Министерство образования и науки Российской Федерации

УДК
ГРНТИ
Инв. №

УТВЕРЖДЕНО:
Исполнитель: **Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский государственный университет имени М.В.Ломоносова»**
От имени Руководителя организации **_____ / В.Е. Подольский /** **М.П.**

НАУЧНО-ТЕХНИЧЕСКИЙ ОТЧЕТ

о выполнении 6 этапа Государственного контракта
№ 16.740.11.0570 от 30 мая 2011 г. и Дополнению от 12 марта 2013 г. № 1

Исполнитель: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский государственный университет имени М.В.Ломоносова»
Программа (мероприятие): Федеральная целевая программа «Научные и научно-педагогические кадры инновационной России» на 2009-2013 гг., в рамках реализации мероприятия № 1.3.1 Проведение научных исследований молодыми учеными - кандидатами наук.
Проект: Свойства дискретных функций и операций над ними
Руководитель проекта: **_____ /Федорова Валентина Сергеевна** (подпись)

Москва
2013 г.

СПИСОК ОСНОВНЫХ ИСПОЛНИТЕЛЕЙ

по Государственному контракту 16.740.11.0570 от 30 мая 2011 на выполнение поисковых научно-исследовательских работ для государственных нужд

Организация-Исполнитель: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский государственный университет имени М.В.Ломоносова»

Руководитель темы:

кандидат физико-математических наук, без ученого звания	_____ подпись, дата	Федорова В. С.

Исполнители темы:

кандидат физико-математических наук, без ученого звания	_____ подпись, дата	Ларионов В. Б.

Реферат

Отчет 36 с., 1 ч., 2 рис., 0 табл., 12 источн., 1 прил.

Многозначная логика , дискретная функция , замкнутый класс , монотонность , частично упорядоченное множество , надструктура , предикат , теория алгоритмического обучения , расшифровка функций

В отчете представлены результаты исследований, выполненных по 6 этапу Государственного контракта № 16.740.11.0570 "Свойства дискретных функций и операций над ними" (шифр "2011-1.3.1-111-001") от 30 мая 2011 по направлению "Проведение научных исследований молодыми кандидатами наук в следующих областях:- математика; - механика" в рамках мероприятия 1.3.1 "Проведение научных исследований молодыми учеными - кандидатами наук.", мероприятия 1.3 "Проведение научных исследований молодыми учеными - кандидатами наук и целевыми аспирантами в научно-образовательных центрах" , направления 1 "Стимулирование закрепления молодежи в сфере науки, образования и высоких технологий." федеральной целевой программы "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы.

Цель работы - Получение результатов для описания новых семейств классов монотонных функций, обладающих бесконечной надструктурой, а также построение алгоритмов порождения монотонных дискретных функций, частично совпадающих с заданной.

Методы теории множеств, теории графов, теории функций многозначной логики, соответствие Галуа между решетками функций и предикатов.

Персональный компьютер; операционная система Microsoft Windows; пакет офисных программ Microsoft Office; текстовый редактор TeXnicCenter и пакет программ MikTeX.

1. Описание новых семейств классов монотонных функций, обладающих бесконечной надструктурой.
2. Статья, содержащая результаты решения исследуемых задач, в высокорейтинговом российском или зарубежном журнале.
3. Описание алгоритмов порождения монотонных дискретных функций, частично совпадающих с заданной.
4. Статья, содержащая результаты решения исследуемых задач, в высокорейтинговом российском или зарубежном журнале.
5. Научно-технический отчёт по шестому этапу.

Содержание

1. Введение

Теория дискретных управляющих систем занимает одно из важнейших мест в области знаний, исследования по которой в отечественной традиции относят к математической кибернетике, а в зарубежной – к theoretical computer science. Различные задачи, связанные с дискретными управляющими системами, играют важную роль как в теоретических исследованиях, так и при решении прикладных задач из разных областей знаний.

Исследования, проводимые в рамках работ по Государственному контракту, связаны с изучением неотъемлемой части теории дискретных управляющих систем – теории дискретных функций. В частности, проведенные в рамках шестого этапа работ по Государственному контракту исследования касались задачи расшифровки функций, одной из ключевых задач теории алгоритмического обучения, а также следующих важных проблем теории функциональных систем: выразимости, классификации элементов и описания замкнутых классов дискретных функций.

На шестом этапе Государственного контракта были выполнены работы по следующим направлениям:

1. Изучение строения фрагментов решетки замкнутых классов функций многозначной логики. Исследовались условия, достаточные для наличия бесконечной надструктуры у некоторых семейств классов монотонных функций, сохраняющих частично упорядоченное множество с единственным минимальным или максимальным элементом.

2. Построение монотонных дискретных функций по заданным точкам немонотонных функций в рамках задачи расшифровки функций. Была решена задача создания неверного образа монотонной дискретной функции на основе неверного предположения о монотонности и верной информации о значениях и описан алгоритм порождения монотонных дискретных функций, частично совпадающих с заданной.

Кроме того, выполненные на шестом этапе работы включали также следующие действия:

3. Подготовка научных статей к публикации: по результатам проведенных исследований опубликованы две статьи в высокорейтинговых российских журналах.

4. Подготовка настоящего научно-технического отчета.

Все перечисленные работы проводились в соответствии с составленным ранее

планом проведения исследований, вошедшим в научно-технический отчет по итогам первого этапа. Подробное изложение результатов проведенных исследований содержится в основной части настоящего отчета.

2. Монотонные функции многозначной логики и булевы, получаемые вследствие ошибочных представлений

2.1. Надрешетка некоторых семейств классов монотонных функций

Одной из основных задач в теории функций многозначной логики является *проблема выразимости функций*: заданную k-значную функцию или класс функций требуется выразить, используя суперпозицию функций некоторого имеющегося множества. Указанную задачу, несколько уменьшив общность постановки, можно переформулировать в задачу описания всех *замкнутых относительно операции суперпозиции* классов функций k-значной логики, то есть таких классов, которые содержат любую функцию, представимую суперпозицией произвольных функций этого класса.

Яновым и Мучником в [1] было показано, что решетка замкнутых относительно операции суперпозиции классов функций k-значной логики для любого $k \geq 3$ содержит континуальное число классов. В силу невозможности ее исчерпывающего описания представляется интересным изучение различных подмножеств этой решетки. В рамках третьего этапа данного Государственного контракта была описана структура всех классов, содержащих произвольный класс самодвойственных функций. В рамках четвертого этапа была описана надструктура класса однородных функций и доказан критерий наличия бесконечной надструктуры для классов монотонных функций, сохраняющих частично упорядоченное множество специального вида. В рамках пятого этапа было доказано, что надструктура некоторых семейств классов монотонных функций может содержать большое число классов, не являющихся предикатно-описуемыми. В рамках данного шестого этапа с использованием схожей техники изучаются условия, достаточные для наличия бесконечной надструктуры у некоторых семейств классов монотонных функций, сохраняющих частично упорядоченное множество с единственным минимальным или максимальным элементом.

В качестве основного инструмента исследований по данной тематике был выбран предикатный подход, но также широко применялись теория Галуа, аппарат теории графов и элементы теории частичного порядка.

В. Б. Ларионовым было доказано [2, 3], что в случае, когда класс монотонных функций не является предполным, его *надструктура* (то есть множество содержащих его классов) может быть бесконечна. Как было показано в работе того же автора [3], минимальной логикой с такими классами функций является четырехзначная логика P_4. В статье [4] В. Б. Ларионовым и В. С. Федоровой было показано, что такая надструктура может содержать бесконечное число классов, не являющихся предикатно-описуемыми. В [2, 5] были получены критерии наличия бесконечной надструктуры для классов монотонных функций, сохраняющих частично упорядоченные множества с единственным минимальным элементом и двумя или тремя максимальными, а также с двумя минимальными и двумя максимальными элементами. Указанные критерии имеют следующий вид: класс монотонных функций имеет бесконечную надструктуру тогда и только тогда, когда порождающее его частично упорядоченное множество содержит некоторое фиксированное подмножество. Естественным образом возникает вопрос: можно ли придумать подобный критерий для произвольного класса монотонных функций.

В данной работе строятся новые классы монотонных функций, обладающие бесконечной надструктурой. При этом частично упорядоченные множества, порождающие указанные классы монотонных функций, образуют бесконечное семейство, элементы которого не удается описать условием наличия в них некоторого конечного подмножества.

Введем необходимые определения. Обозначим через E_k множество $\{0, 1, \ldots, k-1\}$.

Функция $f(x_1, \ldots, x_n)$ называется *функцией k-значной логики* $(k \geq 2)$, если она определена на E_k^n и все ее значения принадлежат E_k.

Будем использовать следующие стандартные обозначения. Множество всех функций *k*-значной логики обозначим P_k. Для любого подмножества *A* из P_k через [*A*] будем обозначать *замыкание* относительно операции суперпозиции (для функций далее везде будет идти речь именно об этом типе замыкания).

Пусть на E_k задано некоторое отношение частичного порядка *r*. Возьмем два произвольных набора $\tilde{a} = (a_1, \ldots, a_n)$ и $\tilde{b} = (b_1, \ldots, b_n)$ из E_k^n. Будем говорить, что $\tilde{a}$ *не превосходит* $\tilde{b}$ относительно частичного порядка *r* и записывать $\tilde{a} \leq_r \tilde{b}$, если для любого $1 \leq i \leq n$ справедливо неравенство $a_i \leq_r b$.

Функция $f(x_1,\ldots,x_n)$ называется *монотонной относительно частичного порядка r*, если для любых двух наборов $\tilde{a},\tilde{b}\in E_k^n$ таких, что $\tilde{a}\le_r\tilde{b}$, выполнено $f(\tilde{a})\le_r f(\tilde{b})$. Множество всех функций из P_k, монотонных относительно *r*, называется *классом монотонных функций* M_r.

Для наглядности везде далее будем задавать частичный порядок *r* частично упорядоченным множеством (ЧУМ) *H* из элементов E_k и соответствующий класс обозначать M_H.

Пусть $p(x_1,\ldots,x_m)$ – некоторый предикат, определенный на E_k^m, $f(y_1,\ldots,y_n)$ – функция из P_k. Говорят, что функция $f(y_1,\ldots,y_n)$ *сохраняет предикат* $p(x_1,\ldots,x_m)$, если для любых *n* наборов $\tilde{a}_i=(a_{i1},\ldots,a_{im}),\quad i\in\{1,\ldots,n\}$, удовлетворяющих предикату *p*, набор $(f(a_{11},\ldots,a_{n1}),\ldots,f(a_{1m},\ldots,a_{nm}))$ также удовлетворяет предикату *p*. По определению будем считать, что тождественно ложный предикат сохраняет любая функция.

Будем обозначать через $Pol(p)$ множество всех функций, сохраняющих предикат *p*. Класс M_H является замкнутым классом функций, сохраняющих предикат $R(x,y)=TRUE\Leftrightarrow x\le_r y$ [6]. Везде далее в выражении «монотонный класс задается предикатом *R*» подразумевается именно описанный предикат $R(x,y)$.

Одним из семейств предполных классов функций *k*-значной логики при $(k\ge 3)$ (везде далее рассматриваются только такие *k*) является некоторое подмножество всех классов монотонных функций [7]. Класс M_H является *предполным* тогда и только тогда, когда ЧУМ *H* обладает в точности одним максимальным и одним минимальным элементом [8].

На множестве предикатов вводятся следующие операции: отождествление переменных, конъюнкция и добавление квантора существования по какой-либо переменной (проекция). Для произвольного множества предикатов *P* через [*P*] будем обозначать его замыкание относительно указанных операций. Подробное определение этих операций можно найти в [9].

Лемма 1 ([9])**.** Если $p_1\in[p_2]$, то $Pol(p_2)\subseteq Pol(p_1)$.

Пусть предикат *p* задается формулой *F* над системой $\{R\}$, где *R* – предикат, задающий класс монотонных функций. Далее будем рассматривать только формулы с

вынесенными вперед кванторами существования, поскольку любую формулу можно привести к указанному виду. Сопоставим F ориентированный граф G_F по следующему правилу: между множеством вершин G_F и множеством переменных F (учитываем и свободные, и связанные) существует взаимно однозначное соответствие. Вершину, соответствующую переменной x, пометим символом «x», если переменная x свободная, и «$\exists x$», если связанная. Данную вершину будем обозначать v_x. В графе G_F есть ориентированное ребро (v_x, v_y) тогда и только тогда, когда в формуле F содержится запись $R(x, y)$.

Далее нам потребуются некоторые свойства предикатов, доказательства которых содержатся в [2]. Обозначим через $\overline{F}$ множество формул над $\{R\}$, графы которых не имеют ориентированных циклов.

Лемма 2 ([2])**.** Пусть R – предикат, задающий класс монотонных функций, $p_1, p_2 \in [R]$, $Pol(p_1) \subseteq Pol(p_2)$, предикат p_2 реализуется над $\{R\}$ формулой из $\overline{F}$. Тогда $p_2 \in [p_1]$.

Предикат $p(x_1,\ldots, x_n)$, где $n \geq 2$, назовем *невырожденным*, если существует набор $\tilde{a} \in E_k^n$ такой, что $p(\tilde{a}) = FALSE$, но для любого номера $i \in \{1,\ldots, n\}$ существует элемент $b_i \in E_k$ такой, что $p(a_1,\ldots, a_{i-1}, b_i, a_{i+1},\ldots, a_n) = TRUE$. Одноместный предикат невырожден тогда и только тогда, когда он отличен от тождественно истинного и ложного предикатов. В противном случае предикат назовем *вырожденным*.

Лемма 3 ([2])**.** Пусть ЧУМ H имеет единственный минимальный элемент, R – предикат, задающий класс монотонных функций M_H. Пусть $p_1(x_1,\ldots, x_{n_1}),\ldots, p_l(x_1,\ldots, x_{n_{l1}}) \in [R]$ – невырожденные предикаты местности соответственно $n_1,\ldots, n_l$, задаваемые формулами из $\overline{F}$, $n = \max(n_1,\ldots, n_l)$, $Pol(p_i) \neq Pol(R)$. Тогда любой невырожденный предикат p' из множества $[p_1,\ldots, p_l]$ имеет местность $r \leq n$.

Обозначим через H_n' ЧУМ, полученное из n-мерного булева куба B^n выбрасыванием минимального и максимального элементов, через H_n обозначим ЧУМ, полученное из H_n' выбрасыванием всех его максимальных элементов (или иначе, выбрасыванием из B^n верхних двух слоев и минимального элемента). Через L_n

обозначим ЧУМ, полученное из H'_n добавлением двух не сравнимых между собой элементов a_1, a_2, которые меньше всех остальных элементов H'_n, а также общего минимума $a_{\min}$ (см. рисунок 1). Максимальные элементы множества L_n обозначим через $m_1,\ldots, m_n$, все остальные элементы обозначим через a_W, где $W \in \{1,\ldots, n\}$ – множество индексов элементов $m_1,\ldots, m_n$, которые превосходят a_W.

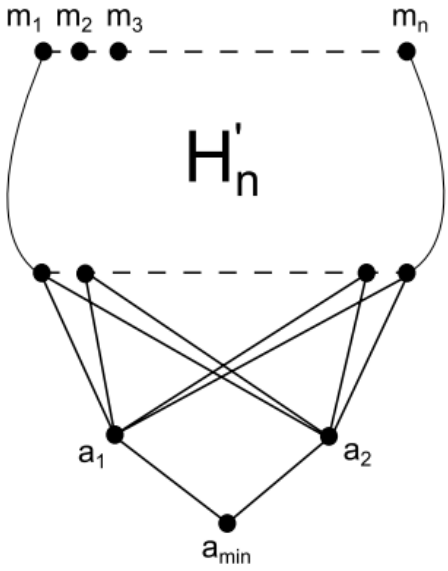

Рис. 1. Частично упорядоченное множество L_n.

Аналогично, для произвольного ЧУМ L, имеющего n максимальных элементов $s_1,\ldots, s_n$, обозначим через M_W, где $W \in \{1,\ldots, n\}$, множество элементов L, каждый из которых меньше максимумов с индексами из W и только их.

Будем говорить, что ЧУМ L принадлежит семейству T_n, если L имеет n максимальных и один минимальный элемент и содержит подмножество L_n со следующими условиями:

1) для любого $i \in \{1,\ldots, n\}$ справедливо: элемент m_i при вложении попадает в множество $M_{\{i\}}$ ЧУМ L;

2) каждый элемент a_W при вложении попадает в множество M_W ЧУМ L;

3) в ЧУМ L не появляется элемента из множества $M_{\{1,\ldots,n\}}$, который больше элементов a_1, a_2

Теорема 1. Для любого числа $n \geq 3$ и любого ЧУМ $L \in T_n$ класс монотонных функций M_L обладает бесконечной надструктурой.

Доказательство. Возьмем любое ЧУМ $L \in T_n$, где $n \geq 3$ – произвольное число. Пусть класс M_L задается предикатом R. Введем $(n + 2l)$-местные предикаты $p_{n,l}$, задаваемые над $\{R\}$ формулами $F_{n,l}$, граф которых изображен на рисунке 2, где $n \geq 3$, $l \geq 2$. Чтобы не загромождать рисунок, ориентация ребер не указана; подразумевается, что все ребра направлены сверху вниз. Данный граф будем трактовать как диаграмму Хассе некоторого ЧУМ, поэтому использование в его изображении множества H_n корректно. Для краткости вершины графа будем обозначать символами переменных формулы (везде далее будет оговорено, идет ли речь о вершинах или самих переменных). В графе присутствует $(l-1)$ фрагмент одинаковой структуры $W_1, \ldots, W_{l-1}$, каждый из которых состоит из множества H_n со своими метками вершин и связанной с ним пары переменных. Причем для любого W_i, $i = 1, \ldots, l-1$, множество H_n вместе с вершинами $y_{(i-1)n+1}, \ldots, y_{in}$, или вместе с вершинами $y_{in+1}, \ldots, y_{(i+1)n}$ образует множество H_n'. Вершины $x_{n+2i-1}, \ldots, x_{n+2i}$ несравнимы и меньше всех остальных элементов W_i. Все переменные x_j, $j = 1, \ldots, n + 2l$, и только они являются свободными.

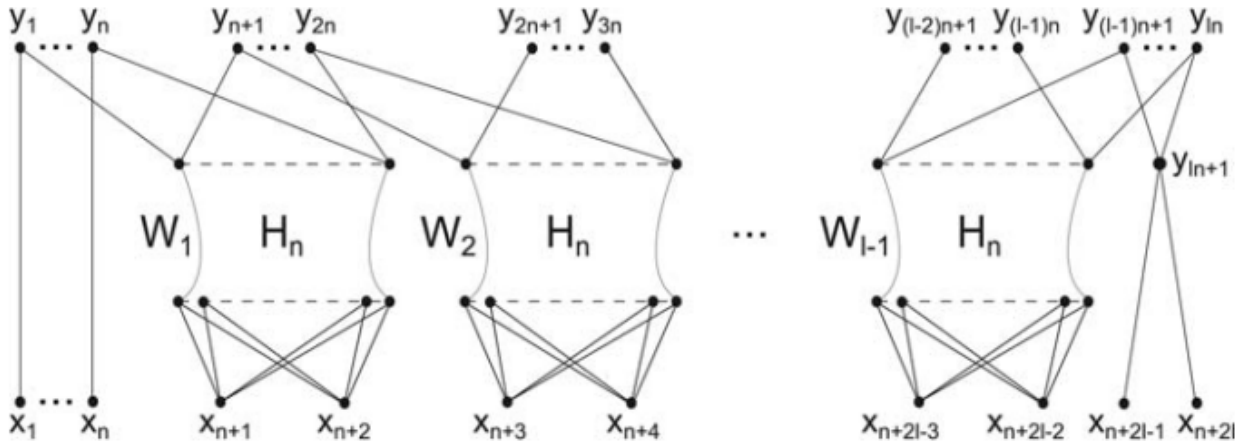

Рис. 2. Граф формулы $F_{n,l}$, задающей предикат $p_{n,l}(x_1, \ldots, x_{n+2l})$.

Покажем далее, что предикаты $p_{n,l}$ являются невырожденными. Обозначим $(n+2l)$-местный набор $(m_1, \ldots, m_n, a_1, a_2, a_1, a_2, \ldots, a_1, a_2,)$ через $\tilde{a}_{n,l}$.

Докажем вспомогательные утверждения.

Лемма 4. $p_{n,l}(\tilde{a}_{n,l}) = FALSE$.

Доказательство. Будем присваивать значения переменным формулы $F_{n,l}$. Переменные $x_1,\ldots,x_n$ принимают на наборе $\tilde{a}_{n,l}$ значения соответственно $m_1,\ldots,m_n$. Поскольку указанные значения являются максимальными элементами множества L_n, то в ЧУМ L указанные значения принадлежат соответственно множествам $M_{\{1\}},\ldots,M_{\{n\}}$, и переменные $y_1,\ldots,y_n$ примут значения соответственно из множеств $M_{\{1\}},\ldots,M_{\{n\}}$ ЧУМ *L*. Везде далее в доказательстве, когда речь будет идти о множествах M_W, будут подразумеваться именно множества ЧУМ *L*.

Рассмотрим далее фрагмент W_1 и покажем, что переменные $y_{n+1},\ldots,y_{2n}$ также примут значения из множеств $M_{\{1\}},\ldots,M_{\{n\}}$ соответственно.

Рассмотрим множество H_n фрагмента W_1. Обозначим его переменные через y_W, где $W\subseteq\{1,\ldots,n\}$ – множество индексов переменных $y_1,\ldots,y_n$, соответствующие которым элементы W_1 больше элемента y_W. Поскольку переменные x_{n+1}, x_{n+2} принимают на наборе $\tilde{a}_{n,l}$ значения a_1, a_2, то все переменные H_n должны принять значения, большие a_1, a_2. В силу присвоенных переменным $y_1,\ldots,y_n$ значений каждая переменная y_W из H_n должна принять значение из множества $M_{W'}$, где $W\subseteq W'$.

Покажем далее по индукции, что для всех переменных H_n будет справедливо $W=W'$.

Рассмотрим самый нижний слой множества H_n фрагмента W_1. Как было сказано выше, каждая переменная y_{W_i} указанного слоя (здесь множества W_i получаются выбрасыванием одного элемента из множества $\{1,\ldots,n\}$) принимает значение из $M_{W_i'}$, где $W_i\in W_i'$. Получаем, что множество W_i' может либо совпадать с W_i, либо с множеством $\{1,\ldots,n\}$. Но в последнем случае был бы получен элемент, меньший всех максимумов $m_1,\ldots,m_n$ и больший a_1, a_2. По определению семейства T_n такого элемента не существует. Таким образом, для всех переменных y_{W_i} нижнего слоя $W_i'=W_i$.

Пусть равенство $W\in W'$ справедливо для всех переменных множества H_n фрагмента W_1 из нижних $(t-1)$ слоев $(t>2)$. Покажем справедливость для *t*-го слоя. Предположим, что для некоторой переменной y_W указанного слоя справедливо $W\subset W'$. Не ограничивая общности, положим $W=\{1,\ldots,n-t\}$. Пусть $b\in W'\setminus W$. Поскольку $t>2$,

найдется элемент c, отличный от $1,\ldots,n-t$ и b. Рассмотрим переменную $y_{W\cup\{c\}}$. По определению ЧУМ H_n справедливо $y_{W\cup\{c\}} \le y_W$ (здесь переменные рассматриваются как элементы ЧУМ). Переменная $y_{W\cup\{c\}}$ принадлежит предыдущему слою ($(t-1)$-й, если считать снизу), для которого уже доказано, что $W\bigcup\{c\}=\{1,\ldots,n-t\,,c\}$. Но поскольку $b\in W'$, то переменная y_W принимает некоторое значение, меньшее элемента m_b, следовательно, и переменная $y_{W\cup\{c\}}$ принимает значение, меньшее m_b, откуда $b\in W\bigcup\{c\}$. Полученное противоречие доказывает, что $W'=\{1,\ldots,n-t\}$.

Итак, было показано, что любая y_W из H_n принимает значение из множества M_W. Поскольку верхний слой H_n состоит из переменных вида $y_{\{i,j\}}$, где $i\ne j,\quad i,\,j\in\{1,\ldots,n\}$, получаем, что переменные $y_{n+1},\ldots,y_{2n}$ принимают значения из множеств $M_{\{1\}},\ldots,M_{\{n\}}$ соответственно.

Рассматривая аналогичным образом фрагмент за фрагментом графа формулы $F_{n,l}$, получим, что переменные $y_{(l-1)n+1},\ldots,y_{\ln}$ также принимают значения из множеств $M_{\{1\}},\ldots,M_{\{n\}}$ соответственно. Но переменные x_{n+2l-1},x_{n+2l} принимают на наборе $\tilde{a}_{n,l}$ значения a_1,a_2. Получаем, что для переменной $y_{\ln+1}$ требуется значение, меньшее всех максимумов $m_1,\ldots,m_n$ и большее элементов a_1,a_2. Но такого элемента в множестве L по определению семейства T_n нет.

Итак, невозможно корректно присвоить значения всем переменным формулы $F_{n,l}$ на наборе $\tilde{a}_{n,l}$. Таким образом, получаем, что $p_{n,l}(\tilde{a}_{n,l})=FALSE$.

Лемма 4 доказана.

Обозначим для любого $i=1,\ldots,n+2l$ через $\tilde{a}^{\,i}_{n,l}$ набор длины $n+2l-1$, совпадающий с набором $\tilde{a}_{n,l}$ с удаленной i-той компонентой.

Лемма 5. Для любого $i\in\{1,\ldots,n+2l\}$ справедливо

$$\left(\exists x_i\ \ p_{n,l}(x_1,\ldots,x_{n+2l})\right)(\tilde{a}^{\,i}_{n,l})=TRUE\ .$$

Доказательство. Рассмотрим вначале случай, когда $i\in\{1,\ldots,n\}$. Не ограничивая общности, будем считать, что $i=1$ (остальные случаи доказываются абсолютно аналогично). По переменной x_1 берется проекция, поэтому ей можно присвоить любое

значение. Пусть это будет m_2. Переменные $x_2,\ldots,x_n$ примут соответственно значения $m_2,\ldots,m_n$. Присвоим переменным $y_1,\ldots,y_n$ соответственно значения $m_2, m_2, m_3, \ldots, m_n$. Рассмотрим фрагмент W_1. Возьмем произвольную переменную y из множества H_n. Рассматривая граф формулы предиката как ЧУМ, имеем, что элемент y меньше элементов из некоторого подмножества множества $\{y_1,\ldots,y_n\}$. Пусть в результате присвоения выше переменные указанного подмножества приняли значения $m_{j_1},\ldots,m_{j_s}$. Присвоим переменной y значение $a_{\{j_1,\ldots,j_s\}}$. В силу определения множества L_n и семейства T_n все указанные значения найдутся и проведенное присвоение корректно. При этом можно присвоить переменным $y_{n+1},\ldots,y_n$ значения $m_2, m_2, m_3, \ldots, m_n$. Проводя аналогичную процедуру для всех фрагментов, вплоть до W_{l-1}, получим, что переменные $y_{(l-1)n+1},\ldots,y_{\ln}$, также принимают значения $m_2, m_2, m_3, \ldots, m_n$. Переменной $y_{\ln+1}$ присвоим значение $a_{\{2,\ldots,n\}}$. Данное присвоение корректно, то есть для любого ориентированного ребра (v_y, v_x) графа формулы $F_{n,l}$ вершине v_x присвоено значение, меньше либо равное в смысле отношения R значения из вершины v_y, что и означает истинность предиката $p_{n,l}$ на рассматриваемом наборе.

Пусть теперь $n+1 \le i \le n+2l-2$. Это означает, что в некотором фрагменте W_j, $1 \le j \le l-1$, берется проекция по одной из переменных x_{n+2j-1}, x_{n+2j}. Присвоим указанной переменной значение так, чтобы пара переменных (x_{n+2j-1}, x_{n+2j}) приняла значение (a_s, a_s), где $s = 1$ или $s = 2$. Во всех фрагментах $W_1,\ldots,W_{j-1}$ присвоим значения переменным, как было описано в лемме 4. При этом переменные $y_{(j-1)n+1},\ldots,y_{jn}$ примут значения из множеств $M_{\{1\}},\ldots,M_{\{n\}}$ соответственно. Всем переменным множества H_n рассматриваемого фрагмента W_j присвоим значения a_s. Всем остальным переменным (фрагменты $W_{j+1},\ldots,W_{l-1}$, переменные $y_{(l-1)n+1},\ldots,y_{\ln+1}$) присвоим значение m_1. Данное присвоение также корректно.

Пусть наконец $i = n+2l-1$ или $i = n+2l$. Возьмем проекцию так, чтобы пара переменных (x_{n+2l-1}, x_{n+2l}) приняла значение (a_s, a_s), где $s = 1$ или $s = 2$. Переменной $y_{\ln+1}$ также присвоим значение a_s. Всем остальным переменным формулы присвоим значения, как это было описано в лемме 4. Данное присвоение также корректно.

Итак, для любого $i \in \{1,\ldots, n+2l\}$ на наборе $\tilde{a}_{n,l}$ можно корректно присвоить значения переменным формулы, задающей проекцию предиката $p_{n,l}$ по переменной x_i.

Лемма 5 доказана.

Из двух доказанных лемм по определению получаем, что предикаты $p_{n,l}$ являются невырожденными. Обозначим классы $A_l = Pol\ p_{n,l}$. По лемме 1 все указанные классы содержат класс монотонных функций M_L.

Предположим далее, что для некоторых различных номеров $i, j \geq 2$ справедливо $A_i = A_j$. Отметим, что формулы, задающие предикаты $p_{n,l}$, принадлежат семейству $\overline{F}$. В силу леммы 2 из соотношений $Pol\ p_{n,l} \subseteq Pol\ p_{n,j}$ и $Pol\ p_{n,j} \subseteq Pol\ p_{n,i}$ следует $p_{n,j} \subseteq [p_{n,i}]$ и $p_{n,l} \subseteq [p_{n,j}]$. Однако, согласно лемме 3, невозможно реализовать невырожденный предикат большей местности невырожденным предикатом меньшей местности. Полученное противоречие доказывает, что все классы A_l различны и образуют бесконечную надструктуру класса монотонных функций M_L.

Теорема 1 доказана.

Поскольку класс монотонных функций не меняется при инвертировании порождающего его ЧУМ [8], все доказанные результаты справедливы, если инвертировать исходное ЧУМ L_n, изображенное на рисунке 1.

Таким образом, было получено бесконечное семейство классов монотонных функций, обладающих бесконечной надструктурой. При этом ЧУМ, порождающие указанные классы, из-за особенностей их строения не удается описать простым критерием содержания некоторого фиксированного подмножества. В свете полученных результатов задача нахождения критерия наличия бесконечной надструктуры для произвольных классов монотонных функций представляется достаточно сложной.

2.2. Построение монотонных дискретных функций по заданным точкам немонотонных функций

Расшифровка функций является ключевой задачей теории алгоритмического обучения, одного из активно развивающихся направлений современной дискретной математики, и заключается в следующем. Пусть фиксирован некоторый класс функций, для определенности булевых, и имеется черный ящик, в котором «содержится» некоторая неизвестная функция из этого класса. Требуется, задавая вопросы типа «Какое значение принимает неизвестная функция на данном входном наборе?», определить, какая именно функция находится в черном ящике. Предполагается, что каждый следующий вопрос может зависеть от ответов на предыдущие. Одной из классических задач такого рода является задача расшифровки монотонных булевых функций, решенная в 1966 году Ж. Анселем [10]; с тех пор задача рассматривается в различных моделях расшифровки для функций из разных классов.

В рамках данного этапа предлагается модель порождения неверного образа дискретной функции на основе неверного предположения о ее свойстве (в данном случае монотонности) и верной информации о ее значениях. Эти результаты могут найти применение в решении задач защиты информации.

Более подробно, рассматривается следующая задача: требуется задать такую булеву функцию, что для любой монотонной функции можно было бы предъявить некоторое количество наборов заданной функции так, чтобы вторая из функций была единственной среди монотонных, совпадающей с заданной на этих наборах. Показано, что это невозможно. В то же время построен пример последовательности функций, предъявляя значения каждой из которых, можно однозначно задавать большое количество функций в предположении их монотонности.

Для булевых векторов $\tilde{x} = (x_1, \ldots, x_n)$ и $\tilde{y} = (y_1, \ldots, y_n)$ соотношение $\tilde{x} \le \tilde{y}$ выполняется тогда и только тогда, когда для любого i, $1 \le i \le n$, выполнено $x_i \le y_i$. Булева функция f называется [11] *монотонной* тогда и только тогда, когда для любых векторов $\tilde{x}$ и $\tilde{y}$ таких, что $\tilde{x} \le \tilde{y}$, выполняется соотношение $f(\tilde{x}) \le f(\tilde{y})$. Будем говорить, что (не обязательно всюду определенная) булева функция f *порождает* монотонную булеву функцию g, если существует такое множество наборов из области определения f (назовем их *предъявляемыми наборами*), что единственной монотонной функцией, совпадающей с f на этих наборах, является g. Булева функция f, которая порождает все монотонные функции, называется *универсальной* [12]. Впервые задача об

изучении свойств порождения и универсальных функций была поставлена для класса линейных функций в работе [12], где было доказано, что требуемое количество предъявляемых наборов универсальной функции растет линейным образом относительно числа переменных порождаемой функции.

Нижней (*верхней*) *тенью* булевого набора $\tilde{x}$ называется множество всех наборов, получаемых из $\tilde{x}$ заменой одной (какой угодно) единицы на ноль (соответственно одного нуля на единицу). *Верхним нулем* (*нижней единицей*) монотонной функции *f* называется набор, на котором функция *f* равна нулю (соответственно единице), но при этом на всех наборах его верхней (соответственно нижней) тени она равна единице (соответственно нулю).

Теорема 1. Пусть $f(x_1,\ldots,x_m)$ – произвольная монотонная функция. Не обязательно всюду определенная булева функция $g(x_1,\ldots,x_m)$ порождает $f(x_1,\ldots,x_m)$ тогда и только тогда, когда *g* принимает значение 0 на всех верхних нулях *f* и 1 на всех нижних единицах *f*.

Доказательство. Достаточность. Докажем, что можно так выбрать множество предъявляемых наборов функции *g*, что для произвольного набора $\tilde{\alpha}$ такого, что $f(\tilde{\alpha}) = a,\ a \in \{0,1\}$, значение порожденной функции действительно совпадет с *a* на наборе $\tilde{\alpha}$. Пусть $a = 0$. Тогда у монотонной функции *f* существует верхний ноль $\tilde{\beta}$ такой, что $\tilde{\alpha} \le \tilde{\beta}$. По условию теоремы $g(\tilde{\beta}) = 0$. Предъявив этот набор *g*, в предположении монотонности получим $f(\tilde{\alpha}) = 0$. Случай $a = 1$ рассматривается аналогично.

Необходимость. Пусть $\tilde{\beta}$ – верхний ноль функции $f(x_1,\ldots,x_m)$ и пусть $g(\tilde{\beta}) = 1$. Наряду с $f(x_1,\ldots,x_m)$ рассмотрим функцию $h(x_1,\ldots,x_m)$, отличающуюся от $f(x_1,\ldots,x_m)$ только на наборе $\tilde{\beta}$. Функция $h(x_1,\ldots,x_m)$ также монотонна, и $f(x_1,\ldots,x_m)$ нельзя отличить от нее, предъявляя значения, общие для *g* и *f*.

Теорема 1 доказана.

Следствие. Универсальных монотонных функций не существует.

Напомним, что *вес булевого набора* – это число единиц в нем. Введем в рассмотрение симметрическую булеву функцию $w(x_1,\ldots,x_n)$. Пусть здесь и далее $n = 2k+1$, если *n* нечетно, и $n = 2k+2$, если *n* четно. Положим $w(\tilde{x}) = 0$, если вес набора

$\tilde{x}$ принадлежит множеству $\{0, 1,\ldots, k-1, k+1\}$, и $w(\tilde{x})=1$, если вес набора $\tilde{x}$ принадлежит множеству $\{k, k+2, k+3,\ldots, n\}$.

Произвольный конечный набор булевых векторов будем называть *кодом*. Пусть некоторый код C состоит из наборов одного веса. Назовем *лункой* множество наборов одного веса, состоящее из некоторого выделенного набора $\tilde{x}$, не принадлежащего коду C, и наборов, удаленных на расстояние два от него при условии, что для любого набора $\tilde{z}$ из нижней тени $\tilde{x}$ существует набор в верхней тени $\tilde{z}$, принадлежащий коду C.

Лемма 1. Функция $w(x_1,\ldots,x_n)$ порождает монотонную функцию $f(x_1,\ldots,x_n)$, равную нулю на всех наборах веса $k-1$ и единице на всех наборах веса $k+2$, если $f(x_1,\ldots,x_n)$ не имеет верхних нулей веса k и все верхние нули $f(x_1,\ldots,x_n)$ в $(k+1)$-м слое образуют множество, свободное от лунок.

Доказательство. Предъявим все наборы веса $k+2$ и $k-1$. На них обе функции $w(x_1,\ldots,x_n)$ и $f(x_1,\ldots,x_n)$ равны единице и нулю соответственно. В предположении монотонности $f(x_1,\ldots,x_n)$ данные значения полностью определяют значения этой функции на наборах всех весов, кроме k и $k+1$. Предъявим значения $w(x_1,\ldots,x_n)$ на множестве всех верхних нулей $f(x_1,\ldots,x_n)$ веса $k+1$ и все единицы $w(x_1,\ldots,x_n)$, не попадающие в нижнюю тень точек этого множества. В предположении монотонности в силу отсутствия лунок получим искомую функцию $f(x_1,\ldots,x_n)$.

Лемма 1 доказана.

Расстояние между наборами кода одной лунки не больше четырех и поэтому справедлива следующая лемма.

Лемма 2. Код с расстоянием не менее шести свободен от лунок.

Теорема 2. Для некоторой константы $c>0$ булева функция $w(x_1,\ldots,x_n)$ порождает

$$2^{\Omega\left(\frac{2^n}{n^c}\right)}$$

монотонных функций при $n\to\infty$.

Доказательство. Достаточно воспользоваться леммами 1 и 2. Заметим, что двоичный логарифм общего числа кодов с расстоянием шесть не меньше максимальной мощности такого кода. Для ее оценки применим жадный алгоритм [11]: на каждом шаге будем добавлять в код произвольный набор веса $k+1$, исключая из рассматриваемого

множества все наборы, удаленные от него на расстояния два и четыре. Количество таких наборов составляет $O(n^4)$, а количество наборов веса $k+1$ составляет $\Omega\left(\frac{2^n}{\sqrt{n}}\right)$. Таким образом, код будет иметь мощность $\Omega\left(\frac{2^n}{n^{4.5}}\right)$, что дает результат теоремы с константой $c = 4.5$. Теорема 2 доказана.

2.3. Публикации результатов НИР

По результатам проведенных исследований опубликованы две статьи в высокорейтинговых российских журналах:

- *В.Б. Ларионов, В.С. Федорова* «О надструктуре некоторых классов монотонных функций многозначной логики» // Известия Иркутского государственного университета. Серия Математика. 2013. Т. 6, № 2, с. 38-47.

- *А.А. Вороненко, В.С. Федорова* «О порождении булевых функций в предположении монотонности» // Вестник московского университета. Серия 15. Вычислительная математика и кибернетика. 2013. № 1. С. 46-47.

Копии статей включены в Приложение А к настоящему отчету.

3. Заключение

В рамках шестого этапа работ по Государственному контракту проведены следующие исследования в соответствии с планом:

1. Описаны новые семейства классов монотонных функций, обладающих бесконечной надструктурой.
2. Описаны алгоритмы порождения монотонных дискретных функций, частично совпадающих с заданной.
3. По результатам исследований опубликованы две статьи в высокорейтинговых российских журналах.
4. Подготовлен научно-технический отчет по итогам шестого этапа.

План проведения исследований шестого этапа выполнен полностью. Копии статей приводятся в Приложении А. Все полученные научные результаты являются новыми. Материалы, описывающие проведение исследований, включают все необходимые сведения для обеспечения возможности воспроизведения результатов.

4. Список использованных источников

1. Янов Ю. И., Мучник А. А. О существовании *k*-значных замкнутых классов, не имеющих конечного базиса // Доклады АН СССР. 1959. Т. 127, № 1. С. 44–46.

2. Ларионов В. Б. Замкнутые классы *k*-значной логики, содержащие классы монотонных или самодвойственных функций // Диссертация на соискание степени к. ф.-м. н., 2009. 157 с.

3. Ларионов В. Б. О положении некоторых классов монотонных *k*-значных функций в решетке замкнутых классов // Дискретная математика. 2009. Т. 21, № 5. С. 111–116.

4. Ларионов В.Б., Федорова В.С. О сложности надструктуры классов монотонных *k*-значных функций специального вида // Известия Иркутского государственного университета. Серия Математика. 2012. Т. 5, № 1. С. 70-79.

5. Ларионов В.Б., Федорова В.С. Критерий бесконечности надструктуры некоторых классов монотонных функций многозначной логики // Материалы 12 межвузовского научно-практического семинара «Комбинаторные конфигурации и их применения» (Кировоград, 14–15 октября 2011 г.). 2011. С. 80-84.

6. Яблонский С. В., Гаврилов Г. П., Набебин А. А. Предполные классы в многозначных логиках. М.: Изд. дом МЭИ, 1997. 144 с.

7. Rosenberg I.G. La structure des fonctions de plusiers variables sur un ensemble fini // Comptes Rendus Acad. Sci. Paris. 1965. V. 260. P. 3817–3819.

8. Мартынюк В. В. Исследование некоторых классов функций в многозначных логиках // Проблемы кибернетики, вып. 3. М.: Наука, 1960. С. 49–61.

9. Боднарчук В.Г., Калужнин В.А., Котов В.Н., Ромов Б.А. Теория Галуа для алгебр Поста // Кибернетика. 1969. № 3. С. 1–10. № 5. С. 1–9.

10. Hansel G. Sur le nombre des fonctions booleennes monotones de variables // C. R. Acad. Sci. Paris. 1966. № 262. P. 1088–1090. (Русский перевод: Ансель Ж. О числе монотонных булевых функций n переменных // Кибернетический сборник, изд-во Мир. Новая серия. Вып. 5, 1968. С. 53–57).

11. Алексеев В.Б. Лекции по дискретной математике. Учебное пособие. М.: Инфра-М, 2012. 90 с.

12. Вороненко А.А. Об универсальных частичных функциях для класса линейных // Дискретная математика. 2012. № 3. С. 62–65.