Министерство образования и науки Российской Федерации

УДК
ГРНТИ
Инв. №

УТВЕРЖДЕНО:
Исполнитель: **Факультет вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова**
От имени Руководителя организации **_____________ / Моисеев Е. И. /** **М.П.**

НАУЧНО-ТЕХНИЧЕСКИЙ ОТЧЕТ

о выполнении 3 этапа Государственного контракта
№ 16.740.11.0570 от 30 мая 2011 г.

Исполнитель: Факультет вычислительной математики и кибернетики Московского государственного университета 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
2012 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: Факультет вычислительной математики и кибернетики Московского государственного университета 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 54 с., 1 ч., 0 рис., 0 табл., 6 источн., 2 прил.

Многозначная логика , дискретная функция , замкнутый класс , самодвойственность , надструктура , предикат

В отчете представлены результаты исследований, выполненных по 3 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 полного описания надструктуры классов самодвойственных, а также квазисамодвойственных функций многозначной логики.

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. Полное описание надструктуры классов квазисамодвойственных функций.
2. Публикация в трудах научной конференции.
3. Полное описание надструктуры для произвольного класса самодвойственных функций и доказательство ее свойств.
4. Статья, содержащая результаты решения исследуемых задач, в высокорейтинговом российском или зарубежном журнале.
5. Научно-технический отчёт по третьему 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 третьего этапа работ по Государственному контракту исследования касались теории функциональных систем, а точнее, проблем выразимости, классификации элементов и описания замкнутых классов.

На третьем этапе Государственного контракта были выполнены работы по следующим направлениям, касающимся изучения строения фрагментов решетки замкнутых классов функций многозначной логики:

1. Исследовалась надструктура замкнутых классов функций многозначной логики, являющихся некоторым обобщением классов самодвойственных функций, – классов квазисамодвойственных функций. Конечность этой надструктуры была доказана во втором этапе данного Государственного контракта. В рамках текущего этапа было получено полное описание структуры и основных свойств надрешетки произвольного класса квазисамодвойственных функций.
2. Исследовалась надструктура самодвойственных классов функций многозначной логики. Получено полное описание всех классов (и их взаимных включений), содержащих произвольный класс самодвойственных функций многозначной логики. Изучены основные свойства надструктуры класса самодвойственных функций многозначной логики.

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

3. Подготовка научных статей к публикации: по результатам проведенных исследований опубликованы статьи в материалах конференции и в высокорейтинговом российском журнале.
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. Самодвойственные и квазисамодвойственные функции

2.1. Описание надструктуры классов квазисамодвойственных функций многозначной логики

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.

Введем необходимые определения и обозначения. 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.

Следуя традиции, будем обозначать через P_k множество всех k-значных функций k-значной логики. 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). Множество всех замкнутых классов в P_k, упорядоченных по отношению включения, будем называть *решеткой замкнутых классов* k-значной логики.

Яновым и Мучником в [1] было показано, что при $k \geq 3$ множество всех замкнутых классов функций из P_k имеет мощность континуум. В связи с этим особенный интерес представляет изучение именно фрагментов решетки замкнутых классов функций из P_k.

Для данного класса A *надструктурой* будем называть множество классов, строго содержащих класс A.

В рамках третьего этапа работ по Государственному контракту рассматривается новое семейство квазисамодвойственных функций и строится их надструктура, конечность которой была доказана на втором этапе данного Государственного контракта.

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

Обозначим через $Pol(p)$ множество функций, сохраняющих предикат p. Для произвольного множества функций A через $Inv\ A$ обозначим множество предикатов, каждый из которых сохраняет любая функция из A. Для произвольного множества предикатов P через $[P]$ будем обозначать его замыкание относительно отождествления переменных, конъюнкции и добавления квантора существования по какой-либо переменной.

Лемма 1 [2]. Если $p_1 \in [p_2]$, то $Pol\,(p_2) \subseteq Pol\,(p_1)$.

Лемма 2 [3]. Пусть $p = p_1 \& \ldots \& p_m$, где предикаты $p_1, \ldots, p_m$ не имеют общих переменных. Тогда

$$Pol\ p = \bigcap_{i=1}^{m} Pol\ p_i .$$

Пусть A и B – произвольные непустые подмножества E_k равной мощности. Обозначим через F_{AB} множество всех различных взаимно однозначных отображений множества A во множество B, а через F_k – объединение множеств F_{AB} для всевозможных пар подмножеств A и B указанного вида. Для $f \in F_{AB}$ обозначим $D_f = A, T_f = A \bigcup B$.

Для произвольного отображения $f \in F_k$ обозначим через $R_f(x_1, x_2)$ предикат, истинный на всех парах $(a, f(a))$, где $a \in D_f$, и только на них.

Замкнутые классы функций $S_f = Pol(R_f)$, где $f \in F_k$, $D_f \subseteq E_k$, будем называть *классами квазисамодвойственных функций*, а сами функции, входящие в указанные классы, – *квазисамодвойственными функциями*.

Отметим, что, если в последнем определении положить $D_f = E_k$, получим определение самодвойственных функций, а если $f(a) = a$ для любого $a \in D_f$ и $D_f \subset E_k$, то S_f – предполный центральный класс [3].

Пусть предикат p реализуется над $\{R_f\}$ формулой F. Везде далее будем считать, что в формуле F вынесены вперед все кванторы существования. Сопоставим F орграф $G(F)$ по следующему правилу: между множеством вершин $G(F)$ и множеством переменных F (и свободных, и связанных) существует взаимно однозначное соответствие. Вершину, соответствующую переменной x, обозначим v_x. В графе $G(F)$ есть дуга (v_x, v_y) тогда и только тогда, когда в формуле F содержится запись $R_f(y,x)$. Отметим, что по графу формулы $G(F)$ формула F с вынесенными вперед кванторами существования восстанавливается однозначно.

Будем рассматривать *пути* из вершины v_1 в вершину v_2 в орграфе G без учета ориентации ребер. *Длиной пути* назовем разность количества ребер, пройденных в прямом направлении, и количества ребер, пройденных в обратном.

Обозначим через $c(G)$ наибольший общий делитель длин всех простых циклов графа G. Если в G нет циклов, положим $c(G) = 0$. Обозначим через $d(v, w)$ минимальное по модулю расстояние в графе G от вершины v до вершины w.

Пусть предикат p реализуется над $\{R_f\}$ формулой F со связным графом $\{G_F\}$. Пусть $y_1,\dots,y_N$ – все переменные формулы F, первые n из которых являются свободными (обозначим их $x_1,\dots,x_n$), $d(v_{y_i},v_{y_j}) = d_{i,j}$. Для произвольной вершины v_y обозначим

$$d_p(y) = \max_{w\in G(F)} d(v_y, w),$$

$$d_n(y) = \min_{w\in G(F)} d(v_y, w),$$

$$D(v_y) = \left\{a\in E_k : \exists\, f^{d_p(y)}(a), f^{-d_n(y)}(a)\right\}.$$

Обозначим также множество $M_c = \left\{a\in E_k : f^c(a) = a\right\}$.

Лемма 3. Пусть G_F – связный граф. Тогда $p(\widetilde{a}) = TRUE$ тогда и только тогда, когда для любого $i\in\left\{1,\dots,n\right\}$ справедливо $a_i\in M_{c(G_F)}\bigcap D(v_{x_i}), a_j = f^{d_{i,j}}(a_i)$ для любого $j\neq i$.

Теорема. Надструктура произвольного класса квазисамодвойственных функций S_f состоит только из классов самодвойственных, квазисамодвойственных функций, их пересечений и P_k.

Доказательство. Рассмотрим произвольный класс A, содержащий S_f. Из [2] имеем $Inv\,A\subseteq Inv\,S_f = Inv\,Pol\,R_f = [R_f, d]$, где $d(x_1,x_2)$ – диагональ

$(d(a,b) = TRUE \Leftrightarrow a = b)$. Для любого $p \in Inv\,A$ справедливо $p \in [R_f, d]$. Рассмотрим формулу F, реализующую предикат p над $\{R_f, d\}$. Для произвольного вхождения $d(z_1, z_2)$ в F отождествим переменные z_1 и z_2, что позволит вычеркнуть сомножитель $d(z_1, z_2)$. В результате мы получим формулу F_1, реализующую предикат p_1 над $\{R_f\}$. Из [2] следует $Pol\ p = Pol\ p_1$.

В силу проведенных рассуждений достаточно показать, что для произвольного предиката $p \in [R_f]$ класс $Pol\ p$ совпадает с одним из перечисленных в теореме.

Пусть снова F – формула, реализующая p над $\{R_f\}$, G_F – ее граф. Предположим вначале, что G_F – связный граф.

Если местность n предиката p равна единице, то по лемме 3 получаем $p(a) = TRUE \Leftrightarrow a \in T = M_{c(G_F)} \cap D(v_x)$. Если $T = E_k$ или $T = \varnothing$, то $Pol\,p = P_k$, в противном случае $Pol\,p$ является предполным центральным классом, при этом $Pol\,p = Pol\,R_{f_0}$, где f_0 – тождественная перестановка на множестве T.

Пусть теперь $n = 2$. По лемме 3 получаем $p(a,b) = TRUE \Leftrightarrow a \in T = M_{c(G_F)} \cap D(v_x)$ и $b = f^d(a)$. Если $T = E_k$, то $Pol\,p$ – класс самодвойственных функций (или P_k, если f – тождественная перестановка), в противном случае $Pol\,p$ – класс квазисамодвойственных функций.

Остается случай $n > 2$. Обозначим предикаты

$$p_i(x_1, x_i) = \exists y_1, \dots, y_{n-2}\ p(x_1, y_1, \dots, y_{i-2}, x_i, y_{i-1}, \dots, y_{n-2}),$$

где $i \in \{2, \dots, n\}$. Получаем, что $p_i \in [p]$, откуда $p_i \in [R_f]$. Предикаты p_i попадают в уже рассмотренный случай. Несложно показать, что $p(x_1, \dots, x_n) = p_2(x_1, x_2) \,\&\, p_3(x_1, x_3) \,\&\, \dots \,\&\, p_n(x_1, x_n)$, то есть $p \in [\{p_2, \dots, p_n\}]$.

Обозначим через t предикат, равный конъюнкции предикатов $p_2, \dots, p_n$ без отождествления переменных. Тогда $p \in [t]$. С другой стороны, из $p_i \in [p]$ следует, что $t \in [p]$. По лемме 1 получаем, что $Pol\,p = Pol\,t$. По лемме 2 класс $Pol\,t$, а значит и $Pol\,p$, является пересечением классов $Pol\,p_i$, т. е. классов самодвойственных и квазисамодвойственных функций.

Случай несвязного графа G_F сводится к предыдущему, если рассмотреть конъюнкцию предикатов, задаваемых каждой из компонент связности, без отождествления переменных. Теорема доказана.

2.2. Надструктура классов самодвойственных функций многозначной логики

Продолжим изучение фрагментов решетки замкнутых классов функций многозначной логики. Рассмотрим классы и их взаимных включения, содержащие произвольный класс самодвойственных функций многозначной логики.

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 $\widetilde{a}_i = (a_{i1},\ldots,a_{im})\,(i \in \{1,\ldots,n\})$, удовлетворяющих предикату *p*, набор $\left(f(a_{11},\ldots,a_{n1}),\ldots,f(a_{1m},\ldots,a_{nm})\right)$ также удовлетворяет предикату *p*. По определению будем считать, что тождественно ложный предикат сохраняет любая функция.

Обозначим через *Pol*(*p*) множество функций, сохраняющих предикат *p*.

На множестве предикатов вводятся следующие операции: отождествление переменных, проекция или добавление квантора существования по какой-либо переменной, конъюнкция. Для произвольного множества предикатов *P* через [*P*] будем обозначать замыкание *P* относительно указанных операций. Подробное определение этих операций можно найти в [2] и [4].

Приведем вначале несколько вспомогательных фактов, касающихся свойств предикатов.

Лемма 1 [2]. Если $p_1 \in [p_2]$, то $Pol(p_2) \subseteq Pol(p_1)$.

Лемма 2 [2]. Пусть *p* – предикат местности *n* > 1. Если существуют различные номера $i, j \in \{1,\ldots,n\}$ такие, что для любого набора $\widetilde{a}$ из $p(\widetilde{a}) = TRUE$ следует $a_i = a_j$, то справедливо

$$Pol(p(x_1,\ldots,x_n)) = Pol(\exists y\ p(x_1,\ldots,x_{j-1},y,x_{j+1},\ldots,x_n)).$$

Лемма 3 [3]. Пусть $p = p_1 \,\&\ldots\&\, p_m$, где предикаты $p_1,\ldots,p_m$ не имеют общих переменных. Тогда

$$Pol\ p = \bigcap_{i=1}^{m} Pol\ p_i\ .$$

Обозначим предикат $d(x_1,x_2) = (x_1 = x_2)$.

Лемма 4. Пусть предикат R таков, что $d \in [R]$, A – произвольный замкнутый класс, содержащий $Pol\,R$. Тогда для любого предиката $p \in Inv\,A$ справедливо $p \in [R]$.

Доказательство. Согласно [2] $Inv\,Pol\,R = [R]$. Используя соотношение $Pol\,R \subseteq A$, получаем $Inv\,A \subseteq Inv\,Pol\,R = [R]$. Отсюда для любого $p \in Inv\,A$ выполнено $p \in [R]$. Лемма 4 доказана.

Пусть на множестве E_k задана некоторая подстановка σ.

Функция k-значной логики $f(x_1, \ldots, x_n)$ называется *самодвойственной относительно подстановки* σ, если выполнено следующее тождество:

$$f(x_1, \ldots, x_n) = \sigma^{-1}(f(\sigma(x_1), \ldots, \sigma(x_n))),$$

где через σ^{-1} обозначена подстановка, обратная к σ.

Известно [5], что множество всех функций из P_k, самодвойственных относительно σ, является замкнутым классом.

Обозначим этот класс через S_σ. Указанный класс является предполным тогда и только тогда, когда подстановка σ распадается в произведение циклов одинаковой длины, являющейся простым числом [5].

Зафиксируем некоторую подстановку σ на E_k. Обозначим множество

$$M_d = \left\{ a \in E_k : \sigma^d(a) = a \right\}, \text{ где } d > 0.$$

Иными словами, M_d – множество элементов E_k, образующих циклы подстановки σ, длины которых кратны числу d. Тот факт, что число a делится на число b, будем обозначать через $b|a$.

Лемма 5. Пусть элементы множества M_d образуют циклы подстановки σ с длинами $m_1, \ldots, m_p$, тогда $M_d = M_{НОК(m_1, \ldots, m_p)}$.

Согласно последней лемме, мы можем рассматривать только множества M_d, где число d равно наименьшему общему кратному длин циклов подстановки σ, элементы которых образуют рассматриваемое множество M_d. Обозначим множество указанных чисел d через D_σ. Через h_σ обозначим наименьшее общее кратное длин всех циклов подстановки σ.

Введем двухместные предикаты $R_{d,i}$ такие, что $R_{d,i}(a,b) = TRUE$ тогда и только тогда, когда $a,b \in M_d$ и $b = \sigma^i(a)$. Обозначим классы $S_{d,i} = Pol\, R_{d,i}$. Из [3] следует, что $S_{h_\sigma,i} = S_{\sigma^i}$. Обозначим предикат $R_\sigma = R_{h_\sigma,1}$.

Лемма 6. Для произвольных $d, j > 0$ выполнено $S_\sigma \subseteq S_{d,j}$.

Доказательство. Согласно нашим обозначениям $S_\sigma = Pol\, R_\sigma$, $S_{d,j} = Pol\, R_{d,j}$. По определению предикатов $R_{d,j}$ справедливо следующее соотношение:

$$\begin{gathered} R_{d,j} = \exists y_1,\ldots,y_{j+d-2}\; R_\sigma(x_1,y_1) \,\&\, R_\sigma(y_1,y_2) \,\&\ldots\&\, R_\sigma(y_{j-1},x_2) \,\& \\ \& \, R_\sigma(x_1,y_j) \,\&\, R_\sigma(y_j,y_{j+1}) \,\&\ldots\&\, R_\sigma(y_{j+d-2},x_1). \end{gathered} \tag{1}$$

Получаем, что $R_{d,j} \in [R_\sigma]$. Использование леммы 1 завершает доказательство.

Лемма 7. Для произвольного $d > 0$ и $i, j > 0$ таких, что $i \mid j$, выполнено $S_{d,i} \subseteq S_{d,j}$

Доказательство. Напомним, что $S_{d,i} = Pol\, R_{d,i}$ и $S_{d,j} = Pol\, R_{d,j}$. Пусть $j = ih$. По определению предикатов $R_{d,m}$ имеем:

$$R_{d,j}(x_1,x_2) = \exists y_1,\ldots,y_{h-1}\; R_{d,i}(x_1,y_1) \,\&\, R_{d,i}(y_1,y_2) \,\&\ldots\&\, R_{d,i}(y_{h-1},x_2).$$

В силу леммы 1 получаем утверждение леммы.

Следствие 1. Если $c = ab \pmod d$, где $d \in D_\sigma$, то $S_{d,a} \subseteq S_{d,c}$.

Доказательство. По лемме 7 получаем, что $S_{d,a} \subseteq S_{d,ab}$. Но поскольку по определению числа d справедливо $\sigma^{ab}(x) = \sigma^c(x)$ для любого $x \in M_d$, то $R_{d,ab} = R_{d,c}$. Получаем, что $S_{d,ab} = S_{d,c}$.

Лемма 8. Пусть $d \in D_\sigma$, $1 < i < d$, $j =$ НОД(i, d). Тогда справедливо $S_{d,i} = S_{d,j}$.

Доказательство. Из условия и алгоритма Евклида [6] получаем, что существуют целые числа a, b такие, что справедливо $ad + bi = j$. Это эквивалентно $bi = j \pmod d$. По следствию леммы 7 получаем $S_{d,i} \subseteq S_{d,j}$. С другой стороны, непосредственно из условия данной леммы и леммы 7 следует, что $S_{d,j} \subseteq S_{d,i}$.

Следствие 2. Любой класс вида $S_{d,i}$, где i не делит d, совпадает с некоторым классом $S_{d,j}$, где $j \mid d$.

Используя данное следствие и лемму 5, будем рассматривать только классы $S_{d,i}$ и предикаты $R_{d,i}$, где i – делитель числа d, $d \in D_\sigma$.

Рассмотрим некоторые понятия, связанные с графами.

Путем из вершины v_1 в вершину v_2 в ориентированном графе G будем называть любую последовательность ребер вида $\{(v_1, w_1), (w_1, w_2), (w_2, w_3), \dots, (w_m, v_2)\}$ (вершины и ребра в последовательности могут повторяться). Ориентация ребер указанной последовательности может быть любой. *Замкнутым* называется путь, в котором первая и последняя вершины совпадают. *Циклом* называется замкнутый путь, в котором каждая вершина встречается не более одного раза (кроме первой и последней). *Длиной пути* будем называть разность количества ребер, пройденных в прямом направлении, и количества ребер, пройденных в обратном.

Лемма 9. Пусть все циклы связного орграфа G имеют длины $c_1, \dots, c_q$. Тогда для любой вершины v и любого целого α в графе G существует замкнутый путь длины αc, где c = НОД ($|c_1|, \dots, |c_q|$), проходящий через вершину v. Замкнутых путей с другими длинами в графе G нет.

Доказательство. Поскольку знак чисел c_i зависит от направления обхода соответствующего цикла, будем считать, что все $c_i > 0$.

Докажем вначале, что для любых целых $\alpha_1, \dots, \alpha_q$ граф G содержит замкнутый путь длины $\sum_{i=1}^{q} \alpha_i c_i$.

Мы можем пройти α_1 раз цикл длины [illegible] (знак числа α_1 указывает направление обхода). Поскольку граф связный, существует путь S' от какой-нибудь вершины указанного цикла к какой-то вершине цикла длины c_2. Пройдем по нему в прямом направлении, пройдем α_2 раз цикл длины c_2, затем вернемся по S' к первому циклу. Получим замкнутый путь длины $\alpha_1 c_1 + \alpha_2 c_2$ (поскольку длина пути [illegible] из-за его прохождения в прямом и обратном направлении будет присутствовать в сумме с плюсом и с минусом). Рассуждая аналогично для циклов с длинами $c_3, \dots, c_q$, получим, что в графе

G существуют замкнутые пути с длинами $\sum_{i=1}^{q} \alpha_i c_i$ для всевозможных целых чисел $\alpha_1, \ldots, \alpha_q$.

Покажем теперь, что других замкнутых путей в G нет.

Рассмотрим произвольный замкнутый путь C в G. Пусть v – некоторая вершина, входящая в путь C. Пойдем по ребрам C из указанной вершины. Если некоторая вершина w встретится второй раз (возможно $w = v$), то разрежем C на два замкнутых пути: T_1 – участок пути C между двумя вхождениями вершины w и замкнутый путь $C_1 = C \setminus T_1$. По построению каждая вершина входит в T_1 один раз. Возможны варианты: либо T_1 представляет собой замкнутый путь, состоящий из одного ребра, проходимого в прямом и обратном направлении, либо T_1 – цикл графа G. Проделаем теперь аналогичную процедуру для замкнутого пути C_1 и так далее. В итоге мы разобъем замкнутый путь C на множество циклов графа G, а также вырожденные замкнутые пути, состоящие из одного ребра, проходимого два раза. Длины последних путей равны 0, поэтому исключим их из рассмотрения. Поскольку каждое ребро C войдет в некоторый цикл или вырожденный замкнутый путь длины 0, то получаем, что длина пути C равна сумме длин некоторых циклов графа G, то есть длина C имеет вид $\boxed{\sum_{i=1}^{q} \alpha_i c_i}$ (каждый цикл в C может проходиться несколько раз).

Пусть теперь c = НОД ($c_1, \ldots, c_q$). Согласно алгоритму Евклида, существуют целые числа $b_1, \ldots, b_q$ такие, что $\sum_{i=1}^{q} b_i c_i$ = НОД ($c_1, \ldots, c_q$) = c. По доказанному выше в графе G существует замкнутый путь длины c. Учитывая связность графа G, получаем требуемое. Лемма 9 доказана.

Пусть все циклы связного орграфа G имеют длины $c_1, \ldots, c_q$. Через $c(G)$ будем обозначать величину НОД ($\boxed{|c_1|, \ldots, |c_q|}$).

Следствие 3. Пусть в связном орграфе G из вершины v в вершину w существует путь длины l. Тогда любой путь из вершины v в вершину w имеет длину $l + \alpha c(G)$, где α – некоторое число.

Лемма 10. 1. Пусть G_1, G_2 – связные орграфы. Обозначим через G_3 граф, полученный склейкой некоторой вершины v графа и вершины w графа G_2 (при этом считаем, что множества вершин графов и не пересекаются). Тогда

$$c(G_3) = \text{НОД}\ (\text{c}(G_1), \text{c}(G_2)).$$

2. Пусть G – связный граф. Обозначим через граф, полученный склейкой некоторых вершин v и w графа G. Пусть в G между вершинами v и w – путь длины l. Тогда

$$c(G_1) = \text{НОД}\ (c(G), l).$$

Доказательство. Докажем первое утверждение леммы. Отметим, что по определению цикла в графе присутствуют только циклы, имеющиеся в графах , . Но тогда по лемме 9 и определению величины $c(G)$ справедливо $c(G_3)$ = НОД (c(G_1), c(G_2)).

Перейдем ко второму утверждению. Любой цикл графа либо является циклом графа G, либо получается из некоторого пути в графе G между вершинами v и w. По лемме 9 длины $c_1, \dots, c_q$ всех циклов графа G кратны числу $c(G)$. По следствию 3 любой путь между вершинами v и w имеет длину $l + \alpha c(G)$, где α – некоторое целое число. Отметим, что в графе G найдется хотя бы один путь указанного вида без повторений вершин и ребер. Данный путь образует цикл в графе . Обозначим его длину $l + \alpha_0 c(G)$.

Получаем, что граф G имеет циклы с длинами $c_1, \dots, c_q$, $l + \alpha_0 c(G)$ и, возможно, еще циклы с длинами вида $l + \alpha_i c(G)$, где α_i – целые числа $(i \in \{1, \dots, p\}, p \geq 0)$. Окончательно имеем

$$c(G_1) = \text{НОД}\ (c_1, \dots, c_q, l + \alpha_0 c(G), l + \alpha_1 c(G), \dots, l + \alpha_p c(G)) = \text{НОД}\ (c(G), l).$$

Лемма 10 доказана.

Пусть предикат $p \in [R_\sigma]$, где R_σ – предикат, задающий класс самодвойственных функций S_σ. Пусть F – формула, реализующая предикат p над $\{R_\sigma\}$. Везде далее будем считать, что в формуле F вынесены вперед все кванторы существования. 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 $R_\sigma(y, x)$.

Отметим, что по графу формулы $G(F)$ формула F с вынесенными вперед кванторами существования восстанавливается однозначно. Поэтому вместо выражения $c(G(F))$ будем для краткости писать $c(F)$.

Пусть $v_{y_1}, \ldots, v_{y_N}$ – все вершины графа $G(F)$. Предположим, что длины всех путей от вершины v_i до v_j образуют множество $D_{i,j}$. Оставим в каждом таком множестве по одному минимальному неотрицательному элементу $d_{i,j}$. Отметим, что по лемме 9 множество $D_{i,j}$ содержит числа $(d_{i,j} + \alpha\ c(F))$ (mod h_σ) для всех α, откуда $0 \le d_{i,j} <$ c(F).

Условимся, что первые n переменных из множества $\{y_1, \ldots, y_N\}$ и только они являются свободными переменными предиката p.

Лемма 11. Предикату $p(y_1, \ldots, y_N)$ удовлетворяют все наборы $(\sigma^{d_{i,1}}(b), \sigma^{d_{i,2}}(b), \ldots, \sigma^{d_{i,i-1}}(b), b, \sigma^{d_{i,i+1}}(b), \ldots, \sigma^{d_{i,n}}(b))$ и только они, где b – произвольный элемент множества $M_{c(F)}$, произвольное $i \in \{1, \ldots, n\}$.

Доказательство. Пусть набор $\tilde{a}$ таков, что $p(a_1, \ldots, a_n) = TRUE$. Рассмотрим некоторую компоненту a_i указанного набора. По лемме 9 существует замкнутый путь длины $c(F)$, проходящий через вершину v_{y_i}. По определению графа G_F получаем, что $\sigma^{c(F)}(a_i) = a_i$, откуда $a_i \in M_{c(F)}$. Пусть $j \in \{1, \ldots, n\}$, $i \ne j$. Между вершинами v_{y_i} и v_{y_j} существует путь длины $d_{i,j}$. Следовательно, должно выполняться соотношение $a_j = \sigma^{d_{i,j}}(b)$. Получаем, что никакие наборы, кроме тех, что указаны в формулировке леммы, не могут удовлетворять предикату p.

Пусть теперь набор $\tilde{a}$ удовлетворяет формулировке леммы. Зафиксируем некоторое число $i \in \{1, \ldots, n\}$ и обозначим $a_i = b$. Присвоим каждой переменной y_j

предиката p (свободной и связанной) значение, равное $\sigma^{d_{i,j}}(b)$. Покажем далее, что $p(\widetilde{a}) = TRUE$.

Рассмотрим произвольное вхождение сомножителя $R_\sigma(y_j, \ldots, y_q)$ в формулу F, задающую предикат p над $\{R_\sigma\}$. Переменные y_i и y_q примут соответственно значения $a_j = \sigma^{d_{i,j}}(b)$ и $a_q = \sigma^{d_{i,q}}(b)$. Сомножителю $R_\sigma(y_j, y_q)$ в $G(F)$ соответствует ребро (v_{y_q}, v_{y_j}). Отметим, что в графе $G(F)$ существуют пути от вершины v_{y_i} к вершинам v_{y_q} и v_{y_j} с длинами соответственно $d_{i,q}$ и $d_{i,j}$. Составим новый путь из вершины v_{y_i} в вершину v_{y_j} через v_{y_q} длины $d_{i,q}+1$. По следствию 3 существует целое число α такое, что $d_{i,j} = d_{i,q} + 1 + \alpha c(F)$.

Учитывая, что $a_q \in M_{c(F)}$, получаем

$$a_j = \sigma^{d_{i,j}}(b) = \sigma^{d_{i,q}+1+\alpha c(F)}(b) = \sigma^{1+\alpha c(F)}(a_q) = \sigma(a_q),$$

откуда $R_\sigma(a_j, a_q) = TRUE$. При описанном присвоении произвольный сомножитель в формуле F истинен, откуда $p(\widetilde{a}) = TRUE$. Лемма 11 доказана.

Обозначим через $G_{d,j}$ графы, соответствующие формулам $F_{d,j}$ из выражения (1), задающим предикаты $R_{d,j}$ над $\{R_\sigma\}$.

Лемма 12. Пусть $P = \left\{R_{d_1,i_1}, \ldots, R_{d_m,i_m}\right\}$, $d_0 =$ НОД($d_1, \ldots, d_m$), $M_{d_0} \neq \varnothing$. Тогда для любых целых чисел a_i, b_i ($i \in \left\{1, \ldots, m\right\}$) справедливо $R_{t,p} \in [P]$, где $t =$ НОД ($\boxed{\ }$, $\sum_{j=1}^{m} a_j i_j$) и $p = \sum_{j=1}^{m} b_j c_j$ (mod p).

Доказательство. Рассмотрим следующий предикат:

$$R_{d_0}(x) = \exists y_1, \ldots, y_m \; R_{d_1,i_1}(x, y_1) \,\&\, R_{d_2,i_2}(x, y_2) \,\&\ldots\&\, R_{d_m,i_m}(x, y_m). \qquad (2)$$

Указанный предикат можно реализовать формулой F_0 над $\{R_\sigma\}$, полученной подстановкой в выражение (2) формул F_{d_j,i_j} (выражение (1)) для предикатов R_{d_j,i_j}.

Отметим, что граф G_{F_0} получается соединением графов G_{d_j,i_j} по одной вершине. Используя лемму 10, получаем, что $c(F_0)$ = НОД ($d_1, \ldots,$ d_m) = $\boxed{\;}$. Откуда по лемме 11 имеем, что $R_{d_0}(b) = TRUE$ тогда и только тогда, когда $b \in M_{d_0}$.

Введем следующие предикаты

$$R^n_{d_j,i_j}(x_1, x_2) = \exists y_1, \ldots, y_{n-1}\ R_{d_j,i_j}(x_1, y_1) \,\&\, R_{d_j,i_j}(y_1, y_2) \,\&\ldots\&\, R_{d_j,i_j}(y_{n-1}, x_2)\,, \qquad (3)$$

$$\overline{R}_a\,(x) = \exists y_1, \ldots, y_{s-1}\ R^{a_{j_1}}_{d_{j_1},i_{j_1}}(x, y_1) \,\&\, R^{a_{j_2}}_{d_{j_2},i_{j_2}}(y_1, y_2) \,\&\ldots\&\, R^{a_{j_s}}_{d_{j_s},i_{j_s}}(y_{s-1}, x_2)\,, \qquad (4)$$

где $j_1, \ldots, j_s$ – номера всех ненулевых чисел из множества $\{a_1, \ldots, a_m\}$. Мы подразумеваем, что все связанные переменные предикатов $R^n_{d_j,i_j}$ различны и отличны от связанных переменных $y_1, \ldots, y_{s-1}$ из формулы (3).

Обозначим через $F^n_{d_j,i_j}$ формулу для предиката $R^n_{d_j,i_j}$, получающуюся подстановкой формул F_{d_j,i_j} в выражение (3). По лемме 10 справедливо $c(F^n_{d_j,i_j})$ = d_j. Аналогично обозначим через $\overline{F}_a$ формулу для предиката $\overline{R}_a$, получающуюся подстановкой формул $F^n_{d_j,i_j}$ в выражение (4). По лемме 10 справедливо $c(\overline{F}_a) =$ НОД $(d_{j_1}, \ldots, d_{j_s}, \sum_{j=1}^{m} a_j i_j)$. Используя лемму 11, имеем $\overline{R}_a(b) = TRUE$ тогда и только тогда, когда $b \in M_{c(\overline{F}_a)}$.

Обозначим $T_1(x) = R_{d_0}(x) \,\&\, \overline{R}_a(x)$. Заметим, что $M_{d_0} \cap M_{c(\overline{F}_a)} = M_t$, откуда получаем, что $T_1(b) = TRUE$ тогда и только тогда, когда $b \in M_t$.

Введем теперь предикат

$$R_b\,(x_1, x_2) = \exists y_1, \ldots, y_{r-1}\ R^{b_{s_1}}_{d_{s_1},i_{s_1}}(x_1, y_1) \,\&\, R^{b_{s_2}}_{d_{s_2},i_{s_2}}(y_1, y_2) \,\&\ldots\&\, R^{b_{s_r}}_{d_{s_r},i_{s_r}}(y_{r-1}, x_2)\,, \qquad (5)$$

где $s_1, \ldots, s_r$ – номера всех ненулевых чисел из множества $\{b_1, \ldots, b_m\}$. Мы опять подразумеваем, что все связанные переменные предикатов $R^n_{d_j,i_j}$ различны и отличны от связанных переменных $y_1, \ldots, y_{r-1}$ из формулы (5).

Обозначим через F_b формулу для предиката R_b, получающуюся подстановкой формул $F^n_{d_j,i_j}$ в выражение (5). По лемме 10 справедливо $c(F_b)=$ НОД ($d_{s_1},\ldots,d_{s_r}$), а по лемме 11 – $R_b(x_1,x_2) = R_{c(F_b),p}$.

В силу $M_t \subseteq M(c(F_b))$ справедливо $R_{t,p}(x_1,x_2) = T_1(x_1)\,\&\,R_b(x_1,x_2)$.

Остается заметить, что согласно выражениям (2), (3), (4), (5) предикаты R_{d_0}, $\overline{R}_a$, R_b реализуются формулами над множеством предикатов *P*. Следовательно, справедливо $R_{t,p} \in [P]$. Лемма 12 доказана.

Лемма 13. Пусть классы S_{d_1,i_1} и S_{d_2,i_2} таковы, что справедливо $M_{d_1} \subseteq M_{d_2}$ и НОД(d_1,i_2) не делит i_1. Тогда существует функция *F*, удовлетворяющая следующим условиям:

1) $F \notin S_{d_1,i_1}$;

2) для любого $d_3 \in D_\sigma$ такого, что $M_{d_1} \not\subset M_{d_3}$, $M_{d_1} \neq M_{d_3}$, выполнено $F \in S_{d_3,m}$, где *m* – любое число;

3) для любого $d_4 \in D_\sigma$ такого, что $M_{d_2} \subseteq M_{d_4}$, и *r* такого, что $i_2 r$ делит h_{d_4}, выполнено $F \in S_{d_4,i_2 r}$.

Доказательство. Обозначим $\pi_1 = \sigma^{i_1}$, $\pi_2 = \sigma^{i_2}$. Пусть множество M_{d_1} состоит из элементов, входящих в циклы подстановки π_1 с длинами $m_1,\ldots,m_p$. Возьмем в каждом из указанных циклов по произвольному элементу $a_1,\ldots,a_p$, пусть $b_q = \pi_1(a_q)$, $q = 1,\ldots,p$.

Поскольку НОД(d_1,i_2) не делит i_1, то $d_1 \neq i_1$, откуда π_1 – не тождественная подстановка на множестве M_{d_1}. Получаем, что у подстановки π_1 на множестве M_{d_1} существует цикл длины, большей 1. Пусть элемент *d* принадлежит этому циклу.

Обозначим через *F* *p*-местную функцию, равную *d* на наборах $\widetilde{a} = (a_1,\ldots,a_p)$ и $\widetilde{b} = (b_1,\ldots,b_p)$; на любом наборе $\widetilde{c} = (c_1,\ldots,c_p)$ таком, что существует число *m*: $c_q = \pi_2^m(a_q)$ для всех $q = 1,\ldots,p$ или $c_q = \pi_2^m(b_q)$ для указанных *q*, значение функции равно $\pi_2^m(d)$ (в дальнейшем множество наборов данного вида вместе с наборами $\widetilde{a}$ и $\widetilde{b}$

будем обозначать *C*), на остальных наборах $F(\widetilde{x}) = x_1$. Докажем корректность определения указанной функции.

Во-первых, покажем, что не существует чисел α, β таких, что $\pi_2^{\alpha}(\widetilde{a}) = \pi_2^{\beta}(\widetilde{b})$. Предположим противное, тогда для всех $q = 1,\ldots,p$ $\sigma^{i_2(\alpha-\beta)}(a_q) = b_q$ или $\sigma^{i_2(\alpha-\beta)-i_1}(a_q) = a_q$. Предположим, что элементы $a_1,\ldots,a_p$ входят в циклы исходной подстановки σ с длинами $m'_1,\ldots,m'_p$, откуда $m'_j \mid (i_2(\alpha-\beta)-i_1)$ для любого $j \in \{1,\ldots,p'\}$. А поскольку мы условились, что $d_1 =$ НОК ($m'_1,\ldots,m'_{p'}$), то $d_1 \mid (i_2(\alpha-\beta)-i_1)$. Следовательно, существуют константы k_1, k_2 такие, что справедливо $k_1 i_2 + k_2 d_1 = i_1$, откуда НОД(d_1, i_2) делит i_1. Получаем противоречие с условием леммы.

Во-вторых, если для некоторого *t* справедливо $\pi_2^t(a_q) = a_q$ для всех $q \in \{1,\ldots,p\}$, то для функции *F* должно выполняться

$$d = f(\widetilde{a}) = f(\pi_2^t(a_1),\ldots,\pi_2^t(a_p)) = \pi_2^t(d),$$

что обеспечивается выбором элемента *d*.

Покажем теперь, что построенная функция удовлетворяет сформулированным условиям.

Согласно выбору элемента *d*, выполнено $\pi_1(d) \neq d$. Заметим, что элементы a_q ($q \in \{1,\ldots,p\}$) принадлежат множеству M_{d_1}, следовательно, указанному множеству принадлежат и все элементы b_q. Поскольку $b_q = \pi_1(a_q)$, то $R_{d_1,i_1}(a_q, b_q) = TRUE$ для любого $q \in \{1,\ldots,p\}$. Итак, получаем, что рассмотрение наборов $\widetilde{a} = (a_1,\ldots,a_p)$ и $\widetilde{b} = (b_1,\ldots,b_p) = (\pi_1(a_1),\ldots,\pi_1(a_p))$ для предиката R_{d_1,i_1} дает $F \notin Pol\, R_{d_1,i_1} = S_{d_1,i_1}$.

Пусть $M_{d_1} \not\subset M_{d_3}$, $M_{d_1} \neq M_{d_3}$. Следовательно, существует цикл C_t подстановки σ длины m_t, элементы которого принадлежат множеству M_{d_1} и не принадлежат M_{d_3}. Рассмотрим любые два *p*-местных набора $\widetilde{x}$ и $\widetilde{y}$, покомпонентно удовлетворяющие предикату $R_{d_3,m}$, где *m* – любое число. Из сказанного выше и того факта, что *t*-я компонента любого набора из множества *C* принадлежит циклу C_t, следует, что $\widetilde{x}, \widetilde{y} \notin C$ Получаем, что $R_{d_3,m}(F(\widetilde{x}), F(\widetilde{y})) = R_{d_3,m}(x_1, y_1) = TRUE$.Следовательно, $F \in Pol\, R_{d_3,m} = S_{d_3,m}$

Пусть, наконец, $M_{d_2} \subseteq M_{d_4}$, i_2, r удовлетворяют условиям леммы. Снова возьмем два произвольных набора $\widetilde{x}$, $\widetilde{y}$, покомпонентно удовлетворяющих предикату R_{d_4,i_2r}

Предположим, что $\widetilde{x} \in C$. Следовательно, существует *m*: $\widetilde{x} = (\pi_2^m(a_1), \ldots, \pi_2^m(a_p))$, откуда $\widetilde{y} = (\pi_2^{m+r}(a_1), \ldots, \pi_2^{m+r}(a_p))$ (либо указанные соотношения справедливы для набора $\widetilde{b}$). Получаем, что $\widetilde{y} \in C$. Итак, либо оба набора $\widetilde{x}$, $\widetilde{y}$ принадлежат множеству *C*, либо оба не принадлежат *C*. Во втором случае $R_{d_4,i_2r}(F(\widetilde{x}), F(\widetilde{y})) = R_{d_4,i_2r}(x_1, y_1) = TRUE$.

В первом случае будет выполнено

$$R_{d_4,i_2r}(F(\widetilde{x}), F(\widetilde{y})) = R_{d_4,i_2r}(F(\pi_2^m(\widetilde{a})), F(\pi_2^{m+r}(\widetilde{a}))) = R_{d_4,i_2r}(d', \pi_2^r(d')) = TRUE,$$

где $d' = \pi_2^m(d)$ (поскольку $d \in M_{d_1}$, то $d' \in M_{d_1}$, откуда $d' \in M_{d_4}$).

Окончательно получаем, что $F \in Pol\, R_{d_4,i_2r} = S_{d_4,i_2r}$. Лемма 13 доказана.

Лемма 14. Пусть классы S_{d_1,i_1} и S_{d_2,i_2} таковы, что справедливо $M_{d_1} \subset E_k$, и у подстановки σ существует цикл $L \subseteq M_{d_2} \setminus M_{d_1}$ длины *l*, удовлетворяющей условию $l \mid$ НОК(i_2, d_1). Тогда существует функция *G*, удовлетворяющая условиям:

1) $G \notin S_{d_1,i_1}$;

2) для любого $d_3 \in D_\sigma$ такого, что $M_{d_1} \not\subset M_{d_3}$, $M_{d_1} \neq M_{d_3}$, выполнено $G \in S_{d_3,m}$, где *m* – любое число;

3) для любого $d_4 \in D_\sigma$ такого, что $M_{d_2} \subseteq M_{d_4}$, и *r* такого, что $i_2 r$ делит h_{d_4}, выполнено $G \in S_{d_4,i_2r}$.

Доказательство. Доказательство аналогично предыдущему. Обозначим $\pi_1 = \sigma^{i_1}$, $\pi_2 = \sigma^{i_2}$, возьмем по элементу a_i из каждого цикла подстановки π_1 на множестве M_{d_1} и составим из указанных элементов *p*-местный набор $\widetilde{a} = (a_1, \ldots, a_p)$. Пусть элемент $d \in L$. Определим *p*-местную функцию *G* следующим образом. Положим $G(\widetilde{a}) = d$; на любом наборе $\widetilde{c} = (c_1, \ldots, c_p)$ таком, что существует число *m*: $c_q = \pi_2^m(a_q)$ для всех $q = 1, \ldots, p$, функция G равна $\pi_2^m(d)$. Обозначим указанное множество p-местных наборов (вместе с $\widetilde{c}$) через C. На всех остальных наборах положим $G^{\sigma}_{d_1,i_1,L}(\widetilde{x}) = x_1$.

Снова покажем корректность определения функции. Пусть число r – минимальное, удовлетворяющее условию $\pi_2^r(a_q) = a_q$ для всех $q \in \{1,\ldots,p\}$. Следовательно, элементы $a_1,\ldots,a_p$ входят в циклы исходной подстановки σ, длины которых делят число $i_2 r$. Число $d_1 \in D_\sigma$ равно наименьшему общему кратному длин циклов исходной подстановки σ, элементы которых образуют множество M_{d_1}. Получаем, что $d_1 | i_2 r$, или существует число t такое, что выполнено $i_2 r = t d_1$. Но поскольку r – минимальное число, удовлетворяющее условию $\pi_2^t(a_q) = a_q$ для всех $q \in \{1,\ldots,p\}$, то ни для какого числа $r' < r$ не справедливо $d_1 | i_2 r'$, откуда

$$i_2 r = t d_1 = \text{НОК}(i_2, d_1). \tag{6}$$

По определению числа r для корректности определения функции G должно выполняться следующее соотношение:

$$d = G(\widetilde{a}) = G(\pi_2^r(a_1),\ldots,\pi_2^r(a_p)) = \pi_2^r(d) = \sigma^{ri_2}(d).$$

Указанное равенство выполнено тогда и только тогда, когда элемент d принадлежит циклу подстановки σ, длина l которого делит число ri_2. Но по условию l | НОК(i_2, d_1), откуда, согласно (6), получаем $l | i_2 r$. Корректность определения функции G доказана.

Покажем, что функция G удовлетворяет сформулированным требованиям. Пусть $\widetilde{b} = (\pi_1(a_1),\ldots,\pi_1(a_p))$. Первый пункт вытекает из соотношения $R_{d_1,i_1}(G(\widetilde{a}), G(\widetilde{b})) = R_{d_1,i_1}(d, G(\widetilde{b})) = FALSE$ (поскольку $d \notin M_{d_1}$). Доказательства второго и третьего пунктов полностью повторяют аналогичные доказательства в предыдущей лемме. Лемма 14 доказана.

Докажем теперь важные следствия рассмотренных утверждений.

Теорема 1. В решетке замкнутых классов k-значной логики над классом самодвойственных функций S_σ находятся только классы вида $S_{d,i}$ и их пересечения.

Доказательство. Из леммы 6 следует, что все классы $S_{d,i}$ содержат класс S_σ. Поэтому нам достаточно показать, что любой замкнутый класс *A*, содержащий класс S_σ, совпадает с одним из указанных классов.

Рассмотрим один из предикатов *p*, который сохраняют все функции системы *A*, то есть $p \in Inv(A)$. По лемме 4 получаем, что предикат *p* реализуется некоторой формулой *F* над $\{R_\sigma\}$. Сопоставим формуле *F* граф G_F.

Рассмотрим вначале случай, когда граф G_F связен.

Покажем, что замкнутый класс $Pol\, p$ совпадает с одним из классов вида $S_{d,i}$.

Перенумеруем вершины графа G_F. Будем предполагать, что первые *n* вершин $v_{x_1},\ldots,v_{x_n}$ $(n \geq 1)$ графа G_F соответствуют свободным переменным $x_1,\ldots,x_n$ формулы *F*, остальные – связанным. Обозначим через $d_{i,j}$ минимальное неотрицательное расстояние от вершины v_{x_i} до вершины v_{x_j}.

Рассмотрим теперь следующие случаи.

Пусть предикат *p* – одноместный (*n* = 1). По лемме 11 получаем, что $p(x) = TRUE$ тогда и только тогда, когда $x \in M_{c(F)}$. Согласно лемме 5 мы можем взять число $d \in D_\sigma$ такое, что $M_{c(F)} = M_d$. Тогда имеем $p(x) = R_{d,d}$, откуда $Pol\, p = S_{d,d}$. Отметим, что в данном случае мы получили либо P_k, либо предполный центральный класс.

Пусть теперь предикат *p* двухместный (*n* = 2). Из леммы 11 следует, что $p(a,b) = TRUE$ тогда и только тогда, когда $a,b \in M_{c(F),\sigma}$ и $b = \sigma^{d_{1,2}}(a)$. Снова по лемме 5 возьмем число $d \in D_\sigma$ такое, что $M_{c(F)} = M_d$, а по следствию из леммы 8 число *i* – делитель *d* такое, что $F_{c(F),d_{1,2}} = S_{d,i}$.

Пусть теперь *n* > 2. Покажем, что в данном случае существует двухместный предикат R' такой, что $p \in R'$, $R' \in [p]$, то есть $Pol\, p = Pol(R')$ (согласно лемме 1), а предикат R' относится ко второму случаю.

Рассмотрим множество элементов $d_{1,1},\ldots,d_{1,p}$. Если среди них найдутся два равных $d_{1,i}$ и $d_{1,j}$, то согласно лемме 11 в любом наборе $\widetilde{a} \in E_k^n$, удовлетворяющем предикату *p*, компоненты a_i и a_j будут равны. По лемме 2 мы можем перейти к предикату, задающему тот же класс $Pol\, p$, в котором все числа $d_{1,1},\dots,d_{1,n}$ различны.

Применив алгоритм Евклида, получим, что существуют целые числа $b_1,\dots,b_n$ такие, что

$$d = \text{НОД}\,(d_{1,1},\dots,d_{1,n}) = \sum_{i=1}^{n} b_i d_{1,i} \tag{7}$$

По лемме 12 справедливо $R_{c(F),d_{1,i}} = R_{c(F),s_i d} \in [R_{c(F),d}\,]$. По леммам 11 и 12 получаем

$$p(x_1,\dots,x_n) = R_{c(F),d_{1,2}}(x_1,x_2) \,\&\, R_{c(F),d_{1,3}}(x_1,x_3) \,\&\dots\&\, R_{c(F),d_{1,n}}(x_1,x_n),$$

откуда $p \in [R_{c(F),d}]$.

Справедливость следующего соотношения вытекает непосредственно из леммы 11.

$$R_{c(F),b_i d_{1,i}}(x_1,x_2) = \exists y_j^i\, p(x_1,y_2^1,\dots,y_{i-1}^1,y_i^1,y_{i+1}^1,\dots,y_n^1) \,\&\, p(y_i^1,y_2^2,\dots,y_{i-1}^2,y_i^2 y_{i+1}^2,\dots,y_n^2)\,\&$$

$$\&\, p(y_i^2,y_2^3,\dots,y_{i-1}^3,y_i^3 y_{i+1}^3,\dots,y_n^3) \,\&\dots\&\, p(y_i^{b_i-1},y_2^{b_i},\dots,y_{i-1}^{b_i},x_2,y_{i+1}^{b_i},\dots,y_n^{b_i}),$$

где под символом $\exists y_j^i$ подразумевается существование всех переменных, имеющих вид y_j^i и встречающихся в формуле.

Далее имеем $R_{c(F),d} \in [\{R_{c(F),b_i d_{1,1}},\dots,R_{c(F),b_i d_{1,n}}\}]$ в силу (7) и леммы 12, откуда окончательно $R_{c(F),d} \in [p]$.

Пусть теперь граф G_F несвязен. В этом случае каждая компонента связности G_F соответствует некоторой формуле F_i, задающей предикат $p_i, i \in \{1,\dots,m\}$. По лемме 3 получаем, что $Pol\, p = \bigcap_{i=1}^{m} Pol\, p_i$, то есть класс $Pol\, p$ совпадает с некоторым пересечением классов из рассмотренных семейств. Теорема 1 доказана.

Рассмотрим структуру надрешетки класса S_σ.

Теорема 2. $S_{d_2,i_2} \subseteq S_{d_1,i_1}$ тогда и только тогда, когда выполнены следующие условия:

1) $M_{d_1} \subseteq M_{d_2}$;

2) $\text{НОД}(i_2,d_1)|i_1$;

3) для любого цикла L длины l подстановки σ на множестве $M_{d_2} \setminus M_{d_1}$ число l не делит НОК(i_2, d_1).

Доказательство. Если нарушается первое требование, то существует цикл L_1 подстановки σ, элементы которого принадлежат множеству $M_{d_1} \setminus M_{d_2}$. Возьмем два элемента a, b, принадлежащие указанному циклу, такие что $b = \sigma^{i_1}(a)$ (при этом возможна ситуация, когда $a = b$). Пусть d – некоторый элемент, не принадлежащий циклу L_1. Рассмотрим следующую функцию:

$$u(x) = \begin{cases} d, & \text{\textit{если} } x = a; \\ x, & \text{\textit{иначе.}} \end{cases}$$

На множестве M_{d_2} справедливо $u(x) = x$, откуда $u(x) \in S_{d_2,i_2}$. Из соотношений $R_{d_1,i_1}(a,b) = TRUE$, $R_{d_1,i_1}(u(a),u(b)) = R_{d_1,i_1}(d,b) = FALSE$ (поскольку элементы d, b принадлежат разным циклам подстановки σ) следует, что $u(x) \notin S_{d_1,i_1}$.

Если нарушается второе требование, то выполнены условия леммы 13 и существует функция $F \in S_{d_2,i_2} \setminus S_{d_1,i_1}$. Если нарушается третье требование, то выполняются все условия леммы 14. Следовательно, существует функция $G \in S_{d_2,i_2} \setminus S_{d_1,i_1}$.

С другой стороны, пусть перечисленные в формулировке условия выполнены.

Напомним, что по лемме 12 для любых чисел a, b справедливо $R_{t,p} \in [R_{d_1,i_1}]$, где t = НОД(d_2, ai_2), $p = bi_2 \pmod t$. Положив $a = \dfrac{НОК(i_2,d_1)}{i_2}$, имеем $t =$ НОД(d_2, НОК(i_2, d_1)).

В силу первого условия $d_1 | d_2$. Очевидно, $d_1 |$ НОК(i_2, d_1). Получаем, что $d_1 | t$, то есть существует число α такое, что $t = \alpha d_1$. Покажем, что $M_{d_1} = M_t$.

Пусть $b \in M_{d_1}$, то есть элемент b принадлежит циклу подстановки σ длины l', делящей d_2. Но тогда $l' | \beta d_1 = t$. Получаем, что $b \in M_t$.

С другой стороны, пусть $b \in M_t$. В этом случае длина l' цикла подстановки σ, содержащего элемент l', делит число t = НОД(d_2, НОК(i_2, d_1)). Но тогда l' делит оба числа d_2 и НОК(i_2, d_1). Из $l'|d_2$ следует, что $b \in M_{d_2}$, а из $l'|$ НОК(i_2, d_1) и третьего условия теоремы следует, что $b \notin M_{d_2} \setminus M_{d_1}$. Получаем, что $b \in M_{d_1}$.

Из второго условия и алгоритма Евклида следует, что существуют целые числа t_1, t_2, t_3 такие, что выполнено

$$i_1 = t_1 \text{НОД}(i_2, d_1) = t_2 i_2 + t_3 d_1$$

Положив $b = t_2$, имеем $p = i_1 - t_3 d_1 \pmod t$. Следовательно, существует число β такое, что $p = i_1 - t_3 d_1 + \beta t = i_1 - t_3 d_1 + \beta\alpha d_1 = i_1 + \gamma d_1$, откуда $i_1 =$ НОД (p, d_1).

Из $M_t = M_{d_1}$ следует, что $R_{t,p} = R_{d_1,p}$. По нашему соглашению $d_1 \in D_\sigma$. Из $i_1 =$ НОД (p, d_1) и леммы 8 следует, что $R_{t,p} = R_{d_1,p} = R_{d_1,i_1}$.

Окончательно получаем, что $R_{d_1,i_1} \in [R_{d_2,i_2}]$. В силу леммы 1 имеем $S_{d_2,i_2} \subseteq S_{d_1,i_1}$. Теорема 2 доказана.

Следствие 4. Для любого фиксированного числа $d \in D_\sigma$ решетка замкнутых классов $S_{d,i}$ изоморфна решетке делителей числа d относительно свойства делимости.

Следствие 5. Решетка классов самодвойственных функций S_{σ^i} изоморфна решетке делителей числа h_σ относительно свойства делимости.

Лемма 15. Пусть $P = \{R_{d_1,i_1}, \ldots, R_{d_m,i_m}\}$, $R_{d,i}$ – произвольный предикат, $A = \{R_{d_1,i_1}, \ldots, R_{d_l,i_l}\}$ – подмножество из предикатов множества *P*, для которых $M_d \subseteq M_{d_{j_l}}$. Пусть $\bar{d} =$ НОД($d_{j_1}, \ldots, d_{j_l}$), $\bar{i} =$ НОД($i_{j_1}, \ldots, i_{j_l}$). Тогда $Pol\,P \subseteq S_{d,i} = Pol\,R_{d,i}$ тогда и только тогда, когда справедливо $S_{\bar{d},\bar{i}} \subseteq S_{d,i}$.

Доказательство. Из леммы 12 следует, что $R_{\bar{d},\bar{i}} \subseteq [A]$, откуда по лемме 1 имеем, что $Pol\,A \subseteq Pol\,R_{\bar{d},\bar{i}} = S_{\bar{d},\bar{i}}$. Получаем, что из $S_{\bar{d},\bar{i}} \subseteq S_{d,i}$ следует $Pol\,P \subseteq Pol\,A \subseteq S_{\bar{d},\bar{i}} \subseteq S_{d,i}$.

Пусть теперь выполнено $Pol\,P \subseteq S_{d,i}$. Предположим, что $S_{\bar{d},\bar{i}} \not\subset S_{d,i}$. Поскольку $M_{\bar{d}} = M_{d_{j_1}} \bigcap \ldots \bigcap M_{d_{j_l}}$ и справедливо $M_d \subseteq M_{\bar{d}}$, то нарушается либо второй, либо третий пункт теоремы 2. Следовательно, справедливы условия либо леммы 13, либо леммы 14.

Получаем, что существует функция $f \in S_{\bar{d},\bar{i}} \setminus S_{d,i}$ (это либо функция *F*, либо функция *G*) с описанными в указанных леммах свойствами.

Возьмем произвольный предикат $R_{d',i'} \in P \setminus A$. По определению множества *A* справедливо $M_d \not\subset M_{d'}$. Согласно вторым пунктам лемм 13 и 14 справедливо $f \in Pol\, R_{d',i'}$. Пусть теперь $R_{d',i'} \in A$. В этом случае справедливо $M_{\bar{d}} \subseteq M_{d'}$. По определению числа $\bar{i}$ справедливо $i' = t\bar{i}$, где *t* – некоторое число. В силу третьих пунктов лемм 13 и 14 опять получаем справедливость $f \in Pol\, R_{d',i'}$.

Итак, мы показали, что $f \in Pol\, P$. С другой стороны $f \notin S_{d,i}$. Получаем противоречие с соотношением $Pol\, P \subseteq S_{d,i}$. Лемма 15 доказана.

По теореме 1 любой класс из надструктуры класса самодвойственных функций S_σ имеет вид $S_{i_1,d_1} \bigcap \ldots \bigcap S_{i_s,d_s}$, или $Pol\,(R_{d_1,i_1},\ldots,R_{d_s,i_s})$. Из леммы 15 получаем следующую теорему.

Теорема 3. Пусть $A = Pol\,(R_{d_1,i_1},\ldots,R_{d_s,i_s})$, $B = Pol\,(R_{t_1,j_1},\ldots,R_{t_m,j_m})$. Для произвольного $p \in \{1,\ldots,m\}$ обозначим через I_p множество номеров *n* чисел из $\{d_1,\ldots,d_s\}$, удовлетворяющих $M_{t_p} \subseteq M_{d_n}$. Пусть $\bar{d}_p, \bar{i}_p$ – НОД чисел с номерами из I_p из множеств $\{d_1,\ldots,d_s\}$ и $\{i_1,\ldots,i_s\}$ соответственно.

$A \subseteq B$ тогда и только тогда, когда для любого $p \in \{1,\ldots,m\}$ справедливо $S_{\bar{d}_p,\bar{i}_p} \subseteq S_{t_p,j_p}$ (то есть для рассматриваемой пары классов выполнены указанные в теореме 2 условия).

Несмотря на громоздкость полученного критерия, он дает простой алгоритм проверки вложения для двух классов из надструктуры класса самодвойственных функций (см. теоремы 2 и 3).

2.3. Публикации результатов НИР

По результатам проведенных исследований сделана публикация в трудах научной конференции и опубликована статья в высокорейтинговом российском журнале:

- *В. Б. Ларионов, В. С. Федорова* «О строении классов, содержащих класс квазисамодвойственных функций» // Материалы 4-й Российской школы-семинара «Синтаксис и семантика логических систем», посвященной 80-летию основания Бурятского государственного университета (Улан-Удэ, 14–19 августа 2012 г.). Изд-во ФГБОУ ВПО «Бурятский государственный университет», 2012, с. 70-73.
- *В.Б. Ларионов, В.С. Федорова* «Надструктура классов самодвойственных k-значных функций» // Известия Иркутского государственного университета. Серия Математика. 2011. Т. 4, № 3, с. 83-98.

Копии статей включены в Приложение А к настоящему отчету, заключения экспертной комиссии по их открытому опубликованию – в Приложение Б.

3. Заключение

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

1. Описана структура и основные свойства надрешетки произвольного класса квазисамодвойственных функций многозначной логики.

2. Получено полное описание всех классов (и их взаимных включений), содержащих произвольный класс самодвойственных функций многозначной логики. Изучены основные свойства надструктуры класса самодвойственных функций многозначной логики.

3. По результатам исследований сделана публикация в трудах научной конференции и опубликована статья в высокорейтинговом российском журнале.

4. Подготовлен научно-технический отчет по итогам третьего этапа.

План проведения исследований третьего этапа выполнен полностью. Копии статей приводятся в Приложении А. Все полученные научные результаты являются новыми; перед их публикацией получено заключение экспертной комиссии по открытому опубликованию (Приложение Б). 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. Бондарчук 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.
3. Яблонский С. В., Гаврилов Г. П., Набебин А. А. Предполные классы в многозначных логиках. – М.: Изд. дом МЭИ, 1997. – 144 с.
4. Марченков С. С. Замкнутые классы булевых функций – М.: Физматлит, 2000. – 128 с.
5. Яблонский С. В. Функциональные построения в k-значной логике // Труды матем. института им. В. А. Стеклова АН СССР. – 1958. – Т. 51. – С. 5-142.
6. Арнольд И. В. Теоретическая арифметика – М.: Учпедгиз, 1938. – 480 с.