} = (S, \mathsf{H}, s_{in}, S_{fin}) \ \ (\mathsf{H} \subseteq \mathsf{F} \times \mathsf{G})$$

является AM-источником.

Исследуем вначале структуру адаптивных решений для AM-источника $\boldsymbol{S}$.

Распространим отношение частичного порядка $\leq_S$ на множество $\mathbf{B}(S)$ следующим образом:

$$S_1 \leq_S S_2 \Leftrightarrow (\forall s_1 \in S_1)(\exists s_2 \in S_2)(s_1 \leq_S s_2)$$

для любых $S_1, S_2 \in \mathbf{B}(S)$. Для любых $H \in \mathsf{H}^*$ и $f \in \mathsf{F}$ положим

$$S_{H(f,*)} = \{s_{in}H(f,g) \mid (f,g) \in \mathsf{H}, s_{in}H \in \mathrm{Dom}\,(f,g)\}.$$

Лемма 2.7. Пусть B - адаптивное решение для AM-источника

$$\boldsymbol{S} = (S, \mathsf{H}, s_{in}, S_{fin}) \ \ (\mathsf{H} \subseteq \mathsf{F} \times \mathsf{G}),$$

$$g_1 \dots g_r \in \mathrm{Dom}\, B \ (r \geq 1),$$
$$H = (B(\Lambda), g_1)(B(g_1), g_2)\dots(B(g_1 \dots g_{r-1}), g_r)$$
и
$$f = B(g_1 \dots g_r).$$
Если существует такой элемент $f_1 \in \mathsf{F}$, что
$$\mathsf{G}_{s_{in}H, f_1} \neq \varnothing \qquad (2.26)$$
и
$$S_{H(f_1,*)} \leq_S S_{H(f,*)}, \qquad (2.27)$$
то существует такое адаптивное решение B_1 для AM-источника $\boldsymbol{S}$, что
$$B_1(g_1 \dots g_i) = B(g_1 \dots g_i) \qquad (2.28)$$
для всех $i = 0,1,\dots,r-1$ и
$$B_1(g_1 \dots g_r) = f_1. \qquad (2.29)$$

Доказательство. Предположим, что существует элемент $f_1 \in \mathsf{F}$, удовлетворяющий условиям (2.26) и (2.27). Исходя из адаптивного решения
$$B : \mathsf{G}^* \to \mathsf{F}$$
построим такое адаптивное решение
$$B_1 : \mathsf{G}^* \to \mathsf{F},$$
что выполнены условия (2.28) и (2.29).

Положим
$$B_1(G) = B(G)$$
для всех $G \in \mathrm{Dom}\, B \setminus g_1 \dots g_r \mathsf{G}^*$ и
$$B_1(g_1 \dots g_r) = f_1.$$
Так как $g_1 \dots g_r \in \mathrm{Dom}\, B$, то $s_{in}H \notin S_{fin}$.

Возможны следующие два случая.

Случай 1. $S_{s_{in}H, f_1} \subseteq S_{fin}$. Тогда положим
$$g_1 \dots g_r \mathsf{G}^+ \cap \mathrm{Dom}\, B_1 = \varnothing.$$
Построение частичного отображения B_1 закончено. Из (2.26) вытекает, что условие 1.11 выполнено для B_1. Следовательно, B_1 - адаптивное решение для AM-источника $\boldsymbol{S}$, что и требовалось показать.

Случай 2. $S_{s_{in}H, f_1} \not\subseteq S_{fin}$. Для всех таких элементов $g \in \mathsf{G}_{s_{in}H, f_1}$, что $s_{in}H(f_1, g) \in S_{fin}$ положим
$$g_1 \dots g_r g \notin \mathrm{Dom}\, B_1.$$

Рассмотрим множество $S' = S_{s_{in}H, f_1} \setminus S_{fin}$. Из (2.27) вытекает, что для каждой ситуации $s' \in S'$ существует такая ситуация $s \in S_{H(f,*)}$, что $s' \leq_S s$. Так как $s' \notin S_{fin}$ и $s' \leq_S s$, то (см. условие 2.30) $s \notin S_{fin}$. Пусть $s' = s_{in}H(f_1, g')$ и $s = s_{in}H(f, g)$. Так как $s \notin S_{fin}$, то $g_1 \dots g_r g \in \mathrm{Dom}\, B$. А так как $s' \leq_S s$ и $\mathsf{G}_{s, B(g_1 \dots g_r g)} \neq \varnothing$, то (см. условие 2.31) $\varnothing \neq \mathsf{G}_{s', B(g_1 \dots g_r g)} \subseteq \mathsf{G}_{s, B(g_1 \dots g_r g)}$. Положим
$$B_1(g_1 \dots g_r g') = B(g_1 \dots g_r g).$$
При этом (см. условие 2.32)

$$s'(B_1(g_1\dots g_r g'),g'')\le_S s(B(g_1\dots g_r g),g'')$$
для всех $g''\in \mathsf{G}_{s',B_1(g_1\dots g_r g')}$.

Если $s(B(g_1\dots g_r g),g'')\in S_{fin}$, то (см. условие 2.30) $s'(B_1(g_1\dots g_r g'),g'')\in S_{fin}$ и полагаем
$$g_1\dots g_r g'\mathsf{G}^+\cap \mathrm{Dom}\, B_1=\varnothing .$$

Если $s'(B_1(g_1\dots g_r g'),g'')\notin S_{fin}$, то продолжаем описанный процесс для ситуаций $s'(B_1(g_1\dots g_r g'),g'')$ и $s(B(g_1\dots g_r g),g'')$. Этот процесс обрывается через конечное число шагов, так как B - адаптивное решение для AM-источника $\boldsymbol{S}$. Его результатом является адаптивное решение B_1 для AM-источника $\boldsymbol{S}$, удовлетворяющее условиям (2.28) и (2.29), что и требовалось показать.

Лемма доказана.

Лемма 2.8. Пусть B - адаптивное решение для AM-источника
$$\boldsymbol{S}=(S,\mathsf{H},s_{in},S_{fin})\ \ (\mathsf{H}\subseteq \mathsf{F}\times\mathsf{G}),$$
$$g_1\dots g_r\in \mathrm{Dom}\, B\ \ (r\ge 1)$$
и
$$H=(B(\Lambda),g_1)(B(g_1),g_2)\dots(B(g_1\dots g_{r-1}),g_r).$$
Если существует такое $j\in\{0,1,\dots,r-1\}$, что
$$s_{in}H_1\le_S s_{in}H, \tag{2.30}$$
где
$$H_1=(B(\Lambda),g_1)(B(g_1),g_2)\dots(B(g_1\dots g_{j-1}),g_j),$$
то существует такое адаптивное решение B_1 для AM-источника $\boldsymbol{S}$, что
$$B_1(g_1\dots g_i)=B(g_1\dots g_i) \tag{2.31}$$
для всех $i=0,1,\dots,j-1$ и
$$B_1(g_1\dots g_j)=B(g_1\dots g_r). \tag{2.32}$$

Доказательство. Предположим, что существует такое $j\in\{0,1,\dots,r-1\}$, что справедливо неравенство (2.30). Исходя из адаптивного решения
$$B:\mathsf{G}^*\to\mathsf{F}$$
построим такое адаптивное решение
$$B_1:\mathsf{G}^*\to\mathsf{F},$$
что выполнены условия (2.31) и (2.32).

Положим
$$B_1(G)=B(G)$$
для всех $G\in \mathrm{Dom}\, B\setminus g_1\dots g_{j-1}\mathsf{G}^*$ и
$$B_1(g_1\dots g_j)=B(g_1\dots g_r). \tag{2.33}$$
Из (2.30) и соотношения $g_1\dots g_r\in \mathrm{Dom}\, B$ вытекает, что
$$\mathsf{G}_{s_{in}H_1,B_1(g_1\dots g_j)}\ne\varnothing \tag{2.34}$$
и
$$S_{H_1(B_1(g_1\dots g_j),*)}\le_S S_{H(B(g_1\dots g_r),*)}. \tag{2.35}$$
Следовательно, доопределение частичного отображения B_1 для элемента $g_1\dots g_j$ в соответствии с равенством (2.33) корректно при построении адаптивного решения.

Из (2.34) и (2.35) вытекает, что доопределение частичного отображения B_1 для всех $G \in g_1 \dots g_j \mathsf{G}^+$ можно осуществить в соответствии с процедурой, используемой в лемме 2.7.

Лемма доказана.

Зафиксируем произвольное отображение

$$\rho : \mathsf{H}^*_{s_{in}} \to \mathbf{B}(\mathsf{F}),$$

удовлетворяющее следующему условию:

Условие 2.37. Для каждого $H \in \mathsf{H}^*_{s_{in}}$ множество

$$\{S_{H(f,*)} \mid f \in \rho(H), \mathsf{G}_{s_{in}H,f} \neq \varnothing\}$$

является минимальным по мощности множеством, содержащим все минимальные по отношению частичного порядка $\leq_S$ элементы множества

$$\{S_{H(f,*)} \mid f \in \mathsf{F}, \mathsf{G}_{s_{in}H,f} \neq \varnothing\}.$$

Из лемм 2.7 и 2.8 вытекает, что для поиска одного, безразлично какого именно, адаптивного решения для AM-источника $\mathbf{S}$ достаточно построить (последовательно, уровень за уровнем) поддерево $\mathsf{D}^{adptv}_{\mathbf{S}}$ дерева $\mathsf{D}_{\mathbf{S}}$, определяемого следующими тремя правилами обрыва путей

Правило 2.4. Вершина v_{Hf} $(H \in \mathsf{H}^*_{s_{in}},\ f \in \mathsf{F})$ (по построению, эта вершина расположена в *нечетном* уровне) и все достижимые из нее вершины (а также инцидентные им дуги) удаляются, если $f \notin \rho(H)$.

Правило 2.5. Вершина v_H $(H \in \mathsf{H}^+_{s_{in}})$ (по построению, эта вершина расположена в *четном* уровне) и все достижимые из нее вершины (а также инцидентные им дуги) удаляются, если на пути, идущем из корня v_Λ в вершину v_H в некотором из *четных* уровней, предшествующих $d(H)$-ому, расположена такая вершина v_{H_1} $(H_1 \in \mathsf{H}^*_{s_{in}})$, что $s_{in}H_1 \leq_S s_{in}H$.

Правило 2.6. Вершина v и все достижимые из нее вершины (а также инцидентные им дуги) удаляются, если на пути, идущем из корня v_Λ в вершину v в некотором из *четных* предшествующих уровней расположена такая вершина v_H $(H \in \mathsf{H}^*)$, что $s_{in}H \in S_{fin}$.

Не представляет особого труда построить детализацию алгоритма 2.1, предназначенную для построения поддерева $\mathsf{D}^{adptv}_{\mathbf{S}}$ дерева $\mathsf{D}_{\mathbf{S}}$. После того, как дерево $\mathsf{D}^{adptv}_{\mathbf{S}}$ построено, его фрагмент, определяющий адаптивное решение B, может быть *вырезан* с помощью обычного *метода поиска выигрышной стратегии для игры двух лиц*. Этот метод основан на двойном проходе дерева $\mathsf{D}^{adptv}_{\mathbf{S}}$ (сначала *снизу вверх*, а затем *сверху вниз*) и состоит в следующем.

Проход дерева $\mathsf{D}^{adptv}_{\mathbf{S}}$ *снизу вверх* основан на *инициализации*, осуществляемой в соответствии с правилом

Правило 2.7. Все *висячие вершины* (или, иными словами, *листья*) дерева $D_{\mathbf{S}}^{adptv}$ (по построению, все эти вершины расположены в *четных* уровнях дерева $D_{\mathbf{S}}^{adptv}$), отмеченные элементами множества S_{fin}, отмечаются символом ♠.

Затем выполняется *итеративная процедура* в соответствии со следующими двумя правилами

Правило 2.8. Если из вершины v, расположенной в *нечетном* уровне, достижимы только вершины следующего уровня, отмеченные символом ♠, то вершина v отмечается символом ♣.

Правило 2.9. Если из вершины v, расположенной в *четном* уровне, достижима хотя бы одна вершина следующего уровня, отмеченная символом ♣, то вершина v отмечается символом ♠.

По завершению этой процедуры (т.е. после того, как достигнут и обработан корень дерева), осуществляется *чистка дерева* в соответствии с правилом

Правило 2.10. Удаляются все некорневые вершины и инцидентные им дуги (а, следовательно, все достижимые из них вершины и инцидентные им дуги), не отмеченные ни символом ♠, ни символом ♣.

Если после выполнения указанных действий получено дерево D, содержащее единственную вершину – корень v_{Λ}, то адаптивное решение для AM-источника $\mathbf{S}$ *не существует* и процесс решения проблемы 1.8 завершен. Если же после выполнения указанных действий получено дерево D, содержащее не только корень v_{Λ}, то адаптивное решение для AM-источника $\mathbf{S}$ *существует*. Для выделения этого решения и осуществляется проход дерева D *сверху вниз*. Такой проход выполняется с помощью *итеративной процедуры* в соответствии со следующими двумя правилами.

Правило 2.11. Для каждой вершины v_H $(H \in H^*)$ (эта вершина расположена в *четном* уровне и отмечена символом ♠) выбирается одна из порождаемых ею вершин v_1 следующего уровня (такая вершина, если она существует, отмечена символом ♣). Вершина v_1 отмечается символом $+$.

Правило 2.12. Удаляются все вершины $(d(H)+1)$-го уровня (и инцидентные им дуги), достижимые из вершины v_H и не отмеченные символом $+$ (а, следовательно, удаляются также все достижимые из них вершины и инцидентные им дуги).

Таким образом, получено полное решение проблемы 1.8 для AM-источника.

Построенное в результате прямого прохода дерево, представляющее адаптивное решение B для AM-источника $\mathbf{S}$ всегда может быть свернуто в частичный автомат Мура с входным алфавитом G и выходным алфавитом F. Следовательно, разработанный подход дает конструктивные средства для представления адаптивных решений *автоматами-экспериментаторами*.

2.6. Неприводимые множества представителей семейства множеств.

В процессе решения ряда как фундаментальных, так и прикладных проблем дискретной математики естественно возникает необходимость поиска *множеств представителей* заданного семейства множеств, т.е. множеств, имеющих непустое пересечение с каждым элементом семейства. Особый интерес представляют множества представителей, никакие собственные подмножества которых таковыми не являются. Назовем такие множества представителей *неприводимыми*.

Целью настоящего пункта и является решение проблемы поиска всех неприводимых множеств представителей заданного семейства множеств. Эта проблема, по своей сути, представляет собой поиск на частично упорядоченных структурах. Именно по этой причине настоящий пункт и включен в данный раздел.

Введем формальные определения.

Пусть зафиксировано семейство подмножеств

$$\boldsymbol{A} = \{\alpha_i\}_{i \in I} \quad (|I| \leq \aleph_0)$$

заданного множества U.

Множеством представителей семейства множеств $\boldsymbol{A}$ назовем любое такое множество V $(V \subseteq U)$, что

$$V \cap \alpha_i \neq \varnothing$$

для всех $i \in I$.

Множество представителей V семейства множеств $\boldsymbol{A}$ назовем *неприводимым*, если для любого его собственного подмножества V_1 существует такое $i \in I$, что

$$V_1 \cap \alpha_i = \varnothing .$$

Таким образом, неприводимые множества представителей являются *минимальными по отношению включения* множествами представителей.

Обозначим через $\boldsymbol{V_A}$ множество всех неприводимых множеств представителей семейства множеств $\boldsymbol{A}$. Основной целью настоящего пункта является решение следующей проблемы

Проблема 2.3. Построить множество $\boldsymbol{V_A}$ для заданного семейства множеств $\boldsymbol{A}$.

Следующие два примера показывают, что проблема 2.3 естественно возникает в процессе решения как фундаментальных, так и прикладных задач дискретной математики.

Пример 2.3 (*Поиск базисов для булевых функций*).

Положим

$$P_2 = (\bigcup_{n \in \mathbf{N}} P_2(n)) \cup \mathbf{E} .$$

Множество булевых функций $S\,(S \subseteq P_2)$ называется *полным*, если

$$[S] = P_2 ,$$

где $[\ ]$ - *операция замыкания по суперпозиции*. Минимальные по отношению включения множеств '$\subset$' полные множества булевых функций принято называть *базисами*.

Отметим, что поиск базисов для булевых функций является не только модельной задачей дискретной математики, но также играет существенную роль в процессе решения широкого класса проблем анализа и синтеза комбинационных схем.

Определим на множестве $\mathbf{E}^n$ $(n \in \mathbf{N})$ отношение частичного порядка $\leq_{\mathbf{E}^n}$ следующим образом: если $\mathbf{x}_1 = (x_1^{(1)}, \ldots, x_n^{(1)})$ и $\mathbf{x}_2 = (x_1^{(2)}, \ldots, x_n^{(2)})$, то

$$\mathbf{x}_1 \leq_{\mathbf{E}^n} \mathbf{x}_2 \Leftrightarrow (\forall i = 1, \ldots, n)(x_i^{(1)} \leq x_i^{(2)}).$$

Булева функция $f \in P_2(n)$ $(n \in \mathbf{N})$ называется:

1) *сохраняющей константу* 0, если

$$f(0, \ldots, 0) = 0;$$

2) *сохраняющей константу* 1, если

$$f(1, \ldots, 1) = 1;$$

3) *самодвойственной*, если

$$\overline{f(\overline{x}_1, \ldots, \overline{x}_n)} = f(x_1, \ldots, x_n);$$

4) *монотонной*, если

$$\mathbf{x}_1 \leq_{\mathbf{E}^n} \mathbf{x}_2 \Rightarrow f(\mathbf{x}_1) \leq f(\mathbf{x}_2) \ (\mathbf{x}_1, \mathbf{x}_2 \in \mathbf{E}^n);$$

5) *линейной*, если

$$f(x_1, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n,$$

где $\oplus$ - *сумма по модулю два*, а $a_0, a_1, \ldots, a_n \in \mathbf{E}$.

Известно, что (см., напр., [18]) множество булевых функций S является полным тогда и только тогда, когда S содержит функцию, не сохраняющую константу 0, функцию, не сохраняющую константу 1, функцию, не являющуюся самодвойственной, функцию, не являющуюся монотонной и функцию, не являющуюся линейной.

Обозначим через $\mathbf{T}_0$, $\mathbf{T}_1$, $\mathbf{S}$, $\mathbf{M}$ и $\mathbf{L}$ множество всех, соответственно, сохраняющих константу 0, сохраняющих константу 1, самодвойственных, монотонных и линейных функций, принадлежащих множеству $P_2(n)$ и положим

$$\overline{\mathbf{T}_0} = P_2 \setminus \mathbf{T}_0, \qquad \overline{\mathbf{T}_1} = P_2 \setminus \mathbf{T}_1, \qquad \overline{\mathbf{S}} = P_2 \setminus \mathbf{S},$$

$$\overline{\mathbf{M}} = P_2 \setminus \mathbf{M}, \qquad \overline{\mathbf{L}} = P_2 \setminus \mathbf{L}.$$

Пусть

$$\boldsymbol{A} = \{\overline{\mathbf{T}_0}, \overline{\mathbf{T}_1}, \overline{\mathbf{S}}, \overline{\mathbf{M}}, \overline{\mathbf{L}}\}.$$

Тогда множество всех множеств представителей семейства множеств $\boldsymbol{A}$ совпадает с множеством всех полных множеств булевых функций. В то же время, множество $\boldsymbol{V_A}$ всех неприводимых множеств представителей семейства множеств $\boldsymbol{A}$ совпадает с множеством всех базисов.

Отметим, что если зафиксировать значение числа n, то множество $\boldsymbol{V_A}$ совпадает с множеством всех базисов, состоящих только из булевых функций от n переменных.

Пример 2.4 (*Поиск неприводимых диагностических тестов для одноуровневых комбинационных схем*).

Предположим, что зафиксирован некоторый базис. Для каждого элемента базиса рассмотрим все те константные неисправности, которые изменяют его функционирование. Разобьем эти неисправности на классы эквивалентных между собой неисправностей. В дальнейшем под *неисправностями* будем понимать классы эквивалентных неисправностей. Для каждого элемента базиса построим множество всех не избыточных диагностических тестов.

Пусть K - одноуровневая комбинационная схема, построенная из элементов

$$v_1, \ldots, v_m$$

рассматриваемого базиса. Обозначим через $C(v_i)$ $(i = 1, \ldots, m)$ множество всех не избыточных диагностических тестов для элемента v_i. Выберем из каждого множества $C(v_i)$ по одному элементу. Иными словами, выберем по одному не избыточному диагностическому тесту

$$p_i = \{\mathbf{x}_1^{(i)}, \ldots, \mathbf{x}_{l_i}^{(i)}\}$$

для каждого элемента v_i. Для каждого теста p_i $(i = 1, \ldots, m)$ следующим образом построим семейство

$$\{\alpha_1^{(i)}, \ldots, \alpha_{l_i}^{(i)}\}$$

подмножеств множества всех входных наборов комбинационной схемы K: множество $\alpha_j^{(i)}$ $(j = 1, \ldots, l_i\}$ состоит из всех тех входных наборов, компоненты которых, питающие входы элемента v_i, образуют такую комбинацию, что на элемент v_i подается входной набор $\mathbf{x}_j^{(i)}$. Положим

$$\boldsymbol{A} = \{\alpha_j^{(i)} \mid j = 1, \ldots, l_i; i = 1, \ldots, m\}.$$

Покажем, что элементами множества $\boldsymbol{V_A}$ всех неприводимых множеств представителей семейства множеств $\boldsymbol{A}$ являются не избыточные диагностические тесты для комбинационной схемы K.

Множеству $V \in \boldsymbol{V_A}$ принадлежат элементы из каждого множества $\alpha_j^{(i)} \in \boldsymbol{A}$. Следовательно, множество V обеспечивает подачу на каждый элемент v_i каждого входного набора, принадлежащего тесту p_i. Поэтому, V - диагностический тест для комбинационной схемы K. Так как $V \in \boldsymbol{V_A}$, то любое собственное подмножество V_1 множества V не является множеством представителей семейства множеств $\boldsymbol{A}$. Это означает, что множество V_1 не обеспечивает подачи диагностического теста p_i хотя бы для одного элемента v_i. Следовательно, V - не избыточный диагностический тест для комбинационной схемы K.

Для поиска множества всех не избыточных диагностических тестов для комбинационной схемы K необходимо выполнить указанное построение для всевозможных выборов диагностических тестов из множеств $C(v_i)$ $(i=1,\dots,m)$. Это означает, что задача поиска множества $\boldsymbol{V}_{\boldsymbol{A}}$ решается

$$\prod_{i=1}^{m} |C(v_i)|$$

раз. То, что при этом строится множество всех не избыточных диагностических тестов для комбинационной схемы K вытекает из следующего факта. Любой не избыточный диагностический тест для комбинационной схемы K обеспечивает подачу на каждый элемент v_i $(i=1,\dots,m)$ некоторого диагностического для этого элемента теста. Диагностический для элемента тест, после удаления из него *лишних* наборов, превращается в не избыточный диагностический для этого элемента тест. Следовательно, рассматриваемый тест принадлежит множеству $\boldsymbol{V}_{\boldsymbol{A}}$ семейства множеств $\boldsymbol{A}$, построенного из указанных не избыточных диагностических для элементов тестов.

Рассмотрим теперь решение проблемы 2.3.

Исследуем вначале структуру множества $\boldsymbol{V}_{\boldsymbol{A}}$.

Очевидно, что $\boldsymbol{V}_{\boldsymbol{A}} = \varnothing$, если существует такое $i \in I$, что $\alpha_i = \varnothing$. Кроме того,

$$\boldsymbol{V}_{\boldsymbol{A}} = \boldsymbol{V}_{\boldsymbol{A} \setminus \boldsymbol{A}'} ,$$

где

$$\boldsymbol{A}' = \{\alpha_i \in \boldsymbol{A} \,|\, \alpha_i = \alpha_{i_0}, i \neq i_0\} \quad (i_0 \in I).$$

Поэтому всюду в дальнейшем будем считать, что все элементы семейства множеств $\boldsymbol{A}$ суть не равные друг другу непустые подмножества множества U.

Теорема 2.12. Для всех $\alpha_{i_0} \in \boldsymbol{A}$ справедливо равенство

$$\boldsymbol{V}_{\boldsymbol{A}} = \boldsymbol{V}_{\boldsymbol{A} \setminus \boldsymbol{A}(i_0)},$$

где

$$\boldsymbol{A}(i_0) = \{\alpha_i \in \boldsymbol{A} \,|\, \alpha_i \supset \alpha_{i_0}\}.$$

Доказательство. Покажем, что

$$\boldsymbol{V}_{\boldsymbol{A} \setminus \boldsymbol{A}(i_0)} \subseteq \boldsymbol{V}_{\boldsymbol{A}}.$$

Пусть $V \in \boldsymbol{V}_{\boldsymbol{A} \setminus \boldsymbol{A}(i_0)}$. Тогда $V \cap \alpha_i \neq \varnothing$ для всех $\alpha_i \in \boldsymbol{A} \setminus \boldsymbol{A}(i_0)$. Так как $\alpha_{i_0} \in \boldsymbol{A} \setminus \boldsymbol{A}(i_0)$, то $V \cap \alpha_{i_0} \neq \varnothing$. Включение $\alpha_i \supset \alpha_0$ справедливо для всех $\alpha_i \in \boldsymbol{A}(i_0)$. Так как $V \cap \alpha_{i_0} \neq \varnothing$ и $\alpha_i \supset \alpha_0$ $(\alpha_i \in \boldsymbol{A}(i_0))$, то $V \cap \alpha_i \neq \varnothing$ для всех $\alpha_i \in \boldsymbol{A}(i_0)$. Из соотношений

$$V \cap \alpha_i \neq \varnothing \quad (\alpha_i \in \boldsymbol{A} \setminus \boldsymbol{A}(i_0))$$

и

$$V \cap \alpha_i \neq \varnothing \quad (\alpha_i \in \boldsymbol{A}(i_0))$$

вытекает, что

$$V \cap \alpha_i \neq \varnothing$$

для всех $\alpha_i \in \boldsymbol{A}$, т.е V - множество представителей семейства множеств $\boldsymbol{A}$. Так как $V \in \boldsymbol{V}_{\boldsymbol{A} \setminus \boldsymbol{A}(i_0)}$, то для любого элемента $v \in V$ существует такое $\alpha_i \in \boldsymbol{A} \setminus \boldsymbol{A}(i_0)$ (и, следовательно $\alpha_i \in \boldsymbol{A}$), что

$$(V \setminus \{v\}) \cap \alpha_i = \varnothing.$$

Поэтому, $V \in \boldsymbol{V}_{\boldsymbol{A}}$. Итак, показано, что $\boldsymbol{V}_{\boldsymbol{A} \setminus \boldsymbol{A}(i_0)} \subseteq \boldsymbol{V}_{\boldsymbol{A}}$.

Предположим, что

$$\boldsymbol{V}_{\boldsymbol{A}\setminus\boldsymbol{A}(i_0)} \subset \boldsymbol{V}_{\boldsymbol{A}}.$$

Тогда существует такое $V \in \boldsymbol{V}_{\boldsymbol{A}}$, что $V \notin \boldsymbol{V}_{\boldsymbol{A}\setminus\boldsymbol{A}(i_0)}$. Так как V - множество представителей семейства множеств $\boldsymbol{A} \setminus \boldsymbol{A}(i_0)$ и $V \notin \boldsymbol{V}_{\boldsymbol{A}\setminus\boldsymbol{A}(i_0)}$, то существует такой элемент $v \in V$, что

$$(V \setminus \{v\}) \cap \alpha_i \neq \varnothing$$

для всех $\alpha_i \in \boldsymbol{A} \setminus \boldsymbol{A}(i_0)$. В частности,

$$(V \setminus \{v\}) \cap \alpha_{i_0} \neq \varnothing.$$

А так как $\alpha_i \supset \alpha_0$ для всех $\alpha_i \in \boldsymbol{A}(i_0)$, то

$$(V \setminus \{v\}) \cap \alpha_i \neq \varnothing$$

для всех $\alpha_i \in \boldsymbol{A}(i_0)$. Из соотношений

$$(V \setminus \{v\}) \cap \alpha_i \neq \varnothing \quad (\alpha_i \in \boldsymbol{A} \setminus \boldsymbol{A}(i_0))$$

и

$$(V \setminus \{v\}) \cap \alpha_i \neq \varnothing \quad (\alpha_i \in \boldsymbol{A}(i_0))$$

вытекает, что

$$(V \setminus \{v\}) \cap \alpha_i \neq \varnothing$$

для всех $\alpha_i \in \boldsymbol{A}$, т.е $V \setminus \{v\}$ - множество представителей семейства множеств $\boldsymbol{A}$. Это противоречит тому, что $V \in \boldsymbol{V}_{\boldsymbol{A}}$. Следовательно, предположение о том, что $\boldsymbol{V}_{\boldsymbol{A}\setminus\boldsymbol{A}(i_0)} \subset \boldsymbol{V}_{\boldsymbol{A}}$ - ложное.

Так как $\boldsymbol{V}_{\boldsymbol{A}\setminus\boldsymbol{A}(i_0)} \subseteq \boldsymbol{V}_{\boldsymbol{A}}$ и $\boldsymbol{V}_{\boldsymbol{A}\setminus\boldsymbol{A}(i_0)} \not\subset \boldsymbol{V}_{\boldsymbol{A}}$, то $\boldsymbol{V}_{\boldsymbol{A}} = \boldsymbol{V}_{\boldsymbol{A}\setminus\boldsymbol{A}(i_0)}$, что и требовалось доказать.

Теорема доказана.

Следствие 2.2. Если $\boldsymbol{A} = \{\alpha_i\}_{i\in I}$ - убывающая цепь относительно включения, то множество $\boldsymbol{V}_{\boldsymbol{A}}$ всех неприводимых множеств представителей семейства множеств $\boldsymbol{A}$ состоит из всех одноэлементных подмножеств множества $\bigcap\limits_{i\in I}\alpha_i$, т.е.

$$\boldsymbol{V}_{\boldsymbol{A}} = \{\{v\} \mid v \in \bigcap_{i\in I}\alpha_i\}.$$

Доказательство. Пусть элементы семейства множеств $\boldsymbol{A} = \{\alpha_i\}_{i\in I}$ образуют убывающую цепь относительно включения. Ясно, что любое одноэлементное подмножество множества $\bigcap\limits_{i\in I}\alpha_i$ является неприводимым множеством представителей семейства множеств $\boldsymbol{A}$, т.е.

$$\{\{v\} \mid v \in \bigcap_{i\in I}\alpha_i\} \subseteq \boldsymbol{V}_{\boldsymbol{A}}.$$

Предположим, что

$$\{\{v\} \mid v \in \bigcap_{i\in I}\alpha_i\} \subset \boldsymbol{V}_{\boldsymbol{A}},$$

т.е., что существует неприводимое множество представителей $V \in \boldsymbol{V}_{\boldsymbol{A}}$, содержащее элемент $v \notin \bigcap\limits_{i\in I}\alpha_i$. Тогда существует такое множество $\alpha_{i_0} \in \boldsymbol{A}$, что $v \notin \alpha_{i_0}$. Следовательно,

$$(V \setminus \{v\}) \cap \alpha_{i_0} = V \cap \alpha_{i_0} \neq \varnothing.$$

Положим

$$\boldsymbol{A}(i_0) = \{\alpha_i \in \boldsymbol{A} \mid \alpha_i \subseteq \alpha_{i_0}\}.$$

Так как $v \notin \alpha_i$ для всех для всех $\alpha_i \in \boldsymbol{A}(i_0)$, то множество $V \setminus \{v\}$ является множеством представителей семейства множеств $\boldsymbol{A}(i_0)$. Следовательно, $V \notin \boldsymbol{V}_{\boldsymbol{A}(i_0)}$. Из соотношений $V \in \boldsymbol{V}_{\boldsymbol{A}}$ и $V \notin \boldsymbol{V}_{\boldsymbol{A}(i_0)}$ вытекает, что

$$\boldsymbol{V}_{\boldsymbol{A}} \neq \boldsymbol{V}_{\boldsymbol{A}(i_0)}.$$

А так как

$$\boldsymbol{A}(i_0) = \boldsymbol{A} \setminus \{\alpha_i \in \boldsymbol{A} \mid \alpha_i \supset \alpha_{i_0}\},$$

то (см. теорему 2.12)

$$\boldsymbol{V}_{\boldsymbol{A}} = \boldsymbol{V}_{\boldsymbol{A}(i_0)}.$$

Полученное противоречие показывает, что предположение о том, что $\{\{v\} \mid v \in \bigcap_{i\in I}\alpha_i\} \subset \boldsymbol{V}_{\boldsymbol{A}}$ - ложное.

Так как $\{\{v\} \mid v \in \bigcap_{i\in I}\alpha_i\} \subseteq \boldsymbol{V}_{\boldsymbol{A}}$ и $\{\{v\} \mid v \in \bigcap_{i\in I}\alpha_i\} \not\subset \boldsymbol{V}_{\boldsymbol{A}}$, то $\{\{v\} \mid v \in \bigcap_{i\in I}\alpha_i\} = \boldsymbol{V}_{\boldsymbol{A}}$, что и требовалось доказать.

Следствие доказано.

Из теоремы 2.12 и следствия 2.2 вытекает, что множество всех неприводимых множеств представителей не изменится, если из семейства множеств $\boldsymbol{A}$ удалить все не являющиеся минимальными по включению множества. Поэтому, в дальнейшем будем считать, что выполнено следующее условие

Условие 2.38. Семейство множеств $\boldsymbol{A}$ состоит из непустых попарно не сравнимых по отношению включения '$\subseteq$' подмножеств заданного множества U.

Определим бинарное отношение

$$\rho \subseteq \boldsymbol{A} \times \boldsymbol{A}$$

следующим образом: $\alpha_i \rho \alpha_j$ $(\alpha_i, \alpha_j \in \boldsymbol{A})$ тогда и только тогда, когда существует такая конечная последовательность

$$\alpha_i = \alpha_{h_0}, \alpha_{h_1}, \ldots, \alpha_{h_n} = \alpha_j,$$

элементов семейства множеств $\boldsymbol{A}$, что

$$\alpha_{h_r} \cap \alpha_{h_{r+1}} \neq \varnothing$$

для всех $r = 0,1,\ldots,n-1$.

Очевидно, что ρ - *отношение эквивалентности* на семействе множеств $\boldsymbol{A}$. Следовательно, отношение ρ определяет разбиение

$$\pi_\rho = \{\boldsymbol{A}_j \mid j \in J\}$$

семейства множеств $\boldsymbol{A}$ на классы эквивалентных друг другу элементов. Значение разбиения π_ρ в процессе решения проблемы 2.3 определяется следующей теоремой.

Теорема 2.13. Если $V_j \in \boldsymbol{V}_{\boldsymbol{A}_j}$ $(j \in J)$, то $\bigcup_{j\in J} V_j \in \boldsymbol{V}_{\boldsymbol{A}}$. Обратно, любое неприводимое множество представителей $V \in \boldsymbol{V}_{\boldsymbol{A}}$ единственным образом может быть представлено в виде $V = \bigcup_{j\in J} V_j$, где $V_j \in \boldsymbol{V}_{\boldsymbol{A}_j}$ $(j \in J)$.

Доказательство. Пусть $V_j \in \boldsymbol{V}_{\boldsymbol{A}_j}$ $(j \in J)$. Тогда $\bigcup_{j \in J} V_j$ - множество представителей семейства множеств $\boldsymbol{A}$. Предположим, что $\bigcup_{j \in J} V_j \notin \boldsymbol{V}_{\boldsymbol{A}}$. Тогда существует такой элемент $v \in \bigcup_{j \in J} V_j$, что $(\bigcup_{j \in J} V_j) \setminus \{v\}$ - также является множеством представителей семейства множеств $\boldsymbol{A}$. Так как элементы семейства множеств $\boldsymbol{A}$, принадлежащие различным блокам разбиения π_ρ, попарно не пересекаются, то и неприводимые множества представителей для различных классов разбиения π_ρ попарно не пересекаются. Поэтому существует такое единственное $j_0 \in J$, что $v \in V_{j_0}$. Следовательно,

$$(\bigcup_{j \in J} V_j) \setminus \{v\} = (\bigcup_{j \in J \setminus \{j_0\}} V_j) \cup (V_{j_0} \setminus \{v\}),$$

откуда вытекает, что $V_{j_0} \setminus \{v\}$ - множество представителей для блока $\boldsymbol{A}_{j_0}$ разбиения π_ρ. Это означает, что $V_{j_0} \notin \boldsymbol{V}_{\boldsymbol{A}_{j_0}}$. Полученное противоречие показывает, что предположение о том, что $\bigcup_{j \in J} V_j \notin \boldsymbol{V}_{\boldsymbol{A}}$ - ложное. Следовательно, $\bigcup_{j \in J} V_j \in \boldsymbol{V}_{\boldsymbol{A}}$, что и требовалось показать.

Пусть $V \in \boldsymbol{V}_{\boldsymbol{A}}$. Положим

$$V_j = \bigcup_{\alpha \in \boldsymbol{A}_j} (V \cap \alpha) \ (j \in J).$$

Ясно, что каждое множество V_j $(j \in J)$ является множеством представителей семейства множеств $\boldsymbol{A}_j$, причем множества V_j $(j \in J)$ попарно не пересекаются. Предположим, что существует такое $j_0 \in J$, что $V_{j_0} \notin \boldsymbol{V}_{\boldsymbol{A}_{j_0}}$. Следовательно, существует такой элемент $v \in V_{j_0}$, что $V_{j_0} \setminus \{v\}$ - множество представителей для класса $\boldsymbol{A}_{j_0}$ разбиения π_ρ. Но тогда множество

$$(V_{j_0} \setminus \{v\}) \cup (\bigcup_{j \in J \setminus \{j_0\}} V_j) = (\bigcup_{j \in J} V_j) \setminus \{v\}$$

является множеством представителей семейства множеств $\boldsymbol{A}$. Это означает, что $V \notin \boldsymbol{V}_{\boldsymbol{A}}$. Полученное противоречие показывает, что предположение о том, что существует такое $j_0 \in J$, что $V_{j_0} \notin \boldsymbol{V}_{\boldsymbol{A}_{j_0}}$ - ложное. Следовательно, $V_j \in \boldsymbol{V}_{\boldsymbol{A}_j}$ $(j \in J)$. Единственность представления множества $V \in \boldsymbol{V}_{\boldsymbol{A}}$ в виде $V = \bigcup_{j \in J} V_j$, где $V_j \in \boldsymbol{V}_{\boldsymbol{A}_j}$ $(j \in J)$ непосредственно следует из того, что множества $V_j \in \boldsymbol{V}_{\boldsymbol{A}_j}$ $(j \in J)$ попарно не пересекаются, что и требовалось показать.

Теорема доказана.

Таким образом, для построения множества $\boldsymbol{V}_{\boldsymbol{A}}$ достаточно построить каждое из множеств $\boldsymbol{V}_{\boldsymbol{A}_j}$ $(j \in J)$ в отдельности, а затем построить всевозможные множества вида $\bigcup_{j \in J} V_j$, где $V_j \in \boldsymbol{V}_{\boldsymbol{A}_j}$ $(j \in J)$. При этом, представление множеств $V \in \boldsymbol{V}_{\boldsymbol{A}}$ в виде $V = \bigcup_{j \in J} V_j$, где $V_j \in \boldsymbol{V}_{\boldsymbol{A}_j}$ $(j \in J)$, дает возможность выделить все те особенности строения множества $\boldsymbol{V}_{\boldsymbol{A}}$, которые определяются только строением множеств $\boldsymbol{V}_{\boldsymbol{A}_j}$ $(j \in J)$.

Отметим значение теоремы 2.13 для важного специального случая, когда $\boldsymbol{A}$ - конечное семейство конечных множеств.

Во-первых, независимое построение множеств $\boldsymbol{V}_{\boldsymbol{A}_1}, \ldots, \boldsymbol{V}_{\boldsymbol{A}_n}$ (где $\boldsymbol{A}_1, \ldots, \boldsymbol{A}_n$ - блоки разбиения π_ρ) дает возможность существенно упростить решение проблемы 2.3. Действительно, перебор, осуществляемый на всем семействе множеств $\boldsymbol{A}$, заменяется *локальными переборами*, осуществляемыми *независимо* на каждом из блоков $\boldsymbol{A}_1, \ldots, \boldsymbol{A}_n$ разбиения π_ρ.

Во-вторых, установлено, что возможно организовать параллельные вычисления в процессе решения проблемы 2.3 и показано, как это можно сделать.

В третьих, предложен способ компактного хранения множества $\boldsymbol{V}_{\boldsymbol{A}}$ в неявном виде. Покажем, что хранение набора множеств $\boldsymbol{V}_{\boldsymbol{A}_1}, \ldots, \boldsymbol{V}_{\boldsymbol{A}_n}$ требует меньший объем памяти, чем хранение множества $\boldsymbol{V}_{\boldsymbol{A}}$. Действительно, примем мощность множества в качестве объема памяти, необходимой для его хранения. Тогда хранение набора множеств $\boldsymbol{V}_{\boldsymbol{A}_1}, \ldots, \boldsymbol{V}_{\boldsymbol{A}_n}$ требует объем памяти, равный

$$\sum_{i=1}^{n} | \boldsymbol{V}_{\boldsymbol{A}_i} |.$$

Выраженный в этих же терминах объем памяти, необходимой для хранения множества $\boldsymbol{V}_{\boldsymbol{A}}$, равен

$$\prod_{i=1}^{n} | \boldsymbol{V}_{\boldsymbol{A}_i} |.$$

Рассмотрим теперь отдельно блок $\boldsymbol{A}_j$ $(j \in J)$ разбиения π_ρ. Положим

$$U_j = \bigcup_{\alpha \in \boldsymbol{A}_j} \alpha$$

и определим отображение

$$\varphi_j : U_j \to \mathbf{B}(\boldsymbol{A}_j)$$

следующим образом

$$\varphi_j(v) = \{\alpha \in \boldsymbol{A}_j \mid v \in \alpha\} \ (v \in U_j).$$

Ядро

$$\ker \varphi_j = \varphi_j \circ \varphi_j^{-1}$$

отображения φ_j является отношением эквивалентности на множестве U_j. Обозначим через $[v]_{\ker \varphi_j}$ $(v \in U_j)$ класс эквивалентности, содержащий элемент v. Так как

$$[v_1]_{\ker \varphi_j} = [v_2]_{\ker \varphi_j} \ (v_1, v_2 \in U_j)$$

тогда и только тогда, когда элементы v_1 и v_2 принадлежат одним и тем же элементам семейства множеств $\boldsymbol{A}_j$, то для любого класса эквивалентности $[v]_{\ker \varphi_j}$ и любого множества $\alpha \in \boldsymbol{A}_j$ либо

$$[v]_{\ker \varphi_j} \subseteq \alpha,$$

либо

$$[v]_{\ker \varphi_j} \cap \alpha = \varnothing.$$

Следовательно, отношение эквивалентности $\ker\varphi_j$ следующим образом характеризует неприводимые множества представителей семейства множеств $\boldsymbol{A}_j$.

Утверждение 2.10. Любое множество $V \in \boldsymbol{V}_{\boldsymbol{A}_j}$ содержит не более одного элемента из любого класса эквивалентности $[v]_{\ker\varphi_j}$ $(v \in U_j)$.

Утверждение 2.11. При замене любого элемента $v \in V$ $(V \in \boldsymbol{V}_{\boldsymbol{A}_j})$ любым элементом $v_1 \in [v]_{\ker\varphi_j}$ получается множество $V_1 \in \boldsymbol{V}_{\boldsymbol{A}_j}$.

Из утверждений 2.10 и 2.11 вытекает, что построение множества $\boldsymbol{V}_{\boldsymbol{A}_j}$ естественно сводится к построению его *гомоморфного образа*, определяемого эквивалентностью $\ker\varphi_j$. Действительно, пусть

$$\mathsf{U}_j = U_j / \ker\varphi_j,$$

а отображение

$$nat_j : U_j \to \mathsf{U}_j$$

определено равенством

$$nat_j(v) = [v]_{\ker\varphi_j} \quad (v \in U_j).$$

Положим

$$\boldsymbol{A}_j / \ker\varphi_j = \{\alpha / (\ker\varphi_j \cap \alpha^2) \mid \alpha \in \boldsymbol{A}_j\}$$

и

$$\boldsymbol{V}_{\boldsymbol{A}_j} / \ker\varphi_j = \{nat_j(V) \mid V \in \boldsymbol{V}_{\boldsymbol{A}_j}\},$$

где

$$nat_j(V) = \{nat_j(v) \mid v \in V\}.$$

Из утверждений 2.10 и 2.11 непосредственно вытекает, что справедливо равенство

$$\boldsymbol{V}_{\boldsymbol{A}_j / \ker\varphi_j} = \boldsymbol{V}_{\boldsymbol{A}_j} / \ker\varphi_j. \tag{2.36}$$

Значение равенства (2.36) состоит в следующем.

Построим множество всех неприводимых множеств представителей $\boldsymbol{V}_{\boldsymbol{A}_j / \ker\varphi_j}$ семейства множеств $\boldsymbol{A}_j / \ker\varphi_j$. Выберем любое множество $\mathsf{V} \in \boldsymbol{V}_{\boldsymbol{A}_j / \ker\varphi_j}$. Заменим каждый элемент $\mathsf{v} \in \mathsf{V}$ любым элементом $v \in (nat_j)^{-1}(\mathsf{v})$. Получим неприводимое множество представителей семейства множеств $\boldsymbol{A}_j$. Произведя все такие замены в каждом множестве $\mathsf{V} \in \boldsymbol{V}_{\boldsymbol{A}_j / \ker\varphi_j}$, построим множество $\boldsymbol{V}_{\boldsymbol{A}_j}$.

Так как строение семейства множеств $\boldsymbol{A}_j / \ker\varphi_j$ проще строения семейства множеств $\boldsymbol{A}_j$, то переход к семействам множеств $\boldsymbol{A}_j / \ker\varphi_j$ $(j \in J)$ дает возможность произвести дальнейшее упрощение построения множества $\boldsymbol{V}_{\boldsymbol{A}}$. А так как

$$|\boldsymbol{V}_{\boldsymbol{A}_j / \ker\varphi_j}| \le |\boldsymbol{V}_{\boldsymbol{A}_j}| \ (j \in J),$$

то представление множества $\boldsymbol{V}_{\boldsymbol{A}}$ набором множеств $\boldsymbol{V}_{\boldsymbol{A}_j/\ker\varphi_j}$ $(j\in J)$ более экономно (с точки зрения затрат памяти, необходимой для хранения), чем представление набором множеств $\boldsymbol{V}_{\boldsymbol{A}_j}$ $(j\in J)$.

Рассмотрим более подробно строение множества $\boldsymbol{V}_{\boldsymbol{A}_j/\ker\varphi_j}$ $(j\in J)$. Определим отображение

$$\Phi_j : U_j \to \mathbf{B}(\boldsymbol{A}_j/\ker\varphi_j)$$

с помощью равенства

$$\Phi_j([v]_{\ker\varphi_j}) = \{\alpha\in \boldsymbol{A}_j/\ker\varphi_j \mid [v]_{\ker\varphi_j}\in\alpha\}.$$

Теорема 2.14. Если V - множество представителей семейства множеств $\boldsymbol{A}_j/\ker\varphi_j$, то $V\in \boldsymbol{V}_{\boldsymbol{A}_j/\ker\varphi_j}$ тогда и только тогда, когда ни один элемент $[v]_{\ker\varphi_j}\in V$ не удовлетворяет включению

$$\Phi_j([v]_{\ker\varphi_j}) \subseteq \bigcup_{[v_1]_{\ker\varphi_j}\in V\setminus\{[v]_{\ker\varphi_j}\}} \Phi_j([v_1]_{\ker\varphi_j}). \tag{2.37}$$

Доказательство. Пусть $V\in \boldsymbol{V}_{\boldsymbol{A}_j/\ker\varphi_j}$. Тогда для каждого элемента $[v]_{\ker\varphi_j}\in V$ существует такое множество $\alpha/(\ker\varphi_j\cap\alpha^2)\in \boldsymbol{A}_j/\ker\varphi_j$ $(\alpha\in \boldsymbol{A}_j)$, что

$$(V\setminus\{[v]_{\ker\varphi_j}\})\cap(\alpha/(\ker\varphi_j\cap\alpha^2))=\varnothing.$$

Следовательно,

$$[v]_{\ker\varphi_j}\in\alpha/(\ker\varphi_j\cap\alpha^2)$$

и

$$[v_1]_{\ker\varphi_j}\notin\alpha/(\ker\varphi_j\cap\alpha^2)$$

для всех $[v_1]_{\ker\varphi_j}\in V\setminus\{[v]_{\ker\varphi_j}\}$, т.е.

$$\alpha/(\ker\varphi_j\cap\alpha^2)\in\Phi_j([v]_{\ker\varphi_j})\setminus \bigcup_{[v_1]_{\ker\varphi_j}\in V\setminus\{[v]_{\ker\varphi_j}\}} \Phi_j([v_1]_{\ker\varphi_j}).$$

Следовательно, включение (2.37) не выполняется ни для одного элемента $[v]_{\ker\varphi_j}\in V$, что и требовалось показать.

Пусть множество V представителей семейства множеств $\boldsymbol{A}_j/\ker\varphi_j$ не содержит элементов, удовлетворяющих включению (2.37). Тогда для каждого элемента $[v]_{\ker\varphi_j}\in V$ существует такое множество $\alpha/(\ker\varphi_j\cap\alpha^2)\in\Phi_j([v]_{\ker\varphi_j})$, что

$$\alpha/(\ker\varphi_j\cap\alpha^2)\notin \bigcup_{[v_1]_{\ker\varphi_j}\in V\setminus\{[v]_{\ker\varphi_j}\}} \Phi_j([v_1]_{\ker\varphi_j}),$$

т.е.

$$[v]_{\ker\varphi_j}\in\alpha/(\ker\varphi_j\cap\alpha^2)$$

и

$$[v_1]_{\ker\varphi_j}\notin\alpha/(\ker\varphi_j\cap\alpha^2)$$

для всех $[v_1]_{\ker\varphi_j}\in V\setminus\{[v]_{\ker\varphi_j}\}$. Поэтому,

$$(V\setminus\{[v]_{\ker\varphi_i})\cap(\alpha/(\ker\varphi_i\cap\alpha^2)=\varnothing,$$

т.е. множество $V \setminus \{[v]_{\ker\varphi_j}\}$ не является множеством представителей семейства множеств $\boldsymbol{A}_j / \ker\varphi_j$. Следовательно, $V \in \boldsymbol{V}_{\boldsymbol{A}_j / \ker\varphi_j}$, что и требовалось показать.

Теорема доказана.

Распространим отображение $\Phi_j : U_j \to \mathbf{B}(\boldsymbol{A}_j / \ker\varphi_j)$ на множество $\mathbf{B}(U_j)$ с помощью равенства

$$\Phi_j(V) = \bigcup_{[v]_{\ker\varphi_j} \in V} \Phi_j([v]_{\ker\varphi_j}).$$

Из определения неприводимого множества представителей семейства множеств и теоремы 2.14 вытекает, что $V \in \boldsymbol{V}_{\boldsymbol{A}_j / \ker\varphi_j}$ тогда и только тогда, когда выполнены следующие два условия

Условие 2.39. $\Phi_j(V) = \boldsymbol{A}_j / \ker\varphi_j$.

Условие 2.40. Отображение Φ_j - строго монотонное на множестве $\mathbf{B}(V)$, т.е.

$$(\forall V_1, V_2 \subseteq V)(V_1 \subset V_2 \Rightarrow \Phi_j(V_1) \subset \Phi_j(V_1)).$$

Условия 2.39 и 2.40 дают возможность в процессе построения множества $\boldsymbol{V}_{\boldsymbol{A}_j / \ker\varphi_j}$ исключить все те элементы множества $\mathbf{B}(U_j)$, которые заведомо не являются неприводимыми множествами представителей семейства множеств $\boldsymbol{A}_j / \ker\varphi_j$. Действительно, определим следующие два правила удаления элементов множества $\mathbf{B}(U_j)$

Правило 2.13. Множество V $(V \in \mathbf{B}(U_j))$ удаляется, если существует такое собственное подмножество V_1 множества V, что $\Phi_j(V_1) = \Phi(V)$.

Правило 2.14. Если удаляется множество V $(V \in \mathbf{B}(U_j))$, то удаляются и все такие множества V' $(V' \in \mathbf{B}(U_j))$, что $V' \supset V$.

Обозначим через $\mathbf{B}'(U_j)$ множество всех элементов множества $\mathbf{B}(U_j)$, оставшихся в результате удаления в соответствии с правилами 2.13 и 2.14. Из условий 2.39 и 2.40 вытекает, что множество $\boldsymbol{V}_{\boldsymbol{A}_j / \ker\varphi_j}$ совпадает с множеством всех максимальных по отношению включения элементов множества $\mathbf{B}'(U_j)$.

Таким образом, получено исчерпывающее решение проблемы 2.3.

В заключение отметим следующее. Если $\boldsymbol{A}_j / \ker\varphi_j$ - конечное семейство конечных множеств, то множество $\boldsymbol{V}_{\boldsymbol{A}_j / \ker\varphi_j}$ может быть построено последовательным, уровень за уровнем, построением структуры $\mathbf{B}'(U_j)$ с применением на каждом шаге правил 2.13 и 2.14 удаления элементов множества $\mathbf{B}(U_j)$. Очевидно, что не представляет особого труда построить детализацию алгоритма 2.1, предназначенную для построения множества $\mathbf{B}'(U_j)$.

2.7. Выводы.

В разделе 2 впервые систематически изложена разработанная автором общая теория поиска на частично упорядоченных структурах. Основные результаты состоят в следующем.

1. Впервые разработана метатеория поиска множеств безусловных решений, определяемых характеристической функцией. Созданы три общие схемы поиска безусловных решений на основе выделения в дереве поиска множеств бесперспективных, финальных и порождающих вершин.

2. Определены и исследованы базовые математические модели для поиска безусловных и адаптивных решений, соответственно, M-источник и AM-источник.

3. Впервые исследованы общие соотношения между моделями, предназначенными для поиска адаптивных и безусловных решений.

4. Получено исчерпывающее решение проблем 1.4-1.8.

5. Разработана общая схема двустороннего поиска минимальных решений для M-источников за счет параллельных действий с прямым и обратным M-источниками.

6. Получено исчерпывающее решение фундаментальной проблемы дискретной математики - поиска всех неприводимых множеств представителей заданного семейства множеств.

Таким образом, в разделе 2 впервые разработана законченная общая теория поиска, включающая в себя в качестве специальных случаев классические теоретико-множественный и основанный на оценивании подходы. Исследования в двух следующих разделах во многом основаны на развитии и детализации моделей и методов настоящего раздела.

Основные результаты раздела 2 опубликованы в работах [71,81,85,86,130,131].

3. АНАЛИЗ КОНЕЧНЫХ АВТОМАТОВ

Настоящий раздел посвящен разработке комбинаторно-алгебраических основ анализа конечных автоматов - фундаментального класса дискретных систем как в теоретическом, так и прикладном смысле. Равное внимание уделяется каждому из трех основных аспектов исследования, а именно: *алгоритмическому*, *метрическому* и *дескриптивному*.

В пп.3.1-3.3 решены проблемы 1.9 и 1.10. Решение проблемы 1.9 получено методами теории поиска на частично упорядоченных структурах, разработанной в разделе 2. В п.3.1 построены прямые и обратные M-источники для поиска идентифицирующих (т.е. диагностических, установочных и синхронизирующих) слов для заданного слабоинициального автомата. В п.3.2 разработан общий метод построения нижних экспоненциальных оценок. На его основе исследован метрический аспект симметрической группы - классической структуры алгебры, имеющей многочисленные применения. В п.3.3, на основе разработанного в п.3.2 метода, получены экспоненциальные нижние оценки длин минимальных диагностических и синхронизирующих слов для слабоинициального автомата с двухбуквенным входным алфавитом. В п.3.4 построены AM-источники для идентификации начального и финального состояний слабоинициального автомата. В п.3.5 исследуются представления функций переходов и выходов автомата конечными группами. В п.3.6, на основе результатов, полученных в пп.3.2, 3.3 и 3.5, решена проблема построения *нестационарных секретных замков* сколь угодно большой сложности расшифровки.

3.1. Поиск идентифицирующих слов.

Основной целью настоящего пункта является решение проблемы 1.9, т.е. детализация разработанных в разделе 2 алгоритмов для организации безусловных экспериментов по идентификации начального или финального состояния заданного слабоинициального автомата (M, Q_0), где

$$M = (Q, X, Y, \delta, \lambda) \quad (|Q| = k \geq 2,\ |X| = m \geq 2,\ |Y| = n \geq 2)$$

и

$$Q_0 \subseteq Q \quad (|Q_0| = r \geq 2)\,.$$

Для достижения этой цели достаточно построить M-источник, множеством выигрышных операторов которого является либо множество всех диагностических слов $D(M, Q_0)$, либо множество всех установочных слов $H(M, Q_0)$, либо множество всех синхронизирующих слов $S(M, Q_0)$. Так как в определении синхронизирующего слова не задействована функция выходов λ, то при поиске множества $S(M, Q_0)$ считаем, что M - автомат без выхода, т.е.

$$M = (Q, X, \delta)\,.$$

Предложенная в разделе 2 классификация обосновывает целесообразность построения как прямых, так и обратных M-источников, что открывает возможность организации параллельных вычислений для соответствующих безусловных экспериментов.

Построение прямых $\mathcal{M}$-источников. В процессе поиска идентифицирующих слов восстановлением их начальных отрезков необходимо *помнить*, какие состояния необходимо в дальнейшем:

1) *различить*, если слово - диагностическое;
2) или *различить*, или *склеить* (т.е. перевести в одно и то же состояние), если слово - установочное;
3) *склеить*, если слово - синхронизирующее.

Следовательно, *множество ситуаций* источника, применяемого в процессе восстановления начальных отрезков идентифицирующих слов естественно определяется следующим образом:

1. Если идентифицирующее слово - диагностическое или установочное, то множество ситуаций – это такое множество $\mathcal{W}(k,r)$ $(\mathcal{W}(k,r) \subseteq \mathbf{B}(\mathbf{B}(Q)))$, что $W \in \mathcal{W}(k,r)$ $(W \subset \mathbf{B}(Q))$ тогда и только тогда, когда выполнены следующие три условия:

Условие 3.1. $|w| \geq 2$ для всех $w \in W$.

Условие 3.2. Если $w_1, w_2 \in W$ $(w_1 \neq w_2)$, то $w_1 \not\subset w_2$ и $w_2 \not\subset w_1$.

Условие 3.3. $\sum\limits_{w \in W} |w| \leq r$.

2. Если идентифицирующее слово - синхронизирующее, то множество ситуаций – это множество
$$\mathbf{B}(k,r) = \{W \in \mathbf{B}(Q) \setminus \{\varnothing\} \mid |W| \leq r\}.$$

Для построенных множеств ситуаций следующая интерпретация - истинная:

1. Ситуация $W \in \mathcal{W}(k,r)$ содержит информацию о том, что любые два состояния, принадлежащие одному и тому же множеству $w \in W$ необходимо в дальнейшем различить, если идентифицирующее слово – диагностическое и различить или склеить, если идентифицирующее слово – установочное.

2. Ситуация $W \in \mathbf{B}(k,r)$ содержит информацию о том, что все состояния, принадлежащие множеству W необходимо в дальнейшем склеить, если идентифицирующее слово - синхронизирующее.

Из этой интерпретации вытекает, что:

1. *Начальной ситуацией* является:

   1) $\{Q_0\}$, если идентифицирующее слово - диагностическое или установочное;
   2) Q_0, если идентифицирующее слово – синхронизирующее.

2. *Множеством финальных ситуаций* является:

   1) $\{\varnothing\}$, если идентифицирующее слово - диагностическое или установочное;
   2) $\mathbf{B}(k,1)$, если идентифицирующее слово – синхронизирующее.

Построенные множества ситуаций дают возможность отождествить множество элементарных операторов с входным алфавитом X автомата M и следующим образом определить действие элементарного оператора x $(x \in X)$ на ситуацию W (т.е. вычисление ситуации Wx).

Пусть $W = \{w_1, \dots, w_h\} \in \mathsf{W}(k,r)$ и $x \in X$.

Если идентифицирующее слово – диагностическое, то ситуация Wx вычисляется в соответствии с алгоритмом

Алгоритм 3.1.

Шаг 1. $W_1 := \{w_j(y) \mid j = 1, \dots, h; y \in Y\}$, где

$$w_j(y) = \{\delta(q,x) \mid q \in w_j \text{ и } \lambda(q,x) = y\} \quad (j = 1, \dots, h; y \in Y).$$

Шаг 2. Если существует такое $j \in \{1, \dots, h\}$, что

$$\sum_{y \in Y} | w_j(y) | < | w_j |,$$

то Wx не определено и конец, иначе переход к шагу 3.

Шаг 3. $Wx := \{w \in W_1 \mid | w | \geq 2\}$ и конец.

Если идентифицирующее слово – установочное, то ситуация Wx вычисляется в соответствии с алгоритмом

Алгоритм 3.2.

Шаг 1. $W' := \{w_j(y) \mid j = 1, \dots, h; y \in Y\}$, где

$$w_j(y) = \{\delta(q,x) \mid q \in w_j \text{ и } \lambda(q,x) = y\} \quad (j = 1, \dots, h; \; y \in Y).$$

Шаг 2. $Wx := \{w \in W' \mid | w | \geq 2\}$ и конец.

Пусть $W \in \mathbf{B}(k,r)$ (т.е. идентифицирующее слово - синхронизирующее) и $x \in X$. Ситуация Wx вычисляется по формуле

$$Wx = \{\delta(q,x) \mid q \in W\}.$$

Таким образом, определены источники

$$\boldsymbol{S}^d_{(M,Q_0)} = (\mathsf{W}(k,r), X, \{Q_0\}, \{\varnothing\}), \tag{3.1}$$

$$\boldsymbol{S}^h_{(M,Q_0)} = (\mathsf{W}(k,r), X, \{Q_0\}, \{\varnothing\}) \tag{3.2}$$

и

$$\boldsymbol{S}^s_{(M,Q_0)} = (\mathbf{B}(k,r), X, Q_0, \mathbf{B}(k,1)). \tag{3.3}$$

Отметим, что записи источников $\boldsymbol{S}^d_{(M,Q_0)}$ и $\boldsymbol{S}^h_{(M,Q_0)}$ идентичны друг другу. Тем не менее эти источники – *различные*. Их отличие друг от друга (причем, *существенное*) состоит в том, что для источника $\boldsymbol{S}^d_{(M,Q_0)}$ действия элементарных операторов осуществляются в соответствии с алгоритмом 3.1, а для источника $\boldsymbol{S}^h_{(M,Q_0)}$ действия элементарных операторов осуществляются в соответствии с алгоритмом 3.2. Из сравнения этих алгоритмов вытекает, что равенство

$$\boldsymbol{S}^d_{(M,Q_0)} = \boldsymbol{S}^h_{(M,Q_0)} \tag{3.4}$$

истинно тогда и только тогда, когда автомат M удовлетворяет следующему условию

Условие 3.4. Для любых двух состояний $q_1,q_2 \in Q$ $(q_1 \neq q_2)$ и любого входного символа $x \in X$

$$\delta(q_1,x) \neq \delta(q_2,x)$$

или

$$\lambda(q_1,x) \neq \lambda(q_2,x).$$

Исследуем источники $\mathbf{S}^d_{(M,Q_0)}$, $\mathbf{S}^h_{(M,Q_0)}$ и $\mathbf{S}^s_{(M,Q_0)}$.

Определим на множествах $W(k,r)$ и $\mathbf{B}(k,r)$ отношения частичного порядка, соответственно, $\leq_W$ и $\leq_{\mathbf{B}}$, следующим образом:

$$W_2 \leq_W W_1 \Leftrightarrow (\forall w_2 \in W_2)(\exists w_1 \in W_1)(w_2 \subseteq w_1) \quad (W_1,W_2 \in W(k,r))$$

и

$$W_2 \leq_{\mathbf{B}} W_1 \Leftrightarrow W_2 \subseteq W_1 \quad (W_1,W_2 \in \mathbf{B}(k,r))$$

Теорема 3.1. Каждый из источников $\mathbf{S}^d_{(M,Q_0)}$, $\mathbf{S}^h_{(M,Q_0)}$ и $\mathbf{S}^s_{(M,Q_0)}$ - M-источник.

Доказательство. Покажем, что для каждого из источников $\mathbf{S}^d_{(M,Q_0)}$, $\mathbf{S}^h_{(M,Q_0)}$ и $\mathbf{S}^s_{(M,Q_0)}$ выполнены условия 2.11-2.13.

Условие 2.11 для каждого из источников $\mathbf{S}^d_{(M,Q_0)}$, $\mathbf{S}^h_{(M,Q_0)}$ и $\mathbf{S}^s_{(M,Q_0)}$ выполнено автоматически, так как множество финальных ситуаций каждого из этих источников - это множество всех минимальных элементов соответствующего множества ситуаций.

Условие 2.12 для источников $\mathbf{S}^h_{(M,Q_0)}$ и $\mathbf{S}^s_{(M,Q_0)}$ выполнено автоматически, так как в каждом из этих источников каждый элементарный оператор – это отображение, определенное на всем соответствующем множестве ситуаций.

Покажем, что условие 2.12 выполнено для источника $\mathbf{S}^d_{(M,Q_0)}$.

Пусть $W_2 \leq_W W_1$ $(W_1,W_2 \in W(k,r))$ и $W_1 \in \mathrm{Dom}\, x$ $(x \in X)$. Так как $W_2 \leq_W W_1$, то для каждого $w_2 \in W_2$ $(w_2 \subseteq Q,\ |w_2| \geq 2)$ существует такое $w_1 \in W_1$ $(w_1 \subseteq Q)$, что

$$w_2 \subseteq w_1. \tag{3.5}$$

Так как $W_1 \in \mathrm{Dom}\, x$ $(x \in X)$ и $w_1 \in W_1$, то (см. алгоритм 3.1)

$$\sum_{y \in Y} |w_1(y)| = |w_1|. \tag{3.6}$$

Равенство (3.6) эквивалентно тому, что

$$\delta(q_1,x) \neq \delta(q_2,x)$$

или

$$\lambda(q_1,x) \neq \lambda(q_2,x)$$

для всех $q_1,q_2 \in w_1$ $(q_1 \neq q_2)$. Следовательно, из (3.5) и (3.6) вытекает, что

$$\sum_{y \in Y} |w_2(y)| = |w_2| \quad (w_2 \in W_2), \tag{3.7}$$

т.е. (см. алгоритм 3.1), $W_2 \in \mathrm{Dom}\, x$, что и требовалось показать.

Покажем, что условие 2.13 выполнено для источников $\mathbf{S}^d_{(M,Q_0)}$ и $\mathbf{S}^h_{(M,Q_0)}$.

Пусть $W_2 \leq_W W_1$ $(W_1,W_2 \in W(k,r))$ и $W_1 \in \mathrm{Dom}\, x$ $(x \in X)$ (последнее условие автоматически выполнено для источника $\mathbf{S}^h_{(M,Q_0)}$, т.к. для него каждый элементарный оператор – это отображение, определенное на всем множестве ситуаций). Так как

$W_2 \leq_{\mathsf{W}} W_1$, то для каждого $w_2 \in W_2$ $(w_2 \subseteq Q, |w_2| \geq 2)$ существует такое $w_1 \in W_1$ $(w_1 \subseteq Q)$, что выполнено включение (3.5). Следовательно,

$$w_2(y) \subseteq w_1(y) \ (y \in Y) \ . \tag{3.8}$$

А так как (см. алгоритмы 3.1 и 3.2),

$$W_2 x = \{w_2(y) \mid w_2 \in W_2, |w_2(y)| \geq 2\} \tag{3.9}$$

и

$$W_1 x = \{w_1(y) \mid w_1 \in W_1, |w_1(y)| \geq 2\}, \tag{3.10}$$

то из (3.8)-(3.10) вытекает, что $W_2 x \leq_{\mathsf{W}} W_1 x$, что и требовалось показать.

Покажем, что условие 2.13 выполнено для источника $\mathbf{S}^s_{(M,Q_0)}$.

Пусть $W_2 \leq_{\mathbf{B}} W_1$ $(W_1, W_2 \in \mathbf{B}(k,r))$ и $W_1 \in \mathrm{Dom}\, x$ $(x \in X)$ (последнее условие автоматически выполнено для источника $\mathbf{S}^s_{(M,Q_0)}$, т.к. для него каждый элементарный оператор – это отображение, определенное на всем множестве ситуаций). Так как $W_2 \leq_{\mathbf{B}} W_1$, то

$$W_2 \subseteq W_1 . \tag{3.11}$$

А так как

$$W_2 x = \{\delta(q,x) \mid q \in W_2\} \tag{3.12}$$

и

$$W_1 x = \{\delta(q,x) \mid q \in W_1\}, \tag{3.13}$$

то из (3.11)-(3.13) вытекает, что $W_2 x \leq_{\mathbf{B}} W_1 x$, что и требовалось показать.

Теорема доказана.

Индукцией по длине оператора $p \in X^*$ нетрудно доказать, что справедливы следующие три утверждения

Утверждение 3.1. Для M-источника $\mathbf{S}^d_{(M,Q_0)}$ любые ситуация $W \in \mathsf{W}(k,r)$ и оператор $p \in X^*$ удовлетворяют следующим двум условиям:

Условие 3.5. $W \in \mathrm{Dom}\, p$ тогда и только тогда, когда

$$\tilde{\delta}(q_1, p) \neq \tilde{\delta}(q_2, p)$$

или

$$\tilde{\lambda}(q_1, p) \neq \tilde{\lambda}(q_2, p)$$

для всех состояний $q_1, q_2 \in w$ $(q_1 \neq q_2)$ в каждом множестве состояний $w \in W$.

Условие 3.6. Если $W \in \mathrm{Dom}\, p$ и $q_1, q_2 \in w$ $(w \in W)$ - два такие различные состояния, что

$$\tilde{\lambda}(q_1, p) = \tilde{\lambda}(q_2, p),$$

то существует такое множество $w' \in Wp$, что

$$\{\tilde{\delta}(q_1, p), \tilde{\delta}(q_2, p)\} \subseteq w'.$$

Утверждение 3.2. Для M-источника $\mathbf{S}^h_{(M,Q_0)}$ для любых ситуации $W \in \mathsf{W}(k,r)$ и оператора $p \in X^*$, если $q_1, q_2 \in w$ $(w \in W)$ - два такие состояния, что

$$\tilde{\delta}(q_1, p) \neq \tilde{\delta}(q_2, p),$$

и

$$\widetilde{\lambda}(q_1, p) = \widetilde{\lambda}(q_2, p),$$
то существует такое множество $w' \in Wp$, что
$$\{\widetilde{\delta}(q_1, p), \widetilde{\delta}(q_2, p)\} \subseteq w'.$$

Утверждение 3.3. Для M-источника $\boldsymbol{S}^{s}_{(M,Q_0)}$ для любых ситуации $W \in \mathbf{B}(k,r)$ и оператора $p \in X^*$, если $q_1, q_2 \in W$ - два такие состояния, что
$$\widetilde{\delta}(q_1, p) \neq \widetilde{\delta}(q_2, p),$$
то
$$\{\widetilde{\delta}(q_1, p), \widetilde{\delta}(q_2, p)\} \subseteq Wp.$$

Теорема 3.2. Для M-источников $\boldsymbol{S}^{d}_{(M,Q_0)}$, $\boldsymbol{S}^{h}_{(M,Q_0)}$ и $\boldsymbol{S}^{s}_{(M,Q_0)}$ справедливы равенства
$$\boldsymbol{L}(\boldsymbol{S}^{d}_{(M,Q_0)}) = D(M, Q_0),$$
$$\boldsymbol{L}(\boldsymbol{S}^{h}_{(M,Q_0)}) = H(M, Q_0)$$
и
$$\boldsymbol{L}(\boldsymbol{S}^{s}_{(M,Q_0)}) = S(M, Q_0).$$

Доказательство. Рассмотрим M-источник $\boldsymbol{S}^{d}_{(M,Q_0)}$. По определению множества выигрышных операторов имеем
$$\boldsymbol{L}(\boldsymbol{S}^{d}_{(M,Q_0)}) = \{p \in X^{+}_{\{Q_0\}} \mid \{Q_0\}p = \varnothing\}.$$
Из утверждения 3.1 и определения диагностического слова для слабоинициального автомата вытекает, что
$$\{Q_0\}p = \varnothing \Leftrightarrow (\forall q_1, q_2 \in Q_0 \;\; (q_1 \neq q_2))(\widetilde{\lambda}(q_1, p) \neq \widetilde{\lambda}(q_2, p)) \Leftrightarrow p \in D(M, Q_0),$$
что и требовалось показать.

Рассмотрим M-источник $\boldsymbol{S}^{h}_{(M,Q_0)}$. По определению множества выигрышных операторов имеем
$$\boldsymbol{L}(\boldsymbol{S}^{h}_{(M,Q_0)}) = \{p \in X^{+} \mid \{Q_0\}p = \varnothing\}.$$
Из утверждения 3.2 определения установочного слова для слабоинициального автомата вытекает, что
$$\{Q_0\}p = \varnothing \Leftrightarrow (\forall q_1, q_2 \in Q_0)(\widetilde{\lambda}(q_1, p) \neq \widetilde{\lambda}(q_2, p) \vee \widetilde{\delta}(q_1, p) = \widetilde{\delta}(q_2, p)) \Leftrightarrow p \in H(M, Q_0),$$
что и требовалось показать.

Рассмотрим M-источник $\boldsymbol{S}^{s}_{(M,Q_0)}$. По определению множества выигрышных операторов имеем
$$\boldsymbol{L}(\boldsymbol{S}^{s}_{(M,Q_0)}) = \{p \in X^{+} \mid |Q_0 p| = 1\}.$$
Из утверждения 3.3 определения синхронизирующего слова для слабоинициального автомата вытекает, что
$$|Q_0 p| = 1 \Leftrightarrow |\{\widetilde{\delta}(q, p) \mid q \in Q_0\}| = 1 \Leftrightarrow p \in S(M, Q_0),$$
что и требовалось показать.

Теорема доказана.

Таким образом, для поиска минимальных идентифицирующих для заданного слабоинициального автомата (M, Q_0) слов восстановлением их начальных отрезков достаточно применить алгоритм 2.4 (для решения проблемы 1.4) или алгоритм 2.5 (для решения проблемы 1.5) к M-источнику $\mathbf{S}^d_{(M,Q_0)}$ в случае диагностических слов, к M-источнику $\mathbf{S}^h_{(M,Q_0)}$ в случае установочных слов и к M-источнику $\mathbf{S}^s_{(M,Q_0)}$ в случае синхронизирующих слов. Аналогичным образом, для поиска неприводимых идентифицирующих для заданного слабоинициального автомата (M,Q_0) слов восстановлением их начальных отрезков достаточно применить алгоритм 2.8 к M-источнику $\mathbf{S}^d_{(M,Q_0)}$ в случае диагностических слов, к M-источнику $\mathbf{S}^h_{(M,Q_0)}$ в случае установочных слов и к M-источнику $\mathbf{S}^s_{(M,Q_0)}$ в случае синхронизирующих слов.

Отметим, что ни один из M-источников $\mathbf{S}^d_{(M,Q_0)}$, $\mathbf{S}^h_{(M,Q_0)}$ или $\mathbf{S}^s_{(M,Q_0)}$ не дает возможности осуществлять поиск кооперативных решений. Действительно, проверка свойства '*быть j-кооперативным решением*' (см. определение 1.6) для множества операторов $\{F_1,\ldots,F_j\}$ основана только на множестве ситуаций $\{s_{in}F_1,\ldots,s_{in}F_j\}$. По построению, для каждого из M-источников $\mathbf{S}^d_{(M,Q_0)}$, $\mathbf{S}^h_{(M,Q_0)}$ или $\mathbf{S}^s_{(M,Q_0)}$ это множество содержит информацию о том, *что нужно еще сделать*, но не содержит информацию о том, *что уже сделано*. Поэтому, M-источники $\mathbf{S}^d_{(M,Q_0)}$, $\mathbf{S}^h_{(M,Q_0)}$ и $\mathbf{S}^s_{(M,Q_0)}$ бесполезны при поиске кооперативных решений.

Очевидно, что M-источники $\mathbf{S}^d_{(M,Q_0)}$ и $\mathbf{S}^h_{(M,Q_0)}$ являются (как алгебраические системы) гомоморфными образами источников, неявно используемых в [11] в процессе построения, соответственно, диагностического и установочного дерева. При этом, ядро гомоморфизма – *нетривиальное*. Поэтому естественно возникает вопрос:

Являются ли M-источники $\mathbf{S}^d_{(M,Q_0)}$ и $\mathbf{S}^h_{(M,Q_0)}$ наилучшими моделями при поиске минимальных и неприводимых, соответственно, диагностических и установочных слов восстановлением их начальных отрезков?

Как показывает следующий пример, ответ на этот вопрос – *отрицательный*.

Пример 3.1. Пусть

$$W_1 = \{\{q_1,q_2,q_3\},\{q_4,q_5\},\{q_4,q_6\},\{q_5,q_6\}\}$$

и

$$W_2 = \{\{q_1,q_2\},\{q_1,q_3\},\{q_2,q_3\},\{q_4,q_5,q_6\}\}.$$

Ситуации W_1 и W_2 не сравнимы между собой, как элементы множества $\mathsf{W}(k,r)$, т.е.

$$W_1 \not\leq_{\mathsf{W}} W_2$$

и

$$W_2 \not\leq_{\mathsf{W}} W_1.$$

Тем не менее, при переводе этих ситуаций в ситуацию $\varnothing$, одни и те же пары состояний должны быть различены (для M-источника $\mathbf{S}^d_{(M,Q_0)}$) и различены или склеены (для M-источника $\mathbf{S}^h_{(M,Q_0)}$).

Пример 3.1 показывает целесообразность перехода при поиске минимальных и неприводимых диагностических и установочных слов от M-источников $\mathbf{S}^d_{(M,Q_0)}$ и $\mathbf{S}^h_{(M,Q_0)}$ к их гомоморфным образам, соответственно, M-источникам

$$\nu(\mathbf{S}^d_{(M,Q_0)}) = (\nu(W(k,r)), X, \nu(\{Q_0\}), \{\varnothing\})$$

и

$$\nu(\mathbf{S}^h_{(M,Q_0)}) = (\nu(W(k,r)), X, \nu(\{Q_0\}), \{\varnothing\}),$$

где гомоморфизм ν определяется равенством

$$\nu(W) = \bigcup_{w\in W}\{\{q_1,q_2\} \mid q_1,q_2 \in w, q_1 \neq q_2\}.$$

Следует отметить, что автору не известна ни одна модель, которая лучше, чем $\nu(\mathbf{S}^d_{(M,Q_0)})$, $\nu(\mathbf{S}^h_{(M,Q_0)})$ и $\mathbf{S}^s_{(M,Q_0)}$ при поиске минимальных и неприводимых, соответственно, диагностических, установочных и синхронизирующих слов восстановлением их начальных отрезков.

Построение обратных M-источников. Поиск идентифицирующих слов восстановлением их финальных отрезков основан на том, чтобы *помнить* какие состояния начальным отрезком искомого слова должны быть:

1) *различены*, если слово – диагностическое;
2) *различены* или *склеены*, если слово - установочное;
3) *склеены*, если слово – синхронизирующее.

Следовательно, *множество ситуаций* источника, применяемого в процессе восстановления финальных отрезков идентифицирующих слов естественно определяется следующим образом:

1. Если идентифицирующее слово – диагностическое или синхронизирующее, то множество ситуаций – это множество Π_Q всех разбиений множества Q.

2. Если идентифицирующее слово – установочное, то множество ситуаций – это множество $\mathbf{B}(Q^{(2)})$, где
$$Q^{(2)} = \{\{q_1,q_2\} \mid q_1,q_2 \in Q \text{ и } q_1 \neq q_2\}.$$

Для построенных множеств ситуаций следующая интерпретация - истинная:

1. В процессе поиска диагностического слова ситуация $\pi \in \Pi_Q$ содержит информацию о том, что состояния, принадлежащие различным блокам разбиения π различены финальным отрезком искомого слова (т.е. начальным отрезком искомого слова достаточно различать только состояния, принадлежащие одному и тому же блоку разбиения π).

2. В процессе поиска установочного слова ситуация $W \in \mathbf{B}(Q^{(2)})$ содержит информацию о том, что любая пара состояний $\{q_1,q_2\} \notin W$ различена или склеена финальным отрезком искомого слова (т.е. начальным отрезком искомого слова достаточно различать или склеивать только пары состояний $\{q_1,q_2\} \in W$).

3. В процессе поиска синхронизирующего слова ситуация $\pi \in \Pi_Q$ содержит информацию о том, что состояния, принадлежащие одному и тому же блоку

разбиения π склеены финальным отрезком искомого слова (т.е. начальным отрезком искомого слова достаточно склеить только состояния, принадлежащие различным блокам разбиения π).

Из этой интерпретации вытекает, что:

1. *Начальной ситуацией* является:

   1) разбиение $\mathbf{1}_Q = \{Q\}$, если идентифицирующее слово – диагностическое;
   2) ситуация $Q^{(2)}$, если идентифицирующее слово – установочное;
   3) разбиение $\mathbf{0}_Q = \{\{q\} \mid q \in Q\}$, если идентифицирующее слово – синхронизирующее.

2. *Множеством финальных ситуаций* является:

   1) в процессе поиска диагностического слова – это множество
   $$\Pi_Q^d(Q_0) = \{\pi \in \Pi_Q \mid \pi\big|_{Q_0} = \mathbf{0}_{Q_0}\},$$
   где
   $$\pi\big|_{Q_0} = \{B \cap Q_0 \neq \varnothing \mid B \in \pi\};$$

   2) в процессе поиска установочного слова – это множество
   $$\mathbf{B}_{Q_0}(Q^{(2)}) = \{W \in \mathbf{B}(Q^{(2)}) \mid (\forall \{q_1, q_2\} \in W)(|\{q_1, q_2\} \cap Q_0| \leq 1\};$$
   3) в процессе поиска синхронизирующего слова – это множество
   $$\Pi_Q^s(Q_0) = \{\pi \in \Pi_Q \mid \pi\big|_{Q_0} = \mathbf{1}_{Q_0}\}.$$

Построенные выше множества ситуаций дают возможность отождествить множество элементарных операторов с входным алфавитом X автомата M и следующим образом определить действие элементарного оператора x $(x \in X)$ на ситуацию:

1. Пусть идентифицирующее слово – диагностическое. Тогда
$$\pi x = \pi_1 \ \ (\pi, \pi_1 \in \Pi_Q, x \in X),$$
где разбиение π_1 определяется соотношением
$$q_1 \equiv q_2 \ (\pi_1) \Leftrightarrow (\delta(q_1, x) \equiv \delta(q_2, x)\,(\pi) \wedge \lambda(q_1, x) = \lambda(q_2, x)).$$

2. Пусть идентифицирующее слово – установочное. Тогда
$$Wx = W_1 \ \ (W, W_1 \in \mathbf{B}(Q^{(2)})),$$
где
$$W_1 = \{\{q_1, q_2\} \in Q^{(2)} \mid \{\delta(q_1, x), \delta(q_2, x)\} \in W \text{ и } \lambda(q_1, x) = \lambda(q_2, x)\}.$$

3. Пусть идентифицирующее слово – синхронизирующее. Тогда
$$\pi x = \pi_1 \ \ (\pi, \pi_1 \in \Pi_Q, x \in X),$$
где разбиение π_1 определяется соотношением
$$q_1 \equiv q_2 \ (\pi_1) \Leftrightarrow \delta(q_1, x) \equiv \delta(q_2, x)\,(\pi).$$

Таким образом, определены источники

$$\boldsymbol{T}^{d}_{(M,Q_0)} = (\Pi_Q, X, \mathbf{1}_Q, \Pi^{d}_{Q}(Q_0)), \tag{3.14}$$

$$\boldsymbol{T}^{h}_{(M,Q_0)} = (\mathbf{B}(Q^{(2)}), X, Q^{(2)}, \mathbf{B}_{Q_0}(Q^{(2)})) \tag{3.15}$$

и

$$\boldsymbol{T}^{s}_{(M,Q_0)} = (\Pi_Q, X, \mathbf{0}_Q, \Pi^{s}_{Q}(Q_0)). \tag{3.16}$$

Исследуем источники $\boldsymbol{T}^{d}_{(M,Q_0)}$, $\boldsymbol{T}^{h}_{(M,Q_0)}$ и $\boldsymbol{T}^{s}_{(M,Q_0)}$.

Из приведенных выше определений элементарных операторов непосредственно вытекает справедливость следующего утверждения.

Утверждение 3.4. Каждый элементарный оператор $x \in X$ для каждого из источников $\boldsymbol{T}^{d}_{(M,Q_0)}$, $\boldsymbol{T}^{h}_{(M,Q_0)}$ и $\boldsymbol{T}^{s}_{(M,Q_0)}$ определен на всем множестве ситуаций.

На множестве ситуаций каждого из источников $\boldsymbol{T}^{d}_{(M,Q_0)}$, $\boldsymbol{T}^{h}_{(M,Q_0)}$ и $\boldsymbol{T}^{s}_{(M,Q_0)}$ следующим образом определим отношение частичного порядка:

1. Отношение частичного порядка $\leq_d$ на множестве ситуаций Π_Q источника $\boldsymbol{T}^{d}_{(M,Q_0)}$ совпадает с обычным для разбиений множества отношением частичного порядка, т.е.
$$\pi_1 \leq_d \pi_2 \Leftrightarrow (\forall B_1 \in \pi_1)(\exists B_2 \in \pi_2)(B_1 \subseteq B_2) \quad (\pi_1, \pi_2 \in \Pi_Q).$$

2. Отношение частичного порядка $\leq_h$ на множестве ситуаций $\mathbf{B}(Q^{(2)})$ источника $\boldsymbol{T}^{h}_{(M,Q_0)}$ совпадает с обычным отношением включения множеств, т.е.
$$W_1 \leq_h W_2 \Leftrightarrow W_1 \subseteq W_2 \quad (W_1, W_2 \in \mathbf{B}(Q^{(2)})).$$

3. Отношение частичного порядка $\leq_s$ на множестве ситуаций Π_Q источника $\boldsymbol{T}^{s}_{(M,Q_0)}$ является обратным к обычному для разбиений множества отношению частичного порядка, т.е.
$$\pi_1 \leq_s \pi_2 \Leftrightarrow (\forall B_2 \in \pi_2)(\exists B_1 \in \pi_1)(B_2 \subseteq B_1) \quad (\pi_1, \pi_2 \in \Pi_Q).$$

Теорема 3.3. Каждый из источников $\boldsymbol{T}^{d}_{(M,Q_0)}$, $\boldsymbol{T}^{h}_{(M,Q_0)}$ и $\boldsymbol{T}^{s}_{(M,Q_0)}$ - M-источник.

Доказательство. Покажем, что для каждого из источников $\boldsymbol{T}^{d}_{(M,Q_0)}$, $\boldsymbol{T}^{h}_{(M,Q_0)}$ и $\boldsymbol{T}^{s}_{(M,Q_0)}$ выполнены условия 2.11-2.13.

Условие 2.11 для источников $\boldsymbol{T}^{d}_{(M,Q_0)}$ и $\boldsymbol{T}^{s}_{(M,Q_0)}$ выполнено автоматически, так как множество финальных ситуаций каждого из этих источников - это наименьший (по соответствующему отношению частичного порядка) элемент множества ситуаций.

Покажем, что условие 2.11 выполнено для источника $\boldsymbol{T}^{h}_{(M,Q_0)}$.

Пусть $W_1 \in \mathbf{B}_{Q_0}(Q^{(2)})$ и $W_2 \leq_h W_1$. Тогда

$$W_1 \in \mathbf{B}_{Q_0}(Q^{(2)}) \Leftrightarrow (\forall \{q_1, q_2\} \in W_1)(|\{q_1, q_2\} \cap Q_0| \leq 1) \tag{3.17}$$

и

$$W_2 \leq_h W_1 \Leftrightarrow (\forall \{q_1, q_2\} \in W_2)(\{q_1, q_2\} \in W_1). \tag{3.18}$$

Из (3.17) и (3.18) вытекает, что

$$(\forall\{q_1,q_2\}\in W_2)(|\{q_1,q_2\}\cap Q_0|\le 1)\Leftrightarrow W_2\in \mathbf{B}_{Q_0}(Q^{(2)}),$$

что и требовалось показать.

Условие 2.12 для источников $\boldsymbol{T}^d_{(M,Q_0)}$, $\boldsymbol{T}^h_{(M,Q_0)}$ и $\boldsymbol{T}^s_{(M,Q_0)}$ выполнено автоматически, так как (см. утверждение 3.4) в каждом из этих источников каждый элементарный оператор – это отображение, определенное на всем соответствующем множестве ситуаций.

Покажем, что условие 2.13 выполнено для источника $\boldsymbol{T}^d_{(M,Q_0)}$.

Пусть $\pi_2\le_d \pi_1$ $(\pi_1,\pi_2\in\Pi_Q)$ и $x\in X$. Из определения элементарных операторов для источника $\boldsymbol{T}^d_{(M,Q_0)}$ вытекает, что

$$q_1\equiv q_2(\pi_2 x)\Leftrightarrow(\delta(q_1,x)\equiv\delta(q_2,x)(\pi_2)\wedge\lambda(q_1,x)=\lambda(q_2,x)) \tag{3.19}$$

и

$$q_1\equiv q_2(\pi_1 x)\Leftrightarrow(\delta(q_1,x)\equiv\delta(q_2,x)(\pi_1)\wedge\lambda(q_1,x)=\lambda(q_2,x)). \tag{3.20}$$

Из определения отношение частичного порядка $\le_d$ для источника $\boldsymbol{T}^d_{(M,Q_0)}$ вытекает, что

$$\pi_2\le_d\pi_1\Rightarrow(\delta(q_1x)\equiv\delta(q_2x)(\pi_2)\Rightarrow\delta(q_1x)\equiv\delta(q_2x)(\pi_1)) \tag{3.21}$$

Из (3.19)-(3.21) вытекает, что

$$(\forall q_1,q_2\in Q)(q_1\equiv q_2(\pi_2x)\Rightarrow q_1\equiv q_2(\pi_1x))\Leftrightarrow\pi_2x\le_d\pi_1x,$$

что и требовалось показать.

Покажем, что условие 2.13 выполнено для источника $\boldsymbol{T}^h_{(M,Q_0)}$.

Пусть $W_2\le_h W_1$ $(W_1,W_2\in\mathbf{B}(Q^{(2)}))$ и $x\in X$. Из определения элементарных операторов для источника $\boldsymbol{T}^h_{(M,Q_0)}$ вытекает, что

$$W_2x=\{\{q_1,q_2\}\in Q^{(2)}\,|\,\{\delta(q_1,x),\delta(q_2,x)\}\in W_2 \text{ и } \lambda(q_1,x)=\lambda(q_2,x)\} \tag{3.22}$$

и

$$W_1x=\{\{q_1,q_2\}\in Q^{(2)}\,|\,\{\delta(q_1,x),\delta(q_2,x)\}\in W_1 \text{ и } \lambda(q_1,x)=\lambda(q_2,x)\}. \tag{3.23}$$

Из определения отношение частичного порядка $\le_h$ для источника $\boldsymbol{T}^h_{(M,Q_0)}$ вытекает, что

$$W_2\le_h W_1\Rightarrow(\{\delta(q_1,x),\delta(q_2,x)\}\in W_2\Rightarrow\{\delta(q_1,x),\delta(q_2,x)\}\in W_1). \tag{3.24}$$

Из (3.22)-(3.24) вытекает, что

$$(\forall\{q_1,q_2\}\in Q^{(2)})(\{q_1,q_2\}\in W_2x\Rightarrow\{q_1,q_2\}\in W_1x)\Leftrightarrow W_2x\le_h W_1x,$$

что и требовалось показать.

Покажем, что условие 2.13 выполнено для источника $\boldsymbol{T}^s_{(M,Q_0)}$.

Пусть $\pi_2\le_s\pi_1$ $(\pi_1,\pi_2\in\Pi_Q)$ и $x\in X$. Из определения элементарных операторов для источника $\boldsymbol{T}^s_{(M,Q_0)}$ вытекает, что

$$q_1\equiv q_2(\pi_2x)\Leftrightarrow\delta(q_1,x)\equiv\delta(q_2,x)(\pi_2) \tag{3.25}$$

и

$$q_1\equiv q_2(\pi_1x)\Leftrightarrow\delta(q_1,x)\equiv\delta(q_2,x)(\pi_1). \tag{3.26}$$

Из определения отношение частичного порядка $\le_s$ для источника $\boldsymbol{T}^s_{(M,Q_0)}$ вытекает, что

$$\pi_2\le_s\pi_1\Rightarrow(\delta(q_1x)\equiv\delta(q_2x)(\pi_1)\Rightarrow\delta(q_1x)\equiv\delta(q_2x)(\pi_2)) \tag{3.27}$$

Из (3.25)-(3.27) вытекает, что

$$(\forall q_1,q_2\in Q)(q_1\equiv q_2(\pi_1x)\Rightarrow q_1\equiv q_2(\pi_2x))\Leftrightarrow\pi_2x\le_s\pi_1x,$$

что и требовалось показать.

Теорема доказана.

Индукцией по длине оператора $p \in X^*$ нетрудно доказать, что справедливы следующие утверждения (через p^{-1} обозначено *зеркальное отражение* слова p, т.е. слово p, записанное в обратном порядке).

Утверждение 3.5. Для $\mathcal{M}$-источника $\boldsymbol{T}^d_{(M,Q_0)}$ для любых ситуации $\pi \in \Pi_Q$ и оператора $p \in X^*$, если $q_1, q_2 \in Q$ - два такие состояния, что

$$\widetilde{\delta}(q_1, p^{-1}) \equiv \widetilde{\delta}(q_2, p^{-1})(\pi)$$

и

$$\widetilde{\lambda}(q_1, p^{-1}) = \widetilde{\lambda}(q_2, p^{-1}),$$

то

$$q_1 \equiv q_2(\pi p).$$

Утверждение 3.6. Для $\mathcal{M}$-источника $\boldsymbol{T}^h_{(M,Q_0)}$ для любых ситуации $W \in \mathbf{B}(Q^{(2)})$ и оператора $p \in X^*$, если $q_1, q_2 \in Q$ - два такие состояния, что

$$\{\widetilde{\delta}(q_1, p^{-1}), \widetilde{\delta}(q_2, p^{-1})\} \in W$$

и

$$\widetilde{\lambda}(q_1, p^{-1}) = \widetilde{\lambda}(q_2, p^{-1}),$$

то

$$\{q_1, q_2\} \in Wp.$$

Утверждение 3.7. Для $\mathcal{M}$-источника $\boldsymbol{T}^s_{(M,Q_0)}$ для любых ситуации $\pi \in \Pi_Q$ и оператора $p \in X^*$, если $q_1, q_2 \in Q$ - два такие состояния, что

$$\widetilde{\delta}(q_1, p^{-1}) \equiv \widetilde{\delta}(q_2, p^{-1})(\pi),$$

то

$$q_1 \equiv q_2(\pi p).$$

Как обычно, для любого множества $A \subseteq X^*$ положим

$$A^{-1} = \{p^{-1} \mid p \in A\},$$

т.е. A^{-1} состоит из всех записанных в обратном порядке слов, принадлежащих множеству A.

Теорема 3.4. Для $\mathcal{M}$-источников $\boldsymbol{T}^d_{(M,Q_0)}$, $\boldsymbol{T}^h_{(M,Q_0)}$ и $\boldsymbol{T}^s_{(M,Q_0)}$ справедливы равенства

$$\boldsymbol{L}(\boldsymbol{T}^d_{(M,Q_0)}) = (D(M,Q_0))^{-1},$$

$$\boldsymbol{L}(\boldsymbol{T}^h_{(M,Q_0)}) = (H(M,Q_0))^{-1},$$

и

$$\boldsymbol{L}(\boldsymbol{T}^s_{(M,Q_0)}) = (S(M,Q_0))^{-1}.$$

Доказательство. Рассмотрим $\mathcal{M}$-источник $\boldsymbol{T}^d_{(M,Q_0)}$. По определению множества выигрышных операторов имеем

$$\boldsymbol{L}(\boldsymbol{T}^d_{(M,Q_0)}) = \{p \in X^+ \mid \mathbf{1}_Q\, p \in \Pi^d_Q(Q_0)\} = \{p \in X^+ \mid (\mathbf{1}_Q\, p)\big|_{Q_0} = \mathbf{0}_{Q_0}\}\,.$$

Из утверждения 3.5 и определения диагностического слова для слабоинициального автомата вытекает, что

$$(\mathbf{1}_Q\, p)\big|_{Q_0} = \mathbf{0}_{Q_0} \Leftrightarrow (\forall q_1, q_2 \in Q_0\ \ (q_1 \neq q_2))(\widetilde{\lambda}(q_1, p^{-1}) \neq \widetilde{\lambda}(q_2, p^{-1})) \Leftrightarrow$$

$$\Leftrightarrow p^{-1} \in D(M, Q_0) \Leftrightarrow p \in (D(M, Q_0))^{-1}\,,$$

что и требовалось показать.

Рассмотрим $\mathcal{M}$-источник $\boldsymbol{T}^h_{(M,Q_0)}$. По определению множества выигрышных операторов имеем

$$\boldsymbol{L}(\boldsymbol{T}^h_{(M,Q_0)}) = \{p \in X^+ \mid Q^{(2)} p \in \mathbf{B}_{Q_0}(Q^{(2)})\} = \{p \in X^+ \mid (\forall \{q_1, q_2\} \in Q^{(2)} p)(\mid \{q_1, q_2\} \cap Q_0 \mid \leq 1)\}$$

Из утверждения 3.6 и определения установочного слова для слабоинициального автомата вытекает, что

$$(\forall \{q_1, q_2\} \in Q^{(2)} p)(\mid \{q_1, q_2\} \cap Q_0 \mid \leq 1) \Leftrightarrow (\forall q_1, q_2 \in Q_0)(\widetilde{\delta}(q_1, p^{-1}) = \widetilde{\delta}(q_2, p^{-1}) \vee$$

$$\vee\, \widetilde{\lambda}(q_1, p^{-1}) \neq \widetilde{\lambda}(q_2, p^{-1})) \Leftrightarrow p^{-1} \in H(M, Q_0) \Leftrightarrow p \in (H(M, Q_0))^{-1}\,,$$

что и требовалось показать.

Рассмотрим $\mathcal{M}$-источник $\boldsymbol{T}^s_{(M,Q_0)}$. По определению множества выигрышных операторов имеем

$$\boldsymbol{L}(\boldsymbol{T}^s_{(M,Q_0)}) = \{p \in X^+ \mid \mathbf{0}_Q\, p \in \Pi^s_Q(Q_0)\} = \{p \in X^+ \mid (\mathbf{0}_Q\, p)\big|_{Q_0} = \mathbf{1}_{Q_0}\}\,.$$

Из утверждения 3.7 и определения синхронизирующего слова для слабоинициального автомата вытекает, что

$$(\mathbf{0}_Q\, p)\big|_{Q_0} = \mathbf{1}_{Q_0} \Leftrightarrow (\forall q_1, q_2 \in Q_0)(\widetilde{\delta}(q_1, p^{-1}) = \widetilde{\delta}(q_2, p^{-1})) \Leftrightarrow$$

$$\Leftrightarrow p^{-1} \in S(M, Q_0) \Leftrightarrow p \in (S(M, Q_0))^{-1}\,,$$

что и требовалось показать.

Теорема доказана.

Таким образом, для поиска минимальных идентифицирующих для заданного слабоинициального автомата (M, Q_0) слов восстановлением их финальных отрезков достаточно применить алгоритм 2.4 (для решения проблемы 1.4) или алгоритм 2.5 (для решения проблемы 1.5) к $\mathcal{M}$-источнику $\boldsymbol{T}^d_{(M,Q_0)}$ в случае диагностических слов, к $\mathcal{M}$-источнику $\boldsymbol{T}^h_{(M,Q_0)}$ в случае установочных слов и к $\mathcal{M}$-источнику $\boldsymbol{T}^s_{(M,Q_0)}$ в случае синхронизирующих слов. Аналогичным образом, для поиска неприводимых идентифицирующих для заданного слабоинициального автомата (M, Q_0) слов восстановлением их финальных отрезков достаточно применить алгоритм 2.8 к $\mathcal{M}$-источнику $\boldsymbol{T}^d_{(M,Q_0)}$ в случае диагностических слов, к $\mathcal{M}$-источнику $\boldsymbol{T}^h_{(M,Q_0)}$ в случае установочных слов и к $\mathcal{M}$-источнику $\boldsymbol{T}^s_{(M,Q_0)}$ в случае синхронизирующих слов.

Следует отметить, что автору не известна ни одна модель, отличная от $\mathcal{M}$-источников $\boldsymbol{T}^d_{(M,Q_0)}$, $\boldsymbol{T}^h_{(M,Q_0)}$ и $\boldsymbol{T}^s_{(M,Q_0)}$, предназначенная для поиска минимальных и неприводимых, соответственно, диагностических, установочных и синхронизирующих слов восстановлением их финальных отрезков.

Известно, что множество всех разбиений любого множества, с определенным на нем обычным образом отношением частичного порядка, является *структурой*. Следовательно, каждое из частично упорядоченных множеств $(\Pi_Q, \leq_d)$ и $(\Pi_Q, \leq_s)$ является нижней полуструктурой. Это означает, что M-источники $\boldsymbol{T}^d_{(M,Q_0)}$ и $\boldsymbol{T}^h_{(M,Q_0)}$ дают возможность для поиска кооперативных решений (т.е. для построения кратных безусловных экспериментов). Для этого достаточно применить алгоритм 2.7 к M-источнику $\boldsymbol{T}^d_{(M,Q_0)}$ - при идентификации начального состояния заданного слабоинициального автомата (M, Q_0) посредством безусловного эксперимента и к M-источнику $\boldsymbol{T}^h_{(M,Q_0)}$ - при идентификации финального состояния заданного слабоинициального автомата посредством безусловного эксперимента.

Построенные выше прямые и обратные M-источники дают возможность организации параллельных вычислений при поиске минимальных идентифицирующих слов для заданного слабоинициального автомата (M, Q_0). Для этого достаточно применить алгоритм 2.6 к M-источникам $\boldsymbol{S}^d_{(M,Q_0)}$ и $\boldsymbol{T}^d_{(M,Q_0)}$ в случае диагностических слов, к M-источникам $\boldsymbol{S}^h_{(M,Q_0)}$ и $\boldsymbol{T}^h_{(M,Q_0)}$ в случае установочных слов и к M-источникам $\boldsymbol{S}^s_{(M,Q_0)}$ и $\boldsymbol{T}^s_{(M,Q_0)}$ в случае синхронизирующих слов. Отображение θ определяется следующим образом:

1. Для M-источников $\boldsymbol{S}^d_{(M,Q_0)}$ и $\boldsymbol{T}^d_{(M,Q_0)}$

$$\theta : \mathsf{W}(k,r) \times \Pi_Q \to \{0,1\},$$

где

$$\theta(W,\pi) = 1 \Leftrightarrow (\forall w \in W)(\forall B \in \pi)(\,|\, w \cap B \,| \leq 1) \quad (W \in \mathsf{W}(k,r), \pi \in \Pi_Q).$$

2. Для M-источников $\boldsymbol{S}^h_{(M,Q_0)}$ и $\boldsymbol{T}^h_{(M,Q_0)}$

$$\theta : \mathsf{W}(k,r) \times \mathbf{B}(Q^{(2)}) \to \{0,1\},$$

где

$$\theta(W_1,W_2) = 1 \Leftrightarrow (\forall w \in W_1)(\forall \{q_1,q_2\} \in W_2)(\,|\, w \cap \{q_1,q_2\} \,| \leq 1) \quad (W_1 \in \mathsf{W}(k,r), W_2 \in \mathbf{B}(Q^{(2)})).$$

3. Для M-источников $\boldsymbol{S}^h_{(M,Q_0)}$ и $\boldsymbol{T}^h_{(M,Q_0)}$

$$\theta : \mathbf{B}(k,r) \times \Pi_Q \to \{0,1\},$$

где

$$\theta(W,\pi) = 1 \Leftrightarrow (\exists B \in \pi)(W \subseteq B).$$

Корректность такого определения отображения θ непосредственно вытекает из утверждений 3.1-3.3 и утверждений 3.5-3.7.

3.2. Построение нижних экспоненциальных оценок.

Целью настоящего пункта является разработка унифицированного подхода к построению нижних экспоненциальных оценок функции Шеннона. Именно этот подход и будет применен в дальнейшем при установлении нижних оценок минимальных идентифицирующих слов.

Выделение этой проблемы обусловлено следующим. Известно, что построение нижних оценок функции Шеннона является актуальной и сложной задачей дискретной математики. Необходимость ее решения постоянно возникает в процессе исследования проблем, связанных с перечислением, анализом сложности алгоритмов, а также доказательством существования в заданном множестве объектов с теми или иными значениями параметров. Сложность построения нижних оценок функции Шеннона определяется тем, что во многих случаях единственным методом является *построение в явном виде объекта*, на котором достигается устанавливаемая оценка. Как правило, выдерживается принцип:

Чем выше нижняя оценка, тем сложнее
построить объект, для которого она достигается.

Естественным методом понижения сложности построения нижних оценок функции Шеннона и является разработка унифицированного подхода, состоящего в *построении абстрактных математических конструкций, обладающих заданными значениями параметров* и интерпретации этих конструкций в терминах конкретных проблем дискретной математики. Предлагаемая конструкция - это *подстановка*, имеющая специальную структуру. Такой выбор обусловлен следующими обстоятельствами.

В процессе решения проблем анализа и синтеза дискретных систем достаточно часто применяется теория конечных групп. Следовательно, для исследования сложности искомых решений важную роль играют оценки параметров используемых теоретико-групповых конструкций. Однако в теории групп метрическим аспектам решаемых проблем внимания уделяется недостаточно. Известно, что любую конечную группу можно представить группой подстановок конечного множества. В то же время открытыми остаются многие вопросы, связанные с описанием всех подгрупп симметрической группы $S(n)$ при фиксированном n. Набор оценок для теоретико-групповых конструкций, которые можно построить на $S(n)$ как раз и характеризует *выразительную мощность* группы $S(n)$ при фиксированном n. Оценим максимальный порядок элементов группы $S(n)$, а также мощности нормализаторов и центров в $S(n)$.

Определим бинарное отношение $\equiv$ на группе $S(n)$ следующим образом: $f_1 \equiv f_2$ $(f_1, f_2 \in S(n))$ тогда и только тогда, когда подстановки f_1 и f_2 *сопряжены* в $S(n)$, т.е. существует такая подстановка $f \in S(n)$, что $f_1 = f^{-1} f_2 f$. В дальнейшем будем использовать стандартное обозначение теории групп: $a^b = b^{-1}ab$ $(a, b \in S(n))$.

Известно, что $\equiv$ является отношением эквивалентности на $S(n)$, причем классы определяемого ею разбиения $S(n)/\equiv$ группы $S(n)$ совпадают с *цикловыми классами подстановок*. Каждый цикловой класс

$$\{1^{\alpha_1} \ldots n^{\alpha_n}\} \ \ (\sum_{i=1}^{n} i\alpha_i = n,\ \alpha_i \in \mathbf{Z}_+ \ (i = 1, \ldots, n))$$

состоит из всех подстановок $f \in S(n)$, содержащих в точности α_i $(i = 1, \ldots, n)$ циклов длины i. Пусть

$$C(\alpha_1,\ldots,\alpha_n)=|\{1^{\alpha_1}\ldots n^{\alpha_n}\}|.$$

Известно, что (см., напр., [48])

$$C(\alpha_1,\ldots,\alpha_n)=\frac{n!}{1^{\alpha_1}\cdot\ldots\cdot n^{\alpha_n}\cdot\alpha_1!\cdot\ldots\cdot\alpha_n!}. \qquad (3.28)$$

Обозначим *нормализатор* одноэлементного множества $\{f\}$ $(f\in S(n))$ в группе $S(n)$ через $N_{S(n)}(f)$, т.е.

$$N_{S(n)}(f)=\{f_1\in S(n)\,|\,f=f^{f_1}\}.$$

Утверждение 3.8. Если $f\in\{1^{\alpha_1}\ldots n^{\alpha_n}\}$, то

$$|N_{S(n)}(f)|=1^{\alpha_1}\cdot\ldots\cdot n^{\alpha_n}\cdot\alpha_1!\cdot\ldots\cdot\alpha_n!. \qquad (3.29)$$

Доказательство. Так как $N_{S(n)}(f)\le S(n)$, то, по теореме Лагранжа,

$$|S(n)|=|N_{S(n)}(f)|\cdot|S(n):N_{S(n)}(f)|.$$

Следовательно,

$$|N_{S(n)}(f)|=\frac{|S(n)|}{|S(n):N_{S(n)}(f)|}=\frac{n!}{|S(n):N_{S(n)}(f)|}.$$

А так как $|S(n):N_{S(n)}(f)|=|f^{S(n)}|$ и $f^{S(n)}=\{1^{\alpha_1}\ldots n^{\alpha_n}\}$, то

$$|S(n):N_{S(n)}(f)|=C(\alpha_1,\ldots,\alpha_n).$$

Таким образом,

$$|N_{S(n)}(f)|=\frac{n!}{C(\alpha_1,\ldots,\alpha_n)}. \qquad (3.30)$$

Подставляя (3.28) в (3.30), получим (3.29).

Утверждение доказано.

Следствие 3.1. Если подстановка $f\in S(n)$ состоит из k независимых циклов, каждый из которых имеет длину $n\cdot k^{-1}$, то

$$|N_{S(n)}(f)|\sim\sqrt{2\pi k}\cdot(n\cdot e^{-1})^k\quad(n\to\infty,\ k\to\infty). \qquad (3.31)$$

Доказательство. Пусть $f\in\{1^{\alpha_1}\ldots n^{\alpha_n}\}$, где

$$\alpha_i=\begin{cases} k, & \text{если } i=\dfrac{n}{k}\\ 0, & \text{если } i=1,\ldots,\dfrac{n}{k}-1,\dfrac{n}{k}+1,\ldots,n\end{cases}.$$

Из (3.29) вытекает, что

$$|N_{S(n)}(f)|=(n\cdot k^{-1})^k\cdot k!.$$

Пусть $n\to\infty$ и $k\to\infty$. Так как

$$k!\sim\sqrt{2\pi k}\cdot k^k\cdot e^{-k}\ \ (k\to\infty),$$

то

$$| N_{S(n)}(f) | \sim (n \cdot k^{-1})^k \cdot \sqrt{2\pi k} \cdot k^k \cdot e^{-k} \quad (n \to \infty,\ k \to \infty),$$

откуда вытекает (3.31).

Следствие доказано.

Следствие 3.2. Пусть подстановка $f \in S(n)$ состоит из k независимых циклов, длины $d_1, \ldots, d_k$ которых - попарно различные. Тогда

$$| N_{S(n)}(f) | = d_1 \cdot \ldots \cdot d_k . \tag{3.32}$$

Доказательство. По условию, $f \in \{1^{\alpha_1} \ldots n^{\alpha_n}\}$, где

$$\alpha_i = \begin{cases} 1 & , \text{ если } i \in \{d_1, \ldots, d_k\} \\ 0 & , \text{ если } i \notin \{d_1, \ldots, d_k\} \end{cases}. \tag{3.33}$$

Подставляя (3.33) в (3.29), получим (3.32).

Следствие доказано.

Следующая теорема устанавливает точные верхнюю и нижнюю границы для значений $| N_{S(n)}(f) |$ $(f \in S(n))$.

Теорема 3.5. Для всех $f \in S(n)$

$$n - 1 \le | N_{S(n)}(f) | \le n!, \tag{3.34}$$

причем достижимы как верхняя, так и нижняя границы.

Доказательство. Покажем справедливость верхней оценки, устанавливаемой неравенствами (3.34).

Так как $N_{S(n)}(f) \subseteq S(n)$ $(f \in S(n))$, то

$$| N_{S(n)}(f) | \le | S(n) | = n! \ (f \in S(n)),$$

т.е. верхняя граница, устанавливаемая неравенствами (3.34) – истинная. Покажем, что эта граница - достижима. Пусть $\mathbf{i} \in S(n)$ - тождественная подстановка. Тогда $\mathbf{i} = \mathbf{i}^f$ для любой подстановки $f \in S(n)$. Это означает, что $N_{S(n)}(i) = S(n)$. Следовательно,

$$| N_{S(n)}(i) | = | S(n) | = n!,$$

что и требовалось показать.

Покажем справедливость нижней оценки, устанавливаемой неравенствами (3.34).

Известно, что цикловой класс $\{1^{\alpha_1} \ldots n^{\alpha_n}\}$ $(\sum_{i=1}^{n} i\alpha_i = n,\ \alpha_i \in \mathbf{Z}_+\ (i = 1, \ldots, n))$, содержит наибольшее число подстановок, если

$$\alpha_i = \begin{cases} 1 & , \text{ если } i \in \{1, n-1\} \\ 0 & , \text{ если } i \notin \{1, n-1\} \end{cases}.$$

Следовательно,

$$\max C(\alpha_1, \ldots, \alpha_n) = C(1,0,\ldots 0,1,0) =$$

$$= n! \cdot (1^1 \cdot 2^0 \cdot \ldots \cdot (n-2)^0 \cdot (n-1)^1 \cdot n^0 \cdot 1! \cdot 0! \cdot \ldots \cdot 0! \cdot 1! \cdot 0!)^{-1} = n! \cdot (n-1)^{-1}, \tag{3.35}$$

где максимум берется по всем таким числам $\alpha_1,\ldots,\alpha_n$, что $\sum\limits_{i=1}^{n} i\alpha_i = n,\ \alpha_i \in \mathbf{Z}_+\ (i=1,\ldots,n)$. Из (3.30) и (3.35) вытекает, что

$$\min_{f\in S(n)} |N_{S(n)}(f)| = \frac{n!}{\max C(\alpha_1,\ldots,\alpha_n)} = \frac{n!}{n!\cdot(n-1)^{-1}} = n-1,$$

что и требовалось показать.

Теорема доказана.

Оценим теперь максимальный порядок элементов группы $S(n)$. Напомним, что, по определению, *порядок подстановки* $f \in S(n)$ - это такое наименьшее число $k \in \mathbf{N}$, что $f^k = \mathbf{i}$, где $\mathbf{i} \in S(n)$ - тождественная подстановка.

Известно, что порядок подстановки $f \in S(n)$ равен наименьшему общему кратному (НОК) длин ее циклов. Таким образом, если

$$f = D_{r_1}\ldots D_{r_l}, \tag{3.36}$$

где $D_h\ \ (h\in\{r_1,\ldots,r_l\})$ - цикл длины h, то

$$|f| = \text{НОК}(r_1,\ldots,r_l). \tag{3.37}$$

где $|f|$ - порядок подстановки f.

Исследуем функцию Шеннона

$$L(n) = \max_{f\in S(n)} |f|. \tag{3.38}$$

Теорема 3.6. Справедливо следующее асимптотическое неравенство

$$L(n) \ge e^{O(\sqrt{n})}\ \ (n\to\infty). \tag{3.39}$$

Доказательство. Рассмотрим специальный случай подстановки (3.36), когда $l = r$ и $r_i = r+i$ для всех $i = 1,\ldots,r$, т.е.

$$f = D_{r+1}D_{r+2}\ldots D_{2r}. \tag{3.40}$$

Так как

$$(r+1)+(r+2)+\ldots+2r \le n \Leftrightarrow \frac{1}{2}(3r+1)r \le n,$$

то

$$r \in \left\{1,\ldots,\left\lfloor \frac{1}{6}(\sqrt{24n+1}-1)\right\rfloor\right\}.$$

Из (3.37) вытекает, что для подстановки (3.40)

$$|f| = \text{НОК}(r+1,\ldots,2r) = \text{НОК}(1,\ldots,r,r+1,\ldots,2r) = \text{НОК}(1,\ldots,2r). \tag{3.41}$$

Из (3.38) и (3.41) вытекает, что

$$L(n) \ge \text{НОК}(1,\ldots,2r), \tag{3.42}$$

где

$$r = \left\lfloor \frac{1}{6}(\sqrt{24n+1}-1)\right\rfloor. \tag{3.43}$$

Известно, что (см., напр., [41]) при $x \ge 2$

$$e^{c_1 x} < \text{НОК}(1, \ldots, x) < e^{c_2 x}, \tag{3.44}$$

где c_1, c_2 $(0 < c_1 < c_2)$ - константы. Из (3.42)-(3.44) вытекает (3.39), что и требовалось доказать.

Теорема доказана.

Следствие 3.3. Для каждого $n \geq 2$ существует такая подстановка $f \in S(n)$, что

$$e^{C_1 \sqrt{n}} < |f| < e^{C_2 \sqrt{n}}, \tag{3.45}$$

где C_1, C_2 $(0 < C_1 < C_2)$ - константы.

Доказательство. Выберем в качестве $f \in S(n)$ подстановку (3.40). Из (3.41) и (3.44) вытекает, что

$$e^{2c_1 r} < |f| < e^{2c_2 r}. \tag{3.46}$$

Выберем значение r, определяемое равенством (3.43). Из (3.43) и (3.46) вытекает справедливость (3.45), что и требовалось доказать.

Следствие доказано.

Следствие 3.4. Для каждого $n \geq 2$ симметрическая группа $S(n)$ содержит циклические подгруппы, порядок которых превосходит $e^{c\sqrt{n}}$, где c $(c > 0)$ - константа.

Доказательство. Для циклической группы (f), порождаемой подстановкой $f \in S(n)$, имеет место равенство

$$|(f)| = |f|. \tag{3.47}$$

Выберем в качестве f подстановку (3.40), а в качестве r - значение, определяемое равенством (3.43). Подстановка f удовлетворяет неравенствам (3.45). Из (3.45) и (3.47) вытекает, что

$$|(f)| \geq e^{c\sqrt{n}},$$

где c $(c > 0)$ - константа, что и требовалось доказать.

Следствие доказано.

Следствие 3.5. Для каждого $n \geq 2$ существуют такие группы подстановок H и G, что

$$H \lhd G \leq S(n), \tag{3.48}$$

причем

$$|H| > e^{c\sqrt{n}}, \tag{3.49}$$

где c $(c > 0)$ - константа.

Доказательство. Известно, что

$$N_{S(n)}(f) \leq S(n)$$

для любой подстановки $f \in S(n)$. А так как

$$f^{f^i} = f$$

для всех $i = 1, 2, \ldots$, то

$$(f) \leq N_{S(n)}(f).$$

Пусть $h \in N_{S(n)}(f)$. Тогда

$$(f^i)^h = h^{-1} f^i h = \underbrace{(h^{-1} fh)\ldots(h^{-1} fh)}_{i \text{ раз}} = \underbrace{f \ldots f}_{i \text{ раз}} = f^i$$

для всех $i = 1,2,\ldots$. Следовательно,

$$f^i h = hf^i$$

для всех $h \in N_{S(n)}(f)$ и $i = 1,2,\ldots$. Это означает, что для всех $h \in N_{S(n)}(f)$

$$h(f) = \{hf^i \mid i = 1,2,\ldots\} = \{f^i h \mid i = 1,2,\ldots\} = (f)h,$$

т.е. левые и правые смежные классы группы $N_{S(n)}(f)$ по подгруппе (f) совпадают. Отсюда вытекает, что

$$(f) \lhd N_{S(n)}(f) \le S(n). \qquad (3.50)$$

Выберем в качестве f подстановку (3.40), а в качестве r - значение, определяемое равенством (3.43). Положим $H = (f)$ и $G = N_{S(n)}(f)$. Из (3.50) вытекает справедливость (3.48), а из следствия 3.4 – справедливость неравенства (3.49).

Следствие доказано.

Обозначим через $C_H(M)$ *централизатор* множества M в подгруппе H, т.е.

$$C_H(M) = \{h \in H \mid m^h = m \text{ для всех } m \in M\}.$$

Следствие 3.6. Для каждого $n \ge 2$ существует такая группа подстановок $G \le S(n)$, что

$$|C_{S(n)}(G)| > e^{c\sqrt{n}}, \qquad (3.51)$$

где c $(c > 0)$ - константа.

Доказательство. В процессе доказательства следствия 3.5 показано, что равенство

$$(f^i)^h = f^i$$

справедливо для всех $h \in N_{S(n)}(f)$ и $i = 1,2,\ldots$. Отсюда вытекает, что

$$C_{S(n)}(N_{S(n)}(f)) \supseteq (f)$$

и, следовательно,

$$|C_{S(n)}(N_{S(n)}(f))| \ge |(f)|. \qquad (3.52)$$

Выберем в качестве f подстановку (3.40), а в качестве r - значение, определяемое равенством (3.43). Положим $G = N_{S(n)}(f)$. Из (3.52) и следствия 3.4 вытекает справедливость неравенства (3.51).

Следствие доказано.

Выше показано, что использование подстановки (3.40) при значении r, определяемом равенством (3.43), является мощным инструментом для характеристики *выразительной мощности* группы $S(n)$ при фиксированном n. В дальнейшем будет показано, что эта конструкция является также мощным инструментом в процессе построения нижних экспоненциальных оценок в теории автоматов.

3.3. Сложность поиска минимальных идентифицирующих слов.

Основной целью настоящего пункта является решение проблемы построения нижних оценок функции Шеннона для длин минимальных диагностических и синхронизирующих слов для слабоинициального автомата с двухбуквенным входным алфавитом. Актуальность именно такой постановки проблемы обусловлена следующими двумя обстоятельствами.

Во-первых, верхняя оценка длины минимального выигрышного оператора для M-источника $\boldsymbol{S} = (S, F, s_{in}, S_{fin})$, определяемая формулой

$$L = |S| - |S_{fin}|,$$

как правило, значительно завышена, сложна и малоинформативная. Эта оценка отражает, скорее, *сложность* модели $\boldsymbol{S}$, а не *сложность* той конкретной проблемы, для решения которой используется $\boldsymbol{S}$.

Во-вторых, сложность поиска минимальных идентифицирующих слов для слабоинициального автомата характеризуется более точно не функцией Шеннона L^u_{kmn} $(u \in \{d, h, s\})$, а отношением

$$L^u_{отн}(k, m, n) = \frac{L^u_{kmn}}{km}, \tag{3.53}$$

где km характеризует *объем памяти*, необходимой для хранения таблицы автомата, т.е. *сложность* исследуемой модели. Ограничения значений m величиной $O(k)$ $(k \to \infty)$ дает возможность оценивать *сложность* поиска минимальных идентифицирующих слов, как функцию только от числа k состояний автомата.

Решение исследуемой проблемы основано на использовании конструкции, разработанной в п.3.2.

Теорема 3.7. При

$$n = \left\lfloor \frac{1}{6}(\sqrt{24k - 23} + 1) \right\rfloor + 1$$

справедлива следующая оценка функции Шеннона для длин минимальных диагностических слов для слабоинициального автомата с двухбуквенным входным алфавитом

$$L^d_{k2n} \geq e^{O(\sqrt{k})} \quad (k \to \infty). \tag{3.54}$$

Доказательство. Для доказательства теоремы нам понадобится следующая лемма.

Лемма 3.1. Для всех $k \geq 2$ и $r \in \{2, \ldots, \left\lfloor \frac{1}{6}(\sqrt{24k - 23} + 1) \right\rfloor\}$

$$L^d_{k2r}(r) > \max \text{НОК}(l + 1, \ldots, l + r - 1), \tag{3.55}$$

где максимум берется по всем $l \in \{1, \ldots, \lfloor 0.5(r-1)^{-1}(2(k-1) - r(r-1)) \rfloor\}$.

Доказательство. Для доказательства леммы достаточно построить такой слабоинициальный автомат (M, Q_0) $(M \in \mathbf{A}_{k2r},\ Q_0 \subseteq Q,\ |Q_0| = r \geq 2)$, что

$$L^d(M,Q_0) = \text{НОК}(l+1,\ldots,l+r-1)+1\,. \qquad (3.56)$$

Выберем такие попарно непересекающиеся подмножества $W_1,\ldots,W_{r-1}$ множества $Q\setminus\{q_1\}$, что

$$W_i = \{q_{g(i)+j} \mid j = 0,1,\ldots,l+i-1\} \quad (i=1,\ldots,r-1)\,,$$

где

$$g(i) = 2 + l(i-1) + 0.5i(i-1)\,.$$

Нетрудно убедиться в том, что существование таких подмножеств гарантируется выбранными значениями r и l.

Пусть $M \in \mathbf{A}_{k2r}$ - такой автомат, что

$$\delta(q_u,x_v) = \begin{cases} q_{u+1}, \text{ если } v=1 \text{ и } q_u \in W_i\setminus\{q_{g(i+1)-1}\}\ (i=1,\ldots,r-1), \\ q_{g(i)}, \quad \text{если } v=1 \text{ и } u=g(i+1)-1\ (i=1,\ldots,r-1), \\ q_1 \quad , \qquad \text{если } v=2 \text{ и } q_u \in \bigcup_{i=1}^{r-1} W_i\,, \\ q_1 \quad , \qquad \text{если } v\in\{1,2\} \text{ и } u=1. \end{cases} \qquad (3.57)$$

и

$$\lambda(q_u,x_v) = \begin{cases} y_1 \quad , \qquad \text{если } v=1 \text{ и } q_u \in \bigcup_{i=1}^{r-1} W_i\,, \\ y_1, \text{ если } v=2 \text{ и } q_u \in W_i\setminus\{q_{g(i+1)-1}\}\ (i=1,\ldots,r-1), \\ y_{i+1}, \quad \text{если } v=2 \text{ и } u=g(i+1)-1\ (i=1,\ldots,r-1) \\ y_1 \quad , \qquad \text{если } v\in\{1,2\} \text{ и } u=1. \end{cases} \qquad (3.58)$$

Положим

$$Q_0 = \{q_1, q_{g(1)},\ldots,q_{g(r-1)}\}\,.$$

Из (3.57) и (3.58) вытекает, что:

1) состояние q_1 и любое состояние $q \in W_i\setminus\{q_{g(i+1)-1}\}$ $(i=1,\ldots,r-1)$ являются x_1-совместимыми;
2) входной символ x_2 попарно различает состояния $q_1, q_{g(2)-1},\ldots,q_{g(r)-1}$;
3) множество Q_0 переходит в множество $\{q_1, q_{g(2)-1},\ldots,q_{g(r)-1}\}$ только под действием слов вида x_1^α, где α - общее кратное чисел $l+1,\ldots,l+r-1$.

Следовательно, единственным минимальным диагностическим словом для слабоинициального автомата (M,Q_0) является слово $x_1^{\alpha_0}x_2$, где

$$\alpha_0 = \text{НОК}(l+1,\ldots,l+r-1)\,.$$

Таким образом, для слабоинициального автомата (M,Q_0) справедливо равенство (3.56).

Лемма доказана.

Из (3.55) вытекает (см. (3.44)), что при $l=r-1$

$$L^d_{k2r}(r) > \text{НОК}(r,\ldots,2(r-1)) = \text{НОК}(1,\ldots,2(r-1)) \geq e^{c(r-1)}\,, \qquad (3.59)$$

где c $(c > 0)$ - константа. Полагая в (3.59) $r = O(\sqrt{k})$ $(k \to \infty)$, получим (3.54), что и требовалось доказать.

Теорема доказана.

Определим отображение

$$\delta_x : Q \to Q \ (x \in X)$$

равенством

$$\delta_x(q) = \delta(q, x) \quad (q \in Q).$$

Отметим, что автомат M, построенный в процессе доказательства леммы 3.1, обладает тем свойством, что $\delta_{x_1}\big|_{W_1 \cup \ldots \cup W_{r-1}}$ является на множестве $W_1 \cup \ldots \cup W_{r-1}$ подстановкой, состоящей из циклов длины $l+1, \ldots, l+r-1$.

Следствие 3.7. При $n = \left\lfloor \frac{1}{6}(\sqrt{24k-23}+1) \right\rfloor + 1$

$$L^d_{отн}(k,2,n) \ge e^{O(\sqrt{k} - \ln k)} \ (k \to \infty). \tag{3.60}$$

Доказательство. Подставив (3.54) в (3.53) (при $m = 2$), получим (3.60).

Следствие доказано.

Теорема 3.8. Справедлива следующая оценка функции Шеннона для длин минимальных синхронизирующих слов для слабоинициального автомата с двухбуквенным входным алфавитом

$$L^s_{k2n} \ge e^{O(\sqrt{k})} \ (k \to \infty). \tag{3.61}$$

Доказательство. По аналогии с доказательством теоремы 3.7, вначале доказывается следующая лемма.

Лемма 3.2. Для всех $k \ge 2$ и $r \in \{2, \ldots, \left\lfloor \frac{1}{6}(\sqrt{24k-47}+1) \right\rfloor\}$

$$L^s_{k2n}(r) > \max \text{НОК}(l+1, \ldots, l+r-1), \tag{3.62}$$

где максимум берется по всем $l \in \{1, \ldots, \lfloor 0.5(r-1)^{-1}(2(k-2) - r(r-1)) \rfloor\}$.

Доказательство. Слабоинициальный автомат (M, Q_0) $(M \in \mathbf{A}_{k2n}$, $Q_0 \subseteq Q$, $|Q_0| = r \ge 2)$, такой, что

$$L^s(M, Q_0) = \text{НОК}(l+1, \ldots, l+r-1) + 1, \tag{3.63}$$

строится следующим образом. Выберем такие попарно непересекающиеся подмножества $U_1, \ldots, U_{r-1}$ множества $Q \setminus \{q_1\}$, что

$$U_i = \{q_{h(i)+j} \mid j = 0, 1, \ldots, l+i-1\} \quad (i = 1, \ldots, r-1),$$

где

$$h(i) = g(i) + 1.$$

Нетрудно убедиться в том, что существование таких подмножеств гарантируется выбранными значениями r и l. Так как речь идет о синхронизирующем слове, то M - автомат без выхода. Функцию переходов автомата M определим равенством

$$\delta(q_u, x_v) = \begin{cases} q_{u+1}\ , \text{ если } v = 1 \text{ и } q_u \in U_i \setminus \{q_{h(i+1)-1}\}\ (i = 1,\dots,r-1), \\ q_{h(i)}\ , \quad \text{если } v = 1 \text{ и } u = h(i+1) - 1\ (i = 1,\dots,r-1), \\ q_2\ , \text{ если } v = 2 \text{ и } q_u \in U_i \setminus \{q_{h(i+1)-1}\}\ (i = 1,\dots,r-1), \\ q_1\ , \quad \text{если } v = 2 \text{ и } u = h(i+1) - 1\ (i = 1,\dots,r-1), \\ q_u\ , \qquad \text{если } \ v \in \{1,2\} \ \text{ и } \ u \in \{1,2\}. \end{cases} \tag{3.64}$$

Положим

$$Q_0 = \{q_1, q_{h(1)}, \dots, q_{h(r-1)}\}.$$

Из (3.64) вытекает, что:

1) состояния q_1 и q_2 не склеиваются никаким входным словом;
2) любое состояние $q \in U_i \setminus \{q_{h(i+1)-1}\}$ $(i = 1,\dots,r-1)$ под действием входного символа x_2 переходит в состояние q_2;
3) входной символ x_2 склеивает состояния $q_1, q_{h(2)-1}, \dots, q_{h(r)-1}$;
4) множество Q_0 переходит в множество $\{q_1, q_{h(2)-1}, \dots, q_{h(r)-1}\}$ только под действием слов вида x_1^{α}, где α - общее кратное чисел $l+1,\dots,l+r-1$.

Следовательно, единственным минимальным синхронизирующим словом для слабоинициального автомата (M, Q_0) является слово $x_1^{\alpha_0} x_2$, где

$$\alpha_0 = \text{НОК}(l+1,\dots,l+r-1).$$

Таким образом, для слабоинициального автомата (M, Q_0) справедливо равенство (3.63).

Лемма доказана.

Из (3.62) вытекает (см. (3.44)), что при $l = r-1$

$$L_{k2n}^{s}(r) > \text{НОК}(r,\dots,2(r-1)) = \text{НОК}(1,\dots,2(r-1)) \geq e^{c(r-1)}, \tag{3.65}$$

где c $(c > 0)$ - константа. Полагая в (3.65) $r = O(\sqrt{k})$ $(k \to \infty)$, получим (3.61), что и требовалось доказать.

Теорема доказана.

Отметим, что автомат M, построенный в процессе доказательства леммы 3.2, обладает тем свойством, что $\delta_{x_1}\big|_{U_1 \cup \ldots \cup U_{r-1}}$ является на множестве $U_1 \cup \ldots \cup U_{r-1}$ подстановкой, состоящей из циклов длины $l+1,\dots,l+r-1$.

Следствие 3.8. Справедливо следующее асимптотическое неравенство

$$L_{отн}^{s}(k,2,n) \geq e^{O(\sqrt{k} - \ln k)}\ \ (k \to \infty). \tag{3.66}$$

Доказательство. Подставив (3.61) в (3.53) (при $m = 2$), получим (3.66).

Следствие доказано.

Из следствий 3.7 и 3.8 вытекает, что любой алгоритм поиска (возможно, не минимальных) диагностических или синхронизирующих слов для слабоинициального автомата имеет экспоненциальную *сложность* (как временную, так и емкостную). Поэтому естественно выделить подмножества автоматов, принадлежащих множеству $\mathbf{A}_{kmn}$, для которых такой поиск имеет полиномиальную *сложность* (как временную, так и емкостную). Это легко сделать в случае диагностических слов, так как достаточно выбрать подмножество автоматов, для которых множества диагностических и установочных слов совпадают. Сложность поиска последних, как известно, полиномиальная (например, с помощью метода P_i-таблиц, предложенного в [11]). Такое подмножество автоматов может быть построено следующим образом.

Назовем состояния q_1 и q_2 автомата $M = (Q, X, Y, \delta, \lambda) \in \mathbf{A}_{kmn}$ *совместимыми*, если существует такой входной символ $x \in X$, что $\delta(q_1, x) = \delta(q_2, x)$ и $\lambda(q_1, x) = \lambda(q_2, x)$. Обозначим через $\mathbf{A}_{kmn}^{нсвм}$ множество всех автоматов $M \in \mathbf{A}_{kmn}$, не имеющих совместимых состояний. Очевидно, что для любого автомата $M \in \mathbf{A}_{kmn}^{нсвм}$ равенство

$$D(M, Q_0) = H(M, Q_0)$$

справедливо для всех $Q_0 \subseteq Q$ $(|Q_0| \geq 2)$.

Утверждение 3.9. Для всех $k \geq 2$, $m \geq 2$ и $n \geq 2$

$$|\mathbf{A}_{kmn}^{нсвм}| = \left(\frac{(kn)!}{(kn-k)!} \right)^m .$$

Доказательство. Подсчитаем число допустимых способов заполнения автоматной таблицы. В каждом столбце автоматной таблицы автомата $M \in \mathbf{A}_{kmn}^{нсвм}$ все элементы (принадлежащие множеству $Q \times Y$) попарно различны. Следовательно, число различных допустимых способов заполнения столбца автоматной таблицы равно

$$l = \prod_{i=0}^{k-1} (kn - i) = \frac{(kn)!}{(kn-k)!} .$$

А так как различные столбцы могут быть заполнены независимо друг от друга, то

$$|\mathbf{A}_{kmn}^{нсвм}| = (l)^m = \left(\frac{(kn)!}{(kn-k)!} \right)^m ,$$

что и требовалось доказать.

Утверждение доказано.

Следует отметить, что автору не известно ни одно компактное описание ни одного нетривиального подмножества автоматов, принадлежащих множеству $\mathbf{A}_{kmn}$, для которых поиск (возможно, не минимальных) синхронизирующих слов имеет полиномиальную *сложность* (как временную, так и емкостную).

3.4. Построение автоматов-экспериментаторов.

Основная цель настоящего пункта – проиллюстрировать применение разработанного в п.2.5 метода поиска адаптивных решений к построению условных экспериментов с автоматами. Как и в п.3.1 ограничимся построением соответствующего AM-источника.

Обобщенный условный установочный эксперимент. Пусть (M,Q_0) - заданный слабоинициальный автомат, где $M=(Q,X,Y,\delta,\lambda)$, $Q_0 \subseteq Q$ ($|Q_0|=r\geq 2$), а π - заданное разбиение множества Q.

Рассмотрим источник

$$\mathbf{S}^{ah}_{(M,Q_0)}(\pi)=(\mathbf{B}(k,r),X\times Y,Q_0,\mathbf{B}^{(\pi)}(k,r)),$$

где

$$\mathbf{B}^{(\pi)}(k,r)=\{\sigma\in\mathbf{B}(k,r)\,|\,\sigma\subseteq B \text{ для некоторого } B\in\pi\},$$

а действие элементарного оператора $(x,y)\in X\times Y$ на ситуацию $\sigma\in\mathbf{B}(k,r)$ определяется в соответствии со следующим алгоритмом.

Алгоритм 3.3.

Шаг 1. Если $\lambda(q,x)\neq y$ для всех $q\in\sigma$, то $\sigma(x,y)$ не определено и конец, иначе переход к шагу 2.

Шаг 2. $\sigma(x,y):=\{\delta(q,x)\,|\,q\in\sigma \text{ и } \lambda(q,x)=y\}$ и конец.

Выберем $\leq_{\mathbf{B}}$ в качестве отношение частичного порядка на множестве $\mathbf{B}(k,r)$.

Утверждение 3.10. Источник

$$\mathbf{S}^{ah}_{(M,Q_0)}(\pi)=(\mathbf{B}(k,r),X\times Y,Q_0,\mathbf{B}^{(\pi)}(k,r))$$

является AM-источником.

Доказательство. Покажем, что для источника $\mathbf{S}^{ah}_{(M,Q_0)}(\pi)$ условия 2.30-2.32 выполнены.

Покажем, что выполнено условие 2.30.

Пусть $\sigma_1\in\mathbf{B}^{(\pi)}(k,r)$ и $\sigma_2\leq_{\mathbf{B}}\sigma_1$. Так как $\sigma_1\in\mathbf{B}^{(\pi)}(k,r)$, то существует такой блок $B\in\pi$, что $\sigma_1\subseteq B$. Так как $\sigma_2\leq_{\mathbf{B}}\sigma_1$, то $\sigma_2\subseteq\sigma_1$. Из включений $\sigma_2\subseteq\sigma_1$ и $\sigma_1\subseteq B$ вытекает, что $\sigma_2\subseteq B$, т.е. $\sigma_2\in\mathbf{B}^{(\pi)}(k,r)$, что и требовалось показать.

Покажем, что выполнено условие 2.31.

Пусть $\sigma_1\in\mathrm{Dom}\,(x,y)$ $((x,y)\in X\times Y)$ и $\sigma_2\leq_{\mathbf{B}}\sigma_1$. Так как $\sigma_2\leq_{\mathbf{B}}\sigma_1$, то $\varnothing\neq\sigma_2\subseteq\sigma_1$. Следовательно,

$$\varnothing\neq Y_{\sigma_2,x}=\{\lambda(q,x)\,|\,q\in\sigma_2\}\subseteq\{\lambda(q,x)\,|\,q\in\sigma_1\}=Y_{\sigma_1,x},$$

что и требовалось показать.

Покажем, что выполнено условие 2.32.

Пусть $\sigma_2\leq_{\mathbf{B}}\sigma_1$. Так как $\sigma_2\subseteq\sigma_1$, то (см. алгоритм 3.3) $\sigma_1\in\mathrm{Dom}\,(x,y)$ и $\sigma_2\in\mathrm{Dom}\,(x,y)$ для любого $y\in Y_{\sigma_2,x}$. Из включения $\sigma_2\subseteq\sigma_1$ вытекает, что

$$\sigma_2(x,y)=\{\delta(q,x)\,|\,q\in\sigma_2 \text{ и } \lambda(q,x)=y\}\subseteq\{\delta(q,x)\,|\,q\in\sigma_1 \text{ и } \lambda(q,x)=y\}=\sigma_1(x,y).$$

Так как $\sigma_2(x,y)\subseteq\sigma_1(x,y)$, то $\sigma_2(x,y)\leq_{\mathbf{B}}\sigma_1(x,y)$, что и требовалось показать.

Утверждение доказано.

Индукцией по длине оператора доказывается следующее утверждение.

Утверждение 3.11. В AM-источнике

$$\mathbf{S}^{ah}_{(M,Q_0)}(\pi) = (\mathbf{B}(k,r), X \times Y, Q_0, \mathbf{B}^{(\pi)}(k,r))$$

для любых ситуации $\sigma \in \mathbf{B}(k,r)$ и оператора $H = (x_1, y_1)\ldots(x_l, y_l) \in (X \times Y)^+$, если $\sigma \in \mathrm{Dom}\, H$, то справедливо равенство

$$\sigma H = \{\widetilde{\delta}(q, x_1 \ldots x_l) \mid q \in \sigma \text{ и } \widetilde{\lambda}(q, x_1 \ldots x_l) = y_1 \ldots y_l\}.$$

Из утверждения 3.11 вытекает, что адаптивное решение для AM-источника $\mathbf{S}^{ah}_{(M,Q_0)}(\pi)$ (если оно существует) идентифицирует финальное состояние слабоинициального автомата (M, Q_0) с точностью до блока разбиения π. Указанное решение (если оно существует) может быть построено методом, разработанным в п.2.5. Свернув дерево, представляющее адаптивное решение, в автомат Мура, получим автомат-экспериментатор, реализующий условный обобщенный установочный эксперимент с заданным слабоинициальным автоматом (M, Q_0).

Условный диагностический эксперимент. Пусть (M, Q_0) - заданный слабоинициальный автомат, где $M = (Q, X, Y, \delta, \lambda)$ и $Q_0 \subseteq Q$ $(|Q_0| = r \ge 2)$.

Рассмотрим источник

$$\mathbf{S}^{ad}_{(M,Q_0)} = (\mathbf{B}(k,r), X \times Y, Q_0, \mathbf{B}(k,1)),$$

где действие элементарного оператора $(x, y) \in X \times Y$ на ситуацию $\sigma \in \mathbf{B}(k,r)$ определяется в соответствии со следующим алгоритмом.

Алгоритм 3.4.

Шаг 1. Если $\lambda(q, x) \ne y$ для всех $q \in \sigma$, то $\sigma(x, y)$ не определено и конец, иначе переход к шагу 2.

Шаг 2. Если существуют такие состояния $q_1, q_2 \in \sigma$ $(q_1 \ne q_2)$, что

$$\delta(q_1, x) = \delta(q_2, x)$$

и

$$\lambda(q_1, x) = \lambda(q_2, x),$$

то $\sigma(x, y)$ не определено и конец, иначе переход к шагу 3.

Шаг 3. $\sigma(x, y) := \{\delta(q, x) \mid q \in \sigma \text{ и } \lambda(q, x) = y\}$ и конец.

Выберем $\le_{\mathbf{B}}$ в качестве отношение частичного порядка на множестве $\mathbf{B}(k,r)$.

Утверждение 3.12. Источник

$$\mathbf{S}^{ad}_{(M,Q_0)} = (\mathbf{B}(k,r), X \times Y, Q_0, \mathbf{B}(k,1))$$

является AM-источником.

Доказательство. Покажем, что для источника $\mathbf{S}^{ad}_{(M,Q_0)}$ условия 2.30-2.32. выполнены.

Условие 2.30 выполнено автоматически, так как множество $\mathbf{B}(k,1)$ состоит из минимальных элементов множества $\mathbf{B}(k,r)$.

Покажем, что выполнено условие 2.31.

Пусть $\sigma_1 \in \mathrm{Dom}\,(x,y)$ $((x,y) \in X \times Y)$ и $\sigma_2 \leq_{\mathbf{B}} \sigma_1$. Так как $\sigma_1 \in \mathrm{Dom}\,(x,y)$, то (см. алгоритм 3.4) *не существуют* такие состояния $q_1, q_2 \in \sigma_1$ $(q_1 \neq q_2)$, что $\delta(q_1,x) = \delta(q_2,x)$ и $\lambda(q_1,x) = \lambda(q_2,x)$. А так как $\sigma_2 \leq_{\mathbf{B}} \sigma_1$, т.е. $\sigma_2 \subseteq \sigma_1$, то *не существуют* такие состояния $q_1, q_2 \in \sigma_2$ $(q_1 \neq q_2)$, что $\delta(q_1,x) = \delta(q_2,x)$ и $\lambda(q_1,x) = \lambda(q_2,x)$. Из включения $\varnothing \neq \sigma_2 \subseteq \sigma_1$ вытекает, что

$$\varnothing \neq Y_{\sigma_2,x} = \{\lambda(q,x) \mid q \in \sigma_2\} \subseteq \{\lambda(q,x) \mid q \in \sigma_1\} = Y_{\sigma_1,x},$$

что и требовалось показать.

Покажем, что выполнено условие 2.32.

Пусть $\sigma_2 \leq_{\mathbf{B}} \sigma_1$. Так как $\sigma_2 \subseteq \sigma_1$, то (см. алгоритм 3.4) $\sigma_1 \in \mathrm{Dom}\,(x,y)$ и $\sigma_2 \in \mathrm{Dom}\,(x,y)$ для любого $y \in Y_{\sigma_2,x}$. Из включения $\sigma_2 \subseteq \sigma_1$ вытекает, что

$$\sigma_2(x,y) = \{\delta(q,x) \mid q \in \sigma_1 \text{ и } \lambda(q,x) = y\} \subseteq \{\delta(q,x) \mid q \in \sigma_1 \text{ и } \lambda(q,x) = y\} = \sigma_1(x,y),$$

Так как $\sigma_2(x,y) \subseteq \sigma_1(x,y)$, то $\sigma_2(x,y) \leq_{\mathbf{B}} \sigma_1(x,y)$, что и требовалось показать.

Утверждение доказано.

Индукцией по длине оператора доказывается следующее утверждение.

Утверждение 3.13. В AM-источнике

$$\mathbf{S}^{ad}_{(M,Q_0)} = (\mathbf{B}(k,r), X \times Y, Q_0, \mathbf{B}(k,1))$$

для любых ситуации $\sigma \in \mathbf{B}(k,r)$ и оператора $H = (x_1,y_1)\ldots(x_l,y_l) \in (X \times Y)^+$, если $\sigma \in \mathrm{Dom}\,H$, то справедливо равенство

$$\sigma H = \{\widetilde{\delta}(q, x_1 \ldots x_l) \mid q \in \sigma \text{ и } \widetilde{\lambda}(q, x_1 \ldots x_l) = y_1 \ldots y_l\}.$$

Из утверждения 3.13 вытекает, что адаптивное решение для AM-источника $\mathbf{S}^{ad}_{(M,Q_0)}$ (если оно существует) идентифицирует начальное состояние слабоинициального автомата (M,Q_0). Указанное решение (если оно существует) может быть построено методом, разработанным в п.2.5. Свернув дерево, представляющее адаптивное решение, в автомат Мура, получим автомат-экспериментатор, реализующий условный диагностический эксперимент с заданным слабоинициальным автоматом (M,Q_0).

Аналогичным образом могут быть построены и автоматы-экспериментаторы, реализующие условные эксперименты по идентификации автомата, принадлежащего заданному классу. В качестве примера можно привести автомат-экспериментатор, осуществляющий контроль правильности функционирования заданного автомата при наличии *сбоев*, предложенный в [50].

3.5. Представление автоматов группами.

Основной целью настоящего пункта является исследование представлений функций переходов и выходов автомата конечными группами. Актуальность такой постановки проблемы обусловлена следующими обстоятельствами.

Если рассматривать автомат как *абстрактную* систему, т.е. состоящую из трех *абстрактных* множеств (множество состояний, входной и выходной алфавиты) и двух *абстрактных* отображений (функции переходов и выходов), то диапазон возможных действий определяется методами, основанными исключительно на исчерпывающем поиске. В то же время автомат – это *алгебраическая система*. Детализация этой системы в терминах алгебраических структур дает возможность *арифметизировать* (или, более точно, *алгебраизировать*) вычисления, осуществляемые автоматом. Таким образом, во-первых, закладываются основы для классификации автоматов в зависимости от вычисляемых ими функций, а, во-вторых, открывается прямой путь для использования всего арсенала современной алгебры в процессе решения проблем теории автоматов. Отметим, что именно на основе такого подхода был выделен специальный (хотя и узкий, но фундаментальный) класс автоматов – *линейные последовательностные машины* (см., напр., [12]).

Существенное отличие предлагаемой постановки проблемы от классической (см., напр., [105-107]) состоит в следующем. В классическом случае исследование сосредоточено исключительно на свойствах входной полугруппы, а функции переходов и выходов – абстрактные отображения. В предлагаемой постановке автомат – это алгебраическая система, в которой функции переходов и выходов реализуются посредством *вычислений* в конечных группах (в дальнейшем в словосочетании *конечная группа* слово *конечная* будет опускаться).

Зафиксируем класс автоматов $\boldsymbol{A}_{kmn}$ $(k \ge 2, m \ge 1, n \ge 1)$. Пусть $\boldsymbol{G}_1 = (G_1, \circ)$ и $\boldsymbol{G}_2 = (G_2, \bullet)$ - заданные группы. Обозначим через $\boldsymbol{F}_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2)$ множество всех упорядоченных наборов из шести отображений

$$\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6),$$

где

$$\varphi_1 : Q_k \to G_1, \qquad \varphi_2 : X_m \to G_1, \qquad \varphi_3 : G_1 \to Q_k,$$

$$\varphi_4 : Q_k \to G_2, \qquad \varphi_5 : X_m \to G_2, \qquad \varphi_6 : G_2 \to Y_n.$$

Каждому набору $\Phi \in \boldsymbol{F}_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2)$ поставим в соответствие такой автомат

$$A_\Phi = (Q_k, X_m, Y_n, \delta_\Phi, \lambda_\Phi),$$

что

$$\delta_\Phi(q, x) = \varphi_3(\varphi_1(q) \circ \varphi_2(x)) \tag{3.67}$$

и

$$\lambda_\Phi(q, x) = \varphi_6(\varphi_4(q) \bullet \varphi_5(x)) \tag{3.68}$$

для всех $q \in Q_k$ и $x \in X_m$. Положим

$$\boldsymbol{A}_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2) = \{A_\Phi \mid \Phi \in \boldsymbol{F}_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2)\}.$$

Очевидно, что для любых групп $\boldsymbol{G}_1$ и $\boldsymbol{G}_2$ справедливо соотношение

$$\varnothing \ne \boldsymbol{A}_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2) \subseteq \boldsymbol{A}_{kmn}. \tag{3.69}$$

Определение 3.1. *Представлением* автомата

$$M = (Q_k, X_m, Y_n, \delta_M, \lambda_M) \in \boldsymbol{A}_{kmn}$$

группами $\boldsymbol{G}_1$ и $\boldsymbol{G}_2$ назовем такой упорядоченный набор отображений

$$\Phi_M = (\varphi_1^M, \varphi_2^M, \varphi_3^M, \varphi_4^M, \varphi_5^M, \varphi_6^M) \in \boldsymbol{F}_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2),$$

что

$$M = A_{\Phi_M}.$$

Из определения 3.1 вытекает, что если для автомата $M \in \mathbf{A}_{kmn}$ существует представление

$$\Phi_M = (\varphi_1^M, \varphi_2^M, \varphi_3^M, \varphi_4^M, \varphi_5^M, \varphi_6^M) \in \mathbf{F}_{kmn}(\mathbf{G}_1, \mathbf{G}_2),$$

то это представление удовлетворяет следующим четырем условиям:

Условие 3.7. Если существует такой входной символ $x \in X_m$, что

$$\delta_M(q_1, x) \neq \delta_M(q_2, x) \ \ (q_1, q_2 \in Q_k),$$

то

$$q_1 \not\equiv q_2 (\ker \varphi_1^M).$$

Условие 3.8. Если существует такой входной символ $x \in X_m$, что

$$\lambda_M(q_1, x) \neq \lambda_M(q_2, x) \ \ (q_1, q_2 \in Q_k),$$

то

$$q_1 \not\equiv q_2 (\ker \varphi_4^M).$$

Условие 3.9. Если существует такое состояние $q \in Q_k$, что

$$\delta_M(q, x_1) \neq \delta_M(q, x_2) \ \ (x_1, x_2 \in X_m),$$

то

$$x_1 \not\equiv x_2 (\ker \varphi_2^M).$$

Условие 3.10. Если существует такое состояние $q \in Q_k$, что

$$\lambda_M(q, x_1) \neq \lambda_M(q, x_2) \ \ (x_1, x_2 \in X_m),$$

то

$$x_1 \not\equiv x_2 (\ker \varphi_5^M).$$

Из условий 3.7-3-10 вытекает, что для любого автомата $A \in \mathbf{A}_{kmn}(\mathbf{G}_1, \mathbf{G}_2)$ число попарно различных как строк, так и столбцов:

1) *в таблице переходов* не превосходит $|G_1|$;
2) *в таблице выходов* не превосходит $|G_2|$.

Следующая теорема указывает конструктивный способ расширения множества представлений автоматов $M \in \mathbf{A}_{kmn}$.

Теорема 3.9. Если $\mathbf{G}_1^{(i)} = (G_1^{(i)}, \circ)$, $\mathbf{G}_2^{(i)} = (G_1^{(i)}, \bullet)$ $(i = 1,2)$ - такие группы, что

$$\mathbf{G}_j^{(1)} \le \mathbf{G}_j^{(2)} \quad (j = 1,2), \tag{3.70}$$

то

$$\mathbf{A}_{kmn}(\mathbf{G}_1^{(1)}, \mathbf{G}_2^{(1)}) \subseteq \mathbf{A}_{kmn}(\mathbf{G}_1^{(2)}, \mathbf{G}_2^{(2)}) \tag{3.71}$$

для всех $k \ge 2,\ m \ge 1$ и $n \ge 1$.

Доказательство. Пусть группы $\mathbf{G}_j^{(i)}$ $(i, j = 1,2)$ удовлетворяют условию (3.70). Зафиксируем значения $k \ge 2,\ m \ge 1$ и $n \ge 1$. Выберем произвольный автомат

$$A_\Phi = (Q_k, X_m, Y_n, \delta_\Phi, \lambda_\Phi) \in \mathbf{A}_{kmn}(\mathbf{G}_1^{(1)}, \mathbf{G}_2^{(1)}),$$

где

$$\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in \mathbf{F}_{kmn}(\mathbf{G}_1^{(1)}, \mathbf{G}_2^{(1)}).$$

Из (3.70) вытекает, что справедливы включения $G_j^{(1)} \subseteq G_j^{(2)}$ $(j = 1,2)$. Следовательно, существует такой упорядоченный набор отображений

$$\widetilde{\Phi} = (\widetilde{\varphi}_1, \widetilde{\varphi}_2, \widetilde{\varphi}_3, \widetilde{\varphi}_4, \widetilde{\varphi}_5, \widetilde{\varphi}_6) \in \mathbf{F}_{kmn}(\mathbf{G}_1^{(2)}, \mathbf{G}_2^{(2)}),$$

что:

1) $\widetilde{\varphi}_1(q) = \varphi_1(q)$ и $\widetilde{\varphi}_4(q) = \varphi_4(q)$ для всех $q \in Q_k$;
2) $\widetilde{\varphi}_2(x) = \varphi_2(x)$ и $\widetilde{\varphi}_5(x) = \varphi_5(x)$ для всех $x \in X_m$;
3) $\widetilde{\varphi}_3\big|_{G_1^{(1)}} = \varphi_3$ и $\widetilde{\varphi}_6\big|_{G_2^{(1)}} = \varphi_6$.

Рассмотрим автомат

$$A_{\widetilde{\Phi}} = (Q_k, X_m, Y_n, \delta_{\widetilde{\Phi}}, \lambda_{\widetilde{\Phi}}) \in \mathbf{A}_{kmn}(\mathbf{G}_1^{(2)}, \mathbf{G}_2^{(2)}).$$

Из (3.67) и (3.68) вытекает, что для всех $q \in Q_k$ и $x \in X_m$

$$\delta_{\widetilde{\Phi}}(q, x) = \widetilde{\varphi}_3(\widetilde{\varphi}_1(q) \circ \widetilde{\varphi}_2(x)) = \widetilde{\varphi}_3(\varphi_1(q) \circ \varphi_2(x))$$

и

$$\lambda_{\widetilde{\Phi}}(q, x) = \widetilde{\varphi}_6(\widetilde{\varphi}_4(q) \bullet \widetilde{\varphi}_5(x)) = \widetilde{\varphi}_6(\varphi_4(q) \bullet \varphi_5(x)).$$

А так как $\mathbf{G}_1^{(1)}$ и $\mathbf{G}_2^{(1)}$ - группы, то

$$\varphi_1(q), \varphi_2(x) \in G_1^{(1)} \Rightarrow \varphi_1(q) \circ \varphi_2(x) \in G_1^{(1)}$$

и

$$\varphi_4(q), \varphi_5(x) \in G_2^{(1)} \Rightarrow \varphi_4(q) \bullet \varphi_5(x) \in G_2^{(1)}.$$

Поэтому, для всех $q \in Q_k$ и $x \in X_m$

$$\delta_{\widetilde{\Phi}}(q, x) = (\widetilde{\varphi}_3\big|_{G_1^{(1)}})(\varphi_1(q) \circ \varphi_2(x)) = \varphi_3(\varphi_1(q) \circ \varphi_2(x)) = \delta_\Phi(q, x)$$

и

$$\lambda_{\widetilde{\Phi}}(q, x) = (\widetilde{\varphi}_6\big|_{G_2^{(1)}})(\varphi_4(q) \bullet \varphi_5(x)) = \varphi_6(\varphi_4(q) \bullet \varphi_5(x)) = \lambda_\Phi(q, x).$$

Это означает, что $A_\Phi = A_{\widetilde{\Phi}}$. Так как для каждого автомата $A_\Phi \in \mathbf{A}_{kmn}(\mathbf{G}_1^{(1)}, \mathbf{G}_2^{(1)})$ существует равный ему автомат $A_{\widetilde{\Phi}} \in \mathbf{A}_{kmn}(\mathbf{G}_1^{(2)}, \mathbf{G}_2^{(2)})$, то включение (3.71) – истинное.

Теорема доказана.

Следствие 3.9. Если $\{\mathbf{G}_1^{(j)} \mid j \in \mathbf{N}\}$ и $\{\mathbf{G}_2^{(j)} \mid j \in \mathbf{N}\}$ - такие последовательности групп, что

$$\mathbf{G}_j^{(1)} \le \mathbf{G}_j^{(2)} \le \ldots \le \mathbf{G}_j^{(i)} \le \ldots \quad (j = 1,2),$$

то

$$\varnothing \ne \mathbf{A}_{kmn}(\mathbf{G}_1^{(1)}, \mathbf{G}_2^{(1)}) \subseteq \mathbf{A}_{kmn}(\mathbf{G}_1^{(2)}, \mathbf{G}_2^{(2)}) \subseteq \ldots \subseteq \mathbf{A}_{kmn}(\mathbf{G}_1^{(i)}, \mathbf{G}_2^{(i)}) \subseteq \ldots \subseteq \mathbf{A}_{kmn}. \quad (3.72)$$

Доказательство. Истинность включений (3.72) вытекает из (3.69), (3.71) и транзитивности отношения включения.

Следствие доказано.

Обозначим через $\boldsymbol{Z}_l = (\mathbf{Z}_l, +)$ $(l \geq 2)$ аддитивную группу вычетов по модулю l. Следующая теорема показывает, что верхняя граница в (3.72) - достижимая.

Теорема 3.10. Пусть $k \geq 2, m \geq 1$ и $n \geq 1$ - фиксированные числа. Если $\boldsymbol{G}_1 = (G_1, \circ)$ и $\boldsymbol{G}_2 = (G_2, \bullet)$ - такие группы, что

$$\boldsymbol{Z}_{l_i} \leq \boldsymbol{G}_i \quad (i = 1,2), \tag{3.73}$$

где

$$\min\{l_1, l_2\} \geq km, \tag{3.74}$$

то истинно равенство

$$\boldsymbol{A}_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2) = \boldsymbol{A}_{kmn}. \tag{3.75}$$

Доказательство. Из (3.73) вытекает (см. теорему 3.9), что

$$\boldsymbol{A}_{kmn}(\boldsymbol{Z}_{l_1}, \boldsymbol{Z}_{l_2}) \subseteq \boldsymbol{A}_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2) \tag{3.76}$$

Покажем, что из (3.74) вытекает истинность включения

$$\boldsymbol{A}_{kmn} \subseteq \boldsymbol{A}_{kmn}(\boldsymbol{Z}_{l_1}, \boldsymbol{Z}_{l_2}). \tag{3.77}$$

Выберем произвольный автомат $M = (Q_k, X_m, Y_n, \delta_M, \lambda_M) \in \boldsymbol{A}_{kmn}$. Из (3.74) вытекает, что существует такой набор отображений

$$\Phi_M = (\varphi_1^M, \varphi_2^M, \varphi_3^M, \varphi_4^M, \varphi_5^M, \varphi_6^M) \in \mathbf{F}_{kmn}(\boldsymbol{Z}_{l_1}, \boldsymbol{Z}_{l_2}),$$

что:

1) $\varphi_1^M(q_i) = \varphi_4^M(q_i) = i - 1$ для всех $i \in \{1, \ldots, k\}$;
2) $\varphi_2^M(x_j) = \varphi_5^M(x_j) = (j-1)k$ для всех $j \in \{1, \ldots, m\}$;
3) для отображений $\varphi_3^M : \mathbf{Z}_{l_1} \to Q_k$ и $\varphi_6^M : \mathbf{Z}_{l_2} \to Y_n$ при всех $h \in \{0, 1, \ldots, km-1\}$ истинны равенства

$$\varphi_3^M(h) = \delta_M(q_{R_k(h)+1}, x_{\lfloor hk^{-1} \rfloor + 1})$$

и

$$\varphi_6^M(h) = \lambda_M(q_{R_k(h)+1}, x_{\lfloor hk^{-1} \rfloor + 1}),$$

где $R_b(a)$ - остаток от деления a на b.

Рассмотрим автомат

$$A_{\Phi_M} = (Q_k, X_m, Y_n, \delta_{\Phi_M}, \lambda_{\Phi_M}) \in \boldsymbol{A}_{kmn}(\boldsymbol{Z}_{l_1}, \boldsymbol{Z}_{l_2}).$$

Из (3.67) и (3.68) вытекает, что для всех $q_i \in Q_k$ и $x_j \in X_m$

$$\delta_{\Phi_M}(q_i, x_j) = \varphi_3^M(\varphi_1^M(q_i) + \varphi_2^M(x_j)) = \varphi_3^M(i - 1 + (j-1)k)$$

и

$$\lambda_{\Phi_M}(q_i, x_j) = \varphi_6^M(\varphi_4^M(q_i) + \varphi_5^M(x_j)) = \varphi_6^M(i - 1 + (j-1)k).$$

Так как $i \in \{1, \ldots, k\}$, то $R_k(i - 1 + (j-1)k) = i - 1$ и $\lfloor (i - 1 + (j-1)k)k^{-1} \rfloor = j - 1$. Следовательно, для всех $q_i \in Q_k$ и $x_j \in X_m$

$$\delta_{\Phi_M}(q_i, x_j) = \delta_M(q_{(i-1)+1}, x_{(j-1)+1}) = \delta_M(q_i, x_j)$$

и

$$\lambda_{\Phi_M}(q_i, x_j) = \lambda_M(q_{(i-1)+1}, x_{(j-1)+1}) = \lambda_M(q_i, x_j),$$

т.е. $M = A_{\Phi_M}$.

Итак, для каждого автомата $M \in \mathbf{A}_{kmn}$ существует такой автомат $A_{\Phi_M} \in \mathbf{A}_{kmn}(\mathbf{Z}_{l_1}, \mathbf{Z}_{l_2})$, что $M = A_{\Phi_M}$. Следовательно, включение (3.77) – истинное, что и требовалось показать.

Из включений (3.76) и (3.77) вытекает, что

$$\mathbf{A}_{kmn} \subseteq \mathbf{A}_{kmn}(\mathbf{G}_1, \mathbf{G}_2). \tag{3.78}$$

Включения (3.69) и (3.78) доказывают, что равенство (3.75) – истинное.

Теорема доказана.

Из (3.67) и (3.68) вытекает, что для любых групп $\mathbf{G}_1$ и $\mathbf{G}_2$ представление Φ_M автомата $M \in \mathbf{A}_{kmn}$ на каждом такте осуществляет вычисления по схеме:

кодирование $\rightarrow$ *групповая операция* $\rightarrow$ *декодирование.*

Такая схема не удобна при работе с расширениями функций переходов и выходов на множество $Q_k \times X_m^*$. Поэтому естественно потребовать, чтобы для функции переходов кодирование осуществлялось только в начале функционирования, а декодирование – только в его конце. Выделим класс представлений, удовлетворяющих этому требованию.

Определение 3.2. Представление $\Phi_M = (\varphi_1^M, \varphi_2^M, \varphi_3^M, \varphi_4^M, \varphi_5^M, \varphi_6^M) \in \mathbf{F}_{kmn}(\mathbf{G}_1, \mathbf{G}_2)$ автомата $M \in \mathbf{A}_{kmn}$ группами $\mathbf{G}_1$ и $\mathbf{G}_2$ назовем согласованным с функцией переходов, если для всех $q \in Q_k$ и $p \in X_m^*$

$$\tilde{\delta}_{\Phi_M}(q, p) = \varphi_3^M(\varphi_1^M(q) \circ \tilde{\varphi}_2^M(p)),$$

где $\tilde{\varphi}_2^M$ - расширение отображения φ_2^M на множество X_m^*.

Обозначим через $\mathbf{F}_{kmn}^c(\mathbf{G}_1, \mathbf{G}_2)$ множество всех представлений $\Phi \in \mathbf{F}_{kmn}(\mathbf{G}_1, \mathbf{G}_2)$, согласованных с функцией переходов. Следующая теорема устанавливает критерий принадлежности отображения $\Phi \in \mathbf{F}_{kmn}(\mathbf{G}_1, \mathbf{G}_2)$ множеству $\mathbf{F}_{kmn}^c(\mathbf{G}_1, \mathbf{G}_2)$.

Теорема 3.11. Для любых групп $\mathbf{G}_1 = (G_1, \circ)$ и $\mathbf{G}_2 = (G_2, \bullet)$ представление $\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in \mathbf{F}_{kmn}(\mathbf{G}_1, \mathbf{G}_2)$ согласовано с функцией переходов тогда и только тогда, когда существует такое расширение $\tilde{\varphi}_2$ отображения $\varphi_2 : X_m \rightarrow G_1$ на множество X_m^*, что для всех $q \in Q_k$, $p \in X_m^*$ и $x \in X_m$ истинны равенства

$$\varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(px)) = \varphi_3(\varphi_1(\varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(p))) \circ \varphi_2(x)), \tag{3.79}$$

$$\varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(\Lambda)) = q. \tag{3.80}$$

Доказательство. Пусть $\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in \mathbf{F}_{kmn}(\mathbf{G}_1, \mathbf{G}_2)$. Из определения автомата $A_\Phi = (Q_k, X_m, Y_n, \delta_\Phi, \lambda_\Phi)$ вытекает, что для всех $q \in Q_k$, $p \in X_m^*$ и $x \in X_m$ истинны равенства

$$\tilde{\delta}_\Phi(q,x) = \varphi_3(\varphi_1(q) \circ \varphi_2(x)), \tag{3.81}$$

$$\tilde{\delta}_\Phi(q,\Lambda) = q, \tag{3.82}$$

$$\tilde{\delta}_\Phi(q,px) = \tilde{\delta}_\Phi(\tilde{\delta}_\Phi(q,p),x). \tag{3.83}$$

Из определения 3.2 вытекает, что $\Phi \in \mathbf{F}^c_{kmn}(\mathbf{G}_1,\mathbf{G}_2)$ тогда и только тогда, когда для всех $q \in Q_k$ и $p \in X^*_m$ истинно равенство

$$\tilde{\delta}_\Phi(q,p) = \varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(p)). \tag{3.84}$$

Из (3.81)-(3.84) вытекает, что $\Phi \in \mathbf{F}^c_{kmn}(\mathbf{G}_1,\mathbf{G}_2)$ тогда и только тогда, когда для всех $q \in Q_k$, $p \in X^*_m$ и $x \in X_m$ истинны равенства

$$q = \tilde{\delta}_\Phi(q,\Lambda) = \varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(\Lambda)),$$

$$\varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(px)) = \tilde{\delta}_\Phi(q,px) = \tilde{\delta}_\Phi(\tilde{\delta}_\Phi(q,p),x) = \tilde{\delta}_\Phi(\varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(p)),x) =$$

$$= \varphi_3(\varphi_1(\varphi_3(\varphi_1(q) \circ \tilde{\varphi}_2(p))) \circ \varphi_2(x)),$$

т.е. когда истинны равенства (3.79) и (3.80), что и требовалось доказать.

Теорема доказана.

В теореме 3.11, с одной стороны, найдены необходимые и достаточные условия, при которых тройка отображений $(\varphi_1,\varphi_2,\varphi_3)$ может быть использована для построения представления $\Phi \in \mathbf{F}^c_{kmn}(\mathbf{G}_1,\mathbf{G}_2)$, а, с другой стороны, описана структура отображений φ_2, допустимых для представлений $\Phi \in \mathbf{F}^c_{kmn}(\mathbf{G}_1,\mathbf{G}_2)$. Это описание дано через свойства расширения $\tilde{\varphi}_2$ отображения φ_2, определяемые равенствами (3.79) и (3.80). Исследуем структуру отображений φ_1 и φ_3, допустимых для представлений $\Phi \in \mathbf{F}^c_{kmn}(\mathbf{G}_1,\mathbf{G}_2)$.

Утверждение 3.14. Если $\Phi = (\varphi_1,\varphi_2,\varphi_3,\varphi_4,\varphi_5,\varphi_6) \in \mathbf{F}^c_{kmn}(\mathbf{G}_1,\mathbf{G}_2)$ $(\mathbf{G}_1 = (G_1,\circ))$, то $\varphi_1 : Q_k \to G_1$ - инъективное отображение.

Доказательство. Пусть $\Phi = (\varphi_1,\varphi_2,\varphi_3,\varphi_4,\varphi_5,\varphi_6) \in \mathbf{F}^c_{kmn}(\mathbf{G}_1,\mathbf{G}_2)$. Из теоремы 3.11 (см. равенство (3.80)) вытекает, что для всех $q_1,q_2 \in Q_k$

$$\varphi_3(\varphi_1(q_i) \circ \tilde{\varphi}_2(\Lambda)) = q_i \quad (i = 1,2). \tag{3.85}$$

Предположим, что $q_1 \equiv q_2(\ker\varphi_1)$, т.е. $\varphi_1(q_1) = \varphi_1(q_2)$. Из (3.85) вытекает, что

$$q_1 = \varphi_3(\varphi_1(q_1) \circ \tilde{\varphi}_2(\Lambda)) = \varphi_3(\varphi_1(q_2) \circ \tilde{\varphi}_2(\Lambda)) = q_2.$$

Таким образом, показано, что для всех $q_1,q_2 \in Q_k$

$$q_1 \equiv q_2(\ker\varphi_1) \Rightarrow q_1 = q_2, \tag{3.86}$$

что и требовалось показать.

Утверждение доказано.

Следствие 3.10. Для любой группы $\mathbf{G}_1 = (G_1, \circ)$ порядка меньшего, чем k

$$\mathbf{F}^c_{kmn}(\mathbf{G}_1, \mathbf{G}_2) = \varnothing .$$

Доказательство. Условие инъективности отображения φ_1 может быть выполнено тогда и только тогда, когда $|G_1| \geq k$.

Следствие доказано.

Утверждение 3.15. Если $\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in \mathbf{F}^c_{kmn}(\mathbf{G}_1, \mathbf{G}_2)$ $(\mathbf{G}_1 = (G_1, \circ))$, то $\varphi_3 : G_1 \to Q_k$ - сюръективное отображение.

Доказательство. Пусть $\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in \mathbf{F}^c_{kmn}(\mathbf{G}_1, \mathbf{G}_2)$. По определению отображения φ_3 включение $\mathrm{Val}\,\varphi_3 \subseteq Q_k$ - истинное. Из теоремы 3.11 (см. равенство (3.80)) вытекает, что

$$\varphi_3(\varphi_1(q) \circ \widetilde{\varphi}_2(\Lambda)) = q$$

для всех $q \in Q_k$. Так как $q \in \mathrm{Val}\,\varphi_3$ для всех $q \in Q_k$, то $Q_k \subseteq \mathrm{Val}\,\varphi_3$. Из включений $\mathrm{Val}\,\varphi_3 \subseteq Q_k$ и $Q_k \subseteq \mathrm{Val}\,\varphi_3$ вытекает, что $\mathrm{Val}\,\varphi_3 = Q_k$, что и требовалось показать.

Утверждение доказано.

Утверждение 3.16. Если $\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in \mathbf{F}^c_{kmn}(\mathbf{G}_1, \mathbf{G}_2)$ $(\mathbf{G}_1 = (G_1, \circ))$, то $\varphi_3\big|_{(\mathrm{Val}\,\varphi_1)\circ\widetilde{\varphi}_2(\Lambda)}$ - инъективное отображение.

Доказательство. Пусть $\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in \mathbf{F}^c_{kmn}(\mathbf{G}_1, \mathbf{G}_2)$. Тогда (см. утверждение 3.14) φ_1 - инъективное отображение. Следовательно, $|\mathrm{Val}\,\varphi_1| = |Q_k| = k$. Так как $\mathbf{G}_1$ - группа, то

$$|(\mathrm{Val}\,\varphi_1) \circ \widetilde{\varphi}_2(\Lambda)| = |\mathrm{Val}\,\varphi_1| = k .$$

Так как (см. равенство (3.80)) $\varphi_3(\varphi_1(q) \circ \widetilde{\varphi}_2(\Lambda)) = q$ для всех $q \in Q_k$, то

$$\mathrm{Val}(\varphi_3\big|_{(\mathrm{Val}\,\varphi_1)\circ\widetilde{\varphi}_2(\Lambda)}) = Q_k .$$

Итак, показано, что $\varphi_3\big|_{(\mathrm{Val}\,\varphi_1)\circ\widetilde{\varphi}_2(\Lambda)}$ - отображение k-элементного множества $(\mathrm{Val}\,\varphi_1) \circ \widetilde{\varphi}_2(\Lambda)$ на k-элементное множество Q_k, т.е. $\varphi_3\big|_{(\mathrm{Val}\,\varphi_1)\circ\widetilde{\varphi}_2(\Lambda)}$ - инъективное отображение, что и требовалось показать.

Утверждение доказано.

В силу следствия 3.10 $\mathbf{F}^c_{kmn}(\mathbf{G}_1, \mathbf{G}_2) = \varnothing$ для любой группы $\mathbf{G}_1 = (G_1, \circ)$ порядка меньшего, чем k. Следующая теорема показывает, что именно число k является таким наименьшим значением порядка группы $\boldsymbol{G}_1$, что множество $\mathbf{F}^c_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2)$ может быть непустым.

Теорема 3.12. Для всех $k \geq 2$ и $m \geq 1$ существуют такие группы $\boldsymbol{G}_1$ порядка k, что

$$\mathbf{F}^c_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2) \neq \varnothing .$$

Доказательство. Зафиксируем числа $k \geq 2$ и $m \geq 1$. Выберем в качестве группы $\boldsymbol{G}_1$ аддитивную группу $\boldsymbol{Z}_k = (\mathbf{Z}_k, +)$ вычетов по модулю k. Выберем такое представление

$$\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in \mathbf{F}_{kmn}(\boldsymbol{Z}_k, \boldsymbol{G}_2),$$

что:

1) $\varphi_1(q_i) = i - 1$ для всех $i = 1, \ldots, k$;
2) $\varphi_2(x) = 0$ для всех $x \in X_m$;
3) $\varphi_3(j) = q_{j+1}$ для всех $j = 0, 1, \ldots, k-1$.

Определим расширение $\widetilde{\varphi}_2$ отображения φ_2 на множество X^*_m равенством

$$\widetilde{\varphi}_2(p) = 0 \quad (p \in X^*_m).$$

Для всех $q_i \in Q_k$, $p \in X^*_m$ и $x \in X_m$

$$\varphi_3(\varphi_1(q_i) + \widetilde{\varphi}_2(px)) = \varphi_3((i-1)+0) = \varphi_3(i-1) = q_{(i-1)+1} = q_i$$

и

$$\varphi_3(\varphi_1(\varphi_3(\varphi_1(q_i) + \widetilde{\varphi}_2(p))) + \varphi_2(x)) = \varphi_3(\varphi_1(\varphi_3((i-1)+0)) + 0) =$$

$$= \varphi_3(\varphi_1(\varphi_3(i-1))) = \varphi_3(\varphi_1(q_{(i-1)+1})) = \varphi_3(\varphi_1(q_i)) = \varphi_3(i-1) = q_i,$$

т.е.

$$\varphi_3(\varphi_1(q_i) + \widetilde{\varphi}_2(px)) = \varphi_3(\varphi_1(\varphi_3(\varphi_1(q_i) + \widetilde{\varphi}_2(p))) + \varphi_2(x)).$$

Кроме того, для всех $q_i \in Q_k$

$$\varphi_3(\varphi_1(q_i) + \widetilde{\varphi}_2(\Lambda)) = \varphi_3((i-1)+0) = \varphi_3(i-1) = q_i.$$

Итак, показано, что для всех $q_i \in Q_k$, $p \in X^*_m$ и $x \in X_m$ равенства (3.79) и (3.80) - истинные. Следовательно, $\Phi = (\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6) \in \mathbf{F}^c_{kmn}(\boldsymbol{Z}_k, \boldsymbol{G}_2)$, т.е. $\mathbf{F}^c_{kmn}(\boldsymbol{Z}_k, \boldsymbol{G}_2) \neq \varnothing$, что и требовалось доказать.

Теорема доказана.

Множество $\mathbf{F}^c_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2)$ всех представлений, согласованных с функцией переходов естественно приводит к подмножеству

$$\boldsymbol{A}^c_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2) = \{A_\Phi \in \boldsymbol{A}_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2) \mid \Phi \in \mathbf{F}^c_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2)\}$$

множества автоматов $\boldsymbol{A}_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2)$. Исследуем структуру автоматов, принадлежащих множеству $\boldsymbol{A}^c_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2)$.

Теорема 3.13. Пусть $\boldsymbol{G}_1 = (G_1, \circ)$ - группа порядка k. Если

$$\Phi = (\varphi_1, \ldots, \varphi_6) \in \boldsymbol{F}^c_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2),$$

то автомат A_Φ состоит из $\dfrac{k}{|\operatorname{Val}\widetilde{\varphi}_2|}$ компонент сильной связанности, каждая из которых содержит $|\operatorname{Val}\widetilde{\varphi}_2|$ состояний.

Доказательство. Пусть $\boldsymbol{G}_1 = (G_1, \circ)$ - группа порядка k и $\Phi \in \boldsymbol{F}^c_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2)$.

Рассмотрим автомат $A_\Phi = (Q_k, X_m, Y_n, \delta_\Phi, \lambda_\Phi)$. Выберем произвольное состояние $q \in Q_k$. Обозначим через S_q множество всех состояний, достижимых из состояния q, т.е.

$$S_q = \{\widetilde{\delta}_\Phi(q, p) \mid p \in X_m^*\}.$$

Так как $\Phi \in \boldsymbol{F}^c_{kmn}(\boldsymbol{G}_1, \boldsymbol{G}_2)$, то (см. определение 3.2)

$$S_q = \{\varphi_3(\varphi_1(q) \circ \widetilde{\varphi}_2(p)) \mid p \in X_m^*\}. \tag{3.86}$$

А так как (см. утверждение 3.14) φ_1 - инъективное отображение k-элементного множества Q_k в k-элементное множество G_1, то φ_1 - сюръективное отображение, т.е. $\operatorname{Val}\varphi_1 = G_1$. Так как $\boldsymbol{G}_1$ - группа, то

$$(\operatorname{Val}\varphi_1) \circ \widetilde{\varphi}_2(\Lambda) = G_1 \circ \widetilde{\varphi}_2(\Lambda) = G_1 \tag{3.87}$$

и

$$|\varphi_1(q) \circ (\operatorname{Val}\widetilde{\varphi}_2)| = |\operatorname{Val}\widetilde{\varphi}_2|. \tag{3.88}$$

Следовательно, (см. утверждения 3.15 и 3.16), $\varphi_3\big|_{(\operatorname{Val}\varphi_1)\circ\widetilde{\varphi}_2(\Lambda)} = \varphi_3\big|_{G_1} = \varphi_3$ - биективное отображение множества G_1 на множество Q_k, откуда вытекает, что

$$|S_q| = |\operatorname{Val}\widetilde{\varphi}_2| \quad (q \in Q_k). \tag{3.89}$$

Покажем, что множество S_q $(q \in Q_k)$ является компонентой сильной связанности автомата A_Φ.

Пусть $q_1 \in S_q$ и $p \in X_m^*$ - такое входное слово, что $\widetilde{\delta}_\Phi(q, p) = q_1$. Тогда

$$S_{q_1} = \{\widetilde{\delta}_\Phi(q_1, p_1) \mid p_1 \in X_m^*\} = \{\widetilde{\delta}_\Phi(q, pp_1) \mid p_1 \in X_m^*\} \subseteq S_q.$$

Покажем, что $S_q \subseteq S_{q_1}$. Для этого достаточно показать, что состояние q достижимо из состояния q_1.

Предположим противное, т.е. что состояние q не достижимо из состояния q_1. Так как (см. равенство (3.89)) $|S_{q_1}| = |\operatorname{Val}\widetilde{\varphi}_2| = |S_q|$, то существует такое состояние

$q_2 \in Q_k$, что $q_2 \in S_{q_1}$ и $q_2 \notin S_q$. Пусть $p_2 \in X_m^*$ - такое входное слово, что $\widetilde{\delta}_\Phi(q_1, p_2) = q_2$. Тогда

$$\widetilde{\delta}_\Phi(q, pp_2) = \widetilde{\delta}_\Phi(\widetilde{\delta}_\Phi(q, p), p_2) = \widetilde{\delta}_\Phi(q_1, p_2) = q_2,$$

т.е. $q_2 \in S_q$. Полученное противоречие показывает, что предположение – ложное. Следовательно, $q \in S_{q_1}$, что и требовалось показать.

Из включений $S_{q_1} \subseteq S_q$ и $S_q \subseteq S_{q_1}$ вытекает, что $S_{q_1} = S_q$ для всех $q_1 \in S_q$. Последнее утверждение эквивалентно утверждению о том, что S_q $(q \in Q)$ - компонента сильной связанности автомата A_Φ, что и требовалось показать.

Каждая компонента сильной связанности S_q $(q \in Q)$ автомата A_Φ содержит $|\operatorname{Val}\widetilde{\varphi}_2|$ состояний. Следовательно, количество компонент сильной связанности автомата A_Φ равно

$$\frac{|Q_k|}{|\operatorname{Val}\widetilde{\varphi}_2|} = \frac{k}{|\operatorname{Val}\widetilde{\varphi}_2|},$$

что и требовалось показать.

Теорема доказана.

До сих пор предполагалось, что $\widetilde{\varphi}_2 : X_m^* \to G_1$ - произвольное отображение, удовлетворяющее равенствам (3.79) и (3.80). Особый интерес представляет случай, когда $\widetilde{\varphi}_2 : X_m^* \to G_1$ - гомоморфизм свободной полугруппы $\boldsymbol{X}_m = (X_m^*, \cdot)$ (где '$\cdot$' – операция конкатенации слов) в группу $\boldsymbol{G}_1$. Известно, что каждое отображение $\varphi_2 : X_m \to G_1$ единственным образом продолжается до гомоморфизма $\widetilde{\varphi}_2$ свободной полугруппы $\boldsymbol{X}_m$ в группу $\boldsymbol{G}_1$ с помощью равенств:

$$\widetilde{\varphi}_2(\Lambda) = 1_{G_1}, \tag{3.90}$$

$$\widetilde{\varphi}_2(px) = \widetilde{\varphi}_2(p) \circ \varphi_2(x) \quad (p \in X_m^*, x \in X_m). \tag{3.91}$$

Исследуем условия, при которых для представлений, согласованных с функцией переходов, отображение φ_2 может быть продолжено до гомоморфизма $\widetilde{\varphi}_2$ свободной полугруппы $\boldsymbol{X}_m$ в группу $\boldsymbol{G}_1$.

Утверждение 3.17. Пусть $\Phi = (\varphi_1, \ldots, \varphi_6) \in \boldsymbol{F}_{kmn}^c(\boldsymbol{G}_1, \boldsymbol{G}_2)$. Отображение

$$\varphi_2 : X_m \to G_1$$

может быть так продолжено до отображения

$$\widetilde{\varphi}_2 : X_m^* \to G_1,$$

что

$$\widetilde{\varphi}_2(\Lambda) = 1_{G_1}$$

тогда и только тогда, когда $\varphi_3\varphi_1 : Q_k \to Q_k$ - тождественное отображение.

Доказательство. Пусть $\Phi = (\varphi_1, \ldots, \varphi_6) \in \boldsymbol{F}_{kmn}^c(\boldsymbol{G}_1, \boldsymbol{G}_2)$.

Предположим, что отображение φ_2 может быть так продолжено до отображения $\widetilde{\varphi}_2$, что $\varphi_2(\Lambda) = 1_{G_1}$. Так как $\Phi \in \boldsymbol{F}_{kmn}^c(\boldsymbol{G}_1, \boldsymbol{G}_2)$, то (см. равенство (3.80))

$$q=\varphi_3(\varphi_1(q)\circ\widetilde{\varphi}_2(\Lambda))=\varphi_3(\varphi_1(q)\circ 1_{G_1})=\varphi_3(\varphi_1(q))=(\varphi_3\varphi_1)(q)$$

для всех $q\in Q_k$. Следовательно, $\varphi_3\varphi_1$ - тождественное отображение множества Q_k на себя, что и требовалось показать.

Предположим теперь, что $\varphi_3\varphi_1$ - тождественное отображение множества Q_k на себя, а $\hat{\varphi}$ - произвольное расширение отображения φ_2 на множество X_m^*, удовлетворяющее равенствам (3.79) и (3.80). Рассмотрим расширение $\widetilde{\varphi}_2 : X_m^* \to G_1$ отображения φ_2, определяемое следующим образом:

$$\widetilde{\varphi}_2(p)=\begin{cases}\hat{\varphi}(p)\,, & \text{если } p\in X_m^+,\\ 1_{G_1}\,, & \text{если } p=\Lambda\end{cases}.$$

Так как $\varphi_3\varphi_1$ - тождественное отображение, то

$$\varphi_3(\varphi_1(q)\circ\widetilde{\varphi}_2(\Lambda))=\varphi_3(\varphi_1(q)\circ 1_{G_1})=\varphi_3(\varphi_1(q))=(\varphi_3\varphi_1)(q)=q$$

для всех $q\in Q_k$, т.е. для расширения $\widetilde{\varphi}_2$ равенство (3.80) – истинное. А так как для расширения $\hat{\varphi}$ равенство (3.79) – истинное, то и для расширения $\widetilde{\varphi}_2$ равенство (3.79) – истинное. Следовательно, отображение φ_2 может быть так продолжено до отображения $\widetilde{\varphi}_2 : X_m^* \to G_1$, что $\widetilde{\varphi}_2(\Lambda)=1_{G_1}$, что и требовалось показать.

Утверждение доказано.

Теорема 3.14. Если для представления $\Phi=(\varphi_1,\ldots,\varphi_6)\in \mathbf{F}_{kmn}^c(\boldsymbol{G}_1,\boldsymbol{G}_2)$:

$$\widetilde{\varphi}_2(\Lambda)=1_{G_1} \tag{3.92}$$

$$(\operatorname{Val}\varphi_1)\circ(\operatorname{Val}\widetilde{\varphi}_2)=\operatorname{Val}\varphi_1\,, \tag{3.93}$$

то расширение $\widetilde{\varphi}_2 : X_m^* \to G_1$ отображения $\varphi_2 : X_m \to G_1$ является гомоморфизмом свободной полугруппы $\boldsymbol{X}_m$ в группу $\boldsymbol{G}_1$.

Доказательство. Пусть $\Phi=(\varphi_1,\ldots,\varphi_6)\in \mathbf{F}_{kmn}^c(\boldsymbol{G}_1,\boldsymbol{G}_2)$ и равенства (3.92) и (3.93) – истинные. Так как равенство (3.92) совпадает с равенством (3.90), то достаточно показать, что равенство (3.91) – истинное.

Так как (см. утверждение 3.17), $\varphi_3\varphi_1 : Q_k \to Q_k$ - тождественное отображение и (см. утверждение 3.16) $\varphi_3\big|_{(\operatorname{Val}\varphi_1)\circ\widetilde{\varphi}_2(\Lambda)}=\varphi_3\big|_{(\operatorname{Val}\varphi_1)\circ 1_{G_1}}=\varphi_3\big|_{\operatorname{Val}\varphi_1}$ - инъективное отображение, то $(\varphi_1\varphi_3)\big|_{\operatorname{Val}\varphi_1}$ - тождественное отображение. Поэтому (см. равенство (3.79))

$$\varphi_1(q)\circ\widetilde{\varphi}_2(px)=(\varphi_1(q)\circ\widetilde{\varphi}_2(p))\circ\varphi_2(x)=\varphi_1(q)\circ(\widetilde{\varphi}_2(p)\circ\varphi_2(x))\,.$$

Так как $\boldsymbol{G}_1$ - группа, то из последнего равенства вытекает, что

$$\widetilde{\varphi}_2(px)=\widetilde{\varphi}_2(p)\circ\varphi_2(x)$$

для всех $p\in X_m^*$ и $x\in X_m$, что и требовалось показать.

Таким образом, для расширения $\widetilde{\varphi}_2$ равенства (3.90) и (3.91) – истинные. Следовательно, $\widetilde{\varphi}_2$ - гомоморфизм свободной полугруппы $\boldsymbol{X}_m$ в группу $\boldsymbol{G}_1$.

Теорема доказана.

Из теоремы 3.13 вытекает, что если порядок группы $\boldsymbol{G}_1$ равен k, то множество $\boldsymbol{A}_{kmn}^c(\boldsymbol{G}_1, \boldsymbol{G}_2)$ состоит из перестановочных автоматов, у которых все компоненты сильной связанности имеют одно и то же число состояний. Естественно возникает проблема представления элементов множества $\boldsymbol{A}_{kmn}^c(\boldsymbol{G}_1, \boldsymbol{G}_2)$ композицией автоматов, у которых множество состояний наделено структурой хорошо изученных групп. Приведем схематическое решение этой задачи для важного специального случая, когда $m = 1$, т.е. для автономных автоматов. Для упрощения обозначений (что, очевидно, ни в коей мере не влияет на общность рассуждений) будем рассматривать автоматы без выхода.

Автомат

$$C(k) = (\mathbf{Z}_k, \{x\}, \delta_k) \ \ (k \geq 2)$$

назовем *счетчиком*, если

$$\delta_k(z, x) = z + 1 \pmod{k}$$

для всех $z \in \mathbf{Z}_k$. С каждой конечной последовательностью счетчиков $C(k_1), \ldots, C(k_n)$ сопоставим автомат

$$\zeta(C(k_1), \ldots, C(k_n)) = (\mathop{\times}_{j=1}^{n} \mathbf{Z}_{k_j}, \{x\}, \delta),$$

где

$$\delta((z_1, \ldots, z_n), x) = (\delta_{k_1}(z_1, x), \ldots, \delta_{k_n}(z_n, x)),$$

т.е. $\zeta(C(k_1), \ldots, C(k_n))$ - декартово произведение счетчиков $C(k_1), \ldots, C(k_n)$ с отождествлением их входов. Нетрудно показать, что:

1. Автомат $\zeta(C(k_1), \ldots, C(k_n))$ состоит из НОД $(k_1, \ldots, k_n)$ компонент сильной связанности, каждая из которых содержит НОК $(k_1, \ldots, k_n)$ состояний.

2. Состояния $(z_1^{(1)}, \ldots, z_n^{(1)}), (z_1^{(2)}, \ldots, z_n^{(2)}) \in \mathop{\times}_{i=1}^{n} \mathbf{Z}_{k_i}$ автомата $\zeta(C(k_1), \ldots, C(k_n))$ принадлежат одной и той же компоненте сильной связанности тогда и только тогда, когда существует такое число $l \in \{0, 1, \ldots, \text{НОК}\,(k_1, \ldots, k_n) - 1\}$, что совместной является система сравнений

$$l \equiv z_i^{(2)} - z_i^{(1)} \pmod{k_i} \quad (i = 1, \ldots, n).$$

Следовательно, для любых двух конечных последовательностей счетчиков $C(k_1^{(1)}), \ldots, C(k_{n_1}^{(1)})$ и $C(k_1^{(2)}), \ldots, C(k_{n_2}^{(2)})$:

1. Автомат $\zeta(C(k_1^{(2)}), \ldots, C(k_{n_2}^{(2)}))$ является гомоморфным образом автомата $\zeta(C(k_1^{(1)}), \ldots, C(k_{n_1}^{(1)}))$ тогда и только тогда, когда

$$\text{НОК}\,(k_1^{(2)}, \ldots, k_{n_2}^{(2)}) \mid \text{НОК}\,(k_1^{(1)}, \ldots, k_{n_1}^{(1)})$$

и

$$\text{НОД}\,(k_1^{(2)}, \ldots, k_{n_2}^{(2)}) \leq \text{НОД}\,(k_1^{(1)}, \ldots, k_{n_1}^{(1)}).$$

2. Автоматы $\zeta(C(k_1^{(1)}),\ldots,C(k_{n_1}^{(1)}))$ и $\zeta(C(k_1^{(2)}),\ldots,C(k_{n_2}^{(2)}))$ - изоморфные тогда и только тогда, когда

$$\prod_{i=1}^{n_1} k_i^{(1)} = \prod_{i=1}^{n_2} k_i^{(2)}$$

и

$$\text{НОК}\,(k_1^{(1)},\ldots,k_{n_1}^{(1)}) = \text{НОК}\,(k_1^{(2)},\ldots,k_{n_2}^{(2)}).$$

Подводя итог сказанному, заключаем, что для автомата $M \in \mathbf{A}_{k1n}$, состоящего из u компонент сильной связанности, каждая из которых состоит из v состояний, существует изоморфный ему автомат $\zeta(C(k_1),\ldots,C(k_l))$ тогда и только тогда, когда канонические разложения

$$k = p_1^{\gamma_1}\ldots p_r^{\gamma_r}, \quad u = p_1^{\alpha_1}\ldots p_r^{\alpha_r}, \quad v = p_1^{\beta_1}\ldots p_r^{\beta_r},$$

$$k_i = p_1^{\mu_{i1}}\ldots p_r^{\mu_{ir}} \quad (i = 1,\ldots,l)$$

удовлетворяют условиям:

$$\alpha_j + \beta_j = \gamma_j \quad (j = 1,\ldots,r),$$

$$\mu_{1j} + \ldots + \mu_{lj} = \gamma_j \quad (j = 1,\ldots,r),$$

$$\min\{\mu_{1j},\ldots,\mu_{lj}\} = \alpha_j \quad (j = 1,\ldots,r),$$

$$\max\{\mu_{1j},\ldots,\mu_{lj}\} = \beta_j \quad (j = 1,\ldots,r).$$

Таким образом, получено решение проблемы представления элементов множества $\mathbf{A}_{k1n}^c(\mathbf{G}_1,\mathbf{G}_2)$ композицией счетчиков.

3.6. Рекурсивная модель секретного замка.

Основная цель настоящего пункта – показать, что автоматы, принадлежащие множеству $\mathbf{A}_{k1n}^c(\mathbf{G}_1,\mathbf{G}_2)$, являются эффективным средством решения актуальных прикладных проблем.

В процессе создания средств защиты доступа к информации ключевую роль играет разработка алгоритмов и структур данных, предназначенных для идентификации последовательностей символов. Традиционный подход основан на непосредственном использовании конечного автомата в качестве *секретного замка* (см., напр. [90]). Он дает возможность строить только *стационарные модели* (т.е. идентифицирующие не изменяющиеся во времени последовательности), достаточно легко поддающиеся расшифровке. Поэтому, разработка общего подхода к унифицированному построению как стационарных, так и нестационарных моделей секретного замка, имеющих любую сколь угодно высокую сложность расшифровки, является актуальной.

Пусть $C(k_1),\ldots,C(k_l)$ - заданная последовательность счетчиков. Построим автомат

$$M = (Q,\{x\},\delta_M) = \zeta(C(k_1),\ldots,C(k_l)).$$

Таким образом,

$$Q = \mathop{\times}_{i=1}^{l} \mathbf{Z}_{k_i} .$$

Положим

$$k_M = \prod_{i=1}^{l} k_i , \qquad m_M = \text{НОК}\,(k_1,\ldots,k_l) , \qquad d_M = \text{НОД}\,(k_1,\ldots,k_l)$$

и

$$\mathbf{N}_a = \{1,\ldots,a\} \ \ (a \in \mathbf{N}) .$$

Упорядочим множество Q с помощью обычного отношения лексикографического порядка $<_Q$ и занумеруем его элементы в порядке их возрастания, т.е.

$$Q = \{q_1,\ldots,q_{k_M}\} ,$$

где

$$q_1 <_Q \ldots <_Q q_{k_M} .$$

Обозначим через π_M разбиение множества Q, блоки которого - множества состояний, принадлежащие одной и той же компоненте сильной связанности автомата M. Занумеруем блоки разбиения π_M в порядке возрастания их минимальных элементов. Таким образом,

$$\pi_M = \{B_i \mid i \in \mathbf{N}_{d_M}\} ,$$

причем

$$i < j \Rightarrow \min B_i <_Q \min B_j$$

для всех $i, j \in \mathbf{N}_{d_M}$ $(i \neq j)$. Определим функцию

$$g_M : \mathbf{N}_{d_M} \to Q$$

равенством

$$g_M(i) = \min B_i \quad (i \in \mathbf{N}_{d_M}) .$$

Пусть задана общерекурсивная функция

$$f : \mathbf{Z}_+ \to \{j_1,\ldots,j_{d_m}\} ,$$

где

$$j_r = \max B_r \ \ (r = 1,\ldots,d_M\} .$$

Обозначим через

$$P_{M,f} : \mathbf{Z}_+ \times \mathbf{N}_{d_M} \times \mathbf{Z}_+ \to \{0,1\}$$

общерекурсивный предикат, значения $P_{M,f}(t,i,h)$ $(t \in \mathbf{Z}_+, i \in \mathbf{N}_{d_M}, h \in \mathbf{Z}_+)$ которого вычисляются в соответствии со следующим алгоритмом.

Алгоритм 3.5.
Шаг 1. $u := g_M(i)$.
Шаг 2. $v := \delta_M(u, x^h)$, $w := q_{f(t+h)}$.
Шаг 3. Если $v = w$, то $P_{M,f}(t,i,h) = 1$, иначе $P_{M,f}(t,i,h) = 0$. Конец.

Предикат $P_{M,f}$ и представляет собой *секретный замок*. При этом, t допускает интерпретацию как момент времени, в который начинается процедура открытия секретного замка, упорядоченная пара (i,h) - как *ключ* к секретному замку, а общерекурсивная функция f - как *средство управления отверстием* в секретном замке.

По построению, в каждый момент времени $t \in \mathbf{Z}_+$ для *ключа* (i,h) существует единственное допустимое значение $i \in \{1,\dots,d_M\}$ и бесконечное множество допустимых значений h, являющихся решениями сравнения

$$h \equiv 0\,(\mathrm{mod}(m_M - 1)).$$

Не располагая информацией о последовательности счетчиков $C(k_1),\dots,C(k_l)$ и общерекурсивной функции f, любое *средство взлома*, даже при известном ему значении верхней границы для $\sum_{i=1}^{l} k_i$ или k_M, должно принимать во внимание любую, из, по крайней мере минимальных, возможных комбинаций (i,h). Число таких комбинаций примерно равно удвоенному числу различных способов разложения k_M на два сомножителя. Следовательно, если время апробации всех допустимых комбинаций (i,h) значительно превосходит длительность интервала постоянства функции f, то *взломать* такой секретный замок практически не представляется возможным.

3.7. Выводы.

Раздел 3 является логическим продолжением раздела 2. Разработанные в нем модели и методы предназначены для исследования алгоритмических, метрических и дескриптивных аспектов проблем анализа конечных автоматов - одного из фундаментальных классов дискретных систем. Основные результаты состоят в следующем:

1. Построены и исследованы прямые и обратные M-источники, предназначенные для решения проблем идентификации внутренних состояний слабоинициального конечного автомата. Таким образом, непосредственное применение алгоритмов, разработанных в разделе 2, дает возможность решить целый спектр проблем теории экспериментов с автоматами, а именно: поиск (всех или одного, безразлично, какого именно) минимальных идентифицирующих (т.е. диагностических, установочных и синхронизирующих) слов восстановлением либо их начальных, либо их финальных отрезков, а также двухсторонним восстановлением; поиск всех неприводимых идентифицирующих слов восстановлением либо их начальных, либо их финальных отрезков; поиск кратных идентифицирующих экспериментов.

2. Разработан общий метод построения нижних экспоненциальных оценок на основе использования подстановок, имеющих специальную структуру. Эффективность и мощь разработанного метода проиллюстрирована исследованием метрических характеристик симметрической группы – классического объекта алгебры, а также построением нижних экспоненциальных оценок длин минимальных диагностических и синхронизирующих слов для слабоинициального автомата с двухбуквенным входным алфавитом. Фундаментальное значение последнего результата состоит в том, что любой алгоритм построения диагностических или синхронизирующих слов для слабоиници-

ального автомата, основанный на восстановлении отрезков фиксированной длины, заведомо имеет экспоненциальную сложность (как временную, так и емкостную).

3. Построены и исследованы AM-источники, предназначенные для решения проблем идентификации внутренних состояний слабоинициального конечного автомата. Таким образом, непосредственное применение алгоритмов, разработанных в разделе 2, дает возможность строить условные эксперименты с автоматами, реализуя их в виде автоматов-экспериментаторов.

4. Получено полное решение проблемы представления функций переходов и выходов конечных автоматов конечными группами. Выделение множества представлений, согласованных с функцией переходов, привело к классу перестановочных автоматов, каждая компонента связанности которых имеет одно и то же число состояний. Показано, что этот класс содержит важный специальный подкласс, состоящий из автоматов, представимых композициями циклических групп (или, что то же самое, декартовым произведением счетчиков с отождествлением их входа). Значение последнего подкласса проиллюстрировано его применением для конструирования нестационарных секретных замков со сколь угодно высокой сложностью расшифровки.

Таким образом, в разделе 3 разработан законченный фрагмент комбинаторно-алгебраической теории анализа конечных автоматов, на основе которой получено исчерпывающее решение проблем 1.9 и 1.10.

Основные результаты раздела 3 опубликованы в [56,60,61,63,72,75,78,84,132].

4. АНАЛИЗ БУЛЕВЫХ ФУНКЦИЙ

Настоящий раздел посвящен разработке комбинаторно-алгебраических основ анализа булевых функций – фундаментального класса дискретных систем как в теоретическом, так и прикладном аспектах.

Пп.4.1 и 4.2 посвящены разработке комбинаторных методов анализа булевых функций. В п.4.1 решены проблемы поиска простых импликант и, на их основе, проблемы поиска ДНФ, состоящих только из простых импликант. П.4.2 является логическим продолжением п.4.1. В нем сформулированы и решены проблемы анализа управляемости/наблюдаемости булевых функций. П.4.3 посвящен разработке алгебраических методов анализа булевых функций. В нем решена проблема идентификации булевой вектор-функции методами теории линейных пространств над полями Галуа.

4.1. Комбинаторные алгоритмы построения ДНФ.

Многочисленные приложения задач минимизации булевых функций в классе ДНФ и возникающие при этом вычислительные трудности обосновывают актуальность разработки алгоритмов минимизации, ориентированных на использование ЭВМ. Основная цель настоящего пункта - разработка общих алгоритмов построения *достаточно простой* ДНФ, а также, *сокращенной* ДНФ, основанных на последовательном построении простых импликант.

Как обычно, под *длиной* ДНФ $D = \bigvee_{i=1}^{h} K_i$ будем понимать количество h составляющих D элементарных конъюнкций. Обозначим через $l(D)$ длину ДНФ D.

Рассмотрим следующие проблемы построения ДНФ

Проблема 4.1. Для заданной булевой функции $f \in P_2(n)$ $(n \in \mathbf{N})$ построить ДНФ $D(f)$ длины

$$l(D(f)) \le |\boldsymbol{N}_f|,$$

состоящую из простых импликант.

Проблема 4.2. Для заданной булевой функции $f \in P_2(n)$ $(n \in \mathbf{N})$ построить сокращенную ДНФ $D_f^{сокр}$.

Проблема 4.3. Для заданной булевой функции $f \in P_2(n)$ $(n \in \mathbf{N})$ построить одну, безразлично какую именно, простую импликанту K, покрывающую заданную точку $\mathbf{s} = (\sigma_1, \ldots, \sigma_n) \in \boldsymbol{N}_f$.

Проблема 4.4. Для заданной булевой функции $f \in P_2(n)$ $(n \in \mathbf{N})$ построить множество всех простых импликант, покрывающих заданную точку $\mathbf{s} = (\sigma_1, \ldots, \sigma_n) \in \boldsymbol{N}_f$.

Очевидно, что решение проблем 4.1, 4.3 и 4.4 может быть получено на основе решения проблемы 4.2. Действительно, построим ДНФ $D_f^{сокр}$ каким-либо из классических методов (см. п.1.4).

Для решения проблемы 4.1 достаточно построить любую *минимальную* ДНФ, т.е. решить проблему поиска какого-либо минимального (по числу элементов) покрытия множества $\boldsymbol{N}_f$ заданными его подмножествами, являющимися максимальными гранями n-мерного единичного куба, содержащимися в множестве $\boldsymbol{N}_f$. Известные методы решения последней проблемы – преобразование специальным образом построенной КНФ в ДНФ за счет раскрытия скобок с применением операции *элементарного поглощения*.

Для решения проблем 4.3 и 4.4 достаточно подставить

$$\mathbf{s} = (\sigma_1, \ldots, \sigma_n)$$

в $D_f^{сокр}$ и выбрать, соответственно, одну или все простые импликанты, значение которых равно 1.

Такой метод решения проблем 4.1, 4.3 и 4.4 обладает существенным недостатком:

сложность каждого решения не меньше, чем сложность построения сокращенной ДНФ.

Этот недостаток действительно является существенным.

Во-первых, как известно, длина сокращенной ДНФ может быть достаточно большой - экспонентой от числа переменных, значительно превышающей мощность множества $\boldsymbol{N}_f$ (см., напр. [18,47]).

Во-вторых, все известные классические методы построения сокращенной ДНФ (см. п.1.4) основаны на аналитических преобразованиях обладающих следующей особенностью. Объем памяти, необходимой на промежуточных шагах алгоритма может существенно превышать объем памяти, необходимой для хранения сокращенной ДНФ и только на завершающих шагах работы алгоритма эти объемы *выравниваются*.

В третьих, проблемы 4.3 и 4.4 представляют и самостоятельный интерес. К ним, например, сводятся проблемы поиска тестов для схем, реализованных на ПЛМ, а также (как будет показано в п.4.2), проблемы анализа *управляемости/наблюдаемости* комбинационных схем.

Таким образом, разработка комбинаторных алгоритмов построения ДНФ, основанных на последовательном построении простых импликант - и актуальная, и естественная проблема.

Рассмотрим решение проблем 4.1-4.4 комбинаторными методами в общем случае.

Вначале решим проблемы 4.3 и 4.4.

Предположим, что зафиксированы такие алгоритмы A и B, что

$$A(f,\mathbf{s}) = \begin{cases} 1, \text{ если } \mathbf{s} \in \boldsymbol{N}_f, \\ 0, \text{ если } \mathbf{s} \notin \boldsymbol{N}_f \end{cases} \qquad (f \in P_2(n),\ \mathbf{s} \in \mathbf{E}^n)$$

и

$$B(f,S) = \begin{cases} \mathbf{s}\ \ (\mathbf{s} \in \boldsymbol{N}_f \setminus S), \text{ если } S \neq \boldsymbol{N}_f \\ \quad * \quad\ , \qquad \text{если } S = \boldsymbol{N}_f \end{cases} \qquad (f \in P_2(n),\ S \subseteq \boldsymbol{N}_f).$$

Таким образом, алгоритм A вычисляет значение булевой функции f в точке $\mathbf{s} \in \mathbf{E}^n$, а алгоритм B порождает точку $\mathbf{s} \in \boldsymbol{N}_f \setminus S$. Обозначим через $t_{C,f}$ и $v_{C,f}$, соответственно, временную и емкостную сложность алгоритма $C \in \{A, B\}$ для функции $f \in P_2(n)$, а через $t_C(n)$ - временную сложность алгоритма $C \in \{A, B\}$ для почти всех функций $f \in P_2(n)$.

Для элементарной конъюнкции $K = \mathop{\wedge}\limits_{j=1}^{r} x_{i_j}^{\alpha_j}$ положим

$$K(i_h) = \mathop{\wedge}\limits_{\substack{j=1 \\ j \neq h}}^{r} x_{i_j}^{\alpha_j} \qquad (h \in \{1, \dots, r\})$$

и

$$K(\bar{i}_h) = (\mathop{\wedge}\limits_{j=1}^{h-1} x_{i_j}^{\alpha_j}) \cdot x_{i_h}^{\bar{\alpha}_h} \cdot (\mathop{\wedge}\limits_{j=h+1}^{r} x_{i_j}^{\alpha_j}) \quad (h \in \{1, \dots, r\}).$$

Решение проблемы 4.3 можно осуществить последовательным *вычеркиванием* литералов, входящих в элементарную конъюнкцию $\mathop{\wedge}\limits_{i=1}^{n} x_i^{\sigma_i}$, что приводит к следующему алгоритму.

Алгоритм 4.1.

Шаг 1. $K_1 := \mathop{\wedge}\limits_{i=1}^{n} x_i^{\sigma_i}$, $j := 1$.

Шаг 2. Если $\boldsymbol{N}_{K_j(\bar{j})} \subseteq \boldsymbol{N}_f$, то $K_{j+1} := K_j(j)$, иначе $K_{j+1} := K_j$.

Шаг 3. $j := j + 1$.

Шаг 4. Если $j \le n$, то переход к шагу 2, иначе $K := K_{n+1}$ и конец.

Теорема 4.1. Алгоритм 4.1 строит простую импликанту K булевой функции $f \in P_2(n)$, покрывающую заданную точку $\mathbf{s} = (\sigma_1, \dots, \sigma_n) \in \boldsymbol{N_f}$ с временной и емкостной сложностью, соответственно, равной

$$T = O((t_{A,f} + n)(1 + Rank\ K)2^{Dim\ K}) \quad (n \to \infty) \tag{4.1}$$

и

$$V = v_{A,f} + O(n) \quad (n \to \infty). \tag{4.2}$$

Доказательство. Докажем корректность алгоритма 4.1.

Покажем вначале, что результат работы алгоритма 4.1 – импликанта булевой функции $f \in P_2(n)$, покрывающая точку $\mathbf{s} \in \boldsymbol{N_f}$.

Так как $\boldsymbol{N}_{K_1} = \{\mathbf{s}\} \subseteq \boldsymbol{N}_f$, то элементарная конъюнкция $K_1 = \mathop{\wedge}\limits_{i=1}^{n} x_i^{\sigma_i}$ - импликанта булевой функции $f \in P_2(n)$, покрывающая заданную точку $\mathbf{s} \in \boldsymbol{N_f}$.

Пусть элементарная конъюнкция $K_j = (\mathop{\wedge}\limits_{u=1}^{m_j} x_{i_u}^{\sigma_{i_u}}) \cdot (\mathop{\wedge}\limits_{i=j}^{n} x_i^{\sigma_i})$ $(j = 1, \dots, n)$ - импликанта булевой функции $f \in P_2(n)$, покрывающая заданную точку $\mathbf{s} \in \boldsymbol{N_f}$.

Если $\boldsymbol{N}_{K_j(\bar{j})} \subseteq \boldsymbol{N}_f$, то $K_{j+1} = K_j(j)$, причем

$$\boldsymbol{N}_{K_{j+1}} = \boldsymbol{N}_{K_j(j)} = \boldsymbol{N}_{K_j \vee K_j(\bar{j})} = \boldsymbol{N}_{K_j} \cup \boldsymbol{N}_{K_j(\bar{j})} \subseteq \boldsymbol{N}_f$$

и

$$\boldsymbol{N}_{K_{j+1}} = \boldsymbol{N}_{K_j(j)} \supset \boldsymbol{N}_{K_j} \supseteq \{\mathbf{s}\},$$

т.е. элементарная конъюнкция K_{j+1} - импликанта булевой функции $f \in P_2(n)$, покрывающая точку $\mathbf{s} \in \boldsymbol{N}_{\boldsymbol{f}}$.

Если же $\boldsymbol{N}_{K_j(\bar{j})} \not\subseteq \boldsymbol{N}_f$, то $K_{j+1} := K_j$ и, следовательно, элементарная конъюнкция K_{j+1} - импликанта булевой функции $f \in P_2(n)$, покрывающая точку $\mathbf{s} \in \boldsymbol{N}_{\boldsymbol{f}}$.

Таким образом, элементарная конъюнкция $K = K_{n+1}$ - импликанта булевой функции $f \in P_2(n)$, покрывающая точку $\mathbf{s} \in \boldsymbol{N}_{\boldsymbol{f}}$.

Покажем теперь, что элементарная конъюнкция $K = K_{n+1}$ - простая импликанта булевой функции $f \in P_2(n)$, покрывающая точку $\mathbf{s} \in \boldsymbol{N}_{\boldsymbol{f}}$.

Предположим противное, т.е. что импликанта

$$K = K_{n+1} = \mathop{\wedge}_{u=1}^{r} x_{i_u}^{\sigma_{i_u}}$$

булевой функции $f \in P_2(n)$ не является простой. Это означает, что существует такое $h \in \{1,\ldots,r\}$, что элементарная конъюнкция $K(i_h)$ - импликанта булевой функции $f \in P_2(n)$. В результате $(i_h - 1)$-й итерации шагов 2-4 алгоритма 4.1 построена импликанта

$$K_{i_h} = (\mathop{\wedge}_{u=1}^{h-1} x_{i_u}^{\sigma_{i_u}}) \cdot (\mathop{\wedge}_{u=i_h}^{n} x_u^{\sigma_u})$$

булевой функции $f \in P_2(n)$. Поэтому, $K_{i_h+1} = K_{i_h}(i_h)$, т.е. литерал $x_{i_h}^{\sigma_{i_h}}$ не входит в импликанту $K = K_{n+1}$. Полученное противоречие показывает, что предположение – ложное. Следовательно, $K = K_{n+1}$ - простая импликанта булевой функции $f \in P_2(n)$, покрывающая точку $\mathbf{s} \in \boldsymbol{N}_{\boldsymbol{f}}$.

Корректность алгоритма 4.1 доказана.

Оценим сложность алгоритма 4.1.

Время выполнения шагов 1, 3 и 4 невелико по сравнению со временем выполнения шага 2. Следовательно, временная сложность алгоритма 4.1 равна

$$T = \sum_{j=1}^{n} T_j,$$

где T_j - время, затраченное на j-е $(j = 1,\ldots,n)$ выполнение шага 2. Так как

$$T_j = O((t_{A,f} + n) \cdot |\boldsymbol{N}_{K_j(\bar{j})}|) = O((t_{A,f} + n) \cdot 2^{Dim\, K_j(\bar{j})}) \quad (n \to \infty),$$

то

$$T = \sum_{j=1}^{Dim\, K} O(t_{A,f} + n) \cdot 2^{j-1} + O(t_{A,f} + n) \cdot 2^{Dim\, K} \cdot Rank\, K =$$

$$= O((t_{A,f} + n)(1 + Rank\ K)2^{Dim\ K}) \quad (n \to \infty),$$

что и требовалось доказать.

Емкостная сложность алгоритма 4.1 определяется объемом памяти, необходимой для реализации алгоритма A и объемом памяти, необходимой для хранения пары импликант K_j и $K_j(\bar{j})$. Следовательно,

$$V = v_{A,f} + O(n) \quad (n \to \infty),$$

что и требовалось доказать.

Теорема доказана.

Следствие 4.1. Для почти всех булевых функций $f \in P_2(n)$ при почти всех $\mathbf{s} \in \boldsymbol{N}_f$ временная сложность алгоритма 4.1 равна

$$T = O((t_A(n) + n)(n - \log\log n)\log n) \quad (n \to \infty). \tag{4.3}$$

Доказательство. Известно (см. напр., [18,47]), что для почти всех простых импликант почти всех булевых функций $f \in P_2(n)$ справедливо неравенство

$$n - \log\log n - \log((1+\varepsilon)\log\log n) < Rank\ K < n - \log\log n, \tag{4.4}$$

где $\varepsilon \to 0$ при $n \to \infty$. Подставим (4.4) в (4.1) и заменим $t_{A,f}$ на $t_A(n)$. Получим (4.3).

Следствие доказано.

Обозначим через $S_{f,\mathbf{s}}$ множество всех простых импликант булевой функции $f \in P_2(n)$, покрывающих заданную точку $\mathbf{s} = (\sigma_1, \ldots, \sigma_n) \in \boldsymbol{N}_f$.

Построение множества $S_{f,\mathbf{s}}$ можно осуществить организацией вычеркивания литералов (определяемого алгоритмом 4.1), входящих в элементарную конъюнкцию $\bigwedge_{i=1}^{n} x_i^{\sigma_i}$, всеми возможными способами. Следовательно, решение проблемы 4.4 естественно сводится к *поиску с возвращением* множества всех неприводимых решений для случая, когда множество элементарных операторов (т.е. операций вычеркивания литералов) – коммутативная полугруппа (см. пп.2.1 и 2.3). Таким образом, приходим к следующему алгоритму решения проблемы 4.4.

Алгоритм 4.2.

/* инициализация значений */

Шаг 1. $K := \bigwedge_{i=1}^{n} x_i^{\sigma_i}$, $S_{f,\mathbf{s}} := \varnothing$, $\mathbf{a} := (1,2,\ldots,n+1)$, $r := 1$.

/* прямой ход */

Шаг 2. Если $\mathbf{a}(r) \le n$, то $j := \mathbf{a}(r)$ и переход к шагу 3, иначе переход к шагу 6.

Шаг 3. Если $\boldsymbol{N}_{K(\bar{j})} \subseteq \boldsymbol{N}_f$, то $K := K(j)$, $r := r+1$ и переход к шагу 2, иначе $h := r$ и переход к шагу 4.

Шаг 4. $\mathbf{a}(h) := \mathbf{a}(h) + 1$, $h := h+1$.

Шаг 5. Если $h \le n+1$, то переход к шагу 4, иначе переход к шагу 2.

Шаг 6. Если $\boldsymbol{N}_K \not\subseteq \boldsymbol{N}_{K_1}$ для всех $K_1 \in S_{f,\mathbf{s}}$, то $S_{f,\mathbf{s}} := S_{f,\mathbf{s}} \cup \{K\}$.

Шаг 7. Если $r > 1$, то переход к шагу 8, иначе конец.

/* обратный ход */

Шаг 8. $r := r - 1$, $j := \mathbf{a}(r)$, $K := K \wedge x_j^{\sigma_j}$, $d := j - r + 1$, $h := r$.

Шаг 9. $\mathbf{a}(h) := d + h$, $h := h + 1$.

Шаг 10. Если $h \le n + 1$, то переход к шагу 9, иначе переход к шагу 2.

Теорема 4.2. Алгоритм 4.2 строит множество $S_{f,\mathbf{s}}$ всех простых импликант булевой функции $f \in P_2(n)$, покрывающих заданную точку $\mathbf{s} = (\sigma_1, \ldots, \sigma_n) \in \boldsymbol{N}_f$ с временной и емкостной сложностью, равной, соответственно,

$$T = O((t_{A,f} + n) \cdot 4^n) \quad (n \to \infty) \tag{4.5}$$

и

$$V = v_{A,f} + O(n \cdot 2^n) \quad (n \to \infty). \tag{4.6}$$

Доказательство. Корректность алгоритма 4.2 вытекает из следующих фактов. Конъюнкции, конструируемые в цикле, определяемом шагами 2 и 3 - импликанты булевой функции $f \in P_2(n)$, покрывающие точку $\mathbf{s} = (\sigma_1, \ldots, \sigma_n) \in \boldsymbol{N}_f$ (см. доказательство теоремы 4.1). В процессе выполнения шага 6 осуществляется проверка, является ли каждая из этих импликант простой. Использование общего алгоритма поиска с возвращением (см. пп.2.1 и 2.3) гарантирует построение всех элементов множества $S_{f,\mathbf{s}}$.

Оценим временную сложность алгоритма 4.2.

Время выполнения шага 1 равно $O(n)$ $(n \to \infty)$, а время выполнения каждого из шагов 4,5,7,8-10 равно $O(1)$ $(n \to \infty)$. Следовательно, время, затрачиваемое на вычисления, осуществляемые до перехода к шагу 2 в цикле, определяемом шагами 4 и 5, а также в цикле, определяемом шагами 9 и 10, равно $O(n)$ $(n \to \infty)$.

Время, затрачиваемое на вычисления, осуществляемые до перехода к шагу 4 в цикле, определяемом шагами 2 и 3, равно

$$O((t_{A,f} + n) \cdot 2^n) \ (n \to \infty).$$

Условие $\boldsymbol{N}_K \not\subseteq \boldsymbol{N}_{K_1}$ проверяется за время $O(n)$ $(n \to \infty)$, так как оно эквивалентно условию $K \not\le K_1$. А так как

$$| S_{f,\mathbf{s}} | \le 2^n,$$

то, во-первых, шаг 6 выполняется за время $O(n \cdot 2^n)$ $(n \to \infty)$, а, во-вторых, переход к каждому из перечисленных выше циклов осуществляется не более, чем 2^n раз. Следовательно,

$$T = 2^n \cdot (O((t_{A,f} + n) \cdot 2^n) + O(n \cdot 2^n) + O(n)) = O((t_{A,f} + n) \cdot 4^n) \quad (n \to \infty),$$

что и требовалось доказать.

Оценим емкостную сложность алгоритма 4.2.

Объем памяти, необходимой для вычислений при реализации алгоритма 4.2 равен

$$V = V_1 + V_2 + V_3, \tag{4.7}$$

где V_1 - объем памяти, необходимой для реализации алгоритма 4.1, V_2 - объем памяти, необходимой для хранения множества $S_{f,\mathbf{s}}$, а V_3 - объем памяти, необходимой непосредственно для организации поиска с возвращением.

Так как множество элементарных операторов (т.е. операций вычеркивания литералов) – коммутативная полугруппа, то (см. теорему 2.4)

$$V_3 = O(n) \quad (n \to \infty). \tag{4.8}$$

Так как $|S_{f,\mathbf{s}}| \le 2^n$, то

$$V_2 = O(n \cdot 2^n) \quad (n \to \infty). \tag{4.9}$$

Кроме того (см. (4.2)) ,

$$V_1 = v_{A,f} + O(n) \quad (n \to \infty). \tag{4.10}$$

Подставим (4.8)-(4.10) в (4.7). Получим (4.6), что и требовалось доказать.

Теорема доказана.

Следствие 4.2. Для почти всех булевых функций $f \in P_2(n)$ при почти всех $\mathbf{s} \in \boldsymbol{N_f}$ временная сложность алгоритма 4.2 равна

$$T = O(2^n \cdot (t_A(n) + n)(n - \log\log n)\log n) \quad (n \to \infty). \tag{4.11}$$

Доказательство. В процессе вычисления временной сложности алгоритма 4.2 оценим формулой (4.3) время, затрачиваемое на вычисления, осуществляемые до перехода к шагу 4 в цикле, определяемом шагами 2 и 3. Кроме того, заменим $t_{A,f}$ на $t_A(n)$. Получим (4.11).

Следствие доказано.

Рассмотрим теперь решение проблем 4.1 и 4.2.

Обозначим через $A_{4.1}(f,\mathbf{s})$ конструируемую в результате работы алгоритма 4.1 простую импликанту булевой функции $f \in P_2(n)$, покрывающую точку $\mathbf{s} \in \boldsymbol{N}_f$, а через $A_{4.2}(f,\mathbf{s})$ - конструируемое в результате работы алгоритма 4.2 множество $S_{f,\mathbf{s}}$ всех простых импликант булевой функции $f \in P_2(n)$, покрывающих точку $\mathbf{s} \in \boldsymbol{N}_f$.

Построение ДНФ булевой функции $f \in P_2(n)$ можно осуществить последовательным поиском с помощью алгоритма 4.1 простых импликант, покрывающих выбираемые точки до тех пор, пока не будет получено покрытие множества $\boldsymbol{N_f}$ содержащимися в нем гранями максимальных размерностей. Таким образом, приходим к следующему алгоритму решения проблемы 4.1.

Алгоритм 4.3.

Шаг 1. $D := 0$, $S := \varnothing$.

Шаг 2. Если $B(f,S) \ne *$, то $\mathbf{s} := B(f,S)$ и переход к шагу 3, иначе $D(f) := D$ и конец.

Шаг 3. $K := A_{4.1}(f,\mathbf{s})$, $D := D \vee K$, $S := S \cup \boldsymbol{N}_K$ и переход к шагу 2.

Теорема 4.3. Алгоритм 4.3 строит ДНФ $D(f)$ $(f \in P_2(n))$, состоящую из простых импликант и имеющую длину $l(D(f)) \le |\boldsymbol{N}_f|$ с временной и емкостной сложностью, соответственно, равной

$$T = O((t_{B,f} + n \cdot 2^n) \cdot l(D(f)) +$$

$$+ (t_{A,f} + n) \cdot \sum_{K \in D(f)} (1 + Rank\ K) \cdot 2^{Dim\ K}) \quad (n \to \infty) \qquad (4.12)$$

и

$$V = v_{A,f} + v_{B,f} + O(n \cdot 2^n) \quad (n \to \infty). \qquad (4.13)$$

Доказательство. Докажем корректность алгоритма 4.3.

Генерация простых импликант K для булевой функции $f \in P_2(n)$ осуществляется на шаге 3. Алгоритм 4.3 прекращает свою работу в результате выполнения шага 2 тогда и только тогда, когда $B(f, S) = *$, т.е. когда

$$\bigcup_{K \in D} \boldsymbol{N}_K = \boldsymbol{N}_f .$$

Последнее равенство и означает, что D - ДНФ булевой функции $f \in P_2(n)$, что и требовалось показать.

Оценим временную сложность алгоритма 4.3.

Время выполнения шага 1 равно $O(1)$ $(n \to \infty)$. Поэтому, временная сложность алгоритма 4.3 определяется общим временем, затрачиваемым на выполнение шагов 2 и 3. Время, затрачиваемое на одно выполнение шага 2 равно

$$T_1 = O(n \cdot |\boldsymbol{N}_f|) + O(t_{B,f}) = O(n \cdot 2^n + t_{B,f}) \quad (n \to \infty).$$

Время, затрачиваемое на одно выполнение шага 3 равно

$$T_2 = O((t_{A,f} + n)(1 + Rank\ K)2^{Dim\ K}) + O(Rank\ K) + O(n \cdot 2^{Dim\ K}) \quad (n \to \infty).$$

Следовательно,

$$T = \sum_{K \in D(f)} (T_1 + T_2) =$$

$$= O((t_{B,f} + n \cdot 2^n) \cdot l(D(f)) + (t_{A,f} + n) \sum_{K \in D(f)} (1 + Rank\ K) \cdot 2^{Dim\ K}) \quad (n \to \infty),$$

что и требовалось доказать.

Емкостная сложность алгоритма 4.3 определяется объемами памяти, необходимой для реализации алгоритмов 4.1 и B, а также для хранения множества S и восстанавливаемой ДНФ. Следовательно,

$$V = v_{A,f} + O(n) + v_{B,f} + O(n \cdot 2^n) = v_{A,f} + v_{B,f} + O(n \cdot 2^n) \quad (n \to \infty),$$

что и требовалось доказать.

Теорема доказана.

Следствие 4.3. Для почти всех булевых функций $f \in P_2(n)$ временная сложность алгоритма 4.3 равна

$$T = O(2^n \cdot (t_B(n) + n \cdot 2^n + (t_A(n) + n)(n - \log\log n)\log n)) \quad (n \to \infty). \qquad (4.14)$$

Доказательство. В процессе вычисления временной сложности алгоритма 4.3 оценим временную сложность алгоритма 4.1 формулой (4.3). Заменим $t_{A,f}$ на $t_A(n)$ и $t_{B,f}$ на $t_B(n)$. Получим (4.14).

Следствие доказано.

Построение сокращенной ДНФ $D_f^{сокр}$ для булевой функции $f \in P_2(n)$ можно осуществить последовательным поиском с помощью алгоритма 4.2 множеств $S_{f,\mathbf{s}}$ для всех $\mathbf{s} \in \boldsymbol{N}_f$. Таким образом, приходим к следующему алгоритму решения проблемы 4.2.

Алгоритм 4.4.

Шаг 1. $D := 0$, $S := \varnothing$.

Шаг 2. Если $B(f,S) \neq *$, то переход к шагу 3, иначе $D_f^{сокр} := D$ и конец.

Шаг 3. $\mathbf{s} := B(f,S)$, $S := S \cup \{\mathbf{s}\}$.

Шаг 4. $S_1 := A_{4.2}(f,\mathbf{s})$, $S_2 := \{K \in S_1 \mid K \notin D\}$.

Шаг 5. $D := D \vee (\bigvee_{K \in S_2} K)$ и переход к шагу 2.

Теорема 4.4. Алгоритм 4.3 строит сокращенную ДНФ $D_f^{сокр}$ $(f \in P_2(n))$ с временной и емкостной сложностью, соответственно, равной

$$T = O(l(D_f^{сокр}) \cdot (t_{B,f} + (t_{A,f} + n) \cdot 4^n + n \cdot l(D_f^{сокр}))) \quad (n \to \infty) \qquad (4.15)$$

и

$$V = O(v_{A,f} + n \cdot 2^n + v_{B,f} + n \cdot l(D_f^{сокр})) \quad (n \to \infty). \qquad (4.16)$$

Доказательство. Корректность алгоритма 4.4 непосредственно вытекает из корректности алгоритма 4.2.

Время выполнения шага 1 равно $O(1)$ $(n \to \infty)$. Поэтому, временная сложность алгоритма 4.4 определяется общим временем, затрачиваемым на выполнение шагов 2 -5.

Время, затрачиваемое на одно выполнение как шага 2, так и шага 3 равно $O(t_{B,f})$ $(n \to \infty)$. Время, затрачиваемое на одно выполнение шага 4 равно

$$O((t_{A,f} + n) \cdot 4^n) + O(n \cdot l(D_f^{сокр})) = O((t_{A,f} + n) \cdot 4^n + n \cdot l(D_f^{сокр})) \quad (n \to \infty).$$

Время, затрачиваемое на одно выполнение шага 5 равно $O(n \cdot 2^n)$ $(n \to \infty)$. Следовательно,

$$T = O(l(D_f^{сокр}) \cdot (t_{B,f} + (t_{A,f} + n) \cdot 4^n + n \cdot l(D_f^{сокр}))) \quad (n \to \infty),$$

что и требовалось доказать.

Емкостная сложность алгоритма 4.4 определяется объемами памяти, необходимой для реализации алгоритмов 4.2 и B, а также для хранения множеств S, S_1, S_2 и восстанавливаемой ДНФ. Следовательно,

$$V = O(v_{A,f} + n \cdot 2^n + v_{B,f} + n \cdot l(D_f^{сокр})) \quad (n \to \infty),$$

что и требовалось доказать.

Теорема доказана.

Алгоритмы 4.1 и 4.2 легко приспособить для работы со случайно выбранной точкой. Это дает возможность так модифицировать алгоритм 4.3, чтобы он для заданной булевой функции $f \in P_2(n)$ строил *случайные* ДНФ, состоящие из простых импликант.

4.2. Управляемость/наблюдаемость булевых функций.

Основной целью настоящего пункта является разработка методов анализа управляемости/наблюдаемости для булевых функций и их композиций. Актуальность этой проблемы обусловлена следующим.

Анализ *параметров управляемости* и *наблюдаемости* (см. напр., [14,22]) играет существенную роль в процессе проектирования схем с учетом их *тестируемости*. Для узла комбинационной схемы параметры управляемости и наблюдаемости характеризуют наименьшие количества внешних входов, управление которыми, соответственно, обеспечивает в узле требуемое значение и дает возможность транспортировать его к внешним выходам. Соответствующие управления внешними входами назовем *множествами управляемости* и *наблюдаемости*. Множества и значения параметров управляемости и наблюдаемости зависят только от функции, реализуемой фрагментом схемы, порождаемой рассматриваемым узлом и совершенно не зависят от структуры самого фрагмента. Это дает возможность их определять и исследовать в терминах единой теории - *теории булевых функций*, разработать алгоритмы их вычисления, установить сложность их вычисления, а также унифицировать разработку средств автоматизации процесса анализа управляемости и наблюдаемости комбинационных схем. Все сказанное выше и обосновывает актуальность проблемы.

Обозначим через

$$f_{\sigma_1,\ldots,\sigma_r}^{i_1,\ldots,i_r} \quad (f \in P_2(n);\ 1 \le i_1 < \ldots < i_r \le n;\ \sigma_1,\ldots,\sigma_r \in \mathbf{E})$$

булеву функцию, полученную из булевой функции f заменой переменных $x_{i_1},\ldots,x_{i_r}$, соответственно, значениями $\sigma_1,\ldots,\sigma_r$.

Определение 4.1. Для булевой функции $f \in P_2(n)$ назовем множество

$$s = \{(i_j,\sigma_j) \mid j = 1,\ldots,r\} \qquad (1 \le i_1 < \ldots < i_r \le n;\ \sigma_1,\ldots,\sigma_r \in \mathbf{E}):$$

1) *множеством* α*-управляемости* $(\alpha \in \mathbf{E})$, если

$$f_{\sigma_1,\ldots,\sigma_r}^{i_1,\ldots,i_r} \equiv \alpha;$$

2) *множеством* (i,α)*-наблюдаемости* $(i \in \{1,\ldots,n\} \setminus \{i_1,\ldots,i_r\},\ \alpha \in \mathbf{E})$, если

$$f_{\sigma_1,\ldots,\sigma_r}^{i_1,\ldots,i_r} \equiv x_i^{\alpha}.$$

Обозначим через $S^c(\alpha,f)$, $S_{ir}^c(\alpha,f)$ и $S_{\min}^c(\alpha,f)$, соответственно, множество всех, всех неприводимых (т.е. минимальных по включению) и всех минимальных (по мощности) множеств α-управляемости для булевой функции $f \in P_2(n)$. Аналогичным образом, обозначим через $S^o(i,\alpha,f)$, $S_{ir}^o(i,\alpha,f)$ и $S_{\min}^o(i,\alpha,f)$, соответственно, множество всех, всех неприводимых и всех минимальных множеств (i,α)-наблюдаемости для булевой функции $f \in P_2(n)$. Положим

$$\nu^c(\alpha,f) = |s| \quad (\alpha \in \mathbf{E},\ f \in P_2(n),\ s \in S_{\min}^c(\alpha,f)) \tag{4.17}$$

и

$$\nu^o(i,\alpha,f) = |s| \quad (\alpha \in \mathbf{E},\ f \in P_2(n),\ 1 \le i \le n,\ s \in S_{\min}^o(i,\alpha,f)). \tag{4.18}$$

Из (4.17) и (4.18) вытекает, что:

1) $\nu^c(\alpha,f) = 0$ (соответственно $\nu^o(i,\alpha,f) = 0$) тогда и только тогда, когда $f \equiv \alpha$ (соответственно $f \equiv x_i^\alpha$);
2) $\nu^c(\alpha,f)$ не определено (в этом случае будем считать, что $\nu^c(\alpha,f) = \infty$) тогда и только тогда, когда $f \equiv 1-\alpha$;
3) $\nu^o(i,\alpha,f)$ не определено (в этом случае будем считать, что $\nu^o(i,\alpha,f) = \infty$) тогда и только тогда, когда, либо переменная x_i не является существенной для булевой функции f, либо когда функция f возрастает по переменной x_i и $\alpha = 0$, либо когда функция f убывает по переменной x_i и $\alpha = 1$.

Определение 4.2. Назовем $\nu^c(\alpha,f)$, $\nu^o(i,\alpha,f)$ $(f \in P_2(n),\ \alpha \in \mathbf{E},\ 1 \le i \le n)$ и

$$\nu^o(i,f) = \min\{\nu^o(i,0,f), \nu^o(i,1,f)\},$$

соответственно, α*-управляемостью*, (i,α)*-наблюдаемостью* и i*-наблюдаемостью* булевой функции f.

Рассмотрим решение проблем построения множеств и вычисления параметров управляемости и наблюдаемости для булевых функций и их композиций.

Пусть $s = \{(i_j,\sigma_j) \mid j = 1,\ldots,r\}$ $(1 \le i_1 < \ldots < i_r \le n;\ \sigma_1,\ldots,\sigma_r \in \mathbf{E})$. Положим

$$K(s) = \bigwedge_{j=1}^{r} x_{i_j}^{\sigma_j}.$$

Теорема 4.5. Для всех булевых функций $f \in P_2(n)$:

1) $s \in S_{ir}^c(\alpha,f)$ $(\alpha \in \mathbf{E})$ тогда и только тогда, когда $K(s) \in D_{f^\alpha}^{сокр}$;
2) $s \in S_{ir}^o(i,\alpha,f)$ $(1 \le i \le n,\ \alpha \in \mathbf{E})$ тогда и только тогда, когда $x_i^\alpha \wedge K(s) \in D_{f_{i,\alpha}}^{сокр}$, где $f_{i,\alpha}$ - такая булева функция, что

$$\boldsymbol{N}_{f_{i,\alpha}} = \{(\beta_1,\ldots,\beta_{i-1},\alpha,\beta_{i+1},\ldots,\beta_n) \in \boldsymbol{N}_f \mid (\beta_1,\ldots,\beta_{i-1},\overline{\alpha},\beta_{i+1},\ldots,\beta_n) \notin \boldsymbol{N}_f\}.$$

Доказательство. По определению, $s \in S_{ir}^{c}(\alpha, f)$ тогда и только тогда, когда $\boldsymbol{N}_{K(s)} \subseteq \boldsymbol{N}_{f^{\alpha}}$ и $\boldsymbol{N}_{K(s_1)} \not\subseteq \boldsymbol{N}_{f^{\alpha}}$ для всех $s_1 \subset s$. Условия $s_1 \subset s$ и $\boldsymbol{N}_{K(s_1)} \supset \boldsymbol{N}_{K(s)}$ - эквивалентные. Следовательно, $s \in S_{ir}^{c}(\alpha, f)$ тогда и только тогда, когда элементарная конъюнкция $K(s)$ определяет максимальную допустимую грань для булевой функции f^{α}, т.е. когда $K(s) \in D_{f^{\alpha}}^{сокр}$, что и требовалось доказать.

По определению, $s \in S_{ir}^{o}(i, \alpha, f)$ тогда и только тогда, когда выполнены следующие три условия:

Условие 4.1. $\boldsymbol{N}_{x_i^{\alpha} \wedge K(s)} \subseteq \boldsymbol{N}_{f}$.

Условие 4.2. $\boldsymbol{N}_{x_i^{\bar{\alpha}} \wedge K(s)} \cap \boldsymbol{N}_{f} = \varnothing$.

Условие 4.3. Для всех $s_1 \subset s$, либо $\boldsymbol{N}_{x_i^{\alpha} \wedge K(s_1)} \not\subseteq \boldsymbol{N}_{f}$, либо $\boldsymbol{N}_{x_i^{\bar{\alpha}} \wedge K(s_1)} \cap \boldsymbol{N}_{f} \neq \varnothing$.

Условия 4.1 и 4.2 эквивалентны тому, что $\boldsymbol{N}_{x_i^{\alpha} \wedge K(s)} \subseteq \boldsymbol{N}_{f_{i,\alpha}}$, а из условия 4.3 вытекает, что элементарная конъюнкция $x_i^{\alpha} \wedge K(s)$ определяет максимальную допустимую грань для булевой функции $f_{i,\alpha}$. Следовательно, $s \in S_{ir}^{o}(i, \alpha, f)$ тогда и только тогда, когда $x_i^{\alpha} \wedge K(s) \in D_{f_{i,\alpha}}^{сокр}$, что и требовалось доказать.

Теорема доказана.

Из теоремы 4.5 вытекает, что:

1. Построение множеств $S_{ir}^{c}(\alpha, f)$ и $S_{ir}^{o}(i, \alpha, f)$ эквивалентно построению сокращенных ДНФ, соответственно, $D_{f^{\alpha}}^{сокр}$ и $D_{f_{i,\alpha}}^{сокр}$.
2. Вычисление $v^{c}(\alpha, f)$ и $v^{o}(i, \alpha, f)$ эквивалентно вычислению минимальных рангов для простых импликант, входящих в сокращенные ДНФ, соответственно, $D_{f^{\alpha}}^{сокр}$ и $D_{f_{i,\alpha}}^{сокр}$.
3. Построение множеств $S_{\min}^{c}(\alpha, f)$ и $S_{\min}^{o}(i, \alpha, f)$ эквивалентно перечислению всех простых импликант, входящих в сокращенные ДНФ, соответственно, $D_{f^{\alpha}}^{сокр}$ и $D_{f_{i,\alpha}}^{сокр}$.

Таким образом, сложность построения множеств $S_{ir}^{c}(\alpha, f)$, $S_{ir}^{o}(i, \alpha, f)$, $S_{\min}^{c}(\alpha, f)$, $S_{\min}^{o}(i, \alpha, f)$ и вычисления параметров $v^{c}(\alpha, f)$, $v^{o}(i, \alpha, f)$, $v^{o}(i, f)$ определяется сложностью построения соответствующих сокращенных ДНФ.

Из оценок типичных значений параметров, характеризующих сокращенную ДНФ (см., напр. [18,47]) непосредственно вытекает справедливость следующей теоремы.

Теорема 4.6. Для почти всех булевых функций $f \in P_2(n)$ при всех $1 \le i \le n$ и $\alpha \in \mathbf{E}$, если $n \to \infty$, то:

1) $|s| \sim n - \log\log n$ для почти всех $s \in S_{ir}^{c}(\alpha, f) \cup S_{ir}^{o}(i, \alpha, f)$;

2) $n - \log n - 2 \le v \le n - \log\log n + 1 \quad (v \in \{v^{c}(\alpha, f), v^{o}(i, \alpha, f)\})$;

3) $|S^c_{\min}(\alpha,f)|=o(|S^c_{ir}(\alpha,f)|)$ и $|S^o_{\min}(i,\alpha,f)|=o(|S^o_{ir}(i,\alpha,f)|)$.

Значение теоремы 4.6 состоит в следующем. Выше было отмечено, что сложность построения множеств $S^c_{\min}(\alpha,f)$, $S^o_{\min}(i,\alpha,f)$ и вычисления параметров $\nu^c(\alpha,f)$, $\nu^o(i,\alpha,f)$, $\nu^o(i,f)$ определяется сложностью построения соответствующих сокращенных ДНФ, т.е. осуществляется с помощью алгоритма 4.4 (или с помощью любого из алгоритмов, приведенных в п.1.4). Построение одного, безразлично какого именно, множества $s\in S^c_{ir}(\alpha,f)$ или $s\in S^o_{ir}(i,\alpha,f)$ можно осуществить с помощью алгоритма 4.1. Значение $|s|$ построенного множества s может быть выбрано в качестве *приближенного значения* $\nu^c(\alpha,f)$, соответственно, $\nu^o(i,\alpha,f)$. Допускаемая при этом ошибка для почти всех $f\in P_2(n)$ при всех $1\le i\le n$ и $\alpha\in\mathbf{E}$ не превосходит величины

$$\Delta=O(\log(n\cdot(\log n)^{-1}))\quad(n\to\infty).$$

Рассмотрим композицию $f^{i_1,\dots,i_k}_{g_1,\dots,g_k}$ булевых функций $f(x_1,\dots,x_n)$ и $g_j(y_{j1},\dots,y_{jm_j})$ $(j=1,\dots,k)$. Известно (см., напр. [10]), что если композиция – *бесповторная*, т.е. переменные $x_1,\dots,x_m,y_{11},\dots,y_{1m_1},\dots,y_{k1},\dots,y_{km_k}$ попарно различны, то сокращенная ДНФ $D^{сокр}_{f^{i_1,\dots i_k}_{g_1,\dots,g_k}}$ может быть получена в результате замены в сокращенной ДНФ $D^{сокр}_f$ каждого вхождения литерала $x^{\sigma_j}_{i_j}$ $(\sigma_j\in\mathbf{E};\ j=1,\dots,k)$ сокращенной ДНФ $D^{сокр}_{g^{\sigma_j}_j}$ и раскрытия скобок на основании закона дистрибутивности: $a\wedge(b\vee c)=a\wedge b\vee a\wedge c$.

Следовательно, построение одного, безразлично какого именно, множества:

1) $s\in S^c_{ir}(\alpha,f^{i_1,\dots i_k}_{g_1,\dots,g_k})$ можно осуществить путем замены в множестве $s_1\in S^c_{ir}(\alpha,f)$ каждой пары (i_j,σ_j) $(j=1,\dots,k)$ множеством $s_j\in S^c_{ir}(\sigma_j,g_j)$;
2) $s\in S^o_{ir}(i,\alpha,f^{i_1,\dots i_k}_{g_1,\dots,g_k})$ можно осуществить при $i\ne i_j$ $(j=1,\dots,k)$ заменой в множестве $s_1\in S^o_{ir}(i,\alpha,f)$ каждой пары (i_j,σ_j) $(j=1,\dots,k)$ множеством $s_j\in S^c_{ir}(\sigma_j,g_j)$, а при $i=hl_h$ - заменой в множестве $s_1\in S^o_{ir}(i,\alpha,f)$ (соответственно, в множестве $s_1\in S^o_{ir}(i,\overline{\alpha},f)$) каждой пары (i_j,σ_j) $(j=1,\dots,k)$ множеством $s_j\in S^c_{ir}(\sigma_j,g_j)$ и добавлением к полученному множеству множества $s_h\in S^o_{ir}(hl_h,1,f)$ (соответственно, множества $s_h\in S^o_{ir}(hl_h,0,f)$).

Построение множеств $S^c_{ir}(\alpha,f^{i_1,\dots i_k}_{g_1,\dots,g_k})$ и $S^o_{ir}(i,\alpha,f^{i_1,\dots i_k}_{g_1,\dots,g_k})$ осуществляется всевозможными такими заменами. Вычисления $\nu^c(\alpha,f^{i_1,\dots i_k}_{g_1,\dots,g_k})$ и $\nu^o(i,\alpha,f^{i_1,\dots i_k}_{g_1,\dots,g_k})$ следующим образом сводятся к арифметическим действиям над значениями $\nu^c(\alpha,f)$, $\nu^c(\sigma_j,g_j)$, $\nu^o(i,\alpha,f)$ и $\nu^o(hl_h,\alpha,f)$. Пусть

$$\mu(x^\sigma_i)=\begin{cases}\nu^c(\sigma,g_{i_j})\ , & \text{если } i\in\{i_1,\dots,i_k\} \text{ и } i=i_j\,,\\ 1\ , & \text{если } i\in\{1,\dots,k\}\setminus\{i_1,\dots,i_k\}\end{cases}.$$

Для элементарной конъюнкции $K=\bigwedge_{l=1}^{r}x^{\sigma_l}_{j_l}$ положим

$$\mu(K)=\sum_{l=1}^{r}\mu(x_{j_l}^{\sigma_l}),$$

считая, что

$$a+\infty=\infty+a=\infty+\infty=\infty.$$

Тогда

$$\nu^c(\alpha,f_{g_1,\ldots,g_k}^{i_1,\ldots,i_k})=\min_{s\in S_{ir}^c(\alpha,f)}\mu(K(s)),$$

и

$$\nu^o(i,\alpha,f_{g_1,\ldots,g_k}^{i_1,\ldots,i_k})=\begin{cases}\min\limits_{s\in S_{ir}^o(i,\alpha,f)}\mu(K(s)) \text{ , если } i\in\{1,\ldots,n\}\setminus\{i_1,\ldots,i_k\},\\ \min\{\nu_1,\nu_2\} \quad , \quad \text{если } i=hl \ \ (h=i_j,\ l=1,\ldots,m_j)\end{cases},$$

где

$$\nu_1=\min_{s\in S_{ir}^o(h,\alpha,f)}\mu(K(s))+\nu^o(hl,1,g_h)$$

и

$$\nu_2=\min_{s\in S_{ir}^o(h,\bar{\alpha},f)}\mu(K(s))+\nu^o(hl,0,g_h).$$

Если композиция $f_{g_1,\ldots,g_k}^{i_1,\ldots,i_k}$ булевых функций $f(x_1,\ldots,x_n)$ и $g_j(y_{j1},\ldots,y_{jm_j})$ $(j=1,\ldots,k)$ не является бесповторной, то замена в сокращенной ДНФ $D_f^{сокр}$ каждого вхождения литерала $x_{i_j}^{\sigma_j}$ $(\sigma_j\in\mathbf{E};\ j=1,\ldots,k)$ сокращенной ДНФ $D_{g_j^{\sigma_j}}^{сокр}$ (с последующим раскрытием скобок на основании закона дистрибутивности) может привести к ДНФ D, которая не является сокращенной ДНФ $D_{f_{g_1,\ldots,g_k}^{i_1,\ldots,i_k}}^{сокр}$. Поэтому необходимо перейти от ДНФ D к сокращенной ДНФ $D_{f_{g_1,\ldots,g_k}^{i_1,\ldots,i_k}}^{сокр}$ и осуществить ее анализ методом, изложенным выше.

Развитые средства являются основой для конструирования совместимой с системой моделирования электронных схем подсистемы, предназначенной для вычисления параметров управляемости и наблюдаемости узлов комбинационных схем, а также для построения входных наборов, обеспечивающих требуемые значения в заданных узлах. Такая подсистема состоит из пяти *блоков*. *Блок 1* формирует описание исследуемой схемы в терминах элементов, выбранных в качестве *стандартных*. Для каждого такого элемента БИБЛИОТЕКА, организованная в *Блоке 2*, содержит описание неприводимых множеств и параметров управляемости и наблюдаемости. БИБЛИОТЕКА допускает пополнение, осуществляемое с помощью *Блоков 3* и *4*. *Блок 3*, взаимодействуя с системой моделирования, формирует исходные данные для *Блока 4*, основу которого составляют алгоритмы 4.1-4.4. *Блок 5* вычисляет множества и параметры управляемости и наблюдаемости для композиций. В случае получения неудовлетворительных результатов, вызванных наличием сходящихся разветвлений, соответствующий фрагмент схемы объявляется *стандартным элементом*, его характеристики вычисляются и заносятся в БИБЛИОТЕКУ. Описание схемы переделывается соответствующим образом и проводится анализ преобразованной схемы.

4.3. Идентификация булевых вектор-функций.

Основной целью настоящего пункта является разработка методов идентификации булевых вектор-функций на основе теории линейных пространств над конечными полями. Актуальность этой проблемы обусловлена следующим. Известно, что идентификация булевой функции является одной из центральных проблем дискретной математики, имеющей многочисленные приложения. Классический подход к решению этой проблемы основан на методе полного перебора и имеет экспоненциальную сложность (как временную, так и емкостную). Известно, что одним из способов понижения сложности решения является замена (там, где это возможно) перебора алгебраическими операциями. Такой подход применим к рассматриваемой проблеме, а именно:

представление булевой вектор-функции в виде подмножества линейного пространства дает возможность идентифицировать ее с помощью специально подобранных линейных операторов.

Введем необходимые понятия и определения. Обозначим через $P_{m,n}$ $(m,n \in \mathbf{N})$ множество всех функций

$$f : \mathbf{E}^m \to \mathbf{E}^n .$$

График функции $f \in P_{m,n}$ определим как множество

$$graph\ f = \{(\alpha_1,\ldots,\alpha_{m+n}) \mid f(\alpha_1,\ldots,\alpha_m) = (\alpha_{m+1},\ldots,\alpha_{m+n})\} .$$

Отметим, что это множество, как и любое функциональное отношение, обладает следующим свойством: если $\mathbf{a} = (\alpha_1,\ldots,\alpha_{m+n}) \in graph\ f$, $\mathbf{b} = (\beta_1,\ldots,\beta_{m+n}) \in graph\ f$ и $\mathbf{a} \neq \mathbf{b}$, то существует, по крайней мере, одно такое значение $j \in \{1,\ldots,m\}$, что $\alpha_j \neq \beta_j$.

Рассмотрим следующую проблему:

Проблема 4.5. Заданы функция $f \in P_{m,n}$ и множество $\Omega \subseteq \mathbf{E}^{m+n}$. Проверить, истинно ли включение

$$\Omega \subseteq graph\ f\ ? \tag{4.19}$$

Известно, что при всех $k \in \mathbf{N}$ система $\mathbf{GF}^k(2) = (\mathbf{E}^k,+,\cdot)$ является k-мерным линейным пространством над полем $\mathbf{GF}(2)$. Поэтому естественно исследовать возможность решения проблемы 4.5 методами теории линейных пространств над полями Галуа. Такой подход дает возможность использовать стандартные алгебраические операции линейного пространства $\mathbf{GF}^k(2)$. Следовательно, могут быть определены *легко вычислимые характеристические функции* – это те функции, которые могут быть представлены множествами линейных операторов. Таким образом, мы естественно приходим к следующему определению.

Определение 4.3. *Линейной характеристической функцией* множества $graph\ f$ $(f \in P_{m,n})$ назовем такое множество

$$\chi_f = \{M_i \mid i = 1,\ldots,l\}$$

матриц над полем $\mathbf{GF}(2)$, что для любого вектора $\mathbf{a} \in \mathbf{E}^{m+n}$

$$\mathbf{a}M_i = \mathbf{0},$$

хотя бы для одного значения $i \in \{1,\dots,l\}$, тогда и только тогда, когда $\mathbf{a} \in graph\ f$

Положим

$$\chi_f(\mathbf{a}) = \{\mathbf{a}M_i \mid i = 1,\dots,l\} \quad (\mathbf{a} \in \mathbf{E}^{m+n}).$$

Таким образом,

$$\mathbf{a} \in graph\ f \Leftrightarrow \mathbf{0} \in \chi_f(\mathbf{a}) \quad (\mathbf{a} \in \mathbf{E}^{m+n}, f \in P_{m,n}).$$

Исследуем структуру множества $graph\ f \quad (f \in P_{m,n})$.

Утверждение 4.1. Для любой функции $f \in P_{m,n}$ число линейно независимых векторов, принадлежащих множеству $graph\ f$, не меньше, чем m.

Доказательство. Для любой функции $f \in P_{m,n}$ множество $graph\ f$ содержит элементы

$$\mathbf{e}_i = (\underbrace{0,\dots,0}_{i-1},1,\underbrace{0,\dots,0}_{m-i},\beta_1,\dots,\beta_n) \quad (i = 1,\dots,m), \tag{4.20}$$

где

$$f(\underbrace{0,\dots,0}_{i-1},1,\underbrace{0,\dots,0}_{m-i}) = (\beta_1,\dots,\beta_n).$$

Векторы $\mathbf{e}_1,\dots,\mathbf{e}_m$ - линейно независимые и их число равно m, что и требовалось показать.

Утверждение доказано.

Очевидно, что $P_{m,n} = (P_{m,1})^n$, где $P_{m,1} = P_2(m)$. Поэтому, когда это удобно, будем представлять функцию $f \in P_{m,n}$ в виде

$$f = (f_1,\dots,f_n),$$

где

$$f_j = pr_j f \quad (j = 1,\dots,n).$$

Обозначим через $\mathbf{T}_0(m)$ множество всех функций $f \in P_{m,1}$, сохраняющих константу 0, а через $\mathbf{L}(m)$ - множество всех линейных функций $f \in P_{m,1}$.

Теорема 4.7. Множество $graph\ f \quad (f \in P_{m,n})$ является подпространством линейного пространства $\mathbf{GF}^{m+n}(2)$ тогда и только тогда, когда

$$f \in (\mathbf{T}_0(m) \cap \mathbf{L}(m))^n.$$

Доказательство. Множество $graph\ f \quad (f \in P_{m,n})$ является подпространством линейного пространства $\mathbf{GF}^{m+n}(2)$ тогда и только тогда, когда

$$\mathbf{0} \in graph\ f \tag{4.21}$$

и

$$(\alpha_1,\ldots,\alpha_{m+n}),(\beta_1,\ldots,\beta_{m+n}) \in graph\ f \Rightarrow (\alpha_1+\beta_1,\ldots,\alpha_{m+n}+\beta_{m+n}) \in graph\ f\,. \tag{4.22}$$

Соотношение (4.21) эквивалентно равенству $f(\mathbf{0}) = \mathbf{0}$. Последнее – истинное тогда и только тогда, когда $pr_j f \in \mathbf{T}_0(m)$ для всех $j = 1,\ldots,n$.

Соотношение (4.22) эквивалентно условию: равенства

$$pr_j f(\alpha_1,\ldots\alpha_m) + pr_j f(\beta_1,\ldots\beta_m) = pr_j f(\alpha_1+\beta_1,\ldots\alpha_m+\beta_m) \quad (j=1,\ldots,n)$$

являются истинными для всех $(\alpha_1,\ldots,\alpha_n),(\beta_1,\ldots,\beta_n) \in \mathbf{E}^m$. Это условие, в свою очередь, эквивалентно тому, что $pr_j f \in \mathbf{L}(m)$ для всех $j = 1,\ldots,n$.

Итак, показано, что множество $graph\ f \quad (f \in P_{m,n})$ является подпространством линейного пространства $\mathbf{GF}^{m+n}(2)$ тогда и только тогда, когда $pr_j f \in \mathbf{T}_0(m) \cap \mathbf{L}(m)$ для всех $j = 1,\ldots,n$. Последнее условие эквивалентно тому, что $f \in (\mathbf{T}_0(m) \cap \mathbf{L}(m))^n$, что и требовалось доказать.

Теорема доказана.

Следствие 4.4. Множество $graph\ f \quad (f \in P_{m,n})$ является подпространством линейного пространства $\mathbf{GF}^{m+n}(2)$ тогда и только тогда, когда

$$pr_j f = x_{j1} + \ldots + x_{jr_j}$$

для всех $j = 1,\ldots,n$.

Доказательство. Так как

$$\mathbf{T}_0^n(m) = \{f \in P_{m,n} \mid f(\mathbf{0}) = \mathbf{0}\}$$

и

$$\mathbf{L}^n(m) = \{f \in P_{m,n} \mid pr_j\ f = \alpha_j + x_{j1} + \ldots + x_{jr_j} \ \ (\alpha_j \in \mathbf{E}) \text{ для всех } j = 1,\ldots,n\},$$

то

$$(\mathbf{T}_0(m) \cap \mathbf{L}(m))^n = \mathbf{T}_0^n(m) \cap \mathbf{L}_0^n(m) =$$

$$= \{f \in P_{m,n} \mid pr_j\ f = x_{j1} + \ldots + x_{jr_j} \text{ для всех } j = 1,\ldots,n\},$$

что и требовалось доказать.

Следствие доказано.

Обозначим через $Dim\,V$ размерность подпространства V линейного пространства $\mathbf{GF}^{m+n}(2)$, а через $V^{\perp}$ - ортогональное дополнение подпространства V.

Утверждение 4.2. Если множество $graph\, f$ $(f \in P_{m,n})$ является подпространством линейного пространства $\mathbf{GF}^{m+n}(2)$, то

$$Dim\, graph\, f = m$$

и

$$Dim\,(graph\, f)^{\perp} = n\,.$$

Доказательство. Пусть $graph\, f$ $(f \in P_{m,n})$ - подпространство линейного пространства $\mathbf{GF}^{m+n}(2)$. Тогда (см. утверждение 4.1)

$$Dim\, graph\, f \geq m\,.$$

Покажем, что векторы $\mathbf{e}_1,\ldots,\mathbf{e}_m$, определяемые соотношением (4.20), образуют базис пространства $graph\, f$. Выберем произвольный вектор

$$\mathbf{a} = (\alpha_1,\ldots,\alpha_m,\gamma_1,\ldots,\gamma_n) \in graph\, f\,.$$

Пусть среди его первых m ненулевыми будут те и только те, которые имеют номера $j_1,\ldots,j_r$ $(1 \leq j_1 < \ldots < j_r \leq m)$. Рассмотрим вектор

$$\mathbf{b} = \mathbf{e}_{j_1} + \ldots + \mathbf{e}_{j_r} = (\alpha_1,\ldots,\alpha_m,\delta_1,\ldots,\delta_n)\,.$$

Так как $\mathbf{a},\mathbf{b} \in graph\, f$ и $graph\, f$ - линейное пространство, то

$$\mathbf{a}+\mathbf{b} = (\underbrace{0,\ldots,0}_{m},\gamma_1+\delta_1,\ldots,\gamma_n+\delta_n) \in graph\, f\,.$$

А так как (см. теорему 4.7) $f \in \mathbf{T}_0^n(m)$, то

$$\gamma_i + \delta_i = 0 \Leftrightarrow \gamma_i = \delta_i$$

для всех $i = 1,\ldots,n$. Это означает, что

$$\mathbf{a}+\mathbf{b} = \mathbf{e}_{j_1} + \ldots + \mathbf{e}_{j_r}\,.$$

Итак, показано, что любой вектор $\mathbf{a} \in graph\, f$ является линейной комбинацией линейно независимых векторов $\mathbf{e}_1,\ldots,\mathbf{e}_m$. Следовательно, векторы $\mathbf{e}_1,\ldots,\mathbf{e}_m$ образуют базис пространства $graph\, f$. Отсюда непосредственно вытекает, что $Dim\, graph\, f = m$, что и требовалось доказать.

Для любого подпространства V линейного пространства U истинно равенство

$$Dim\, V + Dim\, V^{\perp} = Dim\, U\,.$$

Воспользуемся этим равенством. Получим

$$Dim\,(graph\, f)^{\perp} = Dim\,\mathbf{GF}^{m+n}(2) - Dim\, graph\, f = (m+n) - m = n\,,$$

что и требовалось доказать.

Утверждение доказано.

Обозначим через

$$\mathbf{Lin}(graph\ f) \quad (f \in P_{m,n})$$

множество всех максимальных по включению подпространств линейного пространства $\mathbf{GF}^{m+n}(2)$, содержащихся во множестве $graph\ f$.

Теорема 4.8. Множество $\mathbf{Lin}(graph\ f)$ $(f \in P_{m,n})$ - непустое тогда и только тогда, когда $f \in \mathbf{T}_0^n(m)$.

Доказательство. Пусть $f \notin \mathbf{T}_0^n(m)$. Тогда $\mathbf{0} \notin graph\ f$. Следовательно, ни одно подпространство линейного пространства $\mathbf{GF}^{m+n}(2)$ не содержится во множестве $graph\ f$, т.е. $\mathbf{Lin}(graph\ f) = \varnothing$.

Для дальнейшего доказательства нам понадобится следующая лемма.

Лемма 4.1. Для любого вектора $\mathbf{a} \in \mathbf{E}^{m+n} \setminus \{\mathbf{0}\}$ множество $V = \{\mathbf{0}, \mathbf{a}\}$ - подпространство линейного пространства $\mathbf{GF}^{m+n}(2)$.

Доказательство. Так как $\mathbf{0} \in graph\ f$, то условие (4.21) выполнено. А так как

$$\mathbf{0}+\mathbf{0}=\mathbf{0}, \qquad \mathbf{0}+\mathbf{a}=\mathbf{a}+\mathbf{0}=\mathbf{a}, \qquad \mathbf{a}+\mathbf{a}=\mathbf{0},$$

то выполнено и условие (4.22). Следовательно, $V = \{\mathbf{0}, \mathbf{a}\}$ - подпространство линейного пространства $\mathbf{GF}^{m+n}(2)$, что и требовалось доказать.

Лемма доказана.

Пусть $f \in \mathbf{T}_0^n(m)$. Тогда $\mathbf{0} \in graph\ f$. Так как

$$|\ graph\ f\ | = 2^{m+n},$$

то существует ненулевой вектор $\mathbf{a} \in graph\ f$. Следовательно, $\{\mathbf{0}, \mathbf{a}\}$ - подпространство линейного пространства $\mathbf{GF}^{m+n}(2)$, удовлетворяющее включению

$$\{\mathbf{0}, \mathbf{a}\} \subseteq graph\ f.$$

Из этого включения вытекает, что существует максимальное по включению подпространство V линейного пространства $\mathbf{GF}^{m+n}(2)$, удовлетворяющее включениям

$$\{\mathbf{0}, \mathbf{a}\} \subseteq V \subseteq graph\ f.$$

Так как $V \in \mathbf{Lin}(graph\ f)$, то $\mathbf{Lin}(graph\ f) \neq \varnothing$.

Теорема доказана.

Таким образом, множество $\mathbf{Lin}(graph\ f)$ $(f \in P_{m,n})$ может быть использовано для исследования свойств множества $graph\ f$ тогда и только тогда, когда $f \in \mathbf{T}_0^n(m)$. Следующее утверждение показывает, что исследование множества $graph\ f$ $(f \in P_{m,n})$ *всегда можно свести* к исследованию такого множества $graph\ g$, что $g \in \mathbf{T}_0^n(m)$.

Утверждение 4.3. Для любой функции $f \in P_{m,n}$ существует единственный такой вектор $\mathbf{a} \in \mathbf{E}^n$, что

$$g = f + \mathbf{a} \in \mathbf{T}_0^n(m).$$

Доказательство. Пусть $f \in P_{m,n}$ и $g = f + \mathbf{a}$, где $\mathbf{a} \in \mathbf{E}^n$. Тогда

$$g \in \mathbf{T}_0^n(m) \Leftrightarrow g(\mathbf{0}) = \mathbf{0} \Leftrightarrow f(\mathbf{0}) + \mathbf{a} = \mathbf{0} \Leftrightarrow \mathbf{a} = f(\mathbf{0}),$$

откуда вытекает, что для любой функции $f \in P_{m,n}$ требуемый вектор $\mathbf{a} \in \mathbf{E}^n$ существует и единственный.

Утверждение доказано.

Значение утверждения 4.3 состоит в следующем. Пусть $f \in P_{m,n} \setminus \mathbf{T}_0^n(m)$. Заменим множество $graph\, f$ множеством $graph\, g$, где $g = f + f(\mathbf{0}) \in \mathbf{T}_0^n(m)$. Исследуем последнее в терминах множества $\mathbf{Lin}(graph\, g)$. Из построения функции g вытекает, что множество $graph\, g$ - результат *сдвига* множества $graph\, f$ на вектор $f(\mathbf{0})$. Указанная биекция дает возможность переформулировать любое утверждение относительно множества $graph\, g$ в соответствующее утверждение относительно множества $graph\, f$. Поэтому, в дальнейшем будем рассматривать только функции, принадлежащие множеству $\mathbf{T}_0^n(m)$.

Теорема 4.9. Для любой функции $f \in \mathbf{T}_0^n(m)$ истинно равенство

$$graph\, f = \bigcup_{V \in \mathbf{Lin}(graph\, f)} V. \tag{4.23}$$

Доказательство. Пусть $f \in \mathbf{T}_0^n(m)$. Из определения множества $\mathbf{Lin}(graph\, f)$ вытекает, что для любого $V \in \mathbf{Lin}(graph\, f)$ включение $V \subseteq graph\, f$ - истинное. Следовательно, включение

$$graph\, f \supseteq \bigcup_{V \in \mathbf{Lin}(graph\, f)} V. \tag{4.24}$$

является истинным.

Докажем, что обратное включение

$$graph\, f \subseteq \bigcup_{V \in \mathbf{Lin}(graph\, f)} V. \tag{4.25}$$

также является истинным.

Пусть $\mathbf{a} \in graph\, f$. Возможны два случая.

Предположим, что $\mathbf{a} = \mathbf{0}$. Так как вектор $\mathbf{0}$ является элементом любого подпространства линейного пространства $\mathbf{GF}^{m+n}(2)$ и $\mathbf{Lin}(graph\, f) \neq \varnothing$ (см. теорему 4.8), то

$$\mathbf{0} \in \bigcup_{V \in \mathbf{Lin}(graph\, f)} V.$$

Предположим теперь, что $\mathbf{a} \in graph\, f \setminus \{\mathbf{0}\}$. Множество $\{\mathbf{0}, \mathbf{a}\}$ (см. лемму 4.1) - подпространство линейного пространства $\mathbf{GF}^{m+n}(2)$. Следовательно, существует максимальное по включению подпространство V линейного пространства $\mathbf{GF}^{m+n}(2)$, удовлетворяющее включениям $\{\mathbf{0},\mathbf{a}\} \subseteq V \subseteq graph\ f$. А так как $\mathbf{a} \in V$ и $V \in \mathbf{Lin}(graph\ f)$, то

$$\mathbf{a} \in \bigcup_{V \in \mathbf{Lin}(graph\ f)} V.$$

Таким образом, показано, что включение (4.25) – истинное.

Из включений (4.24) и (4.25) вытекает, что равенство (4.23) – истинное, что и требовалось доказать.

Теорема доказана.

Итак, для любой функции $f \in \mathbf{T}_0^n(m)$ множество $graph\ f$ можно *расщепить* на подпространства, принадлежащие множеству $\mathbf{Lin}(graph\ f)$. Это *расщепление* – тривиальное, если (см. теорему 4.7) $f \in (\mathbf{T}_0(m) \cap \mathbf{L}(m))^n$.

Пусть V - подпространство линейного пространства $\mathbf{GF}^{m+n}(2)$. Выберем в ортогональном дополнении $V^{\perp}$ базис $\mathbf{e}_1,\ldots,\mathbf{e}_{m+n-Dim\,V}$. Обозначим через E_V матрицу порядка $(m+n)\times(m+n-Dim\,V)$, столбцы которой – это векторы $\mathbf{e}_1,\ldots,\mathbf{e}_{m+n-Dim\,V}$.

Теорема 4.10. Для любой функции $f \in \mathbf{T}_0^n(m)$ множество матриц

$$\chi_f = \{E_V \mid V \in \mathbf{Lin}(graph\ f)\} \tag{4.26}$$

является линейной характеристической функцией множества $graph\ f$.

Доказательство. Пусть $f \in \mathbf{T}_0^n(m)$ и множество матриц χ_f построено в соответствии с равенством (4.26). Тогда для любого вектора $\mathbf{a} \in \mathbf{E}^{m+n}$

$$\mathbf{0} \in \chi_f(\mathbf{a}) \Leftrightarrow (\exists V \in \mathbf{Lin}(graph\ f))(\mathbf{a} \cdot E_V = \mathbf{0}). \tag{4.27}$$

По построению, столбцы матрицы E_V образуют базис подпространства $V^{\perp}$. Следовательно, для любого вектора $\mathbf{a} \in \mathbf{E}^{m+n}$

$$\mathbf{a} \cdot E_V = \mathbf{0} \Leftrightarrow \mathbf{a} \in V. \tag{4.28}$$

Из (4.27) и (4.28) вытекает, что для любого вектора $\mathbf{a} \in \mathbf{E}^{m+n}$

$$\mathbf{0} \in \chi_f(\mathbf{a}) \Leftrightarrow (\exists V \in \mathbf{Lin}(graph\ f))(\mathbf{a} \in V). \tag{4.29}$$

По условию, $f \in \mathbf{T}_0^n(m)$. Следовательно (см. теорему 4.9), из (4.29) вытекает, что для любого вектора $\mathbf{a} \in \mathbf{E}^{m+n}$

$$\mathbf{0} \in \chi_f(\mathbf{a}) \Leftrightarrow \mathbf{a} \in graph\ f. \tag{4.30}$$

Из (4.30) вытекает, что χ_f - линейная характеристическая функция множества $graph\ f$, что и требовалось доказать.

Теорема доказана.

Из утверждения 4.3 и теоремы 4.10 вытекает, что решение проблемы 4.5 может быть получено с помощью следующего алгоритма.

Алгоритм 4.5.

Шаг 1. Если $f \notin \mathbf{T}_0^n(m)$, то $f := f + f(\mathbf{0})$, $\Omega := \Omega + f(\mathbf{0})$.

Шаг 2. Построить множество матриц χ_f в соответствии с равенством (4.26).

Шаг 3. Вычислить $\chi_f(\mathbf{a})$ для всех $\mathbf{a} \in \Omega$.

Шаг 4. Если $\mathbf{0} \in \chi_f(\mathbf{a})$ для всех $\mathbf{a} \in \Omega$, то включение (4.19) – истинное, иначе включение (4.19) – ложное.

Сложность решения проблемы 4.5 алгоритмом 4.5 определяется как мощностью множества Ω, так и сложностью *расщепления* множества $graph\ f$ на элементы множества $\mathbf{Lin}(graph\ f)$. В [73] показано, что такое *расщепление* может состоять из достаточно большого количества подпространств различных размерностей.

4.4. Выводы.

Раздел 4 является логическим продолжением раздела 2. Разработанные в нем модели и методы предназначены для анализа булевых функций. Основные результаты состоят в следующем:

1. Разработаны алгоритмы решения фундаментальных проблем поиска одной и всех простых импликант, покрывающих заданную точку. Эти алгоритмы основаны на последовательном вычеркивании литералов.

2. На основе последовательного применения указанных выше алгоритмов решены фундаментальные проблемы поиска ДНФ, состоящих только из простых импликант.

3. Впервые построена теория анализа управляемости/наблюдаемости булевых функций. Эта теория основана на моделях и методах поиска простых импликант и состоящих из них ДНФ.

4. Впервые решена проблема идентификации булевых вектор-функций методами теории линейных пространств над полями Галуа.

Таким образом, в разделе 4 разработан законченный фрагмент комбинаторно-алгебраической теории анализа булевых функций, на основе которой получено исчерпывающее решение проблемы 1.11.

Основные результаты раздела 3 опубликованы в [64-68,73].

5. ДДФ-СИСТЕМЫ

Классический подход к задачам управления основан на предположении, что исследуемый объект является *идеальным*, т.е. что все процессы протекают в нем в строгом соответствии с заранее определенными требованиями. Однако в процессе взаимодействия исследуемого объекта с внешней средой действия последней на объект часто носят дестабилизирующий характер. Эта дестабилизация проявляется в следующих двух аспектах. Во-первых, дестабилизации может быть подвергнут непосредственно сам исследуемый объект, т.е. алгоритмы, процессы и структура, определяющие его предназначение. Во-вторых, дестабилизации могут подвергаться как входные воздействия на исследуемый объект, так и его реакция. Таким образом, естественно возникает проблема разработки представления систем, подверженных действиям дестабилизирующих факторов. Актуальность и значение этой проблемы вытекает из того, что именно от этого представления, во многом, и зависит существование эффективных методов исследования указанных систем.

В настоящем разделе разработаны модели и методы, предназначенные для анализа систем, подверженных дестабилизирующим воздействиям внешней среды. Эти модели названы ДДФ-системами. В п.5.1 определены основные понятия. В п.5.2 построены композиции ДДФ-систем. В п.5.3 решена проблема адаптивного управления ДДФ-системой методами теории информации.

5.1. Основные понятия и определения.

Цель настоящего пункта – разработка аксиоматики для ДДФ-систем. Актуальность этой проблемы обусловлена следующим: аксиоматическое построение дает возможность *вложить* ДДФ-системы в математическую теорию систем и, следовательно, использовать весь арсенал ее методов и средств.

Основным понятием является *дестабилизатор* $\boldsymbol{D}$. Говоря неформально, дестабилизатор представляет собой множество наборов отображений и операторов, действующих на объекты *идеальной* модели. Это понятие дает возможность определить ДДФ-систему либо как упорядоченную пару

$$\boldsymbol{T} = (\boldsymbol{S}, \boldsymbol{D}),$$

где $\boldsymbol{S}$ - идеальная модель, либо (что то же самое) как семейство обычных систем

$$\boldsymbol{A} = \{\boldsymbol{S_d} \mid \boldsymbol{d} \in \boldsymbol{D}\}.$$

Выполнение условия

$$\boldsymbol{S} \in \boldsymbol{A}$$

дает возможность исследовать *идеальную* модель в терминах ДДФ-систем.

Для формального определения понятия *дестабилизатор* достаточно построить его в явном виде для основных типов моделей систем. В качестве таких моделей выберем некоторые системы из п.1.1.

Пусть *идеальная* модель - это абсолютный черный ящик

$$\boldsymbol{S} \subseteq X \times Y \quad (X \subseteq A^T, Y \subseteq B^T).$$

Зафиксируем множества операторов

$$D_{in} \subseteq \{f \mid f : X \to X_{ins}\} \quad (X_{ins} \subseteq A^T)$$

и

$$D_{out} \subseteq \{f \mid f : Y \to Y_{ins}\} \quad (Y_{ins} \subseteq B^T),$$

каждое содержит тождественный оператор, соответственно, i_{in} и i_{out}.

Определение 5.1. Дестабилизатором абсолютного черного ящика

$$\boldsymbol{S} \subseteq X \times Y \quad (X \subseteq A^T, Y \subseteq B^T)$$

назовем любое такое множество

$$\boldsymbol{D} \subseteq D_{in} \times D_{out},$$

что

$$(i_{in}, i_{out}) \in \boldsymbol{D}.$$

Из определения 5.1 вытекает, что ДДФ-система $\boldsymbol{A}$ состоит из таких абсолютных черных ящиков $\boldsymbol{S}_{\boldsymbol{d}}$ $(\boldsymbol{d} = (d_{in}, d_{out}) \in \boldsymbol{D})$, что

$$\boldsymbol{S}_{\boldsymbol{d}} = \{(d_{in}(x), d_{out}(y)) \mid (x, y) \in \boldsymbol{S}\}.$$

Пусть *идеальная* модель – это относительный черный ящик

$$\boldsymbol{S} = (C, X, Y, R) \ \ (X \subseteq A^T, Y \subseteq B^T),$$

где C - множество начальных состояний, а

$$R : C \times X \to Y \ \text{-}$$

глобальная реакция. Кроме множеств D_{in} и D_{out} зафиксируем также множество отображений

$$D_{in-st} \subseteq \{f \mid f : C \to C\},$$

содержащее тожественное отображение i_{in-st} и множество операторов

$$D_{gr} \subseteq \{f \mid f : \{R\} \to F_{ins}\} \quad (F_{ins} \subseteq \{f \mid f : C \times X_{ins} \to Y_{ins}\}),$$

содержащее тожественный оператор i_{gr}.

Определение 5.2. Дестабилизатором относительного черного ящика

$$\boldsymbol{S} = (C, X, Y, R) \quad (X \subseteq A^T, Y \subseteq B^T),$$

назовем любое такое множество

$$\boldsymbol{D} \subseteq D_{in-st} \times D_{in} \times D_{out} \times D_{gr},$$

что

$$(i_{in-st}, i_{in}, i_{out}, i_{gr}) \in \boldsymbol{D}$$

и

$$(d_{in-st}, d_{in}, d_{out}, d_{gr}) \in \boldsymbol{D} \Rightarrow \mathrm{Val}\, d_{gr}(R) \subseteq \mathrm{Dom}\, d_{out}\,.$$

Из определения 5.2 вытекает, что ДДФ-система $\boldsymbol{A}$ состоит из таких относительных черных ящиков, что функционирование системы $\boldsymbol{S_d}$ ($\boldsymbol{d} = (d_{in-st}, d_{in}, d_{out}, d_{gr}) \in \boldsymbol{D}$) осуществляется в соответствии с формулой

$$\widetilde{y} = d_{out}((d_{gr}(R))(d_{in-st}(c), d_{in}(x))) \quad (c \in C, x \in X)\,.$$

Пусть *идеальная* модель – это общая динамическая система (в пространстве состояний C) с производящим семейством выхода

$$\boldsymbol{S} = (C, X, Y, \Phi, \Psi) \qquad (X \subseteq A^T, Y \subseteq B^T)\,,$$

где

$$\Phi = \{\varphi_{t_1 t_2} : C \times X_{t_1 t_2} \to C \mid t_1, t_2 \in T, t_1 \le t_2\} \text{ -}$$

семейство функций перехода состояний, а

$$\Psi = \{\mu_{t_1 t_2} : C \times \overline{X}_{t_1 t_2} \to B \mid t_1, t_2 \in T, t_1 \le t_2\} \text{ -}$$

производящее семейство выхода. Кроме множеств D_{in} и D_{out} зафиксируем также множество отображений

$$D_{st} \subseteq \{f \mid f : C \times T \to C\}$$

и множества операторов

$$D_{trnsn} \subseteq \{f \mid f : \Phi \to \Theta\}\,,$$

где

$$\Theta = \{\theta_{t_1 t_2} : C \times X_{t_1 t_2} \to C \mid t_1, t_2 \in T, t_1 \le t_2\} \supseteq \Phi$$

и

$$D_{pof} \subseteq \{f \mid f : \Psi \to \Xi\}\,,$$

где

$$\Xi = \{\xi_{t_1 t_2} : C \times \overline{X}_{t_1 t_2} \to B \mid t_1, t_2 \in T, t_1 \le t_2\} \supseteq \Psi\,.$$

Предположим, что множество D_{st} содержит тождественное отображение i_{st}, а каждое из множеств D_{trnsn} и D_{pof} - тождественный оператор, соответственно, i_{trnsn} и i_{pof}. Кроме того, потребуем, чтобы истинными были следующие утверждения

$$d_{trnsn}(\varphi_{t_1 t_2}) = \theta_{\tau_1 \tau_2} \Rightarrow (t_1 = \tau_1) \wedge (t_2 = \tau_2) \quad (d_{trnsn} \in D_{trnsn}\,,\ \varphi_{t_1 t_2} \in \mathrm{Dom}\, d_{trnsn})$$

и

$$d_{pof}(\mu_{t_1t_2})=\xi_{\tau_1\tau_2} \Rightarrow (t_1=\tau_1)\wedge(t_2=\tau_2) \quad (d_{pof}\in D_{pof}\ ,\ \xi_{t_1t_2}\in \mathrm{Dom}\, d_{pof})\,.$$

Определение 5.3. Дестабилизатором общей динамической системы с производящим семейством выхода

$$\boldsymbol{S}=(C,X,Y,\Phi,\Psi) \qquad (X\subseteq A^T, Y\subseteq B^T)\,,$$

назовем любое такое множество

$$\boldsymbol{D}\subseteq D_{st}\times D_{in}\times D_{out}\times D_{trnsn}\times D_{pof}\,,$$

что

$$(i_{st},i_{in},i_{out},i_{trnsn},i_{pof})\in \boldsymbol{D}$$

и

$$(d_{st},d_{in},d_{out},d_{trnsn},d_{pof})\in \boldsymbol{D}\Rightarrow \mathrm{Val}\, d_{pof}(\mu_{t_1t_2})\subseteq \mathrm{Dom}\, d_{out} \qquad (\mu_{t_1t_2}\in\Psi)\,.$$

Из определения 5.3 вытекает, что ДДФ-система $\boldsymbol{A}$ состоит из таких общих динамических систем с производящим семейством выхода, что функционирование системы $\boldsymbol{S_d}$ $(\boldsymbol{d}=(d_{st},d_{in},d_{out},d_{trnsn},d_{pof})\in \boldsymbol{D})$ осуществляется в соответствии с формулами

$$\tilde{y}(t_2)=d_{out}(d_{pof}(\mu_{t_1t_2})(d_{st}(c,t_1),d_{in}(\bar{x}_{t_1t_2}))) \quad (\bar{x}_{t_1t_2}\in \bar{X}_{t_1t_2}) \tag{5.1}$$

и

$$c(t_2)=d_{trnsn}(\varphi_{t_1t_2})(d_{st}(c,t_1),d_{in}(\bar{x}_{t_1t_2})) \quad (\bar{x}_{t_1t_2}\in \bar{X}_{t_1t_2})\,. \tag{5.2}$$

Важным специальным случаем только что рассмотренной системы является конечный автомат. Из (5.1) и (5.2) вытекает, что для конечного автомата ДДФ-система, представляет собой семейство автоматов с переменной структурой.

Интерпретация ДДФ-системы как семейства обычных систем дает возможность естественным образом перенести на ДДФ-системы все основные понятия теории систем. Общая схема такого переноса имеет следующий вид:

Пусть

$$P(\boldsymbol{S}_1,\ldots,\boldsymbol{S}_k) \text{ -}$$

утверждение относительно обычных систем $\boldsymbol{S}_1,\ldots,\boldsymbol{S}_k$. *Соответствующее утверждение*

$$P(\boldsymbol{T}_1,\ldots,\boldsymbol{T}_k)$$

относительно ДДФ-систем $\boldsymbol{T}_i=(\boldsymbol{S}_i,\boldsymbol{D_i})$ $(i=1,\ldots,k)$ *означает, что*

$$(\forall \boldsymbol{d}_1\in \boldsymbol{D}_1)\ldots(\forall \boldsymbol{d}_k\in \boldsymbol{D}_k)P((\boldsymbol{S}_1)_{\boldsymbol{d}_1},\ldots,(\boldsymbol{S}_k)_{\boldsymbol{d}_k})\,.$$

В соответствии с этой схемой одно из фундаментальных понятий - *эквивалентность* ДДФ-систем, естественно определяется следующим образом.

Определение 5.4. ДДФ-системы $\boldsymbol{T}_1 = (\boldsymbol{S}, \boldsymbol{D}_1)$ и $\boldsymbol{T}_2 = (\boldsymbol{S}, \boldsymbol{D}_2)$ назовем *эквивалентными*, если для каждого $\boldsymbol{d}_1 \in \boldsymbol{D}_1$ существует $\boldsymbol{d}_2 \in \boldsymbol{D}_2$ и, наоборот, для каждого $\boldsymbol{d}_2 \in \boldsymbol{D}_2$ существует $\boldsymbol{d}_1 \in \boldsymbol{D}_1$ такие, что системы $\boldsymbol{S}_{\boldsymbol{d}_1}$ и $\boldsymbol{S}_{\boldsymbol{d}_2}$ - эквивалентные.

Понятие *эквивалентность* ДДФ-систем дает возможность выделить ту или иную *стандартную форму* ДДФ-систем. В частности, из ассоциативности операции композиции отображений вытекает, что как в случае относительного черного ящика, так и в случае общих динамических систем с производящим семейством выхода, в качестве *стандартной формы* может быть выбрана ДДФ-система с одноэлементным множеством D_{out}. Отметим, что именно выделение стандартной формы является основой для разработки эффективных средств сравнительного анализа ДДФ-систем.

Развитые средства дают возможность обычным образом сформулировать проблемы управления траекторией и финальным состоянием ДДФ-систем. Как правило, основной метод решения этих проблем – использование соответствующих систем моделирования. Причина этого - необходимость проверки тех или иных топологических или метрических соотношений для каждого элемента соответствующего семейства обычных систем в фиксированные моменты времени.

5.2. Композиции ДДФ-систем.

Распространим на ДДФ-системы операции F, $+$ и $\circ$, соответственно, замыкания обратной связи, параллельного и каскадного соединений.

Пусть задана ДДФ-система

$$\boldsymbol{T} = (\boldsymbol{S}, \boldsymbol{D}),$$

где

$$\boldsymbol{S} \subset (X \times Z) \times (Y \times Z)$$

и

$$\boldsymbol{D} \subseteq D_{in} \times D_{out} = (D_X \times D_Z^{(1)}) \times (D_Y \times D_Z^{(2)}).$$

Определим множество D_Z равенством

$$D_Z = \{d_1 d_2 \mid d_1 \in D_Z^{(1)}, d_2 \in D_Z^{(2)}, \mathrm{Val}\, d_2 \subseteq \mathrm{Dom}\, d_1\}. \quad (5.3)$$

Положим

$$F(\boldsymbol{T}) = (F(\boldsymbol{S}), \boldsymbol{D}_1),$$

где

$$\boldsymbol{D}_1 = \{(d_x, d_1 d_2, d_y) \mid (d_x, d_1) \in D_{in}, (d_2, d_y) \in D_{out}, d_1 d_2 \in D_Z\}.$$

Пусть заданы две ДДФ-системы

$$\boldsymbol{T}_i = (\boldsymbol{S}_i, \boldsymbol{D}_i) \quad (i = 1,2).$$

Предположим вначале, что

$$\boldsymbol{S}_i \subset (X_i \times Z) \times Y_i$$

и

$$\boldsymbol{D}_i \subseteq D_{in}^{(i)} \times D_{out}^{(i)} = (D_{X_i} \times D_Z^{(i)}) \times D_{Y_i}.$$

Определим множество D_Z равенством

$$D_Z = D_Z^{(1)} \cap D_Z^{(2)}. \tag{5.4}$$

Положим

$$\boldsymbol{T}_1 + \boldsymbol{T}_2 = (\boldsymbol{S}_1 + \boldsymbol{S}_2, \boldsymbol{D}),$$

где

$$\boldsymbol{D} = \{(d_{x_1}, d_{x_2}, d, d_{y_1}, d_{y_2}) \mid (d_{x_i}, d, d_{y_i}) \in \boldsymbol{D}_i \ (i = 1,2), d \in D_Z\}.$$

Предположим теперь, что

$$\boldsymbol{S}_1 \subset X_1 \times (Y_1 \times Z),$$

$$\boldsymbol{D}_1 \subseteq D_{in}^{(1)} \times D_{out}^{(1)} = D_{X_1} \times (D_{Y_1} \times D_Z^{(1)}),$$

$$\boldsymbol{S}_2 \subset (X_2 \times Z) \times Y_2,$$

$$\boldsymbol{D}_1 \subseteq D_{in}^{(2)} \times D_{out}^{(2)} = (D_{X_2} \times D_Z^{(2)}) \times D_{Y_2}.$$

Определим множество D_Z равенством

$$D_Z = \{d_2 d_1 \mid d_1 \in D_Z^{(1)}, d_2 \in D_Z^{(2)}, \operatorname{Val} d_1 \subseteq \operatorname{Dom} d_2\}. \tag{5.5}$$

Положим

$$\boldsymbol{T}_1 \circ \boldsymbol{T}_2 = (\boldsymbol{S}_1 \circ \boldsymbol{S}_2, \boldsymbol{D}),$$

где

$$\boldsymbol{D} = \{(d_{x_1}, d_{x_2}, d_2 d_1, d_{y_1}, d_{y_2}) \mid (d_{x_i}, d_{y_i}, d_i) \in \boldsymbol{D}_i \ (i = 1,2), d_2 d_1 \in D_Z\}.$$

В процессе распространения операций F, $+$ и $\circ$ на ДДФ-системы необходимость определения множества D_Z, соответственно, равенствами (5.3)-(5.5) обусловлена тем обстоятельством, что причиной резких и непредсказуемых изменений траектории могут являться:

1) такие композиции $d_1 d_2$ $(d_1 \in D_Z^{(1)}, d_2 \in D_Z^{(2)})$ дестабилизирующих воздействий, что

$$\operatorname{Val} d_2 \not\subseteq \operatorname{Dom} d_1$$

при замыкании обратной связи для ДДФ-систем;

2) дестабилизирующие воздействия

$$d \in (D_Z^{(1)} \setminus D_Z^{(2)}) \cup (D_Z^{(2)} \setminus D_Z^{(1)})$$

при параллельном соединении ДДФ-систем;

3) такие композиции $d_2 d_1$ $(d_1 \in D_Z^{(1)}, d_2 \in D_Z^{(2)})$ дестабилизирующих воздействий, что

$$\operatorname{Val} d_1 \not\subseteq \operatorname{Dom} d_2$$

при каскадном соединении ДДФ-систем.

Все такие дестабилизирующие воздействия и их композиции должны быть выявлены в результате тщательного анализа и любая возможность их действия на композицию ДДФ-систем должна быть исключена.

Определенные выше операции композиции являются основой для распространения теории Крона-Роудза на ДДФ-системы. Представление исследуемой ДДФ-системы регулярной сетью, состоящей из более простых ДДФ-систем, дает возможность упростить решение проблем анализа.

Для ДДФ-системы, представленной *сетью*, состоящей из ДДФ-систем, возможны две принципиально различные постановки проблем управления траекторией и финальным состоянием. В первой речь идет о *глобальном* управлении ДДФ-системой в целом. Во второй – о *локальных* управлениях каждой из компонент сети. Исследование взаимосвязей между этими типами управлений является основой для разработки эффективных методов анализа ДДФ-систем.

5.3. Адаптивное управление ДДФ-системами.

Основная цель настоящего пункта – решение проблемы адаптивного управления ДДФ-системой методами теории информации. Актуальность такой постановки проблемы обусловлена тем, что, практически во всех случаях, дестабилизирующие воздействия внешней среды могут быть представлены набором случайных факторов. Исходя из этого, представим оценку взаимодействия ДДФ-системы с внешней средой в виде

$$z = f(\mathbf{y}, \mathbf{x}),$$

где f - выбранная функция полезности, $\mathbf{y} = (y_1, \ldots, y_k)$ - вектор управляемых переменных, а $\mathbf{x} = (x_1, \ldots, x_l)$ - вектор независимых переменных, характеризующих состояние внешней среды. Подчеркнем, что $\mathbf{y}$ и $\mathbf{x}$ - временные вектор-функции, причем в каждый момент времени каждая переменная x_j $(j = 1, \ldots, l)$ - случайная величина.

Отметим, что такая модель взаимодействия системы с внешней средой имеет многочисленные приложения, в число которых входят техническая диагностика (построение тестов для комбинационных схем) и экономика (построение стратегии планирования для организации).

Осуществляя (при необходимости) дискретизацию переменных, выделим конечные множества вариантов решений

$$\mathbf{Y} = \{\mathbf{y}_1, \ldots, \mathbf{y}_m\}$$

и состояний внешней среды

$$\mathbf{X} = \{\mathbf{x}_1, \ldots, \mathbf{x}_n\}.$$

Следовательно,

$$f(\mathbf{y}_i, \mathbf{x}_j) \ \ (i = 1, \ldots, m; \ j = 1, \ldots, n)$$

представляет собой оценку варианта решения $\mathbf{y}_i$ при состоянии внешней среды $\mathbf{x}_j$. Такая интерпретация обладает следующими тремя достоинствами.

Во-первых, вариант решения может быть выбран в соответствии с тем или иным *критерием принятия решений*.

Во-вторых, может быть построена временная функция $r_{отн}(x_j)$, представляющая собой *коэффициент влияния* (или, иными словами, *относительную релевантность*) каждой независимой переменной x_j $(j = 1, \ldots, l)$ на ДДФ-систему. Действительно, зафиксируем моменты времени

$$t_1, \ldots, t_h \quad (0 \le t_1 < \ldots < t_h \le T),$$

где $[0; T]$ - рассматриваемый промежуток времени. В каждый момент времени t_ν $(\nu = 1, \ldots, h)$ вычислим коэффициент влияния $r_{отн}(x_j(t_\nu))$ переменной x_j в соответствии со следующим алгоритмом (через $\mathbf{M}(a)$ обозначено математическое ожидание случайной величины a).

Алгоритм 5.1.

Шаг 1.

$$\mathbf{M}(\mathbf{x}(t_\nu)) := (\mathbf{M}(x_1(t_\nu)), \ldots, \mathbf{M}(x_l(t_\nu)));$$

$$\mathbf{M}(\mathbf{x}(t_\nu))(j) := (\mathbf{M}(x_1(t_\nu)), \ldots, \mathbf{M}(x_{j-1}(t_\nu)), x, \mathbf{M}(x_{j+1}(t_\nu)), \ldots, \mathbf{M}(x_l(t_\nu))) \quad (x \in \mathrm{Dom}\, x_j(t_\nu)).$$

Шаг 2. Вычисляем *абсолютную релевантность* $r_{абс}(x_j(t_\nu), \mathbf{y}(t_\nu))$ переменной x_j на каждое решение $\mathbf{y}(t_\nu) \in \mathbf{Y}(t_\nu)$ $(\mathbf{Y}(t_\nu) \subseteq \mathbf{Y})$:

$$r_{абс}(x_j(t_\nu), \mathbf{y}(t_\nu)) := \frac{\max\limits_{x \in \mathrm{Dom}\, x_j} f(\mathbf{y}(t_\nu), \mathbf{M}(\mathbf{x}(t_\nu))(j)) - \min\limits_{x \in \mathrm{Dom}\, x_j} f(\mathbf{y}(t_\nu), \mathbf{M}(\mathbf{x}(t_\nu))(j))}{f(\mathbf{y}(t_\nu), \mathbf{M}(\mathbf{x}(t_\nu)))}.$$

Шаг 3. Вычисляем влияние $r_{отн}(x_j(t_\nu), \mathbf{y}(t_\nu))$ переменной x_j на каждое решение $\mathbf{y}(t_\nu) \in \mathbf{Y}(t_\nu)$ $(\mathbf{Y}(t_\nu) \subseteq \mathbf{Y})$:

$$r_{отн}(x_j(t_\nu), \mathbf{y}(t_\nu)) := \frac{r_{абс}(x_j(t_\nu), \mathbf{y}(t_\nu))}{\sum\limits_{i=1}^{l} r_{абс}(x_i(t_\nu), \mathbf{y}(t_\nu))}.$$

Шаг 4. Вычисляем коэффициент влияния $r_{отн}(x_j(t_\nu))$ переменной x_j:

$$r_{отн}(x_j(t_\nu)) := \max_{\mathbf{y}(t_\nu)\in\mathbf{Y}(t_\nu)} r_{отн}(x_j(t_\nu), \mathbf{y}(t_\nu)).$$

Временная функция $r_{отн}(x_j)$ представляет собой аналитическое представление ряда динамики

$$\{(t_\nu, r_{отн}(x_j(t_\nu))) \,|\, \nu = 1,\ldots,h\},$$

построенное методом наименьших квадратов.

Временная функция $r_{отн}(x_j)$ $(j=1,\ldots,l)$ в каждый момент времени $t\in[0;T]$ характеризует, в среднем, долю влияния независимой переменной x_j на ДДФ-систему. Фиксирование порогового значения α $(\alpha \ge 0)$ дает возможность выделить в множестве $\{x_1,\ldots,x_l\}$ классы *существенных переменных*

$$C_{сущ} = \{x\in\{x_1,\ldots,x_l\} \,|\, \inf_{t\in[0;T]} r_{отн}(x(t)) \ge \alpha\}$$

и *несущественных переменных*

$$C_{несущ} = \{x\in\{x_1,\ldots,x_l\} \,|\, \sup_{t\in[0;T]} r_{отн}(x(t)) < \alpha\}.$$

Эти классы переменных играют следующую роль. В каждый момент времени $t\in[0;T]$:

1) должны быть учтены значения всех переменных $x\in C_{сущ}$;

2) вообще могут не учитываться значения переменных $x\in C_{несущ}$;

3) значение переменной

$$x\in\{x_1,\ldots,x_l\}\setminus(C_{сущ}\cup C_{несущ})$$

учитывается только в том случае, когда $x(t)\ge\alpha$.

Таким образом, построен некоторый вариант *нестационарного решета*.

Отметим, что отбрасывание переменных, принадлежащих классу $C_{несущ}$ (т.е. несущественных факторов внешней среды), дает возможность понизить размерность исследуемой проблемы.

В третьих, может быть вычислена *значимость*

$$s(x_j) = r_{отн}(x_j)\cdot H(x_j)$$

каждой независимой переменной x_j $(j=1,\ldots,l)$, где $H(x_j)$ - *энтропия* случайной величины x_j, построенная методом наименьших квадратов как аналитическое представление ряда динамики

$$\{(t_\nu, H(x_j(t_\nu)) \,|\, \nu = 1,\ldots,h\}.$$

Анализ временных функций $s(x_j)$ $(j=1,\ldots,l)$ дает возможность выделить в явном виде множество моментов времени

$$\bigcap_{j=1}^{l} \mathrm{Arg} \sup_{t\in[0;T]} s(x_j(t)),$$

в которые ДДФ-система наиболее уязвима к изменениям внешней среды.

По аналогии с тем, как это было сделано выше, фиксирование порогового значения β $(\beta > 0)$ дает возможность выделить в множестве $\{x_1,\ldots,x_l\}$ классы *значимых переменных*

$$V_{знч} = \{x \in \{x_1,\ldots,x_l\} \mid \inf_{t\in[0;T]} s(x(t)) \geq \beta\}$$

и *незначимых переменных*

$$V_{незнч} = \{x \in \{x_1,\ldots,x_l\} \mid \sup_{t\in[0;T]} s(x(t)) < \beta\}.$$

Именно факторы внешней среды, принадлежащие классу $V_{знч}$, должны быть наиболее детально изучены, а их изменение во времени должно отслеживаться наиболее тщательно. Дополнительное исследование факторов внешней среды, принадлежащих классу $V_{знч}$, дает возможность понизить значимость некоторых из них за счет снижения энтропии. Отметим, что переменные, принадлежащие классу

$$\{x_1,\ldots,x_l\} \setminus (V_{знч} \cup V_{незнч}),$$

в те моменты времени, когда их значимость превышает порог β, могут служить причиной резких отклонений поведения ДДФ-системы от эталонного.

Энтропия также дает возможность ввести формальную *меру* для вычисления *наблюдаемости* любой независимой переменной x_j $(j=1,\cdots,l)$ относительно любого множества независимых переменных

$$\{x_{r_1},\ldots,x_{r_u}\} \subseteq \{x_1,\ldots,x_l\} \setminus \{x_j\}$$

в соответствии с формулой

$$o_{a_1,\ldots,a_u}(x_j) = \begin{cases} \dfrac{H(x_j) - H_{a_1,\ldots,a_u}(x_j)}{H(x_j)}, & \text{если } H(x_j) \neq 0, \\ 0, & \text{если } H(x_j) = 0 \end{cases},$$

где $H_{a_1,\ldots,a_u}(x_j)$ - *условная энтропия* переменной x_j при значениях переменных $x_{r_1},\ldots,x_{r_u}$, равных, соответственно, $a_1,\ldots,a_u$. Использование этой меры в системе имитационного моделирования дает возможность выявить ситуации, требующие наиболее тщательного отслеживания в процессе реализации стратегии управления ДДФ-системой. Все такие ситуации характеризуются минимальной наблюдаемостью переменной x_j, т.е. они возникают в моменты времени, принадлежащие множеству

$$\mathrm{Arg} \inf_{t\in[0;T]} o_{a_1,\ldots,a_u}(x_j(t)).$$

Развитые средства являются основой для построения эффективного механизма контроля и адаптации ДДФ-системы к условиям нестационарной внешней среды в процессе реализации стратегии управления. Такой механизм определяется следующим алгоритмом (через ε_j $(j=1,\ldots,l)$, δ и E_j $(j=1,\ldots,l)$, Δ обозначены временные функции, являющиеся допустимыми, соответственно, нижними и верхними границами изменения переменных $x_1,\ldots,x_l$ и z).

Алгоритм 5.2.

Шаг 1. Если $\varepsilon_j \le x_j \le \mathrm{E}_j$ для всех $j=1,\ldots,l$ и $\delta \le z \le \Delta$, то никаких изменений в стратегии управления ДДФ-системой не производится и конец, иначе переход к шагу 2.

Шаг 2. Если $\varepsilon_j \le x_j \le \mathrm{E}_j$ для всех $j=1,\ldots,l$ и $z < \delta$, то переход к шагу 3, иначе переход к шагу 4.

Шаг 3. Стратегия управления ДДФ-системой на оставшемся промежутке времени должна быть переработана, так как проявились ошибки, допущенные при ее разработке и конец.

Шаг 4. Если $\varepsilon_j \le x_j \le \mathrm{E}_j$ для всех $j=1,\ldots,l$ и $z > \Delta$, то переход к шагу 5, иначе переход к шагу 6.

Шаг 5. Стратегия управления ДДФ-системой на оставшемся промежутке времени может быть переработана с целью повышения полезности z, так как либо было выбрано не наилучшее решение, либо не полностью учтены благоприятствующие факторы внешней среды и конец.

Шаг 6. Стратегия управления ДДФ-системой на оставшемся промежутке времени должна быть переработана, так как исходные предпосылки, лежащие в основе применяемой стратегии управления перестали быть истинными и конец.

В заключение отметим следующее. Разработанный выше подход является основой для унифицированного построения адаптивных систем управления как траекторией, так и финальным состоянием ДДФ-системы. Все многообразие таких систем управления определяется используемыми критериями принятия решений, возможностями систем имитационного моделирования и прогнозирования, а также схемами управления ДДФ-системами. При этом именно *предельная математическая модель*, получаемая в результате итеративного применения процедур понижения как размерности решаемой задачи, так и значимости факторов внешней среды, определяет *внутреннюю сложность* исследуемой проблемы управления.

5.4. Выводы.

В разделе 5 впервые систематически изложены разработанные автором модели и методы, предназначенные для унифицированного анализа систем, подверженных дестабилизирующим воздействиям внешней среды. Основные результаты состоят в следующем:

1. В рамках применявшегося раннее для разработки математической теории систем аксиоматического подхода проработаны основы как абстрактной, так и структурной теорий ДДФ-систем. Построенные модели, по своей сути, являются семействами обычных систем, что дает возможность использовать для их анализа весь арсенал методов и средств современной математической теории систем.

2. Решена проблема адаптивного управления ДДФ-системой методами теории информации. Предложенный механизм контроля является основой унифицированного построения адаптивных систем управления как траекторией, так и финальным состоянием ДДФ-систем Возможность последовательного понижения размерности является унифицированным средством построения моделей, отражающих внутреннюю сложность исследуемой проблемы.

Таким образом, в разделе 5 разработан новый фрагмент математической теории систем – теория ДДФ-систем, предназначенный для анализа систем, подверженных дестабилизирующим воздействиям внешней среды. Получено решение проблема 1.12.

Основные результаты раздела опубликованы в [40,79,80,82]

ЗАКЛЮЧЕНИЕ

В монографии разработаны модели и методы исследования проблем анализа дискретных систем, основанные на симбиозе комбинаторных методов (в основе которых лежит поиск) с моделями и методами современной алгебры.

Основные результаты состоят в следующем:

1. Разработана общая теория поиска на частично упорядоченных структурах, специальными случаями которой являются классические теоретико-множественный и основанный на оценивании подходы. В рамках этой теории решена общая проблема поиска безусловных решений, определяемых характеристической функцией, что дало возможность с единых позиций провести исчерпывающее исследование проблем поиска как всех основных типов безусловных решений (минимальных, неприводимых, кооперативных), так и адаптивных решений.

2. Получено полное решение фундаментальной проблемы поиска множества всех неприводимых множеств представителей заданного семейства множеств.

3. На основе разработанных методов поиска исследованы проблемы идентификации внутренних состояний слабоинициальных конечных автоматов.

4. Разработан общий метод получения нижних экспоненциальных оценок для функции Шеннона.

5. Исследовано представление функций переходов и выходов конечных автоматов конечными группами.

6. Решена проблема построения нестационарных секретных замков сколь угодно большой сложности.

7. Разработаны комбинаторные методы поиска всех и одной простых импликант, покрывающих заданную точку, а также ДНФ, состоящих из простых импликант.

8. Получено полное решение проблем анализа управляемости/наблюдаемости для булевых функций.

9. Разработан метод идентификации булевых вектор-функций на основе теории линейных пространств над конечными полями.

10. Построен фрагмент математической теории систем, предназначенный для исследования систем, находящихся под действием дестабилизирующих факторов внешней среды.

Таким образом, в монографии разработаны основы комбинаторно-алгебраической теории, предназначенной для анализа дискретных систем.

Полученные результаты являются основой для дальнейших исследований. Эти исследования могут проводиться в следующих направлениях.

Во-первых, это исследование автоматов-экспериментаторов (осуществляющих поиск адаптивных решений), предназначенных для решения конкретных проблем дискретной математики.

Во-вторых, это разработка общего метода решета для частично упорядоченных структур.

В третьих, это адаптация разработанной общей теории поиска решений к новой парадигме вычислений - ДНК-вычислениям.

В четвертых, это классификация конечных автоматов в соответствии с представлениями их функций переходов и выходов классическими группами и сравнение ее с традиционной классификацией.

В пятых, это обобщение разработанного метода идентификации булевых вектор-функций на случай произвольных дискретных функций, отображающих k-элементное множество в m-элементное множество.

В шестых, это детализация разработанной теории ДДФ-систем для конкретных классов дискретных систем.

СПИСОК ЛИТЕРАТУРЫ

1. *Ахо А.*, *Хопкрофт Дж.*, *Ульман Дж.* Построение и анализ вычислительных алгоритмов. – М.: Мир, 1979. – 536с.
2. *Басакер Р.*, *Саати Т.* Конечные графы и сети. – М.: Наука, 1974. – 536с.
3. *Беллман Р.* Применение динамического программирования к задаче о коммивояжере. – В кн.: Кибернетический сборник. Вып. 9 (Старая серия). – М.: Мир, 1964. – С.219-222.
4. *Беллман Р.*, *Дрейфус С.* Прикладные задачи динамического программирования. – М.: Наука, 1965. – 457с.
5. *Бенерджи Р.* Теория решения задач. – М.: Мир, 1972. –224с.
6. *Берж С.* Теория графов и ее применение. – М.: ИЛ, 1962. – 319с.
7. *Биркгоф Г., Барти Т.* Современная прикладная алгебра. – М.: Мир, 1976. – 400с.
8. *Богомолов А.М., Скобелев В.Г.* Об одном алгоритме решения диагностической и установочной задач с автоматом // Кибернетика. – 1975. – № 6. – С.1-6.
9. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576с.
10. *Васильев Ю.Л.* О «суперпозиции» сокращенных дизъюнктивных нормальных форм. – В кн.: Проблемы кибернетики. Вып. 12. – М.: Наука, 1964. – С.239-242.
11. *Гилл А.* Введение в теорию конечных автоматов. - М.: Наука, 1966. – 272с.
12. *Гилл А.* Линейные последовательностные машины. - М.: Наука, 1974. – 287с.
13. *Глушков В.М.* Синтез цифровых автоматов. – М.: Физматгиз, 1962. – 476с.
14. *Горяшко А.П.* Проектирование легко тестируемых дискретных устройств: идеи, методы, реализация // Автоматика и телемеханика. – 1984. – № 7. – С.5-35.
15. *Гэри М.*, *Джонсон Д.* Вычислительные машины и труднорешаемые задачи. – М.: Мир, 1982. – 416с.
16. *Де Брейн Н.Г.* Асимптотические методы в анализе. – М.: ИЛ, 1961. –247с.
17. *Де Брейн Н.Г.* Теория перечисления Пойа. – В кн.: Прикладная комбинаторная математика. – М.: Мир, 1968. – С.1-106.
18. Дискретная математика и математические вопросы кибернетики. Т.1 / Под ред. *С.В. Яблонского* и *О.Б. Лупанова*. – М.: Наука, 1974. – 312с.
19. *Журавлев Ю.И.* Локальные алгоритмы вычисления информации. **I** // Кибернетика. – 1965. – № 1. – С.12-19.
20. *Журавлев Ю.И.* Локальные алгоритмы вычисления информации. **II** // Кибернетика. – 1966. – № 2. – С.1-11.
21. *Калман Р.*, *Фалб П.*, *Арбиб М.* Очерки по математической теории систем. – М.: Мир, 1971. – 400с.
22. *Кирклend Т.*, *Флорес В.* Программные средства анализа тестируемости и автоматическая генерация тестов для СБИС // Электроника. – 1983. – **56.** – № 5. – С.41-48.
23. *Клини Ф.К.* Представление событий в нервных сетях и конечных автоматах. – В кн.: Автоматы / Под ред. *К.Э. Шеннона*, *Дж. Маккарти*. – М.: ИЛ, 1956. – С.15-67.
24. *Кормен Т.*, *Лейзерсон Ч.*, *Ривест Р.* Алгоритмы: построение и анализ. – М.: МЦНМО, 2000. – 960с.
25. *Коршунов А.Д.* О перечислении конечных автоматов. – В кн.: Проблемы кибернетики. Вып. 34. – М.: Наука, 1978. – С.5-82.
26. *Лидл Р.*, *Нидеррайтер Г.* Конечные поля. Т.1. – М.: Мир,1988. – 428с.
27. *Лидл Р.*, *Нидеррайтер Г.* Конечные поля. Т.2. – М.: Мир,1988. – 394с.
28. *Льюнг Л.* Идентификация систем. Теория для пользователя. – М.: Наука, 1991. – 432с.

29. *Мальцев А.И.* Алгебраические системы. – М.: Наука, 1970. – 329с.
30. *Матросов В.М.*, *Анапольский Л.Ю.*, *Васильев С.Н.* Метод сравнения в математической теории систем. – Новосибирск: Наука, 1980. – 480с.
31. *Месарович М.*, *Такахара Я.* Общая теория систем: математические основы. – М.: Мир, 1978. – 311с.
32. *Мур Э.Ф.* Умозрительные эксперименты с последовательностными машинами. – В кн.: Автоматы / Под ред. *К.Э. Шеннона*, *Дж. Маккарти*. – М.: ИЛ, 1956. – С.179-210.
33. *Нигматтулин Р.Г.* Проблема нижних оценок сложности и теория NP-полноты (обзор) // Известия ВУЗов. Математика. – 1981. – № 5. – С.17-25.
34. *Нильсон Н.* Искусственный интеллект. – М.: Мир, 1973. – 270с.
35. *Нильсон Н.* Принципы искусственного интеллекта. – М.: Радио и связь, 1985. – 376с.
36. *Носов В.А.*, *Сачков В.Н.*, *Тараканов В.Е.* Комбинаторный анализ (Неотрицательные матрицы, алгоритмические проблемы). – В кн.: Итоги науки и техники. Теория вероятностей. Математическая статистика. Теоретическая кибернетика. Т. 21. – М.: ВИНИТИ, 1983. – С.120-178.
37. Основы технической диагностики. Кн. 1 / Под ред. *П.П. Пархоменко*. – М.: Энергия, 1976. – 464с.
38. *Пападимитриу Х.*, *Стайглиц К.* Комбинаторная оптимизация. Алгоритмы и сложность. – М.: Мир, 1985. – 510с.
39. *Перфильева И.Г.* Приложения теории нечетких множеств. – В кн.: Итоги науки и техники. Теория вероятностей. Математическая статистика. Теоретическая кибернетика. Т. 29. – М.: ВИНИТИ, 1990. – С.183-151.
40. *Пилюшенко В.Л.*, *Скобелев В.Г.* Адаптивное управление ДДФ-системами // Доп. НАН України. – 2000. - № 11. – С.135-138.
41. *Прахар К.* Распределение простых чисел. – М.: Мир, 1967. – 511с.
42. *Рабин М.О.*, *Скотт Д.* Конечные автоматы и задачи их разрешения. – В кн.: Кибернетический сборник. Вып. 4 (Старая серия). – М.: Мир, 1962. – С.58-91.
43. *Рейнгольд Э.*, *Нивергельт Ю.*, *Део Н.* Комбинаторные алгоритмы. Теория и практика. – М.: Мир, 1980. – 476с.
44. *Роджерс Х.* Теория рекурсивных функций и эффективная вычислимость. – М.: Мир, 1972. – 624с.
45. *Рысцов И.К.* Оценка длины кратчайшего диагностического слова для конечного автомата // Кибернетика. – 1978. – № 6. – С.40-45.
46. *Рысцов И.К.* Асимптотическая оценка длины диагностического слова для конечного автомата // Докл. АН СССР. – 1978. – **241**. – № 3. – С.294-296.
47. *Сапоженко А.А.*, *Чухров И.П.* Минимизация булевых функций в классе дизъюнктивных нормальных форм. – В кн.: Итоги науки и техники. Теория вероятностей. Математическая статистика. Теоретическая кибернетика. Т. 25. – М.: ВИНИТИ, 1987. – С.68-116.
48. *Сачков В.Н.* Введение в комбинаторные методы дискретной математики. – М.: Наука, 1982. – 348с.
49. *Сачков В.Н.* Комбинаторные методы дискретной математики. – М.: Наука, 1977. – 320с.
50. *Скобелев В.Г.* Построение автоматов-экспериментаторов. – В кн.: Методы диагноза и контроля сложных дискретных систем и автоматов. – Киев: ИК АН УССР, 1973. – С.32-44.
51. *Скобелев В.Г.* Построение меры для оценки диагностических свойств класса автоматов. – В кн.: Методы диагноза и контроля сложных систем и автоматов (Препринт 76-18). – Киев: ИК АН УССР, 1976. – С.31-37.

52. *Скобелев В.Г.* Неприводимые множества представителей семейства множеств. – В кн.: Дискретные системы, формальные языки и сложность алгоритмов. Киев: ИК АН УССР, 1977. – С.54-65.
53. *Скобелев В.Г.* Построение минимальных диагностических слов восстановлением их финальных отрезков. – В кн.: Дискретные системы, формальные языки и сложность алгоритмов. Киев: ИК АН УССР, 1978. – С.75-83.
54. *Скобелев В.Г.* Некоторые оценки для автономных автоматов. – В кн.: Методы проектирования схемного и программного оборудования ЭВМ. – Киев: ИК АН УССР, 1979. – С.42-45.
55. *Скобелев В.Г.* Локализация кратных неисправностей магнитной большой интегральной схемы (МБИС) «Ассоциативное ОЗУ» – В кн.: Вопросы технической диагностики. – Ростов-на-Дону: РИСИ, 1980. – С.38-42.
56. *Скобелев В.Г.* Метод поиска минимальных выигрышных решений в классе W-задач и его применение к построению минимальных диагностических слов. - В кн.: Методы и системы технической диагностики. Вып. 1. – Саратов: СГУ, 1980. – С.27-39.
57. *Скобелев В.Г.* О некоторых задачах перечисления конечных автоматов // Докл. АН УССР. – 1980. – № 12. – С.64-66.
58. *Скобелев В.Г.* О количестве графов переходов с заданным числом граничных вершин // Кибернетика. – 1981. – № 2. – С.132-133.
59. *Скобелев В.Г.* О количестве графов переходов с заданным числом близнецов // Кибернетика. – 1981. – № 2. – С.140-141.
60. *Скобелев В.Г.* Методы построения минимальных диагностических слов для автомата и сложность их реализации // Автоматика и телемеханика. – 1981. – № 6. – С.162-169.
61. *Скобелев В.Г.* Алгоритмы и сложность распознавания внутренних состояний конечного автомата // Докл. АН УССР. – 1981. – № 7. – С.71-74.
62. *Скобелев В.Г.* О перечислении возвратных автоматов // Кибернетика. – 1984. – № 5. – С.120-122.
63. *Скобелев В.Г.* Об оценках длин диагностических и возвратных слов для автоматов // Кибернетика. – 1987. – № 4. – С.114-116.
64. *Скобелев В.Г.* Управляемость и наблюдаемость для булевых функций и их композиций // Докл. АН УССР. – 1987. – № 7. – С.65-67.
65. *Скобелев В.Г.* Об исследовании управляемости комбинационных схем // Автоматика и телемеханика. – 1988. – № 1. – С.136-141.
66. *Скобелев В.Г.* Анализ управляемости и наблюдаемости комбинационных схем // Электронное моделирование. – 1989. – **11**. – № 1. – С.63-67.
67. *Скобелев В.Г.* Комбинаторные алгоритмы построения дизъюнктивных нормальных форм (ДНФ) // Докл. АН УССР. – 1989. – № 2. – С.72-75.
68. *Скобелев В.Г.* Об одном методе минимизации булевых функций // Кибернетика. – 1989. – № 5. С.44-48.
69. *Скобелев В.Г.* О реализации булевых функций на мультиплексорах. – В кн.: Теория и моделирование управляющих систем. – Киев: Наукова думка, 1989. – С.52-56.
70. *Скобелев В.Г.*, *Кашеро М.В.* Автоматизация конструирования заданий и текстов программ моделирования распределенных схем. – В кн.: Моделирование и диагностика управляющих систем. – Киев: Наукова думка, 1991. – С.94-96.
71. *Скобелев В.Г.* Поиск на частично упорядоченных структурах // Украинский математический журнал. – 1992. – **44**. – № 2. – С.253-260.
72. *Скобелев В.Г.* Представление автоматов группами // Украинский математический журнал. – 1992. – **44**. – № 10. – С.1412-1416.
73. *Скобелев В.Г.*, *Сперанский Д.В.* Идентификация булевых функций методами линейной алгебры // Украинский математический журнал. – 1995. – **47**. – № 2. – С.260-268.

74. *Скобелев В.Г.* Общерекурсивная модель секретного замка // Доп. НАН України. – 1995. – № 6. – С.73-75.
75. *Скобелев В.Г.* Построение нижних экспоненциальных оценок // Доп. НАН України. – 1997. – № 3. – С.115-117.
76. *Скобелев В.Г.* Принятие решений: комбинаторный подход. – Донецк: ДонГУ, 1997. – 54с.
77. *Скобелев В.Г.*, *Шрамкова Ю.В.* Устойчивость и стабильность множеств двоичных наборов. – В кн.: Идентификация и моделирование управляющих систем. – Киев: Наукова думка, 1997. – С.1-4.
78. *Скобелев В.Г.* Некоторые метрические соотношения в симметрической группе подстановок. – В кн.: Идентификация и моделирование управляющих систем. – Киев: Наукова думка, 1997. – С.5-9.
79. *Скобелев В.Г.*, *Христиановский В.В.* Исследование систем в условиях дестабилизации. – Донецк: ДонГУ, 1997. – 106с.
80. *Скобелев В.Г.*, *Христиановский В.В.* Системы под действием дестабилизирующих факторов: аксиоматический подход // Доп. НАН України. – 1998. – № 5. – С.99-104.
81. *Скобелев В.Г.* Поиск адаптивных решений на частично упорядоченных структурах // Искусственный интеллект. – 1999. – № 1. – С.6-11.
82. *Скобелев В.Г.* Композиции ДДФ-систем // Доп. НАН України. – 2000. – № 1. – С.82-85.
83. *Скобелев В.Г.* Механизм стимулирования в активной системе: общая модель. – В кн.: Труды ИПММ НАН Украины. – 2000. – № 5. – С.132-140.
84. *Скобелев В.Г.* Представление автоматов группами. **II** // Украинский математический журнал. – 2000. – **52**. – № 10. – С.1397-1404.
85. *Скобелев В.Г.* Общие схемы поиска решений на частично упорядоченных структурах. – В кн.: Труды ИППМ НАН Украины. – 2000. – № 5. – С.132-140.
86. *Скобелев В.Г.* Общие схемы поиска безусловных решений // Доп. НАН України. – 2000. – № 12. – С.82-86.
87. Современные методы идентификации систем / Под ред. *П. Эйкхофа*. – М.: Мир, 1983. – 400с.
88. *Соколовский М.Н.* Сложность порождения подстановок и эксперименты с автоматами. – В кн.: Методы дискретного анализа в теории кодов и схем. – Новосибирск: НГУ, 1976. – С.68-86.
89. *Соколовский М.Н.* Оценка длины диагностического слова для конечного автомата // Кибернетика. – 1976. – № 2. – С.16-21.
90. *Трахтенброт Б.А.*, *Барздинь Я.М.* Конечные автоматы (поведение и синтез). – М.: Наука, 1970. – 400с.
91. *Хант Е.Б.* Искусственный интеллект. – М.: Мир, 1978. – 558с.
92. *Харари Ф.* Теория графов. – М.: Мир, 1973. – 300с.
93. *Харари Ф.*, *Палмер Е.М.* Перечисление графов. – М.: Мир, 1977. – 324с.
94. *Хелд М.*, *Карп Р.М.* Применения динамического программирования к задачам упорядочения. – В кн.: Кибернетический сборник. Вып. 9 (Старая серия). – М.: Мир, 1964. – С.202-218.
95. *Adamek J.* Realization theory for automata in categories // J. Pure and Appl. Alg. – 1977. – **9**. – № 3. – P.281-296.
96. *Adamer J.*, *Koubek V.* Functional algebra and automata // Kybernetika (Prague). – 1977. – **13**. – № 4. – P.245-260.
97. *Arbib M.A.*, *Manes E.G.* Machines in a category // SIAM Rev. – 1974. – **16**. – № 2. – P.163.

98. *Bellman R.* Combinatorial processes and dynamic programming in combinatorial analysis. – In: Proceedings of Symposia in Applied Mathematics. Vol. X. American Mathematical Society. – Providence: RI, 1960. – P.293-296.
99. *Bellmore M.*, *Nemhauser G.L.* The travelling salesman problem: a survey // Operat. Res.. – 1968. – № 16. – P.538-568.
100. *Bollobas B.* Modern graph theory. – Springer-Verlag, 1998. – 394p.
101. *Dantzig G.B.*, *Fulkerson D.R.*, *Jonson S.* Solution of large-scale travelling salesman problem // Operat. Res. – 1954. – № 2. – P.393-410.
102. *Dantzig G.B.* Discrete-variable extremum problems // Operat. Res. – 1957. – № 5. – P.266-277.
103. *Dantzig G.B.*, *Blattner W.O.*, *Rao M.R.* All shortest routes from a fixed origin in a graph. – In: Theory of graphs. International Symposia. Rome, July 1966. – Gordon and Breach: NY. – 1967. – P.85-90.
104. *Dijkstra E.W.* A note on two problems in connection with graphs // Numerical Mathematics. – 1959. – № 1. – P.269-271.
105. *Eilenberg S.* Automata, languages and machines. Vol. A. – Academic Press: NY. – 1974. 451p.
106. *Eilenberg S.* Automata, languages and machines. Vol. B. – Academic Press: NY. – 1976. 387p.
107. *Eilenberg S.*, *Wright J.B.* Automata in general algebras // Inf. And Control. – 1967. – № 11. – P.452-470.
108. *Floyd R.W.* Algorithm 97: shortest path // Communication ACM. – 1962. – **5**. – № 6. – P.345.
109. *Fulkerson D.R.* Expected critical path length in PERT networks // Operat. Res. – № 10. – P.808-817.
110. *Hennie F.C.* Finite-state models for logical machines. – John Wiley&Sons INC.: NY, 1962. – 466p.
111. *Hibbard T.N.* Least upper bounds on minimal terminal state experiments for two classes of sequential machines // J. Assoc. Comput. Math. – 1961. – № 8. – P.601-612.
112. *Johnson D.B.* Algorithms for shorted paths. – Ph.D. Thesis. – Dept. Comput. Sci., Cornell Univ., Itaka: NY, 1973.
113. *Kim M.*, *Kang S.*, *Hong K.* Developments in testing transition systems // Testing of Communication Systems. – Vol. 10. – 1997. – P.143-166.
114. *Kohavi Z.* Switching and finite automata theory. – McGrow-Hill Book Company: NY, 1970. – 592p.
115. *Kruskal J.B.Jr.* On the shortest spanning subtree of a graph and the travelling salesman problem // Proceedings of American Mathematical Society. – 1956. – **7**. – № 1. – P.48-50.
116. *Land A.H.*, *Doig A.G.* An automatic method for solving discrete programming problems // Econometrica. – 1960. – **28**. – № 3. – P/497-520.
117. *Lawler E.L.*, *Wood D.E.* Branch-and-bound methods: a survey // Operat. Res. – 1966. – № 14. – P.699-719.
118. *Lee D.*, *Yannakakis M.* Principles and methods of testing finite state machines. – A survey // Proc. of IEEE. – 1996. Vol.84. – № 8. – P.1090-1123.
119. *Lehmer D.H.* The sieve problem for all-purpose computers // Math. Tables Aids Comput. – 1953. – № 7. – P.6-14.
120. *Lehmer D.H.* Combinatorial problems with digital computers. – In: Proc. Fourth Canadian Math. Congress, 1957. – Univ. of Toronto Press. – 1960. – P.160-173.
121. *Little J.D.C.*, *Murty K.G.*, *Sweeny D.W.*, *Karel C.* An algorithm for the travelling-salesman problem // Operat. Res. – 1963. – № 11. – P.972-989.

122. *McNauton R.*, *Yamada H.* Regular expressions and state graphs for automata // Trans. Electron. Comput. – 1960. – **9**. – № 1. – P.39-47.
123. *Moore E.F.* The shortest path through a maze. – In: Proceedings of International Symposium on The Theory of Switching. Part II. Cambrige, Mass. – Harward Univ. Press. – 1959,- P.285-292.
124. *Obruca A.K.* Spanning tree manipulations and the travelling salesman problems // Computer J. – 1968. – № 10. – P.374-377.
125. *Paun G.*, *Rosenberg G.*, *Salomaa A.* DNA computing. New computing paradigms. – Springer-Verlag, 1998. – 402p.
126. *Pierce A.R.* Bibliography on algorithms for shorted path, shorted spanning trees and relative circuit routing problems (1956-1976) // Networks. – 1975. – № 5. – P.129-149.
127. *Pollak M.*, *Wiebenson W.* Solution of the shorted-route problem – A Review // Operat. Res. – 1960. – № 8. – P.224-230.
128. *Shapiro J.F.* Shortest route methods for finite state deterministic dynamic programming // SIAM J. Appl. Math. – 1968. – № 16. – P.1232-1250.
129. *Skobelev V.G.* On finding of minimal distinguishing sequences for finite automata. – In: Diagnostika a zabezpeceni cislovych system. – Brno, ZARI, 1981. – P.145-151.
130. *Skobelev V.G.* Problem-solving: combinatorial-algebraic approach // ZAMM. – 1996. – **76**, S3. – P.563-564.
131. *Skobelev V.G.* Design of irreducible sets of representatives for a family of sets // ZAMM. – 1999. – **79**, S3. – P.915-916.
132. *Skobelev V.G.* Algebraic models for discrete systems' analysis. – Mathematical Notes, Miskolc. – 2001. – **2**. – № 1. – P.61-68.
133. *Spira P.M.* A new algorithm for finding all shorted paths in graph of positive arcs in average time $O(n^2 \log n)$ // SIAM J. Comput. – 1973. – **2**. – № 1. – P.28-32.
134. *Spira P.M.*, *Pan A.* On finding and updating shortest paths and spanning trees. – In: IEEE 14th Annual Symposium on Switching and Automata Theory. – 1973. – P.82-84.
135. *Stairs S.W.* Bibliography of the shortest route problem. – Report LSE-TNT-6: Transport Network Theory Unit. – London School of Economics, 1966. – P.32-47.
136. *Starke P.* Uber experimente an automaten // Zetschr. F. Math. Logic und Grundl. d. Math. – 1967. –13. – P.67-70.
137. *Yannakakis M.*, *Lee D.* Testing finite state machines: fault detection // J. Of Computer and Systems Sci. – 1995. – **50**. – P.209-277.

Владимир Геннадиевич Скобелев

АНАЛИЗ ДИСКРЕТНЫХ СИСТЕМ

ISBN 966-02-2356-0

Подписано к печати 11.11.2001. Формат 60x84 1.16.
Усл. Печ. л. 12. Печать лазерная. Заказ 388. Тираж 300 экз.

Отпечатано в типографии ООО «Норд Компьютер»
на цифровом лазерном издательском комплексе Rank Xerox DocuTech 135.
Адрес: г. Донецк, б. Пушкина, 23. Тел.: (062)-342-14-82.