Федеральное государственное бюджетное образовательное
учреждение высшего образования
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»
Кафедра математического и компьютерного моделирования

На правах рукописи

УДК 519.716

Мещанинов Дмитрий Германович

АДДИТИВНЫЕ ПРЕДСТАВЛЕНИЯ И ЗАМКНУТЫЕ КЛАССЫ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

Специальность 01.01.09 – дискретная математика
и математическая кибернетика

Д И С С Е Р Т А Ц И Я

на соискание учёной степени доктора
физико-математических наук

Москва – 2022

Оглавление

ВВЕДЕНИЕ

Актуальность темы исследования

Работа посвящена классификации дискретных функций, определенных на конечном множестве мощности k, а также некоторых функций, определенных на всем множестве целых чисел.

Классификация объектов какой-либо предметной области — актуальнейшая и принципиальная проблема, влияющая на все дальнейшее развитие этой области. В качестве примеров достаточно указать классификацию живых организмов К. Линнея и классификацию химических элементов Д. И. Менделеева. Классификация чрезвычайно важна в медицине, а также в гуманитарных отраслях знания, в частности, юриспруденции, политической, дипломатической и военной областях (хотя иногда носит несколько субъективный характер). Классификация математических объектов, в отличие от названных областей, не изменяется со временем, не зависит от полноты эмпирических данных, свободна от субъективизма и может быть обоснована чисто логическим путем.

В основе любой классификации лежат свойства (признаки) объектов. Многие свойства объектов сохраняются при их определенных преобразованиях (изменениях) под действием некоторых операций. Множество объектов с заданными операциями над ними образует алгебру. Алгебры, элементами которых являются функции, есть *функциональные системы*. С точки зрения математической кибернетики, функциональная система определяется функциями, реализуемыми управляющими системами, операции соответствуют правилам построения новых управляющих систем из заданных. Таким образом, функциональная система — это математический аппарат для описания структуры и поведения управляющих систем в различных предметных областях: природе, технике, общественных институтах и повседневной жизни.

Естественные и искусственные системы характеризуются множеством состояний, в которых они могут находиться. Если множество состояний конечно (имеет мощность k) или счетно, то для описания такой системы можно применить *функции k-значной* или *счетнозначной логики*. Эти функции и их переменные принимают значения, соответствующие состояниям. Допустимые преобразования функций определяют функциональную систему. Классификация должна учитывать свойства функций, сохраняемые при их преобразованиях, такие классы *замкнуты* относительно операций функциональной системы. Замкнутые классы могут быть заданы формулами, реализующими их элементы.

Описание замкнутых классов в функциональной системе k-значной логики P_k и в счетнозначной логике с операциями *суперпозиции* (они состоят в композиции функций, переименовании и отождествлении переменных) с помощью формул

особого вида — тема проведенного исследования.

Современное состояние дел в области исследования

Исторически первой классификацией в теории функциональных систем явились результаты Э. Поста 1921–1941 гг. о замкнутых классах алгебры P_2 булевых функций (функций алгебры логики) [99, 100]. Множество всех замкнутых классов оказалось счетным, каждый класс имеет конечный базис и является классом сохранения некоторого предиката на множестве $\{0,1\}$. Построена решетка (по отношению включения) $\mathcal{L}(P_2)$ всех замкнутых классов булевых функций. В дальнейшем выявились существенные отличия многозначных функциональных систем P_k при $k \geq 3$ от алгебры логики и принципиальные трудности: множество всех замкнутых классов (если k конечно) имеет мощность континуума, и есть классы, не имеющие конечного базиса [87].

В связи с этим актуальным становится анализ фрагментов решетки $\mathcal{L}(P_k)$, в частности, окрестностей достаточно обширных классов. В качестве одного из таких классов привлекает внимание класс $Polyn$ всех функций, реализуемых полиномами по составному модулю k (если число k простое, то $Polyn = P_k$; и вообще свойства этого класса зависят от состава простых множителей числа k). Интерес к нему объясняется следующими обстоятельствами.

Линейные и аффинные преобразования характерны для всех областей математики, являются наиболее простыми и распространенными и достаточно полно исследованы. Их естественные обобщения — полиномиальные и другие близкие к линейным преобразования (билинейные, квазилинейные, мультиаффинные) позволяют использовать при их анализе хорошо развитые методы линейной алгебры и наглядные геометрические интерпретации.

В связи с этим уже получены следующие результаты.

1. Вычислена мощность $|Polyn^{(n)}|$ класса n-местных функций k-значной логики, реализуемых полиномами по модулю k [94, 101, 93, 42, 106, 79].

2. Найдены критерии принадлежности функций классу $Polyn$ [92, 90, 41, 103, 84, 78, 105].

3. Предложены способы аппроксимации k-значных функций полиномами, обеспечивающие заданную точность приближения [76].

4. Построены разнообразные формулы, содержащие полиномиальные операции, для реализации функций в P_k [68, 69, 59, 70, 77, 81, 78].

5. Найдены критерии полноты в P_k системы функций, содержащей все полиномы по модулю $k = p^n$ [67] и $k = p_1 \cdots p_s$ [83] (числа p, $p_1, \ldots, p_s$ простые).

5. Для ряда значений k изучены надклассы класса $Polyn$ и их решетка [83, 84, 73, 54, 55, 57, 58].

6. Изучены и подклассы класса $Polyn$, в частности, в [60] для $k = 4$ (наи-

меньшее составное число) построена решетка всех подклассов в $Polyn$, содержащих класс L линейных (по модулю k) функций. Эта решетка оказалась счетно-бесконечной, на основании чего сделан вывод о сохранении ее бесконечности и при других составных значениях k. При простом k классы, содержащие целиком класс L^1 одноместных линейных функций, описаны в [104], все подклассы класса L^1 — в [88]. Подклассы в L при составных k проанализированы в [89, 107, 108] (см. обзор в гл. 13 книги [95]).

В последние 20 лет получили развитие новые направления исследований.

1. Применение так называемых сильных операторов замыкания, являющихся расширением суперпозиции [61, 62, 63, 64, 65]. Полная классификация в P_k с такими видами замыкания позволяет сократить количество классов до конечного числа. Как указывает С. С. Марченков в [62, 65], к настоящему моменту известно более 10 различных сильных операторов замыкания.

2. Рассмотрение мультифункций и гиперфункций (значением является не один элемент из $\{0, 1, \ldots, k-1\}$, а их множество), мультиопераций над ними и различных вариантов замыкания [96, 97, 72, 71, 98].

3. Изучение замкнутых по суперпозиции классов, содержащих полиномы над другими кольцами и алгебрами, в частности, над $GF(q)$ [82], $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, множеством $\mathbb{N}_0$ неотрицательных целых чисел с операциями сложения и умножения [20, 11, 21, 13, 14, 39, 45, 22, 12, 23, 46, 40, 47, 48, 64, 66].

Начато исследование надклассов класса полиномов в функциональной системе P_k^* частичных функций [27, 28, 29, 30, 43, 91], состоящих из функций, доопределимых до полиномиальных отображений. Их решетка намного сложнее, чем в P_k, в частности, глубина класса L в P_2^* оказалась континуальной [44], в связи с чем интерес к частичным функциям, доопределимых до линейных, не ослабевает [50, 51, 52, 53].

Не все из указанных здесь результатов конструктивны, что ограничивает их возможности. Так, критерии полиномиальности (кроме работ соискателя и С. Н. Селезневой) не указывали способов построить полином, представляющий данную функцию при выполнении всех критериальных условий. Конструктивность важна с практической точки зрения как возможность осуществить синтез управляющих систем. В теории она облегчает дальнейший анализ объектов, представленных в некотором каноническом виде, в частности, нахождение полных систем и базисов в замкнутых классах, проверку свойств функции, ее принадлежности какому-то классу, установление отношений включения между парами классов, определение их точных нижних граней (пересечение замкнутых классов) и точных верхних граней (замыкание объединения классов) в решетке $\mathcal{L}(P_k)$.

Основные понятия и обозначения

$\tilde{x} = \tilde{x}^n = (x_1, \ldots, x_n)$, $\tilde{0} = (0, \ldots, 0)$ — упорядоченные наборы длины n.

Буквами p, q, возможно с индексами, обозначаются простые числа.

k, d — натуральные числа, $k \geq 2$, $E_d = \{0, 1, \ldots, d-1\}$,

$P_k = \{f : E_k^n \to E_k,\ n = 0, 1, 2, \ldots\}$ — класс всех функций k-значной логики,

P_k^* — класс всех, возможно, не всюду определенных функций k-значной логики.

$[A]$ — замыкание относительно суперпозиции (композиции функций, переименования с возможным отождествлением переменных) системы функций $A \subseteq P_k$ (множество всех функций, получаемых из элементов системы A конечным числом применений операций суперпозиции). Если $[A] = A$, то A — *замкнутый класс*. Если $[A] = B$, то A — *полная в классе B система*. *Базис* — полная система, любая собственная подсистема которой не является полной.

Замкнутый класс A называется *предполным в замкнутом классе B*, если $A \subset B$ и для каждого элемента f из $B \setminus A$ система $A \cup \{f\}$ полна в B (максимальный собственный замкнутый подкласс в B).

$Polyn$ — замкнутый класс в P_k, состоящий из всех функций, реализуемых полиномами над кольцом вычетов $\mathbb{Z}_k = (E_k;\ +, \cdot \pmod k)$. Символы $+, -, \cdot, ^{-1}$, если не оговаривается иное, означают операции сложения, вычитания, умножения и обращения по модулю k. Символом L обозначаем класс линейных по модулю k функций, $L \subset Polyn \subseteq P_k$.

Пусть $d|k$. Функция $f(\tilde{x})$ из P_k называется *d-периодической*, если она удовлетворяет условию

$$\tilde{a} \equiv \tilde{b} \pmod d \ \Rightarrow\ f(\tilde{a}) = f(\tilde{b}).$$

$l(\tilde{x})$ — линейная функция, $G_d(\tilde{x})$ — функция, являющаяся d-периодической.

Верхним индексом в скобках у функционального символа обозначаем число переменных функции. Такой индекс у символа класса функций обозначает подмножество функций этого класса, зависящих от указанного числа переменных.

Решетка — частично упорядоченное множество, в котором любые два элемента имеют точные верхнюю и нижнюю грани.

$\mathcal{L}(P_k)$ — решетка всех замкнутых классов P_k относительно включения. Если A, B — замкнутые классы, то $\sup\{A, B\} = [A \cup B]$, $\inf\{A, B\} = A \cap B$.

Если A, B — замкнутые классы в P_k, то *интервал* $I(A; B)$ решетки $\mathcal{L}(P_k)$ — это множество всех замкнутых классов C таких, что $A \subseteq C \subseteq B$.

Подрешетка в $\mathcal{L}(P_k)$, состоящая из классов $Cl(d)$, зависящих от натурального параметра d, *изоморфна решетке делителей*, если $d_1|d_2 \Leftrightarrow Cl(d_1) \subseteq Cl(d_2)$. Она *антиизоморфна решетке делителей*, если $d_1|d_2 \Leftrightarrow Cl(d_1) \supseteq Cl(d_2)$.

Цели и задачи исследования

Они определяются обрисованным положением дел в рассматриваемой области и состоят в следующем.

1. Описать (выяснить состав и характеристические свойства) замкнутые классы, содержащие класс $Polyn$ всех функций, представимых полиномами по модулю k, и класс L всех линейных функций. Выяснить отношения включения между ними и описать интервалы $I(Polyn;\ P_k)$ и $I(L;\ P_k)$ в решетке $\mathcal{L}(P_k)$ (построить подрешетку или указать способ ее построения).

2. Выяснить необходимые и достаточные условия принадлежности функций таким классам, в частности, классу $Polyn$. Найти способы построения полиномов при выполнении достаточных условий полиномиальности и принадлежности другим классам, содержащим L.

3. Для исчерпывающего описания замкнутых классов и их решетки найти канонические формулы для функций рассматриваемых классов и полные системы в каждом классе.

Методы исследования

Теория функциональных систем, дискретный анализ (с применением оригинальных подходов, предложенных соискателем), алгебра, теория чисел, теория сложности алгоритмов.

Стратегия проведения исследования

Цели исследования достигаются следующим способом.

1. Доказывается, что основными условиями, необходимыми, а в ряде случаев и достаточными для представимости функций из P_k полиномами, являются свойства функций сохранять сравнения по модулю d и d-разности определенного порядка для $d|k$ (разности с шагом d).

2. Известно, что классы $C(d)$ сохранения сравнения по модулю d являются предполными в P_k (максимальными собственными замкнутыми подклассами), откуда следует, что все классы из интервала $I(L;\ P_k)$ являются подклассами в $C(d)$. Классы $C(d)$ определяются как классы всех функций канонического вида

$$f(\tilde{x}) = l(\tilde{x}) + G_d(\tilde{x}) + d \cdot F(\tilde{x}), \qquad (*)$$

где
$l(\tilde{x})$ — это линейная функция,
$G_d(\tilde{x})$ — это d-периодическая функция,
$d \cdot F(\tilde{x})$ — это функция, все значения которой кратны d,
причем слагаемые формулы $(*)$ определены однозначно.
Такие формулы названы аддитивными. Они рассмотрены в разделе 1.3.

3. Все остальные классы интервала $I(L;\ P_k)$ также задаются аддитивными формулами, получающимися из (*) ограничениями на вид слагаемых $G_d(\tilde{x})$ и $d \cdot F(\tilde{x})$. Вывод этих ограничений составляет следующую часть исследования.

4. На основе аддитивной формулы, задающей класс из интервала $I(L;\ P_k)$, находятся полные системы и базисы (если последние существуют) в этом классе.

5. На основе аддитивных формул, задающих пару классов, выясняются отношения включения между этими классами и свойства решетки (по отношению включения) классов с аналогичными определяющими их аддитивными формулами.

Такой подход позволяет вывести и дополнить новыми фактами известные ранее результаты А. В. Кузнецова, Н. Н. Айзенберга и И. В. Семёона, А. Н. Черепова, А. Б. Ремизова, Г. П. Гаврилова, А. А. Крохина, К. Л. Сафина и Е. В. Суханова.

Научная новизна результатов исследования

1. Предложен единый подход к описанию замкнутых классов из интервала $I(L;\ P_k)$ как классов всех функций, представимых единственным образом аддитивными формулами (*). Указан метод построения таких формул для фиксированной функции.

2. Найдены полные системы и базисы (в случае их существования) классов из интервала $(L;\ P_k)$. Выявлены отношения включения для пар классов. Описаны и построены решетки семейств классов в $\mathcal{L}(P_k)$.

3. Найдены условия, необходимые и достаточные, критерии полиномиальной реализации функций, имеющие конструктивный характер. Предложен алгоритм построения полиномов, оценена временная сложность такого алгоритма.

4. Предложен способ сведения случая произвольного k к случаю $k = p^m$ с помощью аддитивных формул разложения функций в суммы периодических.

5. Доказана полиномиальная реализуемость и выведены формулы полиномов для p-периодических функций (p — простой делитель k). Предложены p-сеточные аддитивные представления функций как суммы их p-сеточных ограничений (более простых функций), облегчающие распознавание полиномиальности и построение канонических полиномов заданной функции.

6. Построены подрешетки $I(L, P_k)$ для $k = pq$ и $k = p^2$ в $\mathcal{L}(P_k)$, где p и q — различные простые.

7. Найдены аналоги описанных семейств замкнутых классов конечнозначной (k-значной) логики в счетнозначной логике. Предложены алгоритмы распознавания сооответсвующих свойств функций счетнозначной логики, оценена их временная сложность.

Все эти результаты, за исключением оговоренных в тексте диссертации единичных случаев, являются новыми и получены соискателем самостоятельно.

Положения, выносимые на защиту

1. Существуют замкнутые классы следующих семейств:
$C_e(d), \quad e|d, d|k;$
$R(d), S(d), L(d), \quad d|k;$
$R_dC_e, \quad k = de, \text{НОД}(d, e) = 1;$
$K(d, d_1), \quad d|k, d_1|k.$

Каждый из этих классов, как и известные ранее классы сохранения сравнений по одному модулю d или нескольким модулям d ($d|k$), состоит в точности из всех функций, которые можно представить в виде суммы линейной функции, d-периодической функции и функции, все значения которой кратны d, определяемых единственным образом.

2. Состав базисов и полных систем указанных классов.

3. Отношения включения между указанными классами.

4. Условия, необходимые и достаточные для того, чтобы меньший класс включения был предполным в большем.

5. Подрешетки, образованные указанными классами, в решетке $\mathcal{L}(P_k)$ всех замкнутых классов функций k-значной логики.

6. Необходимые и достаточные условия полиномиальной реализуемости функций в P_k. Канонический вид полинома, облегчающий вычисление его значений. Алгоритм для проверки полиномиальности заданной функции и построения реализующего ее полинома при $k = p^m$. Оценка временной сложности такого алгоритма.

7. Состав и вид следующих интервалов решетки $\mathcal{L}(P_k)$:
$I(L;\ Polyn)$ для всех k, не кратных квадрату простого числа;
$I(L;\ P_k)$ для $k = pq$, где p и q — различные простые числа;
$I(L;\ P_k)$ для $k = p^2$.

8. Существуют замкнутые классы семейств $SV(k)$ и $U(a, b)$, $a \in \mathbb{Z}_+$, $b, k \in \mathbb{N}$, в счетнозначной логике. Состав и вид решеток, образованных классами каждого из этих семейств. Условия, необходимые и достаточные для того, чтобы классы из этих семейств являлись предполными в классе $L(\mathbb{Z})$ всех полиномов первой степени с целыми коэффициентами.

9. Критерии полноты в $L(\mathbb{Z})$ систем, содержащих следующие классы линейных функций:
класс K_0 всех нечетных функций,
класс K_E всех функций со свободным коэффициентом, кратным E ($E \geq 2$),
класс K_1 всех одноместных функций,

класс K_M сохранения модуля (абсолютной величины целого числа),
класс K_S всех сюръекций.

Теоретическая и практическая значимость результатов

Исследование носит главным образом теоретический характер. Значимость результатов состоит в том, что получена новая методология (аддитивные формулы) для решения задач классификации, полноты и выразимости в многозначной логике.

Отметим следующие особенности результатов и методов их получения.

1. Введение и применение d-периодических функций ($d|k$) как частных и легче обозримых случаев k-значных. Однозначное выделение линейной и d-периодической частей произвольной функции.

2. Разложения функций в суммы периодических.

3. Полиномиальность периодической функции в P_k, сохраняющей сравнения по всем модулям d, $d|k$, и имеющей периодом простой делитель числа k.

4. Представление функции суммой d-сеточных ограничений, оказывающихся более простыми функциями. Построение полинома не для всей функции сразу, а для каждого p-сеточного ограничения в отдельности. Это упрощает задачу построения полинома, хотя и не оптимизирует его степень и другие характеристики сложности.

5. Построение верхней окрестности фиксированного замкнутого класса не снизу вверх (такой способ представляется более естественным и обосновывается тем, что легче анализировать наиболее близкие этому классу объекты), а сверху, начиная с максимальных классов и добавляя ограничения к найденным свойствам.

6. При анализе объектов некоторого класса (в частности, функций, представимых полиномами) рассматриваются и более общие объекты (функции, не обязательно полиномиальные).

7. Гомоморфное отображение функций и замкнутых классов k-значной логики в d-значные при значениях $d < k$ (в частности $d|k$) с использованием свойства d-периодичности и слагаемых, кратных d.

8. Найденные аналоги конечнозначных функций среди счетнозначных.

Результаты диссертации позволяют сравнить различные функциональные системы с точки зрения разрешимости и сложности задачи выразимости.

Предложенные аддитивные формулы можно применить для дальнейших исследований в следующих направлениях.

1. Выявление и анализ других замкнутых классов в P_k и алгебре частичных функций P_k^*.

2. Построение интервалов $I(Polyn; P_k)$ и $I(L; P_k)$ при значениях k, кратных кубу простого, объяснение эффекта, обнаруженного А. Б. Ремизовым (если $p^3|k$, то существует бесконечная цепь классов, содержащих $Polyn$), определение мощности множества бесконечных цепей и мощности каждой цепи.

3. Анализ мультифункций.

4. Нахождение аналогов рассмотренных замкнутых относительно суперпозиции классов при других операторах замыкания.

Достоверность результатов исследования

Все результаты математически строго доказаны.

Апробация результатов

Результаты диссертации докладывались на следующих мероприятиях.

XVII, XVIII, XIX Международные конференции "Проблемы теоретической кибернетики" (Казань, 2014 г.; Пенза, 2017 г.; Казань, 2020, 2021 гг.).

XI, XII, XIII Международные семинары "Дискретная математика и ее приложения" (Москва, МГУ, 2012, 2016, 2019 гг.).

II, III, IV, VI, VII, VIII, X Международные конференции "Дискретные модели в теории управляющих систем" (1997, 1998, 2004, 2006, 2009, 2015, 2018 гг.).

4-я российская и 6-я Международная школы-семинары "Синтаксис и семантика логических систем" (Улан-Удэ, 2012 г.; Монголия, Ханх, 2019 г.).

Научные семинары:

"Математические вопросы кибернетики" мех-мат. факультета МГУ имени М. В. Ломоносова и "Дискретная математика и математическая кибернетика", "Многозначные функциональные системы" кафедры математической кибернетики факультета ВМиК МГУ имени М. В. Ломоносова;

семинар регионального научно-образовательного математического центра «Математика технологий будущего» под руководством профессора, д. ф.-м. н. Д. В. Баландина (Национальный исследовательский Нижегородский государственный университет имени Н. И. Лобачевского, 2022 г.);

объединенный межкафедральный семинар "Математические вопросы кибернетики" МГУ имени М. В. Ломоносова (2022 г.);

научно-исследовательский семинар "Дискретные математические модели" кафедры математического моделирования НИУ "МЭИ".

Публикации

Результаты автора опубликованы в работах [1–40], работы [1–14] — из списка ВАК РФ.

Структура и объем работы

Диссертация состоит из введения, 6 глав, разбитых на 48 разделов, заключения и списка литературы, содержащего 108 наименования. Раздел 1.8 главы 1 разбит на 3 параграфа, раздел 5 главы 5 — на 6 параграфов. Общий объем работы составляет 138 страниц.

Благодарности

Автор выражает глубокую благодарность Вадиму Васильевичу Кочергину, Андрею Анатольевичу Вороненко, Дмитрию Сергеевичу Романову за организационную и моральную поддержку и практические советы, Андрею Игоревичу Мамонтову за искренний интерес к работе, товарищеские чувства и плодотворное сотрудничество, Александру Алексеевичу Зотову за помощь в компьютерной верстке материалов.

Глава 1

Классы сохранения сравнений

В этой главе вводятся наиболее общие аддитивные формулы и описываются наиболее обширные из рассматриваемых замкнутых классов — классы сохранения сравнений по модулям, являющимся делителями числа k (классы сохранения особых разбиений множества E_k).

В разделах 1.1 и 1.2 предложены вспомогательные аддитивные формулы для произвольной функции с однозначно выделяемыми слагаемыми в виде линейных и d-периодических функций. Они широко используются в дальнейших построениях.

В разделе 1.3 предлагается аддитивная формула для классов $C(d)$ сохранения сравнения по модулю d, произвольному делителю числа k. При $d \neq 1, d \neq k$ классы $C(d)$ являются предполными (максимальными) в P_k (образуют верхний ярус решетки $\mathcal{L}(P_k)$, ее коатомы). Такие классы давно известны, однако важность предлагаемых здесь формул и базисов в $C(d)$ определяется их применением и дальнейшим уточнением для всех остальных рассматриваемых в работе классов.

В разделе 1.4 вводятся формулы для функций классов $C(d_1, \ldots, d_l)$ сохранения сравнений по нескольким модулям, связанным между собой отношением делимости. Они являются пересечениями классов $C(d_i)$ сохранения сравнения по одному модулю и также давно известны. Их решетка для любого k полностью описана А. Н. Череповым [84], однако это описание ввиду своей общности довольно сложно. В связи с этим доказана теорема 1.1, уточняющая общую конструкцию Черепова в одном частном случае, имеющим место в дальнейших рассмотрениях работы.

В разделе 1.5 вводятся и анализируются классы $C_e(d)$, где $e|d$. Они определяются особыми формулами составляющих их функций, эти же формулы позволяют найти базисы в таких классах и выяснить отношения включения между ними.

В разделе 1.6 находятся условия, при которых класс $C_e(d)$ является предполным в классах $C(e, d)$ $C(e, d)$. Эти результаты (теорема 1.2 и вспомогательные

конструкции) применяются в дальнейших главах.

В разделе 1.7 рассмотрены классы $C(d)$ и $C(d,e)$ при $k = de$, где d и e — взаимно простые собственные делители числа k. Находится еще один базис в $C(d)$, (утверждение 1.17), выводится лемма 1.12, помогающая найти условия, необходимые и достаточные, чтобы класс $C(d,e)$ был при указанных ограничениях предполным в $C(d)$ (утверждение 1.18) и такие же отношения имели бы место и для других пар классов (далее в главе 5).

Наконец, в разделе 1.8 три семейства классов сохранения сравнений по нескольким модулям описываются с помощью свойства перестановочности функций.

1.1 Линейная часть функции

Линейной (по модулю k) называется функция вида

$$l(\tilde{x}) = a_0 + a_1x_1 + \cdots + a_nx_n, \qquad a_0, a_1, \ldots, a_n \in E_k.$$

При любых $k \geq 2$ и $n \in \mathbb{N}$ выделим в E_k^n наборы

$$\tilde{\varepsilon}_i = (\underbrace{0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0), \quad i = 1, \ldots, n.$$

Тогда *произвольную n-местную функцию* $f(\tilde{x})$ *из* P_k *можно однозначно представить в виде*

$$f(\tilde{x}) = l(\tilde{x}) + F(\tilde{x}) \tag{1.1}$$

$$l(\tilde{x}) = a_0 + \sum_{i=1}^{n} a_ix_i, \quad a_0 = f(\tilde{0}), \quad a_i = f(\tilde{\varepsilon}_i) - f(\tilde{0}),$$

$$F(\tilde{x}) = f(\tilde{x}) - l(\tilde{x}), \qquad F(\tilde{0}) = F(\tilde{\varepsilon}_i) = 0, \ i = 1, \ldots, n.$$

Функция $l(\tilde{x})$ называется *линейной частью функции* $f(\tilde{x})$.

1.2 Периодические функции

Пусть $d|k$. Функция, удовлетворяющая условию

$$\tilde{x} \equiv \tilde{y} \pmod{d} \ \Rightarrow \ f(\tilde{x}) = f(\tilde{y}),$$

называется *d-периодической*. При этом 1-периодическая функция есть константа, k-периодической является любая функция из P_k.

Если $d|k$, то *произвольную n-местную функцию* $f(\tilde{x})$ *из* P_k *можно однозначно представить в виде*

$$f(\tilde{x}) = G_d(\tilde{x}) + F(\tilde{x}),$$

$$G_d(\tilde{x}) = f(\tilde{b}), \quad \text{если} \quad \tilde{b} \in E_d^n, \quad \tilde{x} \equiv \tilde{b} \pmod{d},$$

$$F(\tilde{x}) = f(\tilde{x}) - G_d(\tilde{x}). \quad \text{Если} \quad \tilde{x} \in E_d^n, \text{ то } F(\tilde{x}) = 0.$$

Функция $G_d(\tilde{x})$ называется *d-периодической частью функции* $f(\tilde{x})$.

Введем функции

$$j(\tilde{x}) = \begin{cases} 1, & \tilde{x} = \tilde{0}, \\ 0, & \tilde{x} \neq \tilde{0}, \end{cases} \qquad g_d(\tilde{x}) = \begin{cases} 1, & \tilde{x} \equiv \tilde{0} \pmod{d}, \\ 0, & \tilde{x} \not\equiv \tilde{0} \pmod{d}. \end{cases}$$

В частности, $g_1(\tilde{x}) = 1$, $g_k(\tilde{x}) = j(\tilde{x})$.

Утверждение 1.1. *Линейная функция* (1.1) *является d-периодической тогда и только тогда, когда для всех* $i = 1, \ldots, n$ *коэффициенты* a_i *кратны* k/d.

Действительно, $d\tilde{\varepsilon}_i \equiv \tilde{0} \pmod{d}$. Поэтому $a_0 = l(\tilde{0}) = l(d\tilde{\varepsilon}_i) = a_0 + a_i d$ в точности при условии $a_i d$ кратно k.

Замечание 1.1. Периодические функции k-значной логики довольно часто встречаются в различных областях дискретной математики и теории чисел. В частности, периодическими являются так называемые координатные функции, примененные в [41, 54, 55, 57, 67, 73]. Функция $g_d(x)$ оказалась подходящим дискретным аналогом дельта-функции Дирака при построении обратного преобразования Фурье над конечным полем [102].

1.3 Классы $C(d)$

Пусть $d|k$, $f(\tilde{x}) \in P_k$. Рассмотрим класс $C(d)$ функций, *сохраняющих сравнение по модулю d*, т. е. удовлетворяющих условию

$$\tilde{x} \equiv \tilde{y} \pmod{d} \;\Rightarrow\; f(\tilde{x}) \equiv f(\tilde{y}) \pmod{d}.$$

Класс $C(d)$ *замкнут. При этом* $C(1) = C(k) = P_k$, *а если* $d \neq 1, d \neq k$, *то класс* $C(d)$ *является предполным в* P_k [86, §16].

Любая *d-периодическая функция принадлежит классу* $C(d)$. *Если* $f(\tilde{x}) \in C(d)$ *и* $G_d(\tilde{x})$ *есть d-периодическая часть функции* $f(\tilde{x})$, *то все значения функции* $f(\tilde{x}) - G_d(\tilde{x})$ *кратны d.*

Утверждение 1.2. *Класс $C(d)$ состоит в точности из всех функций вида*

$$f(\tilde{x}) = l(\tilde{x}) + G_d(\tilde{x}) + d \cdot F(\tilde{x}). \tag{1.2}$$

Здесь $F(\tilde{x})$ — произвольная функция из P_k, а $l(\tilde{x})$ и $G_d(\tilde{x})$ — произвольные линейная и d-периодическая функции.

Если $l(\tilde{x})$ — линейная часть функции $f(\tilde{x})$, а $G_d(\tilde{x})$ есть d-периодическая часть функции $f(\tilde{x}) - l(\tilde{x})$, то $d \cdot F(\tilde{x}) = 0$ при $\tilde{x} \in E_d^n$. Эти слагаемые формулы (1.2) определены однозначно, а сама формула (1.2) называется *каноническим представлением функции класса $C(d)$*.

Доказательство. Легко видеть, что функция вида (1.2) сохраняет сравнение по модулю d.

Обратно: пусть $f(\tilde{x}) \in C(d)$. Вычтем из f ее линейную часть. Затем из результата такого вычитания вычтем его d-периодическую часть, получим функцию, равную 0 всюду на множестве E_d^n. В силу сохранения сравнения по модулю d последняя функция кратна d, и вся функция представляется в виде (1.2). □

Лемма 1.1. *Справедливы следующие соотношения.*

$$g_d^{(1)}(x) = g_d^{(2)}(x,x), \quad dj^{(1)}(x) = dj^{(2)}(x,x),$$

$$g_d(\tilde{x}^n) = g_d^{(1)}(x_1) \cdots g_d^{(1)}(x_n).$$

Если $n \geq 2$, то

$$g_d^{(n+1)}(\tilde{x},\ y) = g_d^{(2)}(1 - g_d^{(n)}(\tilde{x}),\ y), \quad dj^{(n+1)}(\tilde{x},\ y) = dj^{(2)}(d - dj^{(n)}(\tilde{x}),\ y).$$

Если $d \neq 2$, то

$$g_d^{(2)}(x,y) = g_d^{(1)}(2 - g_d(x) - g_d(y)).$$

Если $k \neq 2d$, то

$$dj^{(2)}(x,y) = dj^{(1)}(2d - dj(x) - dj(y)).$$

Если $k = 2d$ и d нечетно, то

$$dj^{(2)}(x,y) = dj^{(1)}(x) \cdot dj^{(1)}(y).$$

Они проверяются непосредственно.

Следствие 1.1. *При всех $n \geq 1$ справедливы включения*

$$g_d^{(n)}(\tilde{x}) \in [1,\ x+y,\ xy,\ g_d^{(1)}(x)],$$

$$g_d^{(n)}(\tilde{x}) \in [x+y,\ g_d^{(2)}(x,y)], \quad dj^{(n)}(\tilde{x}) \in [1,\ x+y,\ dj^{(2)}(x,y)].$$

Если $d \neq 2$, то $g_d^{(n)}(\tilde{x}) \in [x+y,\ g_d^{(1)}(x)]$.
Если $k \neq 2d$, то $dj^{(n)}(\tilde{x}) \in [x+y,\ dj^{(1)}(x)]$.
Если $k = 2d$ и d нечетно, то $dj^{(n)}(\tilde{x}) \in [1,\ x+y,\ xy,\ dj^{(1)}(x)]$.

Утверждение 1.3. *Базисы в классе $C(d)$ при $d \neq 1,\ d \neq k$ образуют системы*

$$B_d = \{x + y,\ d \cdot j(x, y),\ g_d(x, y)\},$$

а также $\{x + y,\ d \cdot j(x),\ g_d(x)\}$ *при* $d \neq 2,\ k \neq 2d,$

$$\{x + y,\ d \cdot j(x, y),\ g_d(x)\} \text{ при } d \neq 2, \quad \{x + y,\ d \cdot j(x),\ g_d(x, y)\} \text{ при } k \neq 2d.$$

Доказательство. Покажем, что система B_d полна в классе $C(d)$. Представим функцию $f(\tilde{x})$ класса $C(d)$ в виде (1.2). Ясно, что $l(\tilde{x}) \in [1,\ x + y]$. Далее, d-периодическую функцию $G_d(\tilde{x})$ можно представить линейной комбинацией функций $g_d(\tilde{x} - \tilde{a})$, $\tilde{a} \in E_d^n$, а функцию $d \cdot F(\tilde{x})$ — линейной комбинацией функций $dj(\tilde{x} - \tilde{b})$, $\tilde{b} \in E_k^n$. В силу леммы 1.1 и следствия 1.1 получаем:

$$G_d(\tilde{x}) \in [1,\ x + y,\ g_d(x, y)], \quad d \cdot F(\tilde{x}) \in [1,\ x + y,\ dj(x, y)].$$

Остается представить константы суперпозициями элементов системы B_d. Выражаем сначала $0 = x + \cdots + x$ (сумма k одинаковых слагаемых), затем $1 = g_d(0, 0)$ и все остальные константы как суммы единиц. Итак, система B_d полна в $C(d)$. Покажем, что она является базисом.

Подсистема $\{g_d(x, y),\ dj(x, y)\}$ не полна, она сохраняет множество $\{0, 1, d\}$. Подсистема $\{x + y, dj(x, y)\}$ сохраняет множество чисел, кратных d. А для подсистемы $\{x + y, g_d(x, y)\}$ все порождаемые ею функции $h(\tilde{x})$ абсолютно сохраняют d-разности, т. е. для любого фиксированного $i \in \{1, \ldots, n\}$ и всех $\tilde{x} \in E_k^n$ разности

$$h(x_1, \ldots, x_{i-1}, x_i + d, x_{i+1}, \ldots, x_n) - h(\tilde{x})$$

не зависят от $\tilde{x}$, а зависят только от i. Функция $dj(x, y)$ таким свойством не обладает. (Подробнее d-разности будут рассмотрены позже.) □

Замечание 1.2. Дадим несколько пояснений.

1. Этот результат опубликован в [6,7].

2. Существуют и иные базисы.

3. В условиях утверждения $d \neq 1$, $d \neq k$. Как отмечалось, $C(1) = C(k) = P_k$. Базисом в P_k является при $k \geq 3$ система $\{x+y,\ j(x)\}$ [56], а при $k = 2$ — система $\{j(x, y)\}$.

1.4 Классы $C(d_1, \ldots, d_l)$

Пусть $d_1, \ldots, d_l$ — различные делители числа k. Введем замкнутые классы

$$C(d_1, \ldots, d_l) = C(d_1) \cap \cdots \cap C(d_l), \quad M(d_1) = \bigcap_{d | d_1} C(d_1).$$

При этом

$$C(d,d) = C(1,d) = C(d,k) = C(d).$$

Классы $C(d_1,\dots,d_l)$ образуют интервал $(M(k);P_k)$ решетки $\mathcal{L}(P_k)$. Для всех k этот интервал полностью описан А. Н. Череповым [84].

Непосредственно из свойств сравнений вытекает следующий факт.

$$\textit{Если}\ \ d_1|k, d_2|k,\ d_0 = \text{НОД}(d_1,d_2),\ d_3 = \text{НОК}(d_1,d_2),\quad \textit{то}$$

$$C(d_1,d_2) = C(d_0,d_1,d_2,d_3).$$

Утверждение 1.4. *Если $d_1|d_2, d_2|d_3,\dots,d_{l-1}|d_l, d_l|k$, то любую функцию f из $C(d_1,\dots,d_l)$ можно представить в каноническом виде*

$$f(\tilde{x}) = f(\tilde{0}) + G_{d_1}(\tilde{x}) + d_1G_{d_2}(\tilde{x}) + \dots + d_{l-1}G_{d_l}(\tilde{x}) + d_lF(\tilde{x}). \tag{1.3}$$

Здесь слагаемые определены однозначно.

Если $d_1 \neq 1, d_1 \neq d_2, d_2 \neq d_3,\dots,d_{l-1} \neq d_l, d_l \neq k$, то система функций

$$\{x+y,\ g_{d_1}(x,y),\ d_1g_{d_2}(x,y),\ \dots,d_{l-1}g_{d_l}(x,y),\ d_lj(x,y)\}$$

является базисом класса $C(d_1,\dots,d_l)$.

Если положить $d_0 = 1,\ d_{l+1} = k$, то при условии $2d_j \neq d_{j+1}$ двухместную функцию $d_jg_{d_{j+1}}(x,y)$ в этой системе можно заменить на одноместную $d_jg_{d_{j+1}}(x)$, $0 \le j \le l$.

Доказательство аналогично выводу утверждений 1.2 и 1.3.

Это также следует из результатов А. Н. Черепова для произвольных k и его делителей [84]. В частных случаях эти факты выводились другими способами несколькими авторами [5, 54, 73].

Аддитивную формулу (1.3) можно обобщить:

$$f(\tilde{x}) = l(\tilde{x}) + h_1(\tilde{x}) + d_1h_2(\tilde{x}) + \dots + d_{l-1}h_l(\tilde{x}) + d_lH(\tilde{x}). \tag{1.4}$$

Здесь $H(\tilde{x})$ — функция из P_k, а $l(\tilde{x})$, $h_i(\tilde{x})$ — линейная и d_i-периодические функции, $i = 1,\dots,l$, других ограничений на слагаемые нет.

Эквивалентность формул (1.4) и (1.3) проверяется выделением в слагаемых правой части (1.4) однозначно определенных линейной и периодических частей.

Лемма 1.2. *Пусть $e|d, e \neq d,\ d|k,\ \varphi_n(x_1,\dots,x_n) = eg_d(x_1,\dots,x_n)$. Тогда*

$$\varphi_1(x) = \varphi_2(x,x),\ \varphi_{n+1}(\tilde{x},y) = \varphi_2(e - \varphi_n(\tilde{x}),y).$$

Если $d \neq 2e$, то $\varphi_2(x,y) = \varphi_1(2e - \varphi_1(x) - \varphi_1(y))$.

Эти соотношения доказываются непосредственной проверкой.

Замечание 1.3. Если $k = 2e$, где e нечетно, то $eg_2(x) = 2(1 + x) \in L$.

Следствие 1.2. *При $e|d, d|k$ для функций класса $C(e, d)$ справедлива аддитивная формула*

$$f(\tilde{x}) = l(\tilde{x}) + G_e(\tilde{x}) + eG_d(\tilde{x}) + d \cdot F(\tilde{x}). \tag{1.5}$$

Если $e \neq 1, e \neq d, d \neq k$, то базисом в классе $C(e, d)$ является система функций

$$\{x + y,\ g_e(x, y),\ eg_d(x, y),\ dj(x, y)\}.$$

Если также $e \neq 2$, то функцию $g_e(x, y)$ в этой системе можно заменить на $g_e(x)$.

Если $d \neq 2e$, то $eg_d(x, y)$ можно заменить на $eg_d(x)$.

Если $k \neq 2d$, то $dj(x, y)$ можно заменить на $dj(x)$.

Теорема 1.1. *Если $e|d$ и d есть собственный делитель числа k, то класс $C(e, d)$ является предполным в $C(d)$ в точности при $e = p$.*

Доказательство. При $e = p$ имеем

$$C(d) = [1,\ x+y,\ g_d(x, y),\ dj(x, y)],\quad C(p, d) = [1,\ x+y,\ g_p(x, y),\ pg_d(x, y), dj(x, y)].$$

Пусть $f(\tilde{x}) \in C(d) \setminus C(p)$. Покажем, что замыкание $[C(p, d) \cup \{f\}]$ содержит функцию $g_d(x, y)$ и, следовательно, весь класс $C(d)$. Представим f как элемент класса $C(d)$ в виде (1.2). Вычтем функции $l(\tilde{x})$ и $d \cdot F(\tilde{x})$, они принадлежат $C(p)$. Получим функцию, обладающую следующими свойствами:
1) она d-периодическая,
2) она кратна e,
3) на наборе $\tilde{0}$ она принимает значение 0,
4) она не принадлежит классу $C(p)$.
Подстановкой констант (согласно лемме в [86, §16], можно и другим путем: с помощью леммы 1.10 в разделе 1.6) из нее получим одноместную функцию $H(x)$ с теми же свойствами. В силу свойства 4) для некоторых $a, b \in E_d$ имеем:

$$a \equiv b, \qquad H(a) \not\equiv H(b) \pmod{p}.$$

Не ограничивая общности, полагаем $a = 0$, $H(b) = \gamma$, НОД$(\gamma, p) = 1$. Тогда $b = Np$, $1 \leq N \leq d/p$, НОД$(N, p) = 1$. Построим функцию $h(x)$ такую, что $h(0) = 0$, $h(p) = 1$. Возможны два случая.

1. $k = p^m$. Тогда $h(x) = cH(x)$, где $c = \gamma^{-1} \pmod{k}$.

2. НОД$(\gamma, k) > 1$. Тогда $k = p^m Q$, $Q > 1$, НОД$(Q, p) = 1$. Рассматривая вместо $H(x)$ функцию $H(x) + pg_d(Np - x)$, сводим случай к предыдущему.

Имея такую функцию $h(x)$, получаем $g_d(x, y) = h(Npg_d(x, y))$.

Покажем необходимость условия $e = p$.

Если $e = 1$, то $C(e, d) = C(1, d) = C(d)$.

Если же $e = ab$, $a > 1, b > 1$. то $C(e, d) \subset K \subset C(d)$, где K — замкнутый класс всех функций вида

$$l(\tilde{x}) + aG_d(\tilde{x}) + d \cdot F(\tilde{x}).$$

Включения строгие, так как, например, $G_d(x, y) \notin K$ (у функций класса K нелинейная часть кратна a) и $ag_d(x) \in K \setminus C(e)$. □

Лемма 1.3. *Если $d_1|k, d_2|k, d_0 = НОД(d_1, d_2)$, то d_1-периодическая функция $f(\tilde{x})$ принадлежит классу $C(d_2)$ в точности при выполнении условия*

$$\tilde{a} \equiv \tilde{b} \pmod{d_0} \;\Rightarrow\; f(\tilde{a}) \equiv f(\tilde{b}) \pmod{d_2}. \tag{1.6}$$

Доказательство. Достаточность условия (1.6) для сохранения функцией сравнения по модулю d_2 очевидна. Докажем необходимость.

Пусть $\tilde{a} \equiv \tilde{b} \pmod{d_0}$, тогда $\tilde{b} - \tilde{a} = \tilde{c}d_0$. Числа d_1, d_2, k представим в виде $d_1 = Ad_0$, $d_2 = Bd_0$, $k = ABNd_0$, где НОД$(A, B) = 1$. Тогда найдутся целочисленные наборы $\tilde{U}, \tilde{V}$ такие, что $\tilde{c} = \tilde{U}A + \tilde{V}B$. Умножив это равенство на d_0, получим $\tilde{b} - \tilde{a} = \tilde{U}d_1 + \tilde{V}d_2$. В силу d_1-периодичности функции имеем $f(\tilde{b}) = f(\tilde{a} + \tilde{U}d_1 + \tilde{V}d_2) = f(\tilde{a} + \tilde{V}d_2)$. Далее, из условия $f \in C(d_2)$ следует, что $f(\tilde{a} + \tilde{V}d_2) \equiv f(\tilde{a}) \pmod{d_2}$. □

Следствие 1.3. *Если d_1 и d_2 — взаимно простые делители числа k, то d_1-периодическая функция принадлежит классу $C(d_2)$ в том и только том случае, когда все ее значения сравнимы между собой по модулю d_2.*

Лемма 1.4. *Пусть выполнены условия*:

1) *число d имеет вид $d = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, $s \geq 2$;*

2) *числа d и e взаимно простые;*

3) *число k имеет вид $k = p_1^{\beta_1} \cdots p_s^{\beta_s} e$, $\beta_j \geq \alpha_j$, $j = 1, \ldots, s$;*

4) *число d представляется как $d = d_1 \cdots d_r$, где числа $d_1, \ldots, d_r$ попарно взаимно простые, $2 \leq r \leq s$;*

5) *функция $f(\tilde{x})$ является d-периодической и принадлежит классу $K = C(p_1^{\beta_1} \cdots p_s^{\beta_s}, e)$.*

Тогда функцию f можно представить в виде

$$f(\tilde{x}) = f(\tilde{0}) + \sum_{j=1}^{r} f_j(\tilde{x}), \tag{1.7}$$

где $f_j(\tilde{x})$ — это d_j-периодические функции класса K, кратные k/d_j и определяемые однозначно.

Доказательство. Положим $d'_j = p_j^{\alpha_j}$, $j = 1, \ldots, s$. Покажем, что функцию f можно представить в виде

$$f(\tilde{x}) = f(\tilde{0}) + \sum_{j=1}^{s} f'_j(\tilde{x}), \tag{1.8}$$

где $f'_j(\tilde{x})$ — это d'_j-периодические функции класса K, определяемые однозначно.

Положим $F(\tilde{x}) = f(\tilde{x}) - f(\tilde{0})$, тогда $F(\tilde{0}) = 0$. Определим для $j = 1, \ldots, s$ значения функций f'_j так: $f'_j(\tilde{x}) = F(\tilde{y}^{(j)})$, где

$$\tilde{y}^{(j)} \equiv \tilde{x} \pmod{d'_j}, \tag{1.9}$$

$$\tilde{y}^{(j)} \equiv \tilde{0} \pmod{k/d'_j}. \tag{1.10}$$

Если значения j и $\tilde{x}$ фиксированы, то в E_k^n имеется ровно один набор $\tilde{y}^{(j)}$, удовлетворяющий условиям (1.9) и (1.10), что доказывает d'_j-периодичность функции f'_j. Покажем выполнимость равенства (1.8), оно эквивалентно сравнениям

$$F(\tilde{x}) \equiv F(\tilde{y}^{(1)}) + \cdots + F(\tilde{y}^{(s)}) \tag{1.11}$$

по модулям $e, p_1^{\beta_1}, \ldots p_s^{\beta_s}$.

Во-первых, F — это d-периодическая функция класса K, поэтому, согласно следствию 1.3, все ее значения сравнимы между собой по модулю e, сравнение (1.11) по модулю e выполняется.

Далее, фиксируем j, $1 \le j \le s$. Из (1.4), согласно лемме 1.3, следует, что $F(\tilde{y}^{(j)}) \equiv F(\tilde{x}) \pmod{p_j^{\beta_j}}$. Если же $1 \le l \le s$ и $l \ne j$, то $d'_l | (k/d'_j)$ и $d_l = \text{НОД}(p_l^{\beta_l}, d)$. Поэтому из (1.5) получаем соотношения

$$F(\tilde{y}^{(j)}) \equiv F(\tilde{0}) \equiv 0 \pmod{p_l^{\beta_l}}. \tag{1.12}$$

Доказано, что сравнение (1.11) выполнено и по модулю $p_l^{\beta_l}$, следовательно, (1.8) имеет место.

Покажем, что $f'_j \in K$ при $j = 1, \ldots, s$. Во-первых, $f'_j \equiv 0 \pmod{e}$ (так как функция F кратна e), следовательно, $f'_j \in C(e)$. Во вторых, функция f'_j является d'_j-периодической, а значит и $p_j^{\beta_j}$-периодической (так как $d'_j | p_j^{\beta_j}$, поэтому $f'_j \in C(p_j^{\beta_j})$. Наконец, пусть $1 \le l \le s$, $l \ne j$. Из (1.10) и (1.12) следует сравнение $f'_j \equiv 0 \pmod{p_l^{\beta_l}}$, поэтому $f'_j \in C(p_l^{\beta_l})$.

Остается получить представление (1.7) из построенных функций f'_j. Если $d_j = d'_{j_1} \cdots d'_{j_t}$, то $f_j(\tilde{x}) = f'_{j_1}(\tilde{x}) + \cdots + f'_{j_t}(\tilde{x})$. □

Лемма 1.5. *Пусть выполнены условия леммы* 1.4 *и, кроме того,* $f(\tilde{x}) \in C(d_0)$, *где* $d_0 | k$ *и* $d_0 \notin \{p_1^{\beta_1}, \ldots, p_s^{\beta_s}, e\}$. *Тогда* $f_j(\tilde{x}) \in C(d_0)$, $j = 1, \ldots, s$.

Доказательство. Пусть $e = p_{s+1}^{\beta_{s+1}} \cdots p_t^{\beta_t}$. Достаточно показать, что каждая из функций f'_j, определенных при доказательстве леммы 1.4, принадлежит классу $C(d_0)$ для делителей d_0 числа k, имеющих вид $d_0 = p_l^m$, где $l = 1, \ldots, t$ и $m = 1, \ldots, \beta_l$.

Если $l > s$, то функция f'_j кратна $p_l^{\beta_l}$, следовательно, $f'_j \in C(p_l^m)$.

Если $l = j$, $m \geq \alpha_j$, то функция f'_j принадлежит $C(p_l^m)$ в силу своей $p_j^{\alpha_j}$-периодичности.

Пусть $l = j$, $m < \alpha_j$, $\tilde{x} \equiv \tilde{x}' \pmod{p_j^m}$. Тогда $f'_j(\tilde{x}) = F(\tilde{y})$, $f'_j(\tilde{x}') = F(\tilde{y}')$, где $\tilde{y} \equiv \tilde{x}$, $\tilde{y}' \equiv \tilde{x}' \pmod{p_j^{\alpha_j}}$. При этом $\tilde{y} \equiv \tilde{y}' \pmod{p_j^m}$. Функция F, так же, как и f, сохраняет сравнение по модулю p_j^m, поэтому и $f'_j \in C(p_j^m)$.

Наконец, если $1 \leq l \leq s$, $l \neq j$, то функция f' кратна $p_l^{\beta_l}$, поэтому $f'_j \in C(p_l^m)$ при $m = 1, \ldots, \beta_l$. □

Следствие 1.4. *Пусть $k = k_1 \ldots k_s$, где $s \geq 2$, а числа $k_1, \ldots, k_s$ попарно взаимно простые, и пусть $f(\tilde{x}) \in C(k_1, \ldots, k_s)$. Тогда функцию f можно представить в виде*

$$f(\tilde{x}) = f(\tilde{0}) + \sum_{j=1}^{s} f_j(\tilde{x}), \tag{1.13}$$

где $f_j(\tilde{x})$ — это k_j-периодические функции класса $C(k_1, \ldots k_s)$, кратные k/k_j и определяемые однозначно. Если при этом $f(\tilde{x}) \in M(k)$, то и $f_j(\tilde{x}) \in M(k)$, $j = 1, \ldots, s$.

Лемма 1.6. *Пусть d и e — взаимно простые делители числа k, и пусть $h_n(x_1, \ldots, x_n) = eg_d(x_1, \ldots, x_n)$. Тогда*

$$h_n(\tilde{x}) \in [1,\ x + y,\ h_2(x, y)],\ n = 1, 2, \ldots.$$

Если при этом d нечетно, то $h_n(\tilde{x}) \in [1,\ x + y,\ h_1(x)]$, $n = 1, 2, \ldots$.

Доказательство. Легко проверить, что $h_{n+1}(\tilde{x},\ y) = h_2(e - h_n(\tilde{x}), y)$, а если d нечетно, то $h_2(x, y) = h_1(2e - h_1(x) - h_1(y))$. □

Замечание 1.4. Если $k = 2e$ и e нечетно, то $eg_2(x) = e(1 + x) \in L$. Если же $n \geq 2$, то $eg_2(\tilde{x}) \notin L$.

Утверждение 1.5. *Пусть $s \geq 2$, числа $k_1, \ldots, k_s$ попарно взаимно простые, и пусть $k = k_1 \cdots k_s$ и $d_j = k/k_j$ при $j = 1, \ldots, s$. Тогда система функций*

$$A = \left(\bigcup_{j=1}^{s} \{d_j g_{k_j}(x, y)\} \right) \cup \{1,\ x + y\}$$

является полной в классе $C(k_1, \ldots, k_s)$, и для всех $k_j \neq 2$ функции $d_j g_{k_j}(x, y)$ в системе A можно заменить на $d_j g_{k_j}(x)$.

Включение $[A] \subseteq C(k_1, \ldots, k_s)$ доказывается индукцией по сложности формулы над A, задающей функцию из $[A]$. Обратное включение вытекает из следствия 1.4 и леммы 1.6.

1.5 Классы $C_e(d)$

Пусть $d|k$, $e|d$. Рассмотрим класс $C_e(d)$ всех функций вида

$$f(\tilde{x}) = l(\tilde{x}) + eG_d(\tilde{x}) + d \cdot F(\tilde{x}), \tag{1.14}$$

где слагаемые
$l(x)$ — это линейная часть функции $f(\tilde{x})$,
$eG_d(\tilde{x})$ — это d-периодическая часть функции $f(\tilde{x}) - l(\tilde{x})$, все значения которой кратны e,
$d \cdot F(\tilde{x}) = f(\tilde{x}) - l(\tilde{x}) - eG_d(\tilde{x})$ — это функция со значениями, кратными d.
Они определены однозначно.

Легко проверить

Утверждение 1.6. *Класс $C_e(d)$ замкнут относительно введения и удаления фиктивных переменных функций. Он также замкнут относительно линейных операций над функциями.*

Утверждение 1.7. *Справедливо следующее.*

1. *Любую линейную функцию, любую d-периодическую функцию со значениями, кратными e, а также любую функцию, все значения которой кратны d, можно представить в виде* (1.14)*, поэтому такие функции принадлежат классу $C_e(d)$.*

2. *Класс $C_e(d)$ состоит в точности из всех линейных комбинаций, образованных линейными функциями, d-периодическими функциями, кратными e, и функциями, кратными d.*

3. *Имеют место включения $L \subseteq C_e(d) \subseteq C(e, d)$.*

Первые два факта и включение $L \subseteq C_e(d)$ доказываются выделением линейной и d-периодической частей и применением утверждения 1.6. Включение $C_e(d) \subseteq C(e, d)$ следует из того, что $l(\tilde{x}), eG_d(\tilde{x}), d \cdot F(\tilde{x}) \in C(e, d)$, и утверждения 1.6.

Утверждение 1.8. *Равенство $L = C_e(d)$ верно только при $e = d = k$.*

Доказательство. Равенство $C_k(k) = L$ следует из определения класса $C_e(d)$.

Если $d \neq k$, то $d \cdot j(x, y) \in C_e(d) \setminus L$.

Если же $e \neq d$, то $eg_d(x - 1, y - 1) \in C_e(d) \setminus L$. □

Лемма 1.7. *Пусть* $f(\tilde{x}), f'(\tilde{x})$ *— функции из* $C_e(d)$, *функция* $g(x,y)$ *является* d*-периодической,* $H(\tilde{x}) = e \cdot g(f(\tilde{x}), f'(\tilde{x}))$. *Тогда* $H(\tilde{x}) \in C_e(d)$.

Доказательство. Покажем, что функция $H(\tilde{x})$ является d-периодической. Представим функции f, f' в виде (1.14):

$$f(\tilde{x}) = l(\tilde{x}) + eG_d(\tilde{x}) + d \cdot F(\tilde{x}), \quad f'(\tilde{x}) = l'(\tilde{x}) + eG'_d(\tilde{x}) + d \cdot F'(\tilde{x}),$$

$$l(\tilde{x}) = a_0 + a_1x_1 + ... + a_nx_n, \quad l'(\tilde{x}) = a'_0 + a'_1x_1 + ... + a'_nx_n.$$

Тогда $H(\tilde{x}) = e \cdot g(l(\tilde{x}) + eG_d(\tilde{x}),\ l'(\tilde{x}) + eG'_d(\tilde{x}))$ в силу d-периодичности функции g. Если $\tilde{M} \in \mathbb{Z}^n$, то

$$H(\tilde{x} + \tilde{M} \cdot d) =$$

$$= e \cdot g\left(a_0 + \sum_{i=1}^{n} a_i(x_i + M_i d) + eG_d(\tilde{x} + \tilde{M}d),\ a'_0 + \sum_{i=1}^{n} a'_i(x_i + M_i d) + eG'_d(\tilde{x} + \tilde{M}d)\right) =$$

$$= e \cdot g\left(a_0 + \sum_{i=1}^{n} a_i x_i + eG_d(\tilde{x}) + d \cdot \sum_{i=1}^{n} a_i M_i,\ a'_0 + \sum_{i=1}^{n} a'_i x_i + eG'_d(\tilde{x}) + d \cdot \sum_{i=1}^{n} a'_i M_i\right) =$$

$$= e \cdot g(l(\tilde{x}) + eG_d(\tilde{x}) + d \cdot F(\tilde{x}),\ l'(\tilde{x}) + eG'_d(\tilde{x}) + d \cdot F'(\tilde{x})) = H(\tilde{x})$$

(использовалась d-периодичность функций g, G_d и G'_d). Итак, функция $H(\tilde{x})$ является d-периодической, все ее значения кратны e, в силу утверждения 1.7 она принадлежит классу $C_e(d)$. □

Непосредственно из определения классов $C_e(d)$ и $C(d)$ получаем

Следствие 1.5. *Справедливы равенства* $C_1(d) = C(d), \quad C_d(k) = C_d(d)$. *Класс* $C_d(d)$ *состоит в точности из всех функций вида*

$$f(\tilde{x}) = l(\tilde{x}) + d \cdot F(\tilde{x}). \tag{1.15}$$

Утверждение 1.9. *При любых* k, d, e, *таких, что* $e|d, d|k$, *класс* $C_e(d)$ *замкнут. Если* $e \neq 1$ *и* $e \neq d$, *то его базисами являются системы*

$$A_e(d) = \{1,\ x + y,\ eg_d(x,y),\ d \cdot j(x,y)\},$$

а также $\{1,\ x + y,\ eg_d(x),\ d \cdot j(x)\}$ *при* $d \neq 2e,\ k \neq 2d,$

$\{1,\ x+y,\ eg_d(x),\ d \cdot j(x,y)\}$ *при* $d \neq 2e, \quad \{1,\ x+y,\ eg_d(x,y),\ d \cdot j(x)\}$ *при* $k \neq 2d.$

Доказательство. Покажем, что $C_e(d) \subseteq [A_e(d)]$. Рассмотрим представление (1.14) функции f класса $C_e(d)$. Слагаемое $l(\tilde{x})$ порождается системой $\{1,\ x + y\}$.

Слагаемое $eG_d(\tilde{x})$ есть линейная комбинация функций $eg_d(\tilde{x} - \tilde{a})$, $\tilde{a} \in E_d^n$. Положим

$$\varphi_n(\tilde{x}) = eg_d(x_1, \ldots, x_n),\ n = 1, 2, \ldots.$$

Тогда $\varphi_1(x) = \varphi_2(x,x)$ и, если $e \neq d$, то $\varphi_{n+1}(\tilde{x}, y) = \varphi_2(e - \varphi_n(\tilde{x}), y)$ при $n \geq 2$. Таким образом, $eG_d(\tilde{x}) \in [\{1, x+y, \varphi_2(x,y)\}]$.

Далее, слагаемое $d \cdot F(\tilde{x})$ есть линейная комбинация функций $d \cdot j(\tilde{x} - \tilde{b})$, $\tilde{b} \in E_k^n$. Положим

$$\psi_n(\tilde{x}) = d \cdot j(x_1, \ldots, x_n),\ n = 1, 2, \ldots.$$

Тогда $\psi_1(x) = \psi_2(x,x)$, $\psi_{n+1}(\tilde{x}, y) = \psi_2(d - \psi_n(\tilde{x}), y)$ при $n \geq 2$. Таким образом, $d \cdot F(\tilde{x}) \in [A_e(d)]$ и, следовательно, $f(\tilde{x}) \in [A_e(d)]$. Отметим, что

$$\varphi_2(x,y) = \varphi_1(2e - \varphi_1(x) - \varphi_1(y)) \text{ при } d \neq 2e,$$

$$\psi_2(x,y) = \psi_1(2d - \psi_1(x) - \psi_1(y)) \text{ при } k \neq 2d.$$

Обратное включение $[A_e(d)] \subseteq C_e(d)$ доказывается применением утверждений 1.6, 1.7 и леммы 1.7.

Итак, установлено, что система функций $A_e(d)$ полна в классе $C_e(d)$. Покажем, что она является базисом этого класса.

Подсистема $A_e(d) \setminus \{1\} = \{x+y, eg_d(x,y), d \cdot j(x,y)\}$ не полна, так как сохраняет множество чисел, кратных e.

Подсистема $A_e(d) \setminus \{x+y\} = \{1, eg_d(x,y), d \cdot j(x,y)\}$ не полна, так как сохраняет множество, состоящее из 1 и чисел, кратных e.

Подсистема $A_e(d) \setminus \{eg_d(x,y)\} = \{1, x+y, d \cdot j(x,y)\}$ не полна, так как порождает только такие функции $f(\tilde{x})$, для которых нелинейная часть (функция $F(\tilde{x})$ из (1.1)) кратна d.

Наконец, подсистема $A_e(d) \setminus \{d \cdot j(x,y)\} = \{1, x+y, eg_d(x,y)\}$ не полна, так как содержится в классе $L(d)$ абсолютного сохранения d-разностей, но $d \cdot j(x,y) \notin L(d)$ [11,12].

Другие системы из условия утверждения рассматриваются аналогично. □

Итак, найден базис в классе $C_e(d)$, если $e \notin \{1,\ d\}$. При $e = 1$ имеем $C_1(d) = C(d)$. Этот класс описан в разделе 1.3. При $e = d$ из определения класса $C_e(d)$, утверждений 1.6–1.8 и следствия 1.5 получаем

Следствие 1.6. *Если $d \neq 1, d \neq k$, то базисом в классе $C_d(d)$ является система*

$$A_d(d) = \{1,\ x+y,\ d \cdot j(x,y)\}.$$

Если при этом $k \neq 2d$, то функцию $d \cdot j(x,y)$ в этой системе можно заменить на $d \cdot j(x)$. При любом k справедливы равенства

$$C_1(1) = P_k, \quad C_k(k) = L.$$

Утверждение 1.10. *Если $e_1|d, e_2|d, d|k$, то условия $e_1|e_2$ и $C_{e_1}(d) \supseteq C_{e_2}(d)$ равносильны.*

Доказательство. Если $e_2 = ae_1$, то $e_2 g_d(\tilde{x}) = a \cdot e_1 g_d(\tilde{x}) \in [A_{e_1}(d)]$, поэтому

$$C_{e_2}(d) = [A_{e_2}(d)] \subseteq [A_{e_1}(d)] = C_{e_1}(d).$$

Пусть $C_{e_2}(d) \subseteq C_{e_1}(d)$. Если $e_1 = 1$ или $e_2 = d$ или $e_1 = e_2$, то $e_1 | e_2$. В остальных случаях рассмотрим d-периодическую функцию

$$f(x, y) = e_2 g_d(x - (e_1 - 1),\ y - (e_1 - 1))$$

класса $C_{e_2}(d)$. По условию она должна принадлежать и $C_{e_1}(d)$. Представим ее в каноническом для этого класса виде (1.14) при $e = e_1$. Для такой функции однозначно $l(x, y) = d \cdot F(x, y) = 0$, поэтому $f(x, y)$ есть линейная комбинация функций $e_1 g_d(x - a, y - b)$, где $a, b \in E_d$, откуда $e_1 | e_2$. □

Утверждение 1.11. *Пусть* $e_1 | d, e_2 | d, d | k$, $e_0 = НОД(e_1, e_2)$, $e_3 = НОК(e_1, e_2)$. *Тогда*

$$C_{e_1}(d) \cap C_{e_2}(d) = C_{e_3}(d), \qquad [C_{e_1}(d) \cup C_{e_2}(d)] = C_{e_0}(d).$$

Доказательство. Включение $C_{e_3}(d) \subseteq C_{e_1}(d) \cap C_{e_2}(d)$ следует из утверждения 1.10. Докажем обратное включение. Пусть $f(\tilde{x}) \in C_{e_1}(d) \cap C_{e_2}(d)$. Представим эту функцию в каноническом виде (1.7) при $e = e_1$. Здесь $l(\tilde{x})$, $d \cdot F(\tilde{x}) \in C_{e_2}(d)$, поэтому и d-периодическая функция $e_1 G_d(\tilde{x}) = f(\tilde{x}) - l(\tilde{x}) - d \cdot F(\tilde{x})$ принадлежит классу $C_{e_2}(d)$. Представляя ее в виде (1.14) при $e = e_2$, находим линейную часть, равную 0, и убеждаемся, что все ее значения кратны и e_1, и e_2, и, следовательно, e_3, поэтому $f(\tilde{x}) = l(\tilde{x}) + e_3 G_d(\tilde{x}) + d \cdot F_1(\tilde{x}) \in C_{e_3}(d)$.

Докажем включение $[C_{e_1}(d) \cup C_{e_2}(d)] \subseteq C_{e_0}(d)$. Имеем $d_0 | d_1, d_0 | d_2$, откуда, в силу утверждения 1.10, $C_{e_1}(d) \subseteq C_{e_0}(d)$, $C_{e_2}(d) \subseteq C_{e_0}(d)$, $C_{e_1}(d) \cup C_{e_2}(d) \subseteq C_{e_0}(d)$. Далее, переходя к замыканиям, получаем требуемое.

Включение $C_{e_0}(d) \subseteq [C_{e_1}(d) \cup C_{e_2}(d)]$ следует из утверждения 1.9 и выражения

$$e_0 g_d(\tilde{x}) = A_1 e_1 g_d(\tilde{x}) + A_2 e_2 g_d(\tilde{x}), \quad \text{где } A_1, A_2 \in \mathbb{Z},\ A_1 e_1 + A_2 e_2 = e_0.$$

□

Следствие 1.7. *При фиксированном d классы $C_e(d)$ образуют решетку, антиизоморфную решетке делителей e числа d.*

При фиксированном e классы $C_e(d)$ образуют решетку, антиизоморфную решетке делителей d числа k, кратных e.

1.6 Классы $C_e(d)$ и $C(e,d)$

Если $e|d,\ d|k$, *то* $C_e(d) \subseteq C(e,d)$.

Это следует из определения таких классов в разделах 1.3 и 1.4.

Найдем место класса $C_e(d)$ в решетке $\mathcal{L}(P_k)$.

Утверждение 1.12. *Равенство* $C_e(d) = C(e,d)$ *верно только при* $e = 1$.

Доказательство. Уже отмечено, что $C_1(d) = C(1,d) = C(d)$.

Если $e \geq 2$, то для функции $f(x,y) = g_e(x-1, y-1)$ класса $C(e,d)$ имеем $f(1,1) = 1,\ f(0,0) = f(0,1) = f(1,0) = 0$. Эту функцию нельзя представить суммой $eG_d(x,y) + d \cdot F(x,y)$, так как все значения суммы кратны e. □

Утверждение 1.13. *Если* $e|d,\ d \neq k$, *то в точности при* $e = 1$ *и при* $e = 2$ *все одноместные функции класса* $C(e,d)$ *принадлежат классу* $C_e(d)$.

Доказательство. Пусть $f(x) \in C(e,d)$. Представим эту функцию в виде

$$f(x) = l(x) + G_e(x) + eG_d(x) + d \cdot F(x), \qquad l(x) = f(0) + (f(1) - f(0))\, x.$$

При этом $l(x), eG_d(x), d \cdot F(x) \in C_e(d)$. Выясним, когда $G_e(x) \in C_e(d)$. Положим $h(x) = g_e(x-1)$.

Если $e = 1$, то $h(x) = 1 \in C_1(d) = C(d)$.

Если $e = 2$, то k и d четны, функция $x - h(x)$ принимает только четные значения и ее можно представить линейной комбинацией функций $2g_d(x-a)$, $d \cdot j(x-b)$ класса $C_2(d)$ (здесь $a, b \in E_k$).

Итак, если $e = 1$ или $e = 2$, то $h(x), G_e(x), f(x) \in C_e(d)$.

При $e \geq 3$ для функции $f(x) = g_e(x-2)$ имеем $f(0) = f(1) = 0,\ f(2) = 1$, эту функцию нельзя представить суммой $eG_d(x) + d \cdot F(x)$, все значения которой кратны e. □

Следствие 1.8. *Функции* $g_2(x,y)$ *в полных системах для классов* $C(2)$ *и* $C(2, d_2, \ldots, d_l)$, *где* $d_2, \ldots, d_l$ *четны, нельзя заменить на* $g_2(x)$, *так как* $g_2(x) = 1 - x + 2F(x) \in C_2(2)$.

Лемма 1.8. *Если* $p|d,\ d|k,\ f(\tilde{x}) \in C(p,d) \setminus C_p(d)$ *и* $n \geq 2$, *то суперпозициями функции* f *и элементов класса* $C_p(d)$ *можно получить функцию* $G(\tilde{x})$, *обладающую следующими свойствами*:

$C1$) *функция не принадлежит классу* $C_p(d)$,

$C2$) *функция является* p*-периодической,*

$C3$) *все значения функции принадлежат* E_p.

Доказательство. Представим функию $f(\tilde{x})$ в каноническом для $C(p,d)$ виде

$$f(\tilde{x}) = f(\tilde{0}) + G_p(\tilde{x}) + pG_d(\tilde{x}) + d \cdot F(\tilde{x}).$$

Здесь $f(\tilde{0}), pG_d(x), d \cdot F(\tilde{x}) \in C_p(d)$. Вычитая эти слагаемые, получим функцию $G_p(\tilde{x})$. Она обладает свойствами C1) и C2). Вычтем из нее, если необходимо, подходящую p-периодическую функцию со значениями, кратными p (она же является и d-периодической, поэтому принадлежит $C_p(d)$). Результат $G(\tilde{x})$ вычитания — нелинейная функция, так как $f \notin C_p(d)$. Функция $G(\tilde{x})$ обладает свойствами C1), C2) и C3). □

Лемма 1.9. *Пусть $p = 2$ и функция $G(x_1, \ldots, x_n)$ обладает свойствами $C1) - C3)$. Тогда $n \geq 2$. Если при этом $n \geq 3$, то из функции G путем подстановки констант и отождествления переменных можно получить двухместную функцию $g(x,y)$, также обладающую свойствами $C1) - C3)$.*

Доказательство. В силу свойства C1) функция $G(\tilde{x})$ нелинейна. В силу этого же свойства и утверждения 1.13 имеем $n \geq 2$. Если $n = 2$, то $g(x,y) = G(x,y)$.

Пусть $n \geq 3$. В силу нелинейности найдутся наборы $\tilde{\varepsilon}_{i_1}, \ldots, \tilde{\varepsilon}_{i_r}$, $\tilde{\varepsilon}_{j_1}, \ldots, \tilde{\varepsilon}_{j_s}$ такие, что

$$G((\tilde{\varepsilon}_{i_1} + \cdots + \tilde{\varepsilon}_{i_r}) + (\tilde{\varepsilon}_{j_1} + \cdots + \tilde{\varepsilon}_{j_s})) \neq G(\tilde{\varepsilon}_{i_1} + \cdots + \tilde{\varepsilon}_{i_r}) + G(\tilde{\varepsilon}_{j_1} + \cdots + \tilde{\varepsilon}_{j_s}),$$

где $i_1, \ldots, i_r, j_1, \ldots, j_s$ — попарно различные элементы множества $\{1, \ldots, n\}$. Положим:

$$A = \{i_1, \ldots, i_r\}, \quad B = \{j_1, \ldots, j_s\};$$

$$x_i = x, \text{ если } i \in A; \quad x_i = y, \text{ если } i \in B; \quad x_i = 0, \text{ если } i \notin A \cup B.$$

При таком преобразовании переменных функции G получим функцию $g(x,y)$. При этом $g(1,1) \neq g(1,0) + g(0,1)$. Функция g нелинейна и обладает свойствами C1)–C3). □

Утверждение 1.14. *Если k, d четны, то класс $C_2(d)$ является предполным в $C(2,d)$.*

Доказательство. Пусть $f(\tilde{x}^n) \in C(2,d) \setminus C_2(d)$. В силу утверждения 1.9 имеем $n \geq 2$. Применяя лемму 1.2 (при $p = 2$) и лемму 1.3, суперпозициями функции f и элементов класса $C_2(d)$ получим функцию $g(x,y)$ со свойствами C1)–C3). Суперпозициями функции $g(x,y)$ и линейных (принадлежащих классу $C_2(d)$) функций получим функцию $H(x,y)$ со свойствами C1)–C3) и, кроме того,

$$H(0,0) = H(0,1) = H(1,0) = 0, \quad H(1,1) = 1.$$

Тогда $g_2(x,y) = H(x+1, y+1) \in [C_2(d) \cup \{f\}]$ и $[C_2(d) \cup \{f\}] = C(2,d)$. □

Лемма 1.10. *Пусть $n \geq 2$ и пусть n-местная функция f нелинейна. Тогда подстановкой констант на места переменных функции f можно получить одноместную нелинейную функцию.*

Доказательство. Линейность функции $f(x_1, \ldots, x_n)$ эквивалентна следующему свойству, называемому *сохранением 1-разностей*: для каждого $i = 1, \ldots, n$ при всех $\tilde{x}$ величины

$$\Delta_i f(\tilde{x}) = f(x_1, \ldots, x_{i-1}, x_i + 1, x_{i+1}, \ldots, x_n) - f(\tilde{x}),$$

называемыми 1-*разностями по переменной* x_i *функции* f *в точке* $\tilde{x}$, не зависят от $\tilde{x}$.

Пусть $n \geq 1$ и функция $f(\tilde{x}^n,\ y)$ нелинейна. Без ограничения общности полагаем, что она не сохраняет 1-разности по переменной y, т. е. разности $\Delta_{n+1} f(\tilde{x},\ y)$ зависят от $\tilde{x}$ и y. Рассмотрим эти разности как функции переменных $\tilde{x}$, y.

Если $\Delta_{n+1} f(\tilde{x},\ y)$ зависит существенно от y, то одноместная нелинейная функция получается из $f(\tilde{x},\ y)$ подстановкой констант на места переменных $\tilde{x}$.

Если же $\Delta_{n+1} f(\tilde{x},\ y)$ не зависит существенно от y, то отождествим y с одной из переменных $\tilde{x}$. Получим нелинейную функцию меньшего числа аргументов. Повторим те же рассуждения для нее и будем продолжать их, пока не получим требуемую одноместную функцию. □

Лемма 1.11. *Пусть $p \geq 3$ и пусть $f(\tilde{x}^n) \in C(p, d) \backslash C_p(d)$. Тогда суперпозициями функции f и элементов класса $C_p(d)$ можно получить одноместную функцию, обладающую свойствами $C1$)–$C3$).*

Доказательство. Применим лемму 1.8, получим функцию $G(\tilde{x}^n)$ со свойствами C1)–C3). Она нелинейна. Если $n = 1$, цель достигнута. Если же $n \geq 2$, то к $G(\tilde{x}^n)$ применим лемму 1.10. При этом используется только переименование переменных и подстановка констант, т. е. суперпозиции G и элементов класса $C(p, d)$. Результирующая одноместная функция сохраняет свойства C1)–C3). □

Утверждение 1.15. *Если k и d кратны 3, то класс $C_3(d)$ является предполным в $C(3, d)$.*

Доказательство. Пусть $f(\tilde{x}) \in C(3, d) \setminus C_3(d)$. В силу леммы 1.11 суперпозициями функции f и элементов класса $C_3(d)$ получим одноместную функцию со свойствами C1)–C3). Линейными преобразованиями этой функции и ее аргумента получим функцию $H(x)$, которая обладает свойствами C1)–C3) и, кроме того, $H(0) = H(1) = 0,\ H(2) = \gamma \in \{1, 2\}$. Покажем, что $g_3(x) \in [C_3(d) \cup \{H\}]$, тогда и $[C_3(d) \cup \{f\}] = C(3, d)$.

Если $\gamma = 1$, то $g_3(x) = H(x + 2)$.

Если $\gamma = 2$, то сведем случай к предыдущему рассмотрением вместо $H(x)$ функции
$H_1(x) = A \cdot H(x) + B \cdot 3g_3(x-2)$, где $2A + 3B = 1$. $\square$

Утверждение 1.16. *Если $p > 3$, $p|d$, то класс $C_p(d)$ является предполным в $C(p,d)$.*

Доказательство. Пусть $f \in C(p,d) \setminus C_p(d)$. В силу леммы 1.5 суперпозициями функции f и элементов класса $C_p(d)$ получим одноместную функцию $H(x)$ со свойствами C1)–C3) и, кроме того, $H(0) = 0$. Покажем, что $[C_p(d) \cup \{H\}] = [C_p(d) \cup \{f\}]$ содержит функцию $g_p(x)$ и, следовательно, полную в $C(p,d)$ систему.

Пусть $y_i = H(i)$, $i = 0, 1, \ldots, p-1$, $\sigma = \sigma(H) = y_1 + \cdots + y_{p-1}$ (сумма в кольце $\mathbb{Z}$).

Рассмотрим *вес* $W = W(H)$ *функции* H — число ненулевых значений y_i. Имеем $1 \le W \le p-1$ и $y_t = y \ne 0$ при некотором $t \in E_p$. Без ограничения общности полагаем $y = t$ в силу следующих соображений. Всегда НОД$(y,p) = 1$.

Если НОД$(y,k) = 1$, то умножим функцию $H(x)$ на $t \cdot y^{-1} \pmod k$.

Если же

$$k = p^\alpha Q,\ Q > 1,\ \text{НОД}(p,Q) = 1,\ \text{НОД}(y,Q) = q_1^{\beta_1} \cdots q_s^{\beta_s} > 1, \tag{1.16}$$

то

$$Q = q_1^{\gamma_1} \cdots q_s^{\gamma_s} Q_1,\quad Q_1 \ge 1,\quad \text{НОД}(Q_1,\ pq_1 \cdots q_s) = 1,\quad 1 \le \beta_j \le \gamma_j$$

при $j = 1, \ldots, s$. Для $z = y + pQ_1$ получаем НОД$(z,k) = 1$. Действительно, z не кратно p, так как y не кратно p. Далее, z не кратно ни одному q_j, так как pQ_1 не кратно q_j. Наконец, z не кратно ни одному собственному делителю d числа Q_1, так как y не кратно d.

При условиях (1.16) рассмотрим вместо $H(x)$ функцию

$$H(x) + Q_1 p g_p(x - t). \tag{1.17}$$

В точке $x = t$ она принимает значение z, взаимно простое с числом k. Умножим эту функцию на $tz^{-1} \pmod k$.

Таким образом, без ограничения общности полагаем

$$H(i) = y_i, i \in E_p, \quad y_0 = 0,\ y_t = t, \quad 1 \le W(H) \le p-1.$$

Возможны следующие случаи.

1: $W(H) = 1$. Тогда $H(x) = t g_p(x-t)$.

Если НОД$(t,k) = 1$, то $H(x) \cdot t^{-1} \pmod k = g_p(x-t)$ и остается только осуществить линейный сдвиг аргумента такой функции.

Если же выполнены условия (1.16) при $y = t$, то вместо $H(x)$ рассматриваем функцию (1.17).

2: $2 \le W(H), \text{НОД}(\sigma, p) = 1$. Тогда рассмотрим функцию

$$F(x) = \sigma - H(x) - H(2x) - \cdots - H((p-1)x).$$

Имеем $F(0) = \sigma,\ F(i) = 0$ при $i = 1, 2, \ldots, p-1$. Поэтому $F(x) = \sigma g_p(x)$. Если $\text{НОД}(\sigma, k) = 1$, то, умножая последнюю функцию на $\sigma^{-1} \pmod k$, получим $g_p(x)$. Если же при $y = \sigma$ выполнены условия (1.16), то заменим $F(x)$ на функцию $F(x) + Q_1 p g_p(x)$.

3: $2 \le W(H) \le p-2,\ p|\sigma$. Будем последовательно уменьшать вес рассматриваемой функции, пока не придем к одному из случаев 1 или 2. Возможны следующие подслучаи.

3.1: $\exists y_j\ H(y_j) \ne y_j$. Рассмотрим функцию $F(x) = H(x) - H(H(x))$. Если $H(x_0) = 0$ в какой-то точке x_0, то и $F(x_0) = 0$. Кроме того, $F(t) = 0,\ F(j) \ne 0$. Следовательно, $1 \le W(F) < W(H)$.

3.2: $\forall j\ H(y_j) = y_j$ и среди ненулевых значений y_j есть одинаковые. Пусть $y_{j_1} = y_{j_2} = y$. Если $\text{НОД}(y, k) = 1$, то, умножая $H(x)$ на $y^{-1} \pmod k$, получим в точках $x = j_1$ и $x = j_2$ значение 1. Если же выполняются условия (1.16), то вместо $H(x)$ рассмотрим функцию

$$H_1(x) = H(x) + Q_1(p g_p(x - j_1) + p g_p(x - j_2)).$$

Имеем $H_1(j_1) = H_1(j_2) = z = y + pQ_1,\ \text{НОД}(k, z) = 1$. Умножая $H_1(x)$ на $z^{-1} \pmod k$, получим в точках $x = j_1$ и $x = j_2$ значение 1.

Таким образом, без ограничения общности можем предполагать, что для функции $H(x)$ выполняются равенства $H(j_1) = H(j_2) = 1$. Пусть, далее,

$$j_2 - j_1 = m \in \{1, \ldots, p-1\},\ \ l = j_1 m^{-1} \pmod p,\ \ F(x) = H(mx).$$

Тогда для некоторого $r \ge 2$ имеем

$$F(l) = F(l+1) = \cdots = F(l+r-1) = 1, \quad F(l+r) \ne 1.$$

Положим

$$G(x) = F(x + F(x)) - F(x).$$

Функция $F(x)$ принимает те же значения, что и $H(x)$, но в других (при $m \ne 1$) точках, поэтому $W(F) = W(H)$. Далее, если $F(x_0) = 0$ в какой-то точке x_0, то и $G(x_0) = 0$. Кроме того, $G(l) = 0,\ G(l+r-1) \ne 0$, тогда $1 \le W(G) < W(H)$.

3.3: $\forall j\ H(y_j) = y_j$ и среди ненулевых значений y_j нет одинаковых. Тогда при всех $j \in E_p$ либо $y_j = 0$, либо $y_j = j$. Из условий $p|\sigma$ и $1 \le W \le p-2$ следует, что функция H не может принимать все W ненулевых значений в точках

$x = 1, 2, \ldots, W$. Значит, при некотором $l \geq 1$ имеет место $y_l = l \neq 0$ и $y_{l-1} = 0$. При этом найдется i такое, что $i > l$ и $y_i = i \neq 0$.

Если НОД$(i, k) = 1$, то существует $c = i^{-1} \pmod{k}$. Если же при $y = i$ выполняются условия (1.16), то заменим $H(x)$ на функцию $H(x) + Q_1 p g_p(x - i)$.

Таким образом, без ограничения общности можно полагать, что существует $c = i^{-1} \pmod{k}$. Рассмотрим функцию

$$F(x) = cH(x + l - 1).$$

Для нее имеем

$$F(0) = 0,\ F(1) = cy_l = cl \neq 1,\ F(i - l + 1) = cH(i) = ci = 1,\ \ W(F) = W(H).$$

Случай сведен к случаю **3.1**.

4: $p|\sigma,\ W = p - 1$. Рассмотрим функцию $F(x) = x - H(x)$. Для нее имеем $F(0) = F(t) = 0$. Из нелинейности функции $H(x)$ следует, что $F(j) \neq 0$ при некотором $j \in E_p$. Случай сведен к одному из предыдущих.

В ходе преобразований функции с целью уменьшения веса свойства C1)–C3) сохраняются. При умножении функции на константу свойство C3) может нарушиться, но оно восстанавливается вычитанием функций $p g_p(x - a)$, $a \in E_p$, которые принадлежат классу $C_p(d)$ (если $p|d$, то p-периодическая функция является и d-периодической, все ее значения кратны $e = p$, остается применить утверждение 1.7). □

Теорема 1.2. *Класс $C_e(d)$ является предполным в $C(e, d)$ в точности при $e = p$.*

Доказательство. Класс $C_p(d)$ предполный в $C(p, d)$ в силу утверждений 1.14,1.15,1.16.

Обратно: пусть число e составное, $e = ab$, $1 < a < e$. Рассмотрим замкнутый класс $K(a, b;\ d)$ функций канонического вида

$$f(\tilde{x}) = l(\tilde{x}) + aG_e(\tilde{x}) + eG_d(\tilde{x}) + d \cdot F(\tilde{x}).$$

Функции этого класса имеют нелинейную часть, кратную a, поэтому $g_e(x, y) \in C(e, d) \setminus K(a, b;\ d)$. У функций класса $C_e(d)$ нелинейная часть кратна e, поэтому $a g_e(x, y) \in K(a, b;\ d) \setminus C_e(d)$. Тогда

$$C_e(d) \subset K(a, b;\ d) \subset C(e, d).$$

□

Замечание 1.5. Если e — собственный делитель числа d, а также d — это собственный делитель числа k, то верны и строгие включения

$$C_e(d) \subset C(e, d) \subset C(e).$$

1.7 Классы $C(d)$ и $C(d,e)$ при взаимно простых d, e

Всюду в данном разделе

$$k = de, \quad d > 1, e > 1, \quad \text{НОД}(d,e) = 1. \tag{1.18}$$

Утверждение 1.17. *При условиях* (1.18) *базисом класса* $C(d)$ *является система функций*

$$\{x + y,\ g_d(x,y),\ dg_e(x,y)\}.$$

Это следует из утверждения 1.3 и формулы

$$dj^{(n)}(\tilde{x}) = dg_e^{(n+1)}\left(\tilde{x},\ d - dg_e^{(n)}(\tilde{x})\right),$$

справедливой при всех $n \in \mathbb{N}$.

Лемма 1.12. *Пусть* $e = p$ *и* $f(\tilde{x}) \in C(d) \setminus C(p)$. *Тогда замыкание* $[C(d,p) \cup \{f\}]$ *содержит функцию* $g_d(x,y)$.

Доказательство. Имеем $f(\tilde{x}^n) \notin C(p)$. Если $n > 1$, то, применяя лемму из [86, §16], подстановкой констант в эту функцию получим одноместную функцию $f_1(x)$, $f_1(x) \in C(d) \setminus C(p)$. Линейными преобразованиями из нее получим функцию $h(x)$ со свойствами

$$h(0) = 0,\ h(Np) = \gamma,\ \text{НОД}(\gamma, p) = 1,\ N \in \{1, 2, \ldots, d-1\}.$$

Рассмотрим функцию $pg_d(x,y)$ класса $C(d,p)$.

Случай 1. Если $\text{НОД}(\gamma, d) = 1$, то существует $c = \gamma^{-1} \pmod{k}$, тогда

$$g_d(x,y) = c \cdot h(N \cdot pg_d(x,y)).$$

Случай 2. Если же $\text{НОД}(\gamma, d) > 1$, то для функции $h(x) + pg_d(Np - x)$ имеет место случай 1. □

Утверждение 1.18. *Если выполнены условия* (1.18), *то класс* $C(d,e)$ *является предполным в классе* $C(d)$ *в точности при* $e = p$.

Доказательство. Пусть $e = p$, $f \in C(d) \setminus C(e)$. Тогда, согласно утверждению 1.17 и лемме 1.12 заключаем, что $[C(d,p) \cup \{f\}] = C(d)$.

Пусть теперь $e = ab$, $a > 1, b > 1$. Тогда функции класса $C(d,e)$ представляются как

$$l(\tilde{x}) + dG_{ab}(\tilde{x}) + abG_d(\tilde{x}),$$

и $C(d,e) \subset K \subset C(d)$, где $K = [1,\ x + y,\ dg_{ab}(x,y),\ ag_d(x,y)]$ — класс всех функций вида

$$l(\tilde{x}) + dG_{ab}(\tilde{x}) + aG_d(\tilde{x}).$$

□

1.8 Перестановочность функций, сохраняющих сравнения по нескольким модулям

Функция $f(\tilde{y}^n)$ называется *перестановочной с функцией* $u(\tilde{z}^m)$, если для всех x_{ij}, где $i = 1, \ldots, m,\ \ j = 1, \ldots, n$, выполняется условие

$$f(u(x_{11}, x_{21}, \ldots, x_{m1}), \ldots, u(x_{1n}, x_{2n}, \ldots, x_{mn})) =$$

$$= u(f(x_{11}, x_{12}, \ldots, x_{1n}), \ldots, f(x_{m1}, x_{m2}, \ldots, x_{mn})). \tag{1.18}$$

Нетрудно проверить, что все линейные формы над произвольным кольцом перестановочны друг с другом. Таким образом, перестановочность функции f с линейной формой является необходимым условием линейности функции f.

1.8.1 Классы $Z(u)$ и $C(k_1, \ldots, k_m)$

Пусть

$$k = k_1 \cdots k_m,\ m \geq 2, \quad \text{числа } k_1, \ldots, k_m \text{ попарно взаимно простые}, \tag{1.19}$$

$$d_i = k/k_i,\ i = 1, \ldots, m.$$

Рассмотрим линейную форму

$$u(x_1, \ldots, x_m) = a_1 x_1 + \cdots + a_m x_m, \tag{1.20}$$

для которой при всех $i = 1, \ldots, m$ выполнены сравнения

$$a_i \equiv 1 \pmod{k_i}, \quad a_i \equiv 0 \pmod{d_i}. \tag{1.21}$$

Нетрудно проверить следующие ее свойства.

Лемма 1.13. .

1. *Функция* $u(x_1, \ldots, x_m)$ *определена условиями* (1.20), (1.21) *однозначно.*
2. *Для каждого* x *из* E_k *есть ровно один набор* $(x_1, \ldots, x_m) \in E_{k_1} \times \cdots \times E_{k_m}$ *такой, что* $x = u(x_1, \ldots, x_m)$.
3. *Функция* $u(x_1, \ldots, x_m)$ *перестановочна сама с собой, причем*

$$u(u(x_{11}, x_{21}, \ldots, x_{m1}), \ldots, u(x_{1m}, x_{2m}, \ldots, x_{mm})) =$$

$$= u(u(x_{11}, x_{12}, \ldots, x_{1m}), \ldots, u(x_{m1}, x_{m2}, \ldots, x_{mm})) =$$

$$= u(x_{11}, \ldots, x_{mm}).$$

Теорема 1.3. *Пусть $Z(u)$ — класс всех функций в P_k, перестановочных с такой функцией $u(x_1, \ldots, x_m)$. Тогда*

$$Z(u) = C(k_1, \ldots, k_m).$$

Доказательство. Пусть $f \in Z(u)$. Покажем, что $f \in C(k_i)$ для каждого фиксированного i, $1 \le i \le m$. Для простоты записи считаем функцию f одноместной.

Если $b \equiv c \pmod{k_i}$, то $b = u(b_1, \ldots, b_i, \ldots, b_m)$, $c = u(c_1, \ldots, c_i, \ldots, c_m)$, при этом $b_i = c_i$, так как $b_i, c_i \in E_{k_i}$. В силу перестановочности и условий (1.21) получаем

$$f(b) = f(u(b_1, \ldots, b_i, \ldots, b_m)) = u(f(b_1), \ldots, f(b_i), \ldots, f(b_m)) \equiv$$

$$\equiv a_1 f(b_1) + \cdots + a_i f(b_i) + \cdots + a_m f(b_m) \equiv f(b_i) \pmod{k_i}.$$

Аналогично $f(c) \equiv f(c_i) \pmod{k_i}$. Таким образом, $f(b) \equiv f(c) \pmod{k_i}$.

Обратно, пусть $f(x) \in C(k_i)$, $i = 1, \ldots, m$. Тогда $x = u(x_1, \ldots, x_i, \ldots, x_m)$, $f(x) \equiv f(x_i) \pmod{k_i}$. Условие перестановочности в силу (1.21) равносильно сравнениям

$$f(u(x_1, \ldots, x_m)) \equiv f(x_i), \quad u(f(x_1), \ldots, f(x_m)) \equiv f(x_i) \pmod{k_i},$$

$i = 1, \ldots, m$, которые выполняются, так как $f \in C(k_i)$. □

1.8.2 Классы $Z(v)$ и $C(d, d_1, \ldots, d_m)$

Пусть теперь

$$k = de, \quad e > 1, \quad \text{НОД}(d, e) = 1, \quad d = d_1 \cdots d_m, \quad m \ge 2,$$

числа $d_1, \ldots, d_m$ попарно взаимно простые,

$$v(x_1, \ldots, v_m) = a_1 x_1 + \cdots + a_m x_m,$$

$$a_i \equiv 0 \pmod{e},\ a_i \equiv 1 \pmod{d_i},\ a_i \equiv 0 \pmod{d/d_i}, \quad i = 1, \ldots, m.$$

Функция $v(x_1, \ldots, v_m)$ является d-периодической и определена однозначно.

Теорема 1.4. *Пусть $Z(v)$ — класс всех функций в P_k, перестановочных с такой функцией $v(x_1, \ldots, x_m)$. Тогда*

$$Z(v) = C(d, d_1, \ldots, d_m).$$

Доказывается она аналогично теореме 1.3.

1.8.3 Классы $Z(w)$ и $C(k_0, k_1, k_2)$

Пусть теперь $s \geq 1$, простые числа $p_1, \ldots, p_s$ попарно различны,

$$\alpha_i \geq 2, \quad 1 \leq \beta_i < \alpha_i, \qquad i = 1, \ldots, s,$$

$$k_1 = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad k_0 = p_1^{\beta_1} \cdots p_s^{\beta_s},$$

$$k = k_1 Q, \quad Q \geq 1, \quad \text{НОД}(k_1, Q) = 1, \quad k_2 = k_0 Q,$$

$$w(x, y) = ax + by,$$

$$a \equiv 1, \quad b \equiv 0 \pmod{k_1},$$

$$a \equiv 0, \quad b \equiv 1 \pmod{Q}.$$

Легко проверить следующие свойства введенной функции.

Лемма 1.14.

1. *Функция $w(x, y)$ определена однозначно.*
2. *Функция $w(x, y)$ перестановочна сама с собой, причем*

$$w(w(x_1, y_1),\ w(x_2, y_2)) = w(w(x_1, x_2),\ w(y_1, y_2)) = w(x_1, y_2).$$

3. *Для каждого $x \in E_k$ имеется ровно одна пара $(x_1, x_2) \in E_{k_1} \times E_{k_2}$ такая, что*

$$x \equiv x_1 \equiv x_2 \pmod{k_0}, \quad x = w(x_1, x_2).$$

Пример 1.1. Пусть $k = 12$, $k_1 = 2^2$, $Q = 3$, $k_0 = 2$, $k_2 = 6$. Тогда

$$w(x, y) = 9x + 4y.$$

Для четных значений имеем

$$w(0, 0) = 0, \quad w(0, 2) = 8, \quad w(0, 4) = 4,$$

$$w(2, 0) = 6, \quad w(2, 2) = 2, \quad w(2, 4) = 10.$$

Для нечетных:

$$w(1, 1) = 1, \quad w(1, 3) = 9, \quad w(1, 5) = 5,$$

$$w(3, 1) = 7, \quad w(3, 3) = 3, \quad w(3, 5) = 11.$$

Теорема 1.5. *Пусть $Per(w)$ — подкласс в $C(k_0)$, состоящий в точности из функций $f(\tilde{x})$, удовлетворяющих условию: если $\tilde{x}, \tilde{y} \in E_k^n$ и $\tilde{x} \equiv \tilde{y} \pmod{k_0}$, то*

$$f(w(x_1, y_1), \ldots, w(x_n, y_n)) = w(f(\tilde{x}),\ f(\tilde{y})).$$

Тогда

$$Per(w) = C(k_0, k_1, k_2).$$

Доказательство. Для простоты записи рассмотрим только одноместные функции f этих классов.

Пусть $f \in Per(w),\ x \equiv x' \pmod{k_1}, x = w(x_1, x_2), x' = w(x'_1, x'_2)$. Покажем, что $f(x) \equiv f(x') \pmod{k_1}$. Имеем в силу перестановочности

$$f(x) = f(ax_1 + bx_2) = af(x_1) + bf(x_2)$$

и аналогично

$$f(x') = af(x'_1) + bf(x'_2).$$

В силу выбора коэффициентов a, b получаем

$$f(x) \equiv f(x_1),\ f(x') \equiv f(x'_1) \pmod{k_1}.$$

При этом $x_1 = x'_1$, следовательно, $f(x) \equiv f(x') \pmod{k_1},\ f \in C(k_1)$.

Пусть теперь $x \equiv x' \pmod{k_2 = k_0 Q}$. Тогда

$$f(x) = f(ax_1 + bx_2) = af(x_1) + bf(x_2) \equiv f(x_2) \pmod{Q},$$

$$f(x') = f(ax'_1 + bx'_2) = af(x'_1) + bf(x'_2) \equiv f(x'_2) \pmod{Q}.$$

Учтем, что

$$x \equiv x_2,\ x' \equiv x'_2,\ x \equiv x' \pmod{Q},$$

откуда $x_2 \equiv x'_2 \pmod{Q}$. Кроме того, $x_2 \equiv x'_2 \equiv x \equiv x' \pmod{k_0}$. Таким образом, $x_2 \equiv x'_2 \pmod{k_2}$ и, следовательно, $x_2 = x'_2$. Значит, $f(x) \equiv f(x') \pmod{k_2},\ f \in C(k_2)$.

Установлено, что $Per(w) \subseteq C(k_1, k_2) = C(k_0, k_1, k_2)$. Докажем обратное включение.

Пусть $f \in C(k_1, k_2)$. Надо показать, что

$$f(ax + by) \equiv af(x) + bf(y) \pmod{k}, \tag{1.22}$$

если $x \equiv y \pmod{k_0}$. В силу выбора коэффициентов a, b имеем $ax + by \equiv x$, $af(x) + bf(y) \equiv f(x) \pmod{k_1}$. Из условия $f \in C(k_1)$ следует, что $f(ax + by) \equiv f(x) \pmod{k_1}$. Таким образом, выполняется сравнение (1.22) по модулю k_1.

Далее, $ax + by \equiv y,\ af(x) + bf(y) \equiv f(y) \pmod{Q},\ x \equiv y,\ a + b \equiv 1 \pmod{k_0}$. Из условий $f \in C(k_2),\ k_2 = k_0 Q$ следует

$$f(ax + by) \equiv f(y) \equiv af(x) + bf(y) \pmod{k_2},$$

сравнение (1.22) выполняется по модулям k_1, k_2 и $HOK(k_1, k_2) = k$. □

1.9 Заключение к главе 1

Основные результаты главы состоят в следующем.

1. Введены d-периодические функции, $d|k$, (раздел 1.2), применяемые далее в аддитивных представлениях функций и порождающих системах различных замкнутых классов. Предложены разложения функций в суммы периодических (леммы 1.4, 1.5, следствие 1.4, утверждение 1.5).

2. Предложены аддитивные формулы, задающие функции и базисы замкнутых классов:

формула (1.2) для классов $C(d)$, $d|k$, сохранения сравнения по модулю d (утверждения 1.2, 1.3, 1.17);

формулы (1.3) и (1.4) для классов $C(d_1, \ldots, d_l)$ сохранения сравнений по нескольким модулям $d_1, \ldots, d_l$ (утверждения 1.4, 1.5, следствие 1.2);

формулы (1.14) и (1.15) для классов $C_e(d)$ и $C_d(d)$, $e|d$, (утверждение 1.9, следствие 1.6).

3. Выяснено строение решетки классов $C_e(d)$ при фиксированном значении одного из параметров (следствие 1.7).

4. Найдены условия, необходимые и достаточные для того, чтобы класс $C_e(d)$ был предполным в классе $C(e, d)$ (теорема 1.2), а класс $C(e, d)$ — предполным в $C(d)$ при дополнительных ограничениях (1.18) (утверждение 1.18). Последний результат и способ его получения (лемма 1.12) применяются далее в главе 5.

5. Три семейства классов, сохраняющих сравнения по нескольким модулям, описаны с помощью свойства перестановочности функций (теоремы 1.3–1.5).

Глава 2

Классы сохранения d-разностей

В этой главе вводится и анализируется свойство k-значных функций сохранять d-разности (разности с шагом d, $d|k$)[1].

В разделе 2.1 даются основные понятия и примеры.

В разделах 2.2 и 2.4 определяются классы $R(d)$ и $L(d)$ сохранения и абсолютного сохранения d-разностей указанием аддитивных формул их элементов, доказывается замкнутость классов, находятся их базисы. Этому способствует особая аддитивная формула из раздела 2.3, представляющая произвольную функцию суммой более простых функций, d-сеточных ограничений.

В разделах 2.5–2.8 описываются решетки классов $L(d)$ и $R(d)$ для произвольных k и d, находятся условия неуплотняемости некоторых фрагментов решеток.

В разделах 2.9 и 2.10 вводятся особые подклассы классов $R(d)$, находится их место в решетке $\mathcal{L}(P_k)$.

Материалы этой главы опубликованы в [6,7].

2.1 Сохранение d-разностей

Пусть $d|k$, $f(\tilde{x}) \in P_k$. Фиксируем номер i переменной, $1 \le i \le n$. Для различных $\tilde{x}$ из E_k^n рассмотрим величины

$$\Delta_i f(\tilde{x}) = f(x_1, \ldots, x_{i-1},\ x_i + d,\ x_{i+1}, \ldots, x_n) - f(\tilde{x}),$$

называемые (первыми) *d-разностями по переменной x_i функции f в точке $\tilde{x}$*. Для одноместной функции используем более короткое обозначение $\Delta f(x)$ без указания индекса единственной переменной.

[1] Подобные конструкции в более общем случае применены позже А. В. Черемушкиным:
Черемушкин А. В. Аддитивный подход к определению степени нелинейности дискретной функции // Прикладная дискретная матем. // 2010, №2(8). — С. 22–33.
Черемушкин А. В. Об оценке уровня аффинности квадратичных форм // Дискретная математика. — 2017. — Т. 29, №1. — С. 114–125.

Будем говорить, что функция $f(\tilde{x})$ *сохраняет d-разности*, если для всех i, всех $\tilde{\mu}$ из E_d^n и всех $\tilde{x}$ таких, что $\tilde{x} \equiv \tilde{\mu} \pmod{d}$, разности $\Delta_i f(\tilde{x}) = \Delta(i, \tilde{\mu})$ не зависят от $\tilde{x}$. Если при этом разности $\Delta_i f(\tilde{x}) = \Delta(i)$ не зависят и от $\tilde{\mu}$, будем говорить, что функция f *абсолютно сохраняет d-разности*.

Классы функций, сохраняющих и абсолютно сохраняющих d-разности, обозначим как $R(d)$ и, соответственно, $L(d)$.

Пример 2.1. Рассмотрим функции $C(x) = C \in E_k$ (константа), $I(x) = x$, $G_d(\tilde{x})$, $j(x) = g_k(x)$, а также

$$\delta_d(x) = d\lfloor x/d \rfloor, \tag{2.1}$$

$$\chi_{d,j}(\tilde{x}) = x_j g_d(\tilde{x}) = \begin{cases} x_j, & \tilde{x} \equiv \tilde{0} \pmod{d}, \\ 0, & \tilde{x} \not\equiv \tilde{0} \pmod{d}, \end{cases} \qquad j = 1, \ldots, n. \tag{2.2}$$

Вычисляем:

$$\Delta C(x) = \Delta_i G_d(\tilde{x}) = 0, \ (i = 1, \ldots, n), \quad \Delta I(x) = \Delta \delta_d(x) = d,$$

$$\Delta_i \chi_{d,j}(\tilde{x}) = \begin{cases} 0, & i \neq j, \\ 0, & \tilde{x} \not\equiv \tilde{0} \pmod{d}, \\ d, & i = j, \quad \tilde{x} \equiv \tilde{0} \pmod{d}, \end{cases} \qquad i, j = 1, \ldots, n,$$

$$\Delta j(x) = \begin{cases} k-1, & x = 0, \\ 1, & x = k - d, \\ 0, & x \notin \{0, k-d\}. \end{cases}$$

Следовательно,

$$C(x), I(x), G_d(\tilde{x}), \delta_d(x) \in L(d), \ \chi_{d,j}(\tilde{x}) \in R(d) \setminus L(d) \ (j = 1, \ldots n), \ \ j(x) \notin R(d).$$

Легко проверяются следующие факты.

Утверждение 2.1. *Справедливы соотношения*:

$$L(1) = R(1) = L, \quad L(k) = R(k) = P_k; \qquad \text{если } d \neq 1, d \neq k, \text{ то } L(d) \subset R(d).$$

Лемма 2.1. *Классы $R(d)$ и $L(d)$ замкнуты относительно линейных операций над функциями, т. е. линейная комбинация функций каждого класса принадлежит тому же классу.*

Лемма 2.2. *Классы $R(d)$ и $L(d)$ замкнуты относительно введения и удаления фиктивных переменных.*

Доказательство. Пусть y — фиктивная переменная функции $f(\tilde{x}, y) = h(\tilde{x})$. Тогда для $i = 1, \ldots, n$ имеем $\Delta_i f(\tilde{x}, y) = \Delta_i h(\tilde{x})$.

Пусть $(\mu_1, \ldots, \mu_n,\ \nu)$ — наименьшие неотрицательные вычеты компонент набора $(x_1, \ldots, x_n,\ y)$ по модулю d. Тогда разности $\Delta_i f(\tilde{x}, y)$ зависят только от i и $(\tilde{\mu}, \nu)$ (лишь от i) в том и только том случае, когда разности $\Delta_i h(\tilde{x})$ зависят лишь от i и $\tilde{\mu}$ (только от i). Далее, разности $\Delta_{n+1} f(\tilde{x}, y)$ равны 0 при любых $\tilde{x}$ и y. Таким образом, функции $f(\tilde{x}, y)$ и $h(\tilde{x})$ одновременно сохраняют или не сохраняют (абсолютно сохраняют или не сохраняют) d-разности. □

Следствие 2.1. *Любая линейная функция, любая d-периодическая функция, функция $\delta_d(x)$ и все линейные комбинации указанных функций принадлежат классу $L(d)$.*

Лемма 2.3. *Функция $f(\tilde{x})$ сохраняет d-разности в том и только том случае, когда для всех $\tilde{\mu}$ из E_d^n и всех $\tilde{M}$ из $\mathbb{Z}_+^n$ выполняется соотношение*

$$F(\tilde{\mu} + \tilde{M}d) = f(\tilde{\mu}) + \sum_{i=1}^{n} M_i \Delta_i f(\tilde{\mu}). \tag{2.3}$$

Доказательство. Достаточность условия (2.3) для сохранения функцией d-разностей очевидна. Необходимость докажем индукцией по n. При $n = 1$ равенство (2.3) легко выводится из определения свойства сохранения d-разностей. Осуществим индуктивный переход.

Пусть условие (2.3) выполняется для всех n-местных функций класса $R(d)$. Рассмотрим функцию $f(\tilde{x}^n,\ y)$, сохраняющую d-разности. Фиксируем $(\tilde{\mu}, \nu)$ из E_d^{n+1} и $(\tilde{M},\ N)$ из $\mathbb{Z}_+^{n+1}$. Не ограничивая общности, положим для простоты записи $(\tilde{\mu}, \nu) = \tilde{0}^{n+1}$. Необходимо показать, что

$$f(\tilde{\mu},\ Nd) = f(\tilde{0}, 0) + \sum_{i=1}^{n} M_i \Delta_i f(\tilde{0}, 0) + N \Delta_{n+1} f(\tilde{0}, 0). \tag{2.4}$$

Рассмотрим одноместную функцию $h(y) = f(\tilde{M}d,\ y)$ и n-местную функцию $H(\tilde{x}) = f(\tilde{x}, 0)$. Как уже установлено, $h(Nd) = h(0) + N\Delta h(0)$, т. е.

$$f(\tilde{M}d,\ Nd) = f(\tilde{M}d, 0) + N \Delta_{n+1} f(\tilde{M}d, 0). \tag{2.5}$$

Функция $f(\tilde{x}, y)$ сохраняет d-разности и $\tilde{M}d \equiv \tilde{0} \pmod{d}$, поэтому

$$\Delta_{n+1} f(\tilde{M}d, 0) = \Delta_{n+1} f(\tilde{0}, 0). \tag{2.6}$$

Далее, по предположению индукции для n-местной функции $H(\tilde{x})$ справедливо равенство

$$H(\tilde{M}d) = H(\tilde{0}) + \sum_{i=1}^{n} M_i \Delta_i H(\tilde{0}),$$

эквивалентное соотношению

$$f(\tilde{M}d, 0) = f(\tilde{0}, 0) + \sum_{i=1}^{n} M_i \Delta_i f(\tilde{0}, 0).$$

Подставляя последнее равенство в (2.5) и учитывая (2.6), убеждаемся в справедливости (2.4). □

Следствие 2.2. *Если $d_2 = ed_1$ и функция $f(\tilde{x})$ сохраняет d_1-разности, то она сохраняет и d_2-разности. Если $\Delta'_i f(\tilde{x})$ и $\Delta''_i f(\tilde{x})$ есть ее d_1- и, соответственно, d_2-разности по переменной x_i, то*

$$\Delta''_i f(\tilde{x}) = e\Delta'_i f(\tilde{x}).$$

Это вытекает из формулы (2.3) при $d = d_1, M = e$.

Лемма 2.4. *Если $f \in R(d)$, то все d-разности функции f кратны d.*

Доказательство. Пусть $k = de$. Положим $\tilde{M} = \tilde{\varepsilon}e$. Тогда $\tilde{M}d \equiv \tilde{0} \pmod{k}$, и из (2.3) следует, что разности $\Delta_i f(\tilde{\mu})$ кратны d. Если $\tilde{\mu}$ — наименьшие неотрицательные вычеты компонент набора $\tilde{x}$ по модулю d, то $\Delta_i f(\tilde{x}) = \Delta_i f(\tilde{\mu})$ и разности во всех точках кратны d. □

Следствие 2.3. *Справедливы включения $L(d) \subseteq R(d) \subseteq C(d)$. Оба включения строгие в точности при $d \neq 1, d \neq k$.*

Лемма 2.5. *Пусть $d^2|k$. Тогда произведение функций класса $R(d)$ принадлежит этому классу.*

Доказательство. Пусть $g, h \in R(d), f(\tilde{x}) = g(\tilde{x})h(\tilde{x})$ (переменные всех трех функций считаем одинаковыми в силу леммы 2.2. Покажем, что функция h удовлетворяет условию (2.3). Положим, не ограничивая общности, $\tilde{\mu} = \tilde{0}$. Пусть $y_0 = g(\tilde{0})$, $z_0 = h(\tilde{0})$. Тогда левая часть (2.3) преобразуется так:

$$f(\tilde{M}d) = \left(y_0 + \sum_{i=1}^{n} M_i(y_i - y_0)\right)\left(z_0 + \sum_{i=1}^{n} M_i(z_i - z_0)\right). \tag{2.7}$$

Функции g и h сохраняют сравнение по модулю d, поэтому

$$y_i \equiv y_0,\ z_i \equiv z_0 \pmod{d}, \quad (y_i - y_0)(z_i - z_0) \equiv 0 \pmod{k},$$

и последнее выражение в (2.7) принимает вид

$$y_0 z_0 + \sum_{i=1}^{n} M_i(y_i z_0 + y_0 z_i - 2y_0 z_0).$$

В правой части (2.3) имеем

$$y_0z_0 + \sum_{i=1}^{n} M_i(y_iz_i - y_0z_0).$$

Остается проверить, что $y_iz_0 + y_0z_i - y_0z_0 = y_iz_i$. Это верно, так как

$$y_iz_0 - y_0z_0 + y_0zi - y_iz_i = (y_i - y_0)(z_i - z_0) \equiv 0 \pmod{k}.$$

□

Лемма 2.6. *Функция xy принадлежит классу $R(d)$ в точности при $k|d^2$ и принадлежит классу $L(d)$ в точности при $d = k$.*

Доказательство. Пусть $f(x_1, x_2) = x_1x_2$, $\mu_1, \mu_2 \in E_d$, $M_1, M_2 \in \mathbb{Z}_+$. Тогда

$$\Delta_1(\mu_1 + M_1d, \mu_2 + M_2d) = \mu_2d + M_2d^2, \quad \Delta_2(\mu_1 + M_1d, \mu_2 + M_2d) = \mu_1d + M_1d^2.$$

Следовательно, d-разности не зависят от M_1 и M_2 лишь при условии $k|d^2$. Они не зависят от μ_1, μ_2 только в двух случаях: либо $d = k$, либо μ_1, μ_2 из E_d принимают единственное значение, т. е. $d = 1$. В последнем случае 1^2 не кратно k и $xy \notin R(1)$. Однако всегда $L(d) \subseteq R(d)$, поэтому $xy \notin L(1)$. □

Утверждение 2.2. *Пусть $d \neq k$. Тогда*:

1) *функция x^2 принадлежит классу $R(d)$ в точности при $k|d^2$ и при $k = 2d$,*

2) *функция x^2 принадлежит классу $L(d)$ в точности при $k = 2d$.*

Доказательство. Пусть $f(x) = x^2$, $\mu \in E_d$, $M \in \mathcal{Z}_+$. Тогда разности $\Delta f(\mu + Md) = 2\mu d + 2Md^2 + d^2$ не зависят от M только в двух случаях: $k|d^2$ или $k|2d$. В последнем из них разности не зависят и от μ. Поскольку $d|k$ и $d \neq k$, условие $k|2d$ эквивалентно $k = 2d$. □

Замечание 2.1. Если $k = 2d$ и d четно, то функция x^2 является d-периодической.

При $k = p^m$, $m \geq 2$, А. В. Кузнецовым построен замкнутый класс K, $Polyn \subseteq K \subset M(p^m)$ [86, §18], он состоит из всех функций с условием

$$f(\tilde{x} + \tilde{l}p) \equiv c_0(\tilde{x}) + c_1(\tilde{x})l_1p + \cdots + c_n(\tilde{x})l_np \pmod{p^2}.$$

Утверждение 2.3. *При $k = p^2$ и только при таком условии имеет место равенство $K = R(p)$.*

Доказательство. Если $k = p^2$, то равенство $K = R(p)$ следует из лемм 2.3 и 2.4.

Пусть теперь $p^3|k$. А. В. Кузнецовым указана функция $f(x_1, x_2)$ класса K (при всех $k = p^m$):

$$f(x_1 + l_1p,\ x_2 + l_2p) = l_1l_2p.$$

Покажем, что $f \in K \setminus R(p)$.

Пример 2.2. При $k = 2^3$ рассмотрим ее 2-сеточное ограничение $f^{00}(x_1, x_2)$:

x_1 / x_2	0	2	4	6
0	0	0	0	0
2	0	2	4	6
4	0	4	0	4
6	0	6	4	2

Легко видеть, что $f(x_1, x_2) \notin R(2)$. □

Лемма 2.7. *Пусть функция $g(\tilde{x})$ является d-периодической, и пусть $f_1(\tilde{x}), \dots f_n(\tilde{x}) \in C(d)$. Тогда $h(\tilde{x}) = g(f_1(\tilde{x}), \dots f_n(\tilde{x})) \in L(d)$.*

Нетрудно проверить, что функция h является d-периодической и, следовательно, абсолютно сохраняет d-разности.

2.2 Замкнутость класса $L(d)$. Каноническая формула, базис

Лемма 2.8. *Пусть* $A = \{1,\ x + y,\ g_d(x, y)\}$, $B = \{1,\ x + y,\ xy,\ g_d(x, y)\}$. *Тогда* $[A] \subseteq L(d)$, *а если* $k|d^2$, *то* $[B] \subseteq R(d)$.

Доказательство. Применим индукцию по сложности формулы над системой A (над B), задающей функцию из $[A]$ (из $[B]$).

Если $f \in A$ ($f \in B$), то $f \in L(d)$ ($f \in R(d)$) на основании примеров 2.1, следствия 2.1 и леммы 2.6.

Пусть все функции из $[A]$ (из $[B]$), реализуемые формулами сложности не более l, принадлежат $L(d)$ (принадлежат $R(d)$) и функция f реализуется формулой сложности $l + 1$ над соответствующей системой. Тогда $f = f_0(f_1, \dots, f_m)$, где $f_0 \in A$ ($f_0 \in B$), а $f_1, \dots, f_m$ — функции из $[A]$ (из $[B]$), представленные формулами сложности не выше l. В силу леммы 2.2 можно считать, что все функции зависят от одних и тех же переменных $\tilde{x}^n$, при этом $m = n$. Применение лемм 2.1, 2.5, 2.7 завершает индуктивный переход. □

Утверждение 2.4. *Класс $L(d)$ состоит в точности из всех функций вида*

$$f(\tilde{x}) = l(\tilde{x}) + G_d(\tilde{x}) + \sum_{i=1}^{n} a_i \delta_d(x_i),\ a_i \in E_k. \tag{2.8}$$

Доказательство. Функция вида (2.8) принадлежит $L(d)$ в силу следствия 1.

Обратно: пусть $f(\tilde{x}) \in C(d)$. Вычтем из f линейную часть, а затем из результата вычтем d-периодическую часть. Получим функцию $h(\tilde{x})$ со следующими свойствами:

(R1) $h(\tilde{x}) \in L(d)$;

(R2) если $\tilde{x} \in E_d^n$, то $h(\tilde{x}) = 0$;

(R3) функция $h(\tilde{x})$ кратна d (так как сохраняет сравнение по модулю d).

Функция h сохраняет d-разности, для нее выполняется формула (2.3), которая с учетом свойства (R2) примет вид

$$h(\tilde{\mu} + \tilde{M}d) = \sum_{i=1}^{n} M_i \Delta_i h(\tilde{\mu}). \tag{2.9}$$

Пусть $\tilde{x} = \tilde{\mu} + \tilde{M}d$, где $\tilde{\mu}$ — наименьшие неотрицательные вычеты компонент набора $\tilde{x}$ по модулю d. Тогда для $i = 1, \ldots, n$ получаем $M_i = (x_i - \mu_i)/d = \lfloor x_i/d \rfloor$. В силу леммы 2.4 имеем $\Delta_i h(\tilde{\mu}) = a_i d$, поэтому $M_i \Delta_i h(\tilde{\mu}) \lfloor x_i/d \rfloor a_i d = a_i \delta_d(x_i)$, справедливость представления (2.8) установлена. □

Замечание 2.2. Функция $\delta_d(x)$ есть линейная комбинация линейных и d-периодических:

$$\delta_1(x) = x; \quad \delta_2(x) = -1 + x + g_2(x);$$

если $d > 2$, то

$$\delta_d(x) = -1 + x + g_d(x) - \sum_{i=2}^{d-1} (i-2) g_d(x-i).$$

Таким образом, формулу (2.8) можно упростить, а *класс $L(d)$ состоит в точности из всех функций вида*

$$f(\tilde{x}) = l(\tilde{x}) + G_d(\tilde{x}).$$

Следствие 2.4. *Класс $L(d)$ замкнут. Система функций $\{x + y,\ g_d(x, y)\}$ является его базисом. При $d \neq 2$ функцию $g_d(x, y)$ в ней можно заменить на $g_d(x)$.*

2.3 Ограничение функции на сетке с шагом d

Пусть $d|k$, $f(\tilde{x}) \in P_k$, $\tilde{\mu} \in E_d^n$. Функцию

$$f^{\tilde{\mu}}(\tilde{x}) = f(\tilde{x}) g_d(\tilde{x} - \tilde{\mu}) = \begin{cases} f(\tilde{x}), & \tilde{x} \equiv \tilde{\mu} \pmod{d}, \\ 0, & \tilde{x} \not\equiv \tilde{\mu} \pmod{d}, \end{cases}$$

назовем *d-сеточным ограничением функции f.*

Под *d-разностями d-сеточного ограничения* $f^{\tilde{\mu}}(\tilde{x})$ будем иметь в виду d-разности функции $f(\tilde{x})$ только в точках $\tilde{x} \equiv \tilde{\mu} \pmod{d}$.

Легко проверить следующие факты.

Лемма 2.9. *Справедливо представление*

$$f(\tilde{x}) = \sum_{\tilde{\mu} \in E_d^n} f^{\tilde{\mu}}(\tilde{x}).$$

Условия $f \in R(d)$ *и* $\forall \tilde{\mu} \in E_d^n \ \left(f^{\tilde{\mu}} \in R(d)\right)$ *равносильны.*
Ограничение $f^{\tilde{\mu}}$ *функции* f *можно получить как* $f^{\tilde{\mu}}(\tilde{x}) = \chi_{d,1}(f(\tilde{x}),\ \tilde{x} - \tilde{\mu})$.

2.4 Замкнутость класса $R(d)$. Каноническая формула, базисы

Утверждение 2.5. *Класс* $R(d)$ *состоит в точности из всех функций вида*

$$f(\tilde{x}) = l(\tilde{x}) + G_d(\tilde{x}) + H_d(\tilde{x}), \tag{2.10}$$

где

$$H_d(\tilde{x}) = \sum_{\tilde{\mu} \in E_d^n} \sum_{i=1}^{n} a_i(\tilde{\mu}) \chi_{d,i}(\tilde{x} - \tilde{\mu}),\ a_i(\tilde{\mu}) \in E_k. \tag{2.11}$$

Доказательство. Так же, как в примере 2.1, нетрудно видеть, что для любого набора констант $\tilde{c} \in E_k^n$ функции $\chi_{d,i}(\tilde{x} + \tilde{c})$ сохраняют d-разности. Тогда и функция $H_d(\tilde{x})$, и вся правая часть в (2.10) принадлежат $R(d)$ в силу леммы 2.1 и следствия 2.1.

Обратно: пусть $f(\tilde{x}) \in R(d)$. Вычтем из f линейную часть, а затем из результата вычтем d-периодическую часть. Получим функцию $h(\tilde{x})$ со свойствами (R1)–(R3). Докажем равенство $h(\tilde{x}) = H_d(\tilde{x})$, эквивалентное системе соотношений

$$h^{\tilde{\mu}}(\tilde{x}) = H_d^{\tilde{\mu}}(\tilde{x}) \tag{2.12}$$

для всех $\tilde{\mu} \in E_d^n$.

Если $\tilde{x} \not\equiv \tilde{\mu} \pmod{d}$, то соотношение (2.12) верно, обе его части равны 0. Пусть $\tilde{x} \equiv \tilde{\mu} \pmod{d}$. Функция $h^{\tilde{\mu}}$ сохраняет d-разности, для нее выполняется формула (2.3), которая с учетом свойства (R2) примет вид (2.9). Пусть $\tilde{x} = \tilde{\mu} + \tilde{M}d$, где $\tilde{\mu}$ — наименьшие неотрицательные вычеты компонент набора $\tilde{x}$ по модулю d. Тогда для $i = 1, \ldots, n$ получаем $M_i = (x_i - \mu_i)/d$. В силу леммы 2.4 имеем $\Delta_i h(\tilde{\mu}) = a_i d$. Рассмотрим одно слагаемое в правой части (2.9):

$$\frac{x_i - \mu_i}{d}(h(\tilde{\mu} + \tilde{\varepsilon}d) - 0) = \frac{x_i - \mu_i}{d} \cdot a_i d = a_i(x_i - \mu_i) g_d(\tilde{x} - \tilde{\mu}) = a_i \chi_{d,i}(\tilde{x} - \tilde{\mu}).$$

Равенства (2.12) и $h(\tilde{x}) = H_d(\tilde{x})$ доказаны, функции класса $R(d)$ представляются в виде (2.10). □

Примем более короткое обозначение для одноместной функции

$$\chi_{d,1}(x) = \chi_d(x).$$

Утверждение 2.6. *Справедливы равенства*

$$\chi_{d,i}(x_1, \ldots, x_i, \ldots, x_n) = \chi_{d,1}(x_i, \ldots, x_1, \ldots, x_n),\ i = 2, \ldots, n;$$

$$\chi_{d,1}^{(n+1)}(\tilde{x}, y) = \chi_d(\chi_{d,1}^{(n)}(\tilde{x}) + y) - \chi_d(y),\ n = 1, 2, \ldots.$$

Эти соотношения проверяются непосредственно.

Лемма 2.10. *Пусть* $f(\tilde{x}) \in R(d),\ F(\tilde{x}) = \chi_d(f(\tilde{x}))$. *Тогда* $F(\tilde{x}) \in R(d)$.

Доказательство. Пусть $\tilde{\mu}$ — наименьшие неотрицательные вычеты компонент набора $\tilde{x}$ по модулю d. Фиксируем $i, 1 \le i \le n$. Функция f сохраняет сравнение по модулю d, поэтому $f(\tilde{x}) \equiv f(\tilde{\mu}) \pmod{d}$ и значение $g_d(f(\tilde{x})) = g_d(f(\tilde{\mu})) = c(\tilde{\mu})$ зависит только от $\tilde{\mu}$.

Пусть $\tilde{y} = \tilde{x} + \tilde{\varepsilon}_i d$, тогда $g_d(f(\tilde{y})) = c(\tilde{\mu})$ и значение разности

$$\Delta_i F(\tilde{x}) = F(\tilde{y}) - F(\tilde{x}) = f(\tilde{y}) g_d(f(\tilde{y})) - f(\tilde{x}) g_d(f(\tilde{x})) =$$

$$= (f(\tilde{y}) - f(\tilde{x})) c(\tilde{\mu}) = \Delta_i f(\tilde{x}) c(\tilde{\mu}) = \Delta_i f(\tilde{\mu}) c(\tilde{\mu})$$

зависит только от $\tilde{\mu}$. □

Утверждение 2.7. *Класс* $R(d)$ *замкнут. Если* $d \ne 1, d \ne k$, *то система функций* $\{x + y,\ g_d(x, y),\ \chi_d(x)\}$ *его является базисом. При* $d \ne 2$ *функцию* $g_d(x, y)$ *можно заменить на* $g_d(x)$.

Доказательство. Замкнутость класса $R(d)$ и полнота указанной системы в нем следуют из лемм 2.1, 2.7, 2.9, утверждений 2.6 и 2.7. Покажем, что данная система является базисом.

Подсистема $\{g_d(x, y),\ \chi_d(x)\}$ не полна в $R(d)$, она сохраняет множество, состоящее из 1 и всех чисел, кратных d.

Подсистема $\{x + y,\ \chi_d(x)\}$ сохраняет множество чисел, кратных d.

Подсистема $\{x + y,\ g_d(x, y)\}$ содержится в подклассе $L(d)$. □

Аналогично выводится следующий результат.

Утверждение 2.8. *Если* $k | d^2$, *то система функций* $\{x + y,\ xy, g_d(x)\}$ *является базисом в классе* $R(d)$.

2.5 Решетка классов $L(d)$

Утверждение 2.9. *Следующие условия эквивалентны*:

1) $d_1|d_2$;
2) $R(d_1) \subseteq R(d_2)$;
3) $L(d_1) \subseteq L(d_2)$.

Доказательство. Если выполнено условие 1), то имеют место также 2) и 3) на основании следствия 2.

Пусть теперь выполнено условие 2) или 3). Рассмотрим функцию $f(x) = g_{d_1}(x)$ класса $L(d_1)$. Пусть $y = f(d_2)$. Из сохранения d_2-разностей для всех целых M получаем $f(Md_2) = f(0) + M(f(d_2) - f(0)) = 1 + M(y-1)$.

Если $k = d_2e_2$, то $1 = f(0) = f(k) = f(e_2d_2) = 1 + e_2(y-1)$, откуда $e_2(y-1) \equiv 0 \pmod{d_2e_2}$, следовательно, $y = g_{d_1}(d_2) = 1$ и $d_1|d_2$. □

Утверждение 2.10. *Пусть* $d_1|k, d_2|k$, $d_0 = НОД(d_1, d_2), d_3 = НОК(d_1, d_2)$. *Тогда*

$$L(d_1) \cap L(d_2) = L(d_0), \quad [L(d_1) \cup L(d_2)] = L(d_3).$$

Доказательство. Имеем $d_0|d_1, d_0|d_2$ и, по утверждению 2.9, $L(d_0) \subseteq L(d_1) \cap L(d_2)$.

Пусть $f \in L(d_1) \cap L(d_2)$. Покажем, что $f \in L(d_0)$. В силу леммы 2.3 последнее равносильно условию

$$f(\tilde{x} + \tilde{M}d_0) = f(\tilde{x}) + \sum_{i=1}^{n} M_i\Delta_i,$$

где Δ_i — некоторые постоянные.

Имеем $d_0 = \text{НОД}(d_1, d_2)$, поэтому $d_0 = Ad_1 + Bd_2$ для некоторых целых A, B. При этом $f \in L(ad_1) \cap L(Bd_2)$. Из абсолютного сохранения Ad_1-разностей следует, что

$$f(\tilde{x} + \tilde{M}Bd_2 + \tilde{M}Ad_1) = f(\tilde{x} + \tilde{M}Bd_2) + \sum_{i=1}^{n} M_i\Delta'_i,$$

где Δ'_i — постоянные. Далее, из абсолютного сохранения Bd_2-разностей следует, что

$$f(\tilde{x} + \tilde{M}Bd_2) = f(\tilde{x}) + \sum_{i=1}^{n} M_i\Delta''_i,$$

где Δ''_i — постоянные. Таким образом,

$$f(\tilde{x} + \tilde{M}d_0) = f(\tilde{x} + \tilde{M}(Ad_1 + Bd_2)) = f(\tilde{x}) + \sum_{i=1}^{n} M_i(\Delta'_i + \Delta''_i).$$

Требуемое включение и равенство $L(d_1) \cap L(d_2) = L(d_0)$ доказаны.

Аналогично, $d_1|d_3, d_2|d_3$ и, по утверждению 2.9, $L(d_1) \cup L(d_2) \subseteq L(d_3)$. Тогда, в силу замкнутости класса $L(d_3)$,

$$[L(d_1) \cup L(d_2)] \subseteq L(d_3).$$

Для доказательства обратного включения учтем, что

$$L(d_i) = [1,\ x+y,\ g_{d_i}(x,y)],\ i = 1,2,3.$$

При этом

$$g_{d_3}(\tilde{x}) = g_{d_1}(\tilde{x},\ 1 - g_{d_2}(\tilde{x})) \in [L(d_1) \cup L(d_2)]. \tag{2.13}$$

□

2.6 Решетка классов $R(d)$

Лемма 2.11. *Пусть* $d_1|k, d_2|k, d_0 = НОД(d_1, d_2)$, $K = C(d_0, d_1, d_2)$, $f(\tilde{x}) \in K$. *Тогда функцию* f *можно однозначным образом представить в виде*

$$f(\tilde{x}) = f_0(\tilde{x}) + f_1(\tilde{x}) + f_2(\tilde{x}), \tag{2.14}$$

где $f_i(\tilde{x})$ *— это* d_i*-периодические функции класса* K, $(i = 0,1,2)$, *причем функция* f_1 *кратна* d_2, *функция* f_2 *кратна* d_1.

Доказательство.

1. Пусть $\tilde{\mu}$ — наименьшие неотрицательные вычеты компонент набора $\tilde{x}$ по модулю d_0.

2. Определим функцию f_0 условием $f_0(\tilde{x}) = f(\tilde{\mu})$.

3. Положим $F(\tilde{x}) = f(\tilde{x}) - f_0(\tilde{x})$. Очевидно, $F(\tilde{x}) = 0$, если $\tilde{x} \in E^n_{d_0}$.

4. Определим функции f_1, f_2 следующими условиями:

$$f_1(\tilde{x}) = F(\tilde{y}'),\ f_2(\tilde{x}) = F(\tilde{y}''),$$

где

$$\tilde{y}' \equiv \tilde{x} \pmod{d_1},\ \tilde{y}' \equiv \tilde{\mu} \pmod{d_2},$$
$$\tilde{y}'' \equiv \tilde{x} \pmod{d_2},\ \tilde{y}'' \equiv \tilde{\mu} \pmod{d_1}.$$

Такие наборы $\tilde{y}', \tilde{y}''$ в E^n_k по данному набору $\tilde{x}$ определены однозначно.

5. Тогда равенство (2.14) эквивалентно сравнениям

$$F(\tilde{x}) \equiv F(\tilde{y}') + F(\tilde{y}'') \pmod{d_j},\ j = 1,2.$$

Они проверяются аналогично похожим условиям в доказательстве лемм 1.4 и 1.5. Таким же образом проверяется, что функции f_0, f_1, f_2 удовлетворяют всем указанным требованиям. □

Лемма 2.12. *Пусть d_0, d_1, d_2 — делители k, $d_0 = (d_1, d_2)$, функция f является d_1-периодической. Тогда условия $f \in R(d_2)$ и $f \in R(d_0)$ эквивалентны.*

Доказательство. Имеем $d_0|d_1, d_0|d_2$, $R(d_0) \subseteq R(d_2)$.

Пусть $f(\tilde{x}) \in R(d_2)$, $\tilde{\mu} \in E^n_{d_0}, \tilde{M} \in \mathbb{Z}^n$. Найдем целое c такое, что $cd_2 \equiv d_0 \pmod{d_1}$. В силу d_1-периодичности имеем

$$f(\tilde{\mu} + \tilde{M}cd_2) = f(\tilde{\mu} + \tilde{M}d_0). \tag{2.15}$$

Далее, из условия $f \in R(cd_2)$ по лемме 2.3 имеем

$$f(\tilde{\mu} + \tilde{M}cd_2) = f(\tilde{\mu}) + \sum_{i=1} nM_i D_i f(\tilde{\mu}), \tag{2.16}$$

где $D_i f(\tilde{\mu})$ — это cd_2-разности. Полагая в (2.15) $\tilde{M} = \varepsilon_i$, убеждаемся, что величины $D_i f(\tilde{\mu})$ являются d_0-разностями функции f в точке $\tilde{\mu}$. Тогда (2.16) преобразуется в равенство (2.3) при $d = d_0$, функция f сохраняет d_0-разности. □

Утверждение 2.11. *Пусть $d_1|k, d_2|k$, $d_0 = НОД(d_1, d_2)$, $d_3 = НОК(d_1, d_2)$. Тогда*

$$R(d_1) \cap R(d_2) = R(d_0), \quad [R(d_1) \cup R(d_2)] = R(d_3).$$

Доказательство. Докажем первое равенство. Включение $R(d_0) \subseteq R(d_1) \cap R(d_2)$ верно, так как $d_0|d_1$ и $d_0|d_2$. Пусть теперь $f \in R(d_1) \cap R(d_2)$. Тогда $f \in C(d_0, d_1, d_2)$. Рассмотрим два случая.

1. Пусть $\text{НОК}(d_1, d_2) = k$. Тогда применим лемму 2.11 и представим f в виде (2.14), откуда $f_1(\tilde{x}) = f(\tilde{x}) - f_0(\tilde{x}) - f_2(\tilde{x})$. Функции f_0 и f_2 сохраняют d_2-разности в силу d_2-периодичности. Тогда и $f_1 \in R(d_2)$, а в силу леммы 2.12 получаем $f_2 \in R(d_0)$. Аналогично доказывается, что $f_1 \in R(d_0)$. Тогда из (2.14) по лемме 2.8 следует, что $f \in R(d_0)$.

2. Пусть $\text{НОК}(d_1, d_2) < k$. Тогда $k = abcd_0, d_1 = ad_0, d_2 = bd_0$, $\text{НОД}(a, b) = 1$. Сведем этот случай к предыдущему. Пусть $p_1, \ldots, p_s$, $q_1, \ldots, q_t$, $r_1, \ldots, r_m$ — попарно различные простые и

$$a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \qquad c = p_1^{\gamma_1} \cdots p_s^{\gamma_s} q_1^{\delta_1} \cdots q_t^{\delta_t} r_1^{\varepsilon_1} \cdots r_m^{\varepsilon_m},$$

$$b = q_1^{\beta_1} \cdots q_t^{\beta_t}, \qquad d_0 = p_1^{\pi_1} \cdots p_s^{\pi_s} q_1^{\kappa_1} \cdots q_t^{\kappa_t} r_1^{\rho_1} \cdots r_m^{\rho_m} \cdot e,$$

где $\text{НОД}(e,\ p_1 \cdots p_s q_1 \cdots q_t r_1 \cdots r_m) = 1$. Тогда

$$k = \prod_{i=1}^{s} p_i^{\alpha_i+\gamma_i+\pi_i} \prod_{j=1}^{t} q_j^{\beta_j+\delta_j+\kappa_j} \prod_{l=1}^{m} r_l^{\varepsilon_l+\rho_l},$$

$$d_1 = e \cdot \prod_{i=1}^{s} p_i^{\alpha_i+\pi_i} \prod_{j=1}^{t} q_j^{\kappa_j} \prod_{l=1}^{m} r_l^{\rho_l}, \qquad d_2 = e \cdot \prod_{i=1}^{s} p_i^{\pi_i} \prod_{j=1}^{t} q_j^{\beta_j+\kappa_j} \prod_{l=1}^{m} r_l^{\rho_l}.$$

Положим

$$d'_1 = e \cdot \prod_{i=1}^{s} p_i^{\alpha_i+\gamma_i+\pi_i} \prod_{j=1}^{t} q_j^{\beta_j+\delta_j+\kappa_j} \prod_{l=1}^{m} r_l^{\rho_l}, \qquad d'_2 = e \cdot \prod_{i=1}^{s} p_i^{\pi_i} \prod_{j=1}^{t} q_j^{\kappa_j} \prod_{l=1}^{m} r_l^{\varepsilon_l+\rho_l}.$$

При этом $d_1|d'_1, d_2|d'_2, \text{НОД}(d'_1, d'_2) = d_0, \text{НОК}(d'_1, d'_2) = k$. Тогда $f \in R(d'_1, d'_2)$ и мы пришли к случаю 1.

Первое равенство утверждения доказано. Докажем второе.

Включение $[R(d_1) \cup R(d_2)] \subseteq R(d_3)$ следует из условий $d_1|d_3, d_2|d_3$. Докажем обратное включение. Известно, что

$$R(d_3) = [x + y,\ g_{d_3}(x, y),\ \chi_{d_3}(x)],$$

$$[R(d_1) \cup R(d_2)] = [x + y,\ g_{d_1}(x, y),\ g_{d_2}(x, y),\ \chi_{d_1}(x),\ \chi_{d_2}(x)].$$

Легко проверить равенства

$$\chi_{d_3}(x) = \chi^{(2)}_{d_1,1}(x,\ 1 - g_{d_2}(x)), \quad g_{d_3}(x, y) = g^{(3)}_{d_1}(x, y,\ 1 - g_{d_2}(x, y)).$$

Из этих выражений, формулы (2.13) и свойств функций $g_d(\tilde{x})$, $\chi_{d,i}(\tilde{x})$ следует, что $R(d_3) \subseteq [R(d_1) \cup R(d_2)]$. □

Из утверждений 2.10 и 2.11 непосредственно следует более общий результат.

Теорема 2.1. *Классы $R(d)$ образуют решетку по включению, изоморфную решетке делителей d числа k. Такую же решетку образуют классы $L(d)$.*

2.7 Классы $R(d)$ и $C(d)$

Пусть d — собственный делитель числа k. Тогда $R(d) \subset C(d)$, причем

$$R(d) = [x + y,\ g_d(x, y),\ \chi_d(x)], \quad C(d) = [x + y,\ g_d(x, y),\ dj(x, y)],$$

и если $k \neq 2d$, то функцию $dj(x, y)$ можно заменить на $dj(x)$. Найдем условия, при которых класс $R(d)$ является предполным в $C(d)$.

Утверждение 2.12. *Если $d|k$, то все одноместные функции класса $C(d)$ принадлежат $R(d)$ в точности при $k = 2d$ и при $k = d$.*

Нетрудно проверить, что в точности при этих условиях функция $dj(x)$ сохраняет d-разности.

Следствие 2.5. *Если d — собственный делитель числа k, то система функций $\{x + y,\ g_d(x, y),\ dj(x)\}$ образует базис класса $C(d)$ в точности при $k \neq 2d$.*

Лемма 2.13. *Пусть $n \geq 3$ и пусть n-местная функция f не сохраняет d-разности. Тогда подстановкой констант на места переменных функции f можно получить одноместную или двухместную функцию, также не сохраняющую d-разности.*

Доказательство. Если существует набор из $n-1$ констант, при подстановке которых в функцию f получается одноместная функция, не сохраняющая d-разности, то утверждение леммы выполнено.

Предположим противное: все одноместные функции, получающиеся подстановкой в f констант, сохраняют d-разности. По условию $f \notin R(d)$, поэтому найдется номер i (без ограничения общности полагаем $i = n$) и набор $\tilde{\mu} \in E_d^n$ такие, что для некоторых $\tilde{a}^{n-1}, \tilde{b}^{n-1}$ с условием $\tilde{a}^{n-1} \equiv \tilde{b}^{n-1} \equiv \tilde{\mu}^{n-1} \pmod{d}$ одноместные функции $h_a(x) = f(\tilde{a}^{n-1}, x)$, $h_b(x) = f(\tilde{b}^{n-1}, x)$ имеют в точках $x \equiv \mu_n \pmod{d}$ неравные d-разности.

Покажем, что существуют такие наборы $\tilde{a}^{n-1}$ и $\tilde{b}^{n-1}$, имеющие общую компоненту. Допустим противное: все наборы, при подстановке которых в f получаются одноместные функции с неравными d-разностями в точках $x \equiv \mu_n \pmod{d}$, не имеют общих компонент. Рассмотрим пару таких наборов $\tilde{b}^{n-1}$, $\tilde{c}^{n-1}$ и набор $\tilde{a}^{n-1}$, в котором $a_1 = b_1, \ldots, a_{n-2} = b_{n-2}$, $a_{n-1} = c_{n-1}$.

Наборы $\tilde{a}^{n-1}$ и $\tilde{c}^{n-1}$ имеют общую компоненту, поэтому функция $h_a(x)$ имеет в точках $x \equiv \mu_n \pmod{d}$ те же d-разности, что и функция $h_c(x)$, т. е. они отличны от d-разностей функции $h_b(x)$. Мы указали пару наборов $\tilde{a}^{n-1}$ и $\tilde{b}^{n-1}$ с общими компонентами и обладающих тем свойством, что при подстановке их в f получаются одноместные функции с неравными d-разностями.

Подставляя в f константы, общие для указанных наборов, получим функцию меньшего числа переменных, также не сохраняющую d-разности. С ней поступим аналогично и продолжаем процесс, пока не придем к двухместной функции. □

Лемма 2.14. *Пусть $d|k$, $k \neq 2d$, $k \neq d$. Пусть при этом $n \geq 2$ и n-местная функция f не сохраняет d-разности. Тогда подстановкой констант на места переменных функции f можно получить одноместную функцию, также не сохраняющую d-разности.*

Это усиление леммы 1.10. Доказательство повторяет вывод той леммы с заменой всюду оборота "1-разности" на "d-разности".

Теорема 2.2. *Если d — собственный делитель числа k, то класс $R(d)$ является предполным в $C(d)$ в точности при $k = pd$.*

Доказательство. Пусть $k = abd, a > 1, b > 1$. Тогда

$$R(d) = R(d) \cap R(ad) \subset C(d, ad) \subset C(d).$$

Пусть теперь $k = pd$, $f(x_1, \ldots, x_n) \in C(d) \setminus R(d)$. Покажем, что $R(d) \cup \{f\}] = C(d)$. Возможны два случая.

Случай 1. $k = 2d$. Тогда, в соответствии с утверждением 2.12, $n \geq 2$. Построим функцию $dj(x, y)$. Если $n \geq 3$, то применим лемму 2.13 и получим двухместную функцию $h(x, y)$ класса $C(d) \setminus R(d)$. Можем считать, что она кратна d, иначе вычтем из $h(x, y)$ соответствующую d-периодическую функцию (она принадлежит $R(d)$). Фиксируем $\mu, \nu \in E_d$, для которых $H(x, y) = h^{\mu,\nu}(x, y)$ не сохраняет d-разности, при этом, как было отмечено в разделе 2.3, $H(x, y) \in [R(d) \cup \{f\}]$. Не ограничивая общности, полагаем $\mu = \nu = 0$. Пусть также $H(0, 0) = 0$, иначе вычтем из $H(x, y)$ соответствующую d-периодическую функцию. Положим $S = \{0, d\}$ и рассмотрим значения функции H на множестве S^2, все они принадлежат S. Из условия $H \notin R(d)$ следует, что значение d принимается функцией H на S^2 нечетное число раз. Если оно принимается трижды, то $dj(x, y) = dg_d(x, y) - H(x, y)$. Если же оно принимается лишь один раз — скажем, $d = H(a, b)$, $a, b \in S$, — то $dj(x, y) = H(x + a, y + b)$. Итак, $[R(d) \cup \{f\}]$ содержит функцию $dj(x, y)$ и весь класс $C(d)$.

Случай 2. $k \neq 2d$. Достаточно показать, что $dj(x) \in [R(d) \cup \{f\}]$.

Применяя леммы 2.13, 2.14, из функции f получим (если требуется) одноместную функцию $h(x)$ класса $C(d) \setminus R(d)$. Ее сделаем кратной d вычитанием d-периодической функции (последняя принадлежит $R(d)$). Фиксируем μ из E_d, для которого d-сеточное ограничение $H(x) = h^{\mu}(x) = \chi_{d,1}(h(x), x - \mu)$ не сохраняет d-разности. Без ограниченининия общности полагаем $\mu = 0$. Пусть $y_i = H(id)$ при $i = 0, \ldots, p - 1$. Все значения y_i сравнимы между собой по модулю d, так как $H \in C(d)$. Будем применять следующие преобразования функции $H(x)$ с помощью элементов класса $R(d)$.

П1. Вычитание d-периодической функции.

П2. Линейная замена переменных.

П3. Умножение функции на константу.

Полагаем $y_0 = 0$, иначе применим преобразование П1. Пусть

$$\sigma(H) = y_1 + \cdots + y_{p-1}$$

(сумма в кольце целых чисел), и пусть $W(H)$ (*вес функции* H) — количество ненулевых значений среди $y_1, \ldots, y_{p-1}$. Из условия $H \notin R(d)$ следует, что $W(H) \geq 1$ и $y_t \neq 0$ при некотором t. Можно считать, что $y_t = t$, иначе применим преобразование П3. Далее рассмотрим четыре случая.

1. Пусть $W(H) = 1$. Тогда $dj(x)$ строится из $H(x)$ с помощью преобразований П2 и П3.

2. Пусть $W(H) > 1$, $\sigma(H) \not\equiv 0 \pmod{k}$. Рассмотрим функцию

$$F(x) = H(x) + H(2x) + \cdots + H((p - 1)x).$$

Имеем $F^0(x) = F(x)$, $F(0) = 0$, $F(id) = \sigma(H) = ad$, где НОД$(a, p) = 1$ $(i = 1, \ldots, p-1)$. Тогда

$$dj(x) = dg_d(x) - cF(x), \text{ где } c = a^{-1} \pmod{p}.$$

3. Пусть $1 < W(H) \leq p-2$, $\sigma(H) \equiv 0 \pmod{k}$. Будем последовательно уменьшать вес функции, пока не придем к одному из случаев 1 или 2. Возможны следующие подслучаи.

3.1. Имеется такое y_j, что $H(y_j) \neq y_j$. Пусть $F(x) = H(x) - H(H(x))$. Функция F сохраняет нули функции H (если $H(x_0) = 0$, то и $F(x_0) = 0$). Кроме того, $F(td) = 0$ и $F(jd) \neq 0$. Значит, $1 \leq W(F) < W(H)$.

3.2. Для каждого i выполнено $H(y_i) = y_i$, и среди ненулевых y_i есть одинаковые. Можно считать, что одинаковые значения y_{i_1} и y_{i_2} равны d, иначе применим преобразование П3. Пусть $i_2 - i_1 = l$, $l \in \{1, \ldots, p-1\}$. Положим $j = i_1 l^{-1} \pmod{p}$, $F(x) = H(lx)$. При этом для некоторого r, $r \geq 2$, получаем

$$F(jd) = F((j+1)d) = \cdots = F((j+r-1)d) = d, \quad F((j+r)d) \neq d.$$

Пусть $G(x) = F(x + F(x) - F(x)$. Функция F принимает те же значения, что и функция H, но в других точках (если $l \neq 1$), поэтому $W(F) = W(H)$. Далее, если $F(x_0) = 0$, то $G(x_0) = 0$. Кроме того, $G(jd) = 0$ и $G((j+r-1)d) \neq 0$. Следовательно, $1 \leq W(G) < W(H)$.

3.3. Для всех i выполнено $H(y_i) = y_i$ и среди ненулевых значений y_i нет одинаковых. Тогда при всех i из E_p либо $y_i = 0$, либо $y_i = id$. Из условий $k|\sigma(H)$, $1 \leq W(H) \leq p-2$ следует, что функция H не может принимать все $W(H)$ ненулевых значений в точках $x = d, 2d, \ldots, W(H)d$. Значит, найдется такое l, $l \geq 2$, что $y_l = ld \neq 0$, $y_{l-1} = 0$. При этом также найдется j, $j > l$, для которого $y_j = jd \neq 0$. Пусть $c = j^{-1} \pmod{p}$, $F(x) = cH(x + (l-1)d)$. Тогда $F(0) = 0$, $F((j-l+1)d) = d$, $F(d) \neq d$. Рассматривая вместо $H(x)$ функцию $F(x)$, приходим к случаю 3.1.

4. Пусть $k|\sigma(H)$, $W(H) = p-1$. Для функции $F(x) = \chi_d(x) - H(x)$ получаем $F(0) = F(td) = 0$. Из условия $H \notin R(d)$ следует, что $F(jd) \neq 0$ при некотором j. Случай сведен к одному из предыдущих. □

2.8 Классы $L(d)$ и $R(d)$

Пусть d — собственный делитель числа k. Тогда $L(d) \subset R(d)$, причем

$$L(d) = [x + y,\ g_d(x, y)], \quad R(d) = [x + y,\ g_d(x, y),\ \chi_d(x)],$$

и если $d \neq 2$, то функцию $g_d(x, y)$ можно заменить на $g_d(x)$. Найдем условия, при которых класс $L(d)$ является предполным в $R(d)$.

Лемма 2.15. *Пусть $n \geq 1$, и пусть $(n+1)$-местная функция $f(\tilde{x}^n,\ y)$ не сохраняет d-разности абсолютно. Тогда подстановкой констант и отождествлением переменных функции f можно получить одноместную функцию, также не сохраняющую d-разности абсолютно.*

Доказательство. Без ограничения общности полагаем, что не сохраняются абсолютно d-разности по переменной y, т. е. величины $\Delta_{n+1}f(\tilde{x}, y)$ зависят от $\tilde{x}$ и y. Рассмотрим эти величины как функции переменных $\tilde{x}, y$.

Если $\Delta_{n+1}f(\tilde{x}, y)$ зависит существенно от y, то требуемая одноместная функция получается подстановкой в функцию $f(\tilde{x}, y)$ констант вместо всех переменных $\tilde{x}$.

Если $\Delta_{n+1}f(\tilde{x}, y)$ не зависит существенно от y, а зависит только от $\tilde{x}$, то, отождествляя переменную y с какой-либо из переменных $\tilde{x}$, получим функцию меньшего числа аргументов, также не сохраняющую d-разности абсолютно. Повторим такие же рассуждения для нее и будем продолжать их, пока не получим требуемую одноместную функцию. □

Теорема 2.3. *Если d — собственный делитель числа k, то класс $L(d)$ является предполным в $R(d)$ в точности при $k = pd$.*

Доказательство. Пусть $k = abd, a > 1, b > 1$. Тогда $L(d) \subset R(d) \cap L(ad) \subset R(d)$. Включения строгие, так как $b\chi_d(x) \in R(d) \cap L(ad) \setminus L(d)$, $\chi_d(x) \in R(d) \setminus L(ad)$.

Пусть теперь $k = pd$, $f \in R(d) \setminus L(d)$. Можно считать функцию f одноместной, иначе применим лемму 2.15. Вычитая d-периодическую функцию из $f(x)$, получим функцию $h(x)$, равную 0 всюду на E_d и кратную d. Пусть $h(d) = Ad$. Положим $h_1(x) = h(x) - A\delta_d(x)$. Тогда $h_1(x) = 0$ во всех точках x, кратных d. Из условий $f, h, h_1 \notin L(d)$ следует, что при некотором i, $1 \leq i \leq d-1$, имеем $h_1(d+i) = Bd \neq 0$. При этом $h_1 \in R(d)$, следовательно, $h_1(ld+i) = lBd$ при $l = 0, 1, \ldots, p-1$. Далее, положим $h_2(x) = h_1(\delta_d(x) + ig_d(x))$. Нетрудно проверить, что $h_2(x) = B\chi_d(x)$, причем B не кратно p. Пусть $C = B^{-1} \pmod p$. Тогда $\chi_d(x) = Ch_2(x)$. Таким образом, замыкание $[R(d) \cup \{f\}]$ содержит функцию $\chi_d(x)$ и весь класс $R(d)$. □

Следствие 2.6. *При $k = p^2$ рассмотренные классы образуют в решетке $\mathcal{L}(P_k)$ неуплотняемую цепь $L(p) \subset R(p) \subset C(p) \subset P_k$.*

2.9 Классы $S(d)$

Пусть $d|k$. Введем замкнутый класс

$$S(d) = C_d(d) \cap R(d).$$

При этом $S(1) = S(k) = L$.

Утверждение 2.13. *Класс $S(d)$ состоит в точности из функций вида*

$$f(\tilde{x}) = l(\tilde{x}) + dG_d(\tilde{x}) + H_d(\tilde{x}), \tag{2.17}$$

где функция $H_d(\tilde{x})$ определена формулой (2.11).

Доказательство. Легко проверить, что функции вида (2.17) принадлежат классу $S(d)$.

Обратно: пусть $f(\tilde{x}) \in S(d)$. Представим f как элемент класса $C_d(d)$ в виде

$$f(\tilde{x}) = l_1(\tilde{x}) + d \cdot F(\tilde{x}).$$

Кратное d слагаемое $d \cdot F(\tilde{x})$ должно принадлежать классу $R(d)$ и представляться в виде, аналогичном (2.10):

$$d \cdot F(\tilde{x}) = l_2(\tilde{x}) + d \cdot G_d(\tilde{x}) + H_d(\tilde{x}).$$

Здесь линейная функция $l_2(\tilde{x})$ кратна d. Положим $l(\tilde{x}) = l_1(\tilde{x}) + l_2(\tilde{x})$ и получим представление (2.17) для функции f. □

С помощью очевидной формулы

$$dg_d(\tilde{x}) = \chi_{d,1}(x_1 + d,\ x_2, \ldots, x_n) - \chi_{d,1}(x_1,\ x_2, \ldots, x_n),$$

следствия 1.6 и утверждения 6 находим базис в классе $S(d)$.

Следствие 2.7. *Если d — собственный делитель числа k, то система функций $\{1,\ x + y,\ \chi_d(x)\}$ образует базис класса $S(d)$.*

Из утверждения 1.13 и определения класса $S(d)$ получаем

Следствие 2.8. *Если $d \neq k$, то все одноместные функции класса $R(d)$ принадлежат классу $S(d)$ в точности при $d = 1$ и при $d = 2$.*

Лемма 2.16. *Если $f(x_1, \ldots, x_n) \in R(p) \setminus S(p)$ и $n \geq 2$, то суперпозициями функции f и элементов класса $S(p)$ можно получить двухместную функцию $g(x, y)$, обладающую следующими свойствами*:

1) *функция не принадлежит классу $S(p)$,*
2) *функция является p-периодической,*
3) *все значения функции принадлежат E_p.*

Доказательство. Представим функию $f(\tilde{x})$ в каноническом для класса $R(p)$ виде

$$f(\tilde{x}) = l(\tilde{x}) + G_p(\tilde{x}) + H_p(\tilde{x}), \tag{2.18}$$

где функция $H_p(\tilde{x})$ определена условиями (2.11) при $d = p$. Вычитая принадлежащие классу $S(p)$ функции $l(\tilde{x})$ и $H_p(\tilde{x})$, получим p-периодическую функцию. Вычтем из последней, если это необходимо, подходящую функцию со значениями, кратными p (она принадлежит $S(p)$), добьемся свойств 2) и 3). Результирующая функция $G(\tilde{x})$ нелинейна (так как $f \notin S(p)$). Далее действуем так же, как при доказательстве леммы 1.8. □

Далее по аналогии с теоремой 1.1 выводится

Теорема 2.4. *Класс $S(d)$ является предполным в классе $R(d)$ в точности при $d = p$.*

Отличие в доказательстве только одно: при $p = 2$ вместо леммы 1.8 применяется лемма 2.16.

Из утверждения 2.12 получаем

Следствие 2.9. *Все одноместные функции класса $C_d(d)$ принадлежат классу $S(d)$ ровно в двух случаях: при $k = 2d$ и при $k = d$.*

Теорема 2.5. *Класс $S(d)$ является предполным в классе $C_d(d)$ в точности при $k = dp$.*

Доказательство. Пусть $k = dp$, тогда, если $f \in C_d(d) \setminus S(d)$, то $f \in C(d) \setminus R(d)$, с помощью функции f и элементов класса $S(d)$ строится функция $d \cdot j(x)$ при $p \neq 2$ или $d \cdot j(x, y)$ при $p = 2$. Эта часть полностью аналогична доказательству теоремы 2.2. Таким образом, $[S(d) \cup \{f\}] = C_d(d)$.

Пусть $k = dab, a > 1, b > 1$. Тогда $S(d) \subset K \subset C_d(d)$, где

$$K = \left[\{1,\ x + y,\ \chi_d(x)\} \cup \bigcup_{n=1}^{\infty} \{dg_{ad}(\tilde{x}^n)\}\right]$$

— класс всех функций вида $f(\tilde{x}) = l(\tilde{x}) + dG_{ad}(\tilde{x}) + H_d(\tilde{x})$, функция $H_d(\tilde{x})$ определена условиями (2.11). Заметим, что $K \subset R(ad)$. □

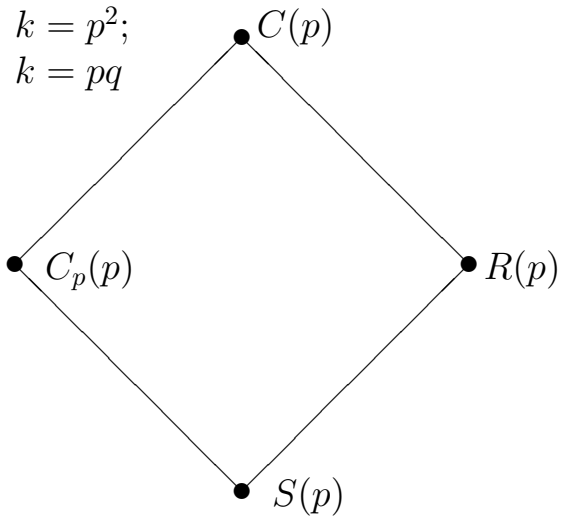
Теорема 2.6. *Если $k = p^2$ или $k = pq$, то не существует отличных от $C_p(p)$ и $R(p)$ замкнутых классов K таких, что $S(p) \subset K \subset C(p)$.*

Доказательство. Пусть K — замкнутый класс, $S(p) \subset K \subset C(p)$, $K \neq C_p(p)$, $K \neq R(p)$. Класс $S(p)$ является предполным в $C_p(p)$ и $R(p)$, а оба последних класса предполны в $C(p)$, поэтому каждое из четырех включений $C_p(p) \subseteq K$, $R(p) \subseteq K$, $K \subseteq C_p(p)$, $K \subseteq R(p)$ невозможно. Следовательно, класс K содержит функции f_1, f_2 такие, что $f_1 \notin C_p(p)$, $f_2 \notin R(p)$. Тогда, согласно теореме 2.5,

$$K = [K \cup \{f_1\}] \supseteq [S(p) \cup \{f_1\}] \supseteq C_p(p),$$

что противоречит невозможности такого включения, обоснованной выше. □

Следствие 2.10. *Если $k = p^2$ или $k = pq$, то классы $C(p)$, $C_p(p)$, $R(p)$, $S(p)$ образуют решетку по отношению включения, имеющую следующий вид.*



2.10 Классы R_dC_e и L_dM_e при взаимно простых d, e

Пусть

$$k = de, \quad \text{НОД}(d, e) = 1.$$

Рассмотрим классы

$$R_dC_e = R(d) \cap C(e), \quad L_dM_e = L(d) \cap M(e).$$

Утверждение 2.14. *Имеет место равенство* $R_dC_e = L_dM_e$.

Доказательство. Из определений классов и утверждения 2.1 следует, что $L_dM_e \subseteq R_dC_e$. Докажем обратное включение.

Пусть $f \in R_dM_e$. Тогда $f \in C(d, e)$. Согласно следствию 1.4 эту функцию можно однозначно представить в виде

$$f(\tilde{x}) = f(\tilde{0}) + eG_d(\tilde{x}) + dG_e(\tilde{x}).$$

Отсюда $dG_e(\tilde{x}) = f(\tilde{x}) - f(\tilde{0}) - eG_d(\tilde{x})$, следовательно,

$$dG_e(\tilde{x}) \in R(d) \cap R(e) = R(\text{НОД}(d, e)) = R(1) = L$$

и, в силу утверждения 2.4 и формулы (2.8),

$$f(\tilde{x}) = l(\tilde{x}) + eG_d(\tilde{x}) \tag{2.19}$$

и $f \in L(d)$. Из представления (2.19) также ясно, что $f \in M(e)$. □

Следствие 2.11. *Класс R_dC_e состоит в точности из функций вида* (2.19).

Утверждение 2.15. *Пусть*

$$A = \{1,\ x+y,\ eg_d(x,y)\}, \quad A_1 = \{1,\ x+y,\ eg_d(x)\}.$$

Тогда система функций A образует базис в классе R_dC_e, а система A_1 является базисом этого класса в точности при $d \neq 2$.

Доказательство. Положим $\varphi_n(x_1,\ldots,x_n) = eg_d(x_1,\ldots,x_n)$. Тогда полнота систем A и A_1 в классе R_dC_e следует из представления (2.19), соотношений

$$\varphi^{(n+1)}(\tilde{x},\ y) = \varphi^{(2)}\left(e - \varphi^{(n)}(\tilde{x}),\ y\right) \quad \text{при } n \geq 1,$$

$$\varphi^{(2)}(x,y) = \varphi^{(1)}\left(2e - \varphi^{(1)}(x) - \varphi^{(1)}(y)\right) \quad \text{при } d \neq 2$$

и того факта, что при $k = 2e$ одноместная функция $eg_2(x) = e(x+1)$ линейна. Нетрудно проверить, что такие полные системы являются базисами. □

Следствие 2.12. *При $k = 2e$, где e нечетно, все одноместные функции класса R_dC_e линейны.*

Лемма 2.17. *Пусть $k = pd$, $НОД(d,p) = 1$, $f \notin C(p)$. Тогда замыкание $[R_dC_p \cup \{f\}]$ содержит функцию $g_d(x,y)$.*

Доказательство. Если $f(x_1,\ldots,x_n) \notin C(p)$, то подстановкой констант на места переменных функции f можно получить одноместную функцию, также не принадлежащую классу $C(p)$ (если $n = 1$, то $f_1 = f$) [86, §17]. При этом найдутся такие a, b из E_k, что $a \equiv b,\ f_1(a) \not\equiv f_1(b) \pmod p$. Без ограничения общности полагаем $b = f(b) = 0$, иначе применим линейные преобразования функции и переменной. Итак, $f_1(0) = 0$, $f_1(ip) = \gamma$, и γ не кратно p при некотором i, $1 \leq i \leq d-1$. Построим функцию $h(x)$ такую, что $h(0) = 0$, $h(ip) = 1$. Возможны два случая.

1. Если НОД$(\gamma, d) = 1$, то $h(x) = cf_1(x)$, где $c = \gamma^{-1} \pmod k$.

2. Если же НОД$(\gamma, d) > 1$, то для функции $f_1(x) - pg_d(ip - x)$ будем иметь предыдущий случай, при этом $pg_d(x) \in R_dC_p$.

Тогда $g_d(x) = h(i \cdot pg_d(x))$. □

Теорема 2.7. *Класс L_dM_e является предполным в классе $L(d)$ в точности при $e = p$.*

Доказательство. Если $e = ab,\ a > 1,\ b > 1$, то имеют место включения $L_dM(ab) \subset L_dM_a \subset L(d)$. Они строгие, так как, например, $g_d(x) \in L(d) \setminus C(a)$, $ag_d(x,y) \in L_dM_a \setminus C(ab)$.

Пусть $e = p$. Напомним, что $L(d) = [\{1,\ x+y, g_d(x,y)\}]$ и силу утверждений 2.14 и 2.15 имеем $L_dM_p = [\{1,\ x+y,\ pg_d(x,y)\}]$. Применяя лемму 2.17, убеждаемся, что $[L_dM_p \cup \{f\}] = L(d)$. □

Теорема 2.8. *Класс L является предполным в L_dM_e в точности при $d = p$.*

Доказательство. Если $d = ab$, $a > 1$, $b > 1$, то имеют место включения $L \subset L_aM_e \subset L_dM_e$, $eg_a(x,y) \in L_aM_e \setminus L$, $eg_d(x,y) \in L_dM_e \setminus L(a)$.

Пусть $k = pe$, e не кратно p. Напомним, что $L_pM_e = [\{1,\ x+y, eg_p(x,y)\}]$ и, если $p \neq 2$, то полной в этом классе является и система $\{1,\ x+y, eg_p(x)\}$. Пусть $f \in L_pM_e \setminus L$, тогда

$$f(\tilde{x}) = l(\tilde{x}) + eG_p(\tilde{x}).$$

Вычитая из f функцию $l(\tilde{x})$, получим $h(\tilde{x}) = eG_p(\tilde{x})$, причем $h(\tilde{0}) = 0$. Далее рассмотрим два случая.

I. $p = 2$. Пусть функция h зависит от n переменных, тогда $n \geq 2$. Если $n > 2$, то согласно лемме 2.13 подстановкой на места переменных функции h констант получим двухместную функцию $H(x,y)$. При $n = 2$ полагаем $H(x,y) = h(x,y)$. Из способа построения функции $l(\tilde{x})$ следует, что $H(0,0) = H(1,0) = H(0,1) = 0$. Кроме того, 2-периодическая функция $H(x,y)$ нелинейна, поэтому $H(1,1) = ej$, $1 \leq j \leq e-1$. Тогда $eg_2(x,y) = j^{-1}H(x+1, y+1) \in [L \cup \{f\}]$. Итак, построен базис класса L_2M_e, класс L является предполным в L_2M_e.

II. $p > 2$. Если функция h зависит от n переменных и $n \geq 2$, то, применив леммы 2.13 и 2.14, получим одноместную нелинейную функцию $H(x)$, при $n = 1$ полагаем $H(x) = h(x)$. Далее повторяем рассуждения из доказательства теоремы 2.2, положив $d = 1$. Заметим только, что $H(1) = 0$, поэтому $1 \leq W(H) \leq p-2$, случай 4 невозможен. □

2.11 Заключение к главе 2

Основные результаты состоят в следующем.

1. Введено понятие сохранения и абсолютного сохранения функциями d-разностей (раздел 2.1). Доказана замкнутость классов $R(d)$ и $L(d)$ функций, сохраняющих и абсолютно сохраняющих d-разности, предложены аддитивные формулы (2.10) и (2.8) для элементов этих классов, найдены базисы классов (утверждения 2.4, 2.5, 2.7, 2.8, следствие 2.4).

2. Предложена вспомогательная формула, представляющая произвольную функцию суммой ее d-сеточных ограничений (лемма 2.9). Она используется и в этой, и в последующих главах.

3. Описаны решетка всех классов $L(d)$ и решетка всех классов $R(d)$ для всех k и делителей d числа k (теорема 2.1).

4. Введен особый замкнутый подкласс $S(d)$ классов $R(d)$ и $C_d(d)$, предложена аддитивная формула (2.17), задающая его элементы (утверждение 2.13), найден базис (следствие 2.7).

5. Введены особые подклассы R_dC_e классов $R(d)$, предложена аддитивная формула (2.19) для их элементов (следствие 2.11), найдены базисы (утверждение 2.15).

6. Найдены условия неуплотняемости некоторых фрагментов решетки $\mathcal{L}(P_k)$, содержащих введенные классы (теоремы 2.2–2.8, следствие 2.10).

7. Выяснено (утверждение 2.3), что в точности при $k = p^2$ класс Кузнецова есть $R(p)$.

Глава 3

Классы абсолютного сохранения d-разностей

В данной главе анализируется семейство классов $K(d_1, d)$, где d и d_1 — произвольные делители произвольного $k \geqslant 2$. Это семейство содержит, в частности, L и классы $L(d)$ абсолютного сохранения d-разностей, рассмотренные в главе 2. Классы $K(d_1, d)$ определяются каноническими формулами в виде сумм линейных и d-периодических функций. Такие формулы позволяют найти порождающие системы в классах $K(d_1, d)$ и установить свойства подрешетки этих классов в $\mathcal{L}_k$.

В разделе 3.1 определяются классы $K(d_1, d)$ как подклассы в $L(d)$, находятся их в общем случае бесконечные полные системы и устанавливаются свойства решетки классов $K(d_1, d)$, аналогичные свойствам решетки классов $L(d)$. В разделе 3.2 для некоторых k, d, d_1 из бесконечной полной в $K(d, d_1)$ системы выделяется конечный базис, позволяющий далее, в разделах 3.3 и 3.4, найти неуплотняемые цепи классов $K(d, d_1)$ в решетке $\mathcal{L}(P_k)$.

Материал этой главы опубликован в [9].

3.1 Классы $K(d_1, d)$

Пусть $d|k$, $d_1|k$. Рассмотрим в $L(d)$ подкласс [1] $K(d_1, d)$, состоящий из функций вида

$$f(\tilde{x}) = l(\tilde{x}) + d_1 G_d(\tilde{x}). \tag{3.1}$$

Нетрудно проверить следующие факты.

Утверждение 3.1. *Классы $K(d_1, d)$ обладают следующими свойствами.*

1. *Любая линейная и все d-периодические кратные d_1 функции принадлежат классу $K(d_1, d)$.*

[1] Символ K означает букву „каппа“.

2. *Класс $K(d_1, d)$ замкнут относительно введения и удаления фиктивных переменных, а также всех линейных операций над функциями.*

Лемма 3.1. *Пусть* $f(\tilde{x}^n) \in K(d_1, d)$, $h(\tilde{x}) = d_1 g_d^{(n)}(f(\tilde{x}), x_2, \ldots, x_n)$. *Тогда* $h(\tilde{x}) \in K(d_1, d)$.

Доказательство. Функция h кратна d_1. Покажем, что она d-периодична. Представим функцию f в виде (3.1). Пусть $\tilde{B} \in E^n_{k/d}$ и $l(\tilde{x}) = a_0 + a_1 x_1 + \cdots + a_n x_n$. Тогда, в силу d-периодичности функций G_d и g_d получаем

$$h(\tilde{x} + \tilde{B}d) = d_1 g_d(l(\tilde{x} + \tilde{B}d) + d_1 G_d(\tilde{x} + \tilde{B}d), x_2 + B_2 d, \ldots, x_n + B_n d) =$$

$$= d_1 g_d(a_0 + a_1(x_1 + B_1 d) + \cdots + a_n(x_n + B_n d) + d_1 G_d(\tilde{x}), x_2, \ldots, x_n) =$$

$$= d_1 g_d(a_0 + a_1 x_1 + \cdots + a_n x_n + d(a_1 B_1 + \cdots + a_n B_n) + d_1 G_d(\tilde{x}), x_2, \ldots, x_n) =$$

$$= d_1 g_d(l(\tilde{x}) + d_1 G_d(\tilde{x}), x_2, \ldots, x_n) = h(\tilde{x}).$$

Таким образом, d-периодическая кратная d_1 функция h принадлежит классу $K(d_1, d)$. □

Утверждение 3.2. *Пусть*

$$A = \{1, x + y\} \cup \bigcup_{n=1}^{\infty} \{d_1 g_d(\tilde{x}^n)\}. \tag{3.2}$$

Тогда $K(d_1, d) = [A]$.

Доказательство. Включение $K(d_1, d) \subseteq [A]$ следует из (3.1) и выразимости $d_1 G_d(\tilde{x})$ в виде линейной комбинации функций $d_1 g_d(\tilde{x} - \tilde{b})$, $\tilde{b} \in E^n_d$. Обратное включение $[A] \subseteq K(d_1, d)$ доказывается индукцией по сложности формулы над A, задающей функцию из $[A]$. Базис индукции — отношение $A \subset K(d_1, d)$. Индуктивный переход осуществляется при помощи утверждения 3.1 и леммы 3.1. □

Рассмотрим классы $K(d_1, d)$ с условием $d_1 | d$. Нетрудно проверить следующие факты.

Утверждение 3.3. *Если $d_1 | d$, то справедливо включение $K(d_1, d) \subseteq C_{d_1}(d)$. Равенство имеет место только при $d = k$.*

(Классы $C_e(d)$ введены в разделе 1.5.) Если $d \neq k$, то $d \cdot j(x) \in C_{d_1}(d) \setminus K(d_1, d)$.

Утверждение 3.4. *Если $d_1 | k$, $d_2 | k$, то условия $d_1 | d_2$ и $K(d_1, d) \supseteq K(d_2, d)$ эквивалентны. При фиксированном d классы $K(d_1, d)$ для $d_1 | d$ образуют в $\mathcal{L}(P_k)$ подрешетку, антиизоморфную решетке делителей d_1 числа d, с минимумом $K(d, d)$ и максимумом $K(1, d) = L(d)$.*

Относительно классов $K(d_1, d)$ с условием $d|d_1$ справедливо следующее.

Утверждение 3.5. *Если* $d_1|k,\ d_2|k,\ d|d_1,\ d|d_2$, *то условия* $K(d_1, d) \supseteq K(d_2, d)$ *и* $d_1|d_2$ *эквивалентны. При фиксированном* d *классы* $K(d_1, d)$ *для* $d|d_1$ *образуют в* $\mathcal{L}(P_k)$ *подрешетку, антиизоморфную решетке кратных* d *делителей* d_1 *числа* k *с минимумом* $K(k, d) = L$ *и максимумом* $K(d, d)$.

3.2 Базисы классов $K(d_1, d)$ при некоторых k, d, d_1

Мы указали бесконечную полную в классе $K(d_1, d)$ систему (3.2). В ряде случаев из нее можно выделить конечный базис. Для этого потребуется следующее легко проверяемое тождество, справедливое для всех $d|k$ и $d_1|k$:

$$\sum_{i=0}^{d-1} d_1 g_d(x - i) = d_1. \tag{3.3}$$

В дальнейшем всюду в данном разделе

$$k = pQR, \quad \text{НОД}(pQ, R) = 1, \quad Q \geqslant 1, \quad R > 1, \quad d = p, \quad d_1 = pQ. \tag{3.4}$$

Положим $\varphi_n(x_1, \ldots, x_n) = d_1 g_d(x_1, \ldots, x_n)$.

Лемма 3.2. *При условиях* (3.4), *если* $p = 2,\ C = 2^{-1} \pmod R,\quad n \geqslant 1,\quad$ *то*

$$\varphi_2(x_1, x_2) = C \cdot \big(\varphi_1(x_1) + \varphi_1(x_2) - \varphi_1(x_1 + x_2 - 1)\big), \tag{3.5}$$

$$\varphi_{n+2}(x_1, x_2, \tilde{y}) = C \cdot \big(\varphi_{n+1}(x_1, \tilde{y}) + \varphi_{n+1}(x_2, \tilde{y}) - \varphi_{n+1}(x_1 + x_2 - 1, \tilde{y})\big). \tag{3.6}$$

Если p *нечетно,* $C = p^{-1} \pmod R,\quad$ *то*

$$\varphi_2(x_1, x_2) = C \cdot \Big(\varphi_1(x_1) + \varphi_1(x_2) - p + \sum_{i=1}^{(p-1)/2} \big(\varphi_1(x_1 + ix_2) + \varphi_1(x_1 - ix_2)\big)\Big), \tag{3.7}$$

$$\varphi_{n+2}(x_1, x_2, \tilde{y}) = C \cdot \Big(\varphi_{n+1}(x_1, \tilde{y}) + \varphi_{n+1}(x_2, \tilde{y}) - \varphi_n(\tilde{y}) + \\ + \sum_{i=1}^{(p-1)/2} \big(\varphi_{n+1}(x_1 + ix_2, \tilde{y}) + \varphi_{n+1}(x_1 - ix_2, \tilde{y})\big)\Big). \tag{3.8}$$

Тождества (3.5) и (3.7) нетрудно проверить с помощью (3.3). Далее с учетом (3.5) проверяется (3.6) и аналогично с помощью (3.7) — тождество (3.8).

Следствие 3.1. *При условиях* (3.4) *система* $\{1,\ x + y,\ pQg_p(x)\}$ *образует базис в классе* $K(pQ, p)$.

3.3 Классы $K(d)$ и $L(d)$

В дальнейшем для класса $K(d,d)$ применяем более короткое обозначение $K(d)$. Это класс всех функций вида

$$f(\tilde{x}) = l(\tilde{x}) + dG_d(\tilde{x}). \tag{3.9}$$

Следствие 3.2. *Имеют место соотношения*

$$K(d) = C_d(d) \cap L(d), \qquad L \subseteq K(d) \subseteq L(d),$$

$$K(1) = L(1) = L; \qquad \textit{если } d = k, \textit{ то } K(d) = L,\ L(d) = P_k.$$

При всех n функции $dg_d(x_1, \ldots, x_n)$ принадлежат классу $K(d)$. Напомним, что класс $L(d)$ порождается системой $\{1, x+y, g_d(x,y)\}$, а при $d \neq 2$ — также системой $\{1, x+y, g_d(x)\}$.

Утверждение 3.6. *Если k четно, то все одноместные функции класса $L(2)$ принадлежат $K(2)$.*

Это верно согласно следствию 2.8.

Теорема 3.1. *Если d — собственный делитель числа k, то класс $K(d)$ является предполным в классе $L(d)$ в точности при $d = p$.*

Доказательство. Если число d составное, d_1 — его собственный делитель, то имеют место строгие включения $K(d) \subset K(d_1, d) \subset L(d)$.

Покажем теперь, что класс $K(p)$ является предполным в классе $L(p)$. Пусть $f \in L(p) \setminus K(p)$, тогда $f \in C(p) \setminus C_p(p)$. Согласно теореме 1.2 замыкание $[C_p(p) \cup \{f\}]$ содержит функцию $g_p(x,y)$, в суперпозициях используются только линейные функции и $pg_p(\tilde{x})$, все они принадлежат $K(p)$. Итак, $[K(p) \cup \{f\}] = L(p)$. □

3.4 Классы L и $K(d)$

Теорема 3.2. *Если $k = dp$, где $НОД(d,p) = 1$, то класс L является предполным в $K(p)$ в точности при $d = q$.*

Доказательство. Если число d составное, d_1 — его собственный делитель, $p|d_1$, то имеют место строгие включения $L \subset K(d_1, p) \subset K(p)$.

Как отмечено в следствии 3.1, система $\{1, x+y, pg_p(x)\}$ полна в классе $K(p)$. Пусть $d = q$, $f(\tilde{x}) \in K(p) \setminus L$. Покажем, что система $L \cup \{f\}$ порождает функцию $pg_p(x)$ и, следовательно, весь класс $K(p)$.

Представим функцию $f(\tilde{x})$ в виде (3.9). Вычитая из нее линейную функцию, получим функцию $pG_p(\tilde{x})$. Она нелинейна, т. е. не сохраняет 1-разности. Применяя к ней леммы 2.13 и 2.14, получим одноместную p-периодическую функцию $H(x)$, все значения которой кратны p. Без ограничения общности можно считать, что $H(0) = 0$, в противном случае вычтем константу $H(0)$. Построим из линейных функций и $H(x)$ функцию $pg_p(x)$.

Если $p = 2$, то $H(x+1) = a \cdot 2g_2(x)$, $a \in \{1, 2, \ldots, q-1\}$. Остается лишь умножить $H(x)$ на константу $a^{-1} \pmod q$.

Пусть далее p нечетно. Имеем одноместную функцию $H(x)$, обладающую следующими свойствами.

1°. Функция p-периодична.

2°. Все значения функции кратны p.

3°. Функция нелинейна.

4°. В точке $x = 0$ функция принимает значение 0.

Пусть $H(i) = a_i p$, $a_i \in E_q$ при $i = 1, \ldots, p-1$. В силу нелинейности найдется коэффициент $a_{i_0} \neq 0$. Можно считать, что $i_0 = 1$, иначе заменим функцию $H(x)$ на $H(\alpha x)$, где $\alpha = i_0^{-1} \pmod q$. Итак, $H(0) = 0$, $H(1) = a_1 p$, $(a_1, p) = 1$. Можно также считать, что $a_1 = 1$ (иначе умножим функцию $H(x)$ на константу $a_1^{-1} \pmod p$). Имеем кроме свойств 1°–4° условие $H(1) = p$. Если при этом

$$a_2 = a_3 = \cdots = a_{p-1} = 0, \tag{3.10}$$

то $pg_p(x) = H(x+1)$ и доказательство завершается. Пусть условие (3.10) не выполняется. Рассмотрим сумму $\sigma(H) = H(1) + H(2) + \cdots + H(p-1)$. Она равна bp, $b \in E_q$. Возможны два случая.

Случай I: $b \neq 0$. Тогда образуем функцию

$$F(x) = H(x) + H(2x) + \cdots + H((p-1)x).$$

Она обладает свойствами 1°–4° и, кроме того, $F(x) = bp$ при $x = 1, 2, \ldots, p-1$. Значит, $bp - F(x) = b \cdot pg_p(x)$. Умножая на константу $b^{-1} \pmod q$, получим функцию $pg_p(x)$.

Случай II: $b = 0$. Тогда образуем функцию $F(x) = H(x+1) - p$. Она обладает свойствами 1°–4°, а сумма $\sigma(F) = F(1) + F(2) + \cdots + F(p-1)$ равна $\sigma(H) - p^2$ и не кратна q. Заменяя $H(x)$ на $F(x)$, сводим случай II к случаю I. $\square$

3.5 Заключение к главе 3

Основные результаты главы состоят в следующем.

1. Выделены классы семейства $K(d_1, d)$, определяемые аддитивной формулой (3.1).

2. Найдена бесконечная полная система (3.2) в каждом классе $K(d_1, d)$.

3. Описана решетка классов $K(d_1, d)$ при фиксированном d (утверждения 3.4 и 3.5).

4. Найден конечный базис в классе $K(d_1, d)$ при ограничениях (3.4) на делители d, d_1 числа k (следствие 3.1).

5. Найдены условия, необходимые и достаточные для того, чтобы класс $K(d, d)$ являлся предполным в $L(d)$ (теорема 3.1), а также условия, необходимые и достаточные для того, чтобы класс L являлся предполным в $K(d, d)$ (теорема 3.2). Тем самым охарактеризовано положение классов $K(d, d)$ в решетке $\mathcal{L}(P_k)$ для чисел k с определенным составом множителей.

Глава 4

Полиномиальные представления

В этой главе рассматривается замкнутый класс $Polyn$ всех функций, представимых полиномами над кольцом $\mathbb{Z}_k = (E_k;\ +, \cdot \pmod k)$. Полином — это частный случай аддитивной формулы. Полиномы над каждым кольцом (в нашем случае мы имеем дело с кольцом вычетов по составному модулю k) сами образуют кольцо с теми же операциями. Цель заключается в нахождении условий полиномиальной реализуемости функций $E_k^n \to E_k$; желательно получить условия, одновременно являющиеся и необходимыми, и достаточными, однако полезными, как часто бывает, оказываются отдельно необходимые и отдельно достаточные условия. Их совпадения, как правило, встречаются в ограниченном множестве случаев. Другая цель состоит в нахождении канонических формул полиномов, представляющих данную функцию. Если кольцо не является полем, то одна функция реализуется множеством полиномов, а не одним, да и один и тот же полином можно представить в разных формах с применением тождественных преобразований. Эти обстоятельства усложняют наши задачи. Однако полезными оказываются определенные в предыдущих главах аддитивные формулы и свойства d-периодичности, сохранения сравнений, d-разностей $(d|k)$, канонические формулы для функций с такими свойствами.

Глава устроена следующим образом.

В разделе 4.1 дается исторический очерк становления и решения проблемы.

В разделе 4.2 определяются d-разности произвольного порядка R для функций из P_k и свойство функции сохранять такие разности $(d|k)$.

В разделе 4.3 рассматривается случай $k = p^m$. Выводятся необходимые (теорема 4.1) и достаточные (утверждение 4.1, теорема 4.2) условия полиномиальной реализации функции в терминах ее p-разностей порядков $R = 1, 2, \ldots, m-1$. При этом существенно используется представление функции суммой ее p-сеточных ограничений.

В разделе 4.4 представлен алгоритм для распознавания полиномиальности p^m-значной функции и построения реализующего ее полинома. Выводится оценка

временной сложности алгоритма.

В разделе 4.5 полученные результаты для $k = p^m$ обобщаются на все случаи произвольного составного k. При этом существенно используются разложения функций в суммы $p_i^{m_i}$-периодических, где $p_i^{m_i}|k$.

В разделе 4.6 рассмотрены все случаи, когда число k не кратно кубу простого. Устанавливается критерий (условия, одновременно необходимые и достаточные) полиномиальности в терминах сохранения сравнений и разностей только первого порядка.

4.1 Очерк истории

Известному результату А. В. Кузнецова, изложенному С. В. Яблонским в 1958 г. [86, §16], о том, что *равенство* $Polyn = P_k$ *имеет место тогда и только тогда, когда число* k *простое*, предшествовали следующие.

В 1863 г. Ш. Эрмит, анализируя перестановочные многочлены над полем $GF(p^m)$, установил, что при $k = p$ любая функция из $P_k^{(1)}$ представима полиномом [92].

В 1921 г. О. Кемпнер [94] вычислил мощность $|Polyn^{(1)}|$ для $k = p^m$, откуда следует, что равенство $Polyn^{(1)} = P_k^{(1)}$ справедливо в точности при $m = 1$.

Позже мощность $|Polyn^{(n)}|$ вычислена для всех значений k и n, а результат Кемпнера получил более краткий вывод. В частности, эти проблемы рассмотрены в работах [101, 93, 42, 106, 79].

В начале проблема относилась к области алгебры и теории чисел. Особое внимание уделялось случаю $k = p^m$ с надеждой на аналогии с полем $GF(k)$.

Очевидный способ проверить полиномиальность функции и построить реализующий ее полином состоит в анализе системы линейных уравнений над кольцом $\mathbb{Z}_k$ для коэффициентов полинома. Иногда только этого бывает достаточно для быстрого решения проблемы [86, 54].

Дальнейшие исследования привели к выделению свойств, сохраняемых суперпозициями функций. В связи с развитием теории функциональных систем и универсальной алгебры актуальным стало рассмотрение замкнутых классов и клонов.

Задачи поиска критериев полиномиальности и описания решетки замкнутых классов взаимосвязаны. Для выделения и анализа классов требуются условия полиномиальной реализуемости; с другой стороны, рассмотрение не всех функций, а лишь принадлежащих определенным классам, облегчает нахождение условий их полиномиальности.

Из свойств сравнений вытекает включение

$$Polyn \subseteq M(k), \text{ где } M(k) = \bigcap_{d|k} C(d).$$

В этом состоит одно из необходимых условий полиномиальности.

Кроме условия равенства $Polyn = P_k$ А. В. Кузнецовым получена

ТЕОРЕМА 1 [86, §16].

Если $p_1|k$, $p_2|k$, $p_1 \neq p_2$, *то* $Polyn \subseteq C(p_1, p_2) \subset P_k$.

Если $k = p^m, m \geq 2$, *то существует замкнутый класс* K *такой, что* $Polyn \subseteq K \subset C(p) \subset P_k$. *Класс* K *состоит из функций* f *с условием: для всех* $\tilde{y}$ *из* E_k^n *функции* $f(\tilde{x} + p\tilde{y})$ *по модулю* p^2 *линейны относительно* $py_1, \ldots py_n$:

$$f(\tilde{x} + p\tilde{y}) \equiv c_0(\tilde{x}) + py_1c_1(\tilde{x}) + \cdots + py_nc_n(\tilde{x}) \pmod{p^2}.$$

После этого были получены следующие результаты.

1. **Теоремы Л. Карлица** [90], 1964.

ТЕОРЕМА 2. *При* $k = p^m$ *функция* $f(x)$ *принадлежит классу* $Polyn^{(1)}$ *тогда и только тогда, когда для всех* $c \in E_p$, $r \in E_{p^{m-1}}$ *выполняется соотношение*

$$\sum_{s=0}^{m} (-1)^{r-s} \binom{r}{s} f(c+s) \equiv 0 \pmod{p^{\nu(rp)}},$$

где $\nu(t) = \min\{m, \mu(t)\}$, $\mu(t)$ *— показатель наибольшей степени* p, *делящей* $t!$.

ТЕОРЕМА 3. *При* $k = p^m$ *функция* $f(x)$ *принадлежит классу* $Polyn^{(1)}$ *тогда и только тогда, когда для всех* $l \in \mathbb{Z}$ *существуют функции* $f_1, \ldots, f_{m-1} \in P_k^{(1)}$ *такие, что*

$$f(x + lp) = f_0(x) + lpf_1(x) + (lp)^2 f_2(x) + \cdots + (lp)^{m-1} f_{m-1}(x).$$

ТЕОРЕМА 4. *При* $k = p^m$ *функция* $f(x, y)$ *принадлежит классу* $Polyn^{(2)}$ *тогда и только тогда, когда для всех* $r, s \in E_k$ *выполняется соотношение*

$$\sum_{i=0}^{r} \sum_{j=0}^{s} (-1)^{r+s-i-j} \binom{r}{i} \binom{s}{j} \equiv 0 \pmod{p^E},$$

$E = \min\{m, \mu(rp) + \mu(sp)\}$.

ТЕОРЕМА 5. *При* $k = p^m$ *функция* $f(x, y)$ *принадлежит классу* $Polyn^{(2)}$ *тогда и только тогда, когда для всех* $r, s \in \mathbb{Z}$ *существуют функции* $f_{i,j} \in P_k^{(2)}$ *такие, что*

$$f(x + rp, y + sp) = \sum_{i+j<m} (rp)^i (sp)^j f_{ij}(x, y) = 0.$$

3. Результаты Н. Н. Айзенберга и И. В. Семйона [41], 1971.

ТЕОРЕМА 6. *Если $k = p^m$ и $f \in Polyn$, то существует такой полином, представляющий функцию f, в который каждая переменная входит в степени не выше $mp - 1$.*

ТЕОРЕМА 7. *При $k = p_1 \cdots p_s$ имеет место равенство $Polyn = M(k)$.*

4. Уточнение теоремы 7 сделали в 1986 г. А. Н. Черепов [84] и независимо в 1987 г. Д. Г. Мещанинов [6, 24].

ТЕОРЕМА 8. *Равенство $Polyn = M(k)$ справедливо только при $k = p_1 \cdots p_s$.*

5. В 1974 г. И. Розенберг — обобщение теорем 3 и 5 на случай произвольного k и произвольного числа n переменных [103].

4. В 1986 г. А. Н. Черепов [84] — критерий полиномиальности для любых k и n, основанный на свойствах конечных разностей и интерполяционных формулах в кольце функций над $\mathbb{Z}$.

5. В 1988 г. Д. Г. Мещанинов [1] — критерии полиномиальности в терминах конечных разностей первого порядка для всех $k \not\equiv 0 \pmod{p^3}$.

6. В 1989 г. А. Б. Ремизов [73] — критерий для $k = p^2$ с помощью p-ичного разложения функций (линейной комбинации координатных функций).

7. В 1992 г. Д. Г. Мещанинов [4] — критерий полиномиальности для $k = p^3$ на языке конечных разностей второго порядка с шагом p (вторых p-разностей).

8. В 1995 г. Д. Г. Мещанинов [5] — конечно-разностный критерий для всех k, алгоритм проверки полиномиальности и построения полинома при $k = p^m$, сложность алгоритма (вычисление и анализ p-разностей порядка $m - 1$) есть $O(N \log^m N)$, где $N = k^n$ — размер входных данных, таблицы n-местной функции.

9. В 2011 г. С. Н. Селезнева [78, 79, 105] — критерий полиномиальности, основанный на теореме 2 и результатах Н. Н. Айзенберга, И. В. Семйона, А. И. Циткина [42], а также Д. Сингмастера [106], наилучший по сложности ($O(N)$) алгоритм построения полинома. Такой алгоритм однако требует объемных предварительных данных: необходим список всех одноместных полиномиальных функций (например, при $k = p^2$ их количество есть p^{3p}), неясно к тому же, как распознать полиномиальность унарной k-значной функции, если $k \neq p^m$, но $q^3 | k$.

При $k = p^m$ многие авторы (Н. Н. Айзенберг и И. В. Семйон, А. А. Нечаев [67], А. Н. Черепов, А. Б. Ремизов, Г. П. Гаврилов, М. В. Заец, В. Г. Никонов и А. Б. Шишков [57, 58]) применяют так называемые *координатные функции* — функции p-значной логики, которые, домноженные на последовательные степени p, составляют в сумме исходную p^m-значную функцию (аналогично представлению числа в p-ичной системе). Этот метод, заимствованный из алгебры и теории чисел, оказался результативен и в функциональной системе P_k, однако его применимость ограничена значениями $k = p^m$. Нулевую координатную функцию можно рассматривать как p-периодическую функцию p^m-значной логики, последовательные линейные комбинации координатных функций — как p^l-периодические функции, $l = 1, 2, \ldots, m-1$. На языке координатных функций несложно выражаются и свойства сохранения сравнений по модулям p^l. Именно эти обстоятельства привлекают внимание к координатным функциям и значеням $k = p^m$ при исследовании полиномиальности и замкн.тых класссов в P_k.

Особое внимание М. В. Заец, В. Г. Никонов и А. Б. Шишков уделили способу последовательного вычисления координат (при $k = p^m$) решением системы линейных уравнений над $\mathbb{Z}_k$ и выделили классы функций с так называемой *вариационно-координатной полиномиальностью*; они содержат, в частности, весь класс $Polyn$. Это один из способов сведéния p^m-значной логики к p-значной. Другие способы сведения k-значной логике к d-значной ($d < k$, $d|k$) описаны соискателем в [34].

Также отметим, что системы линейных уравнений над кольцом вычетов $\mathbb{Z}_k$ чрезвычайно важны, они неизбежно возникают во всех проблемах, связанных с полиномами в P_k, в том числе и в случае неполной определенности [17, 18, 19].

4.2 Сохранение d-разностей произвольного порядка

Для набора $\tilde{t} \in \mathbb{Z}_+^n$ обозначим как $\sigma(\tilde{t})$ сумму всех его компонент, вычисленную в кольце $\mathbb{Z}$.

Пусть $d|k$, $f(\tilde{x}) \in P_k$. Для фиксированных $\tilde{r} \in \mathbb{Z}_+^n$, $R = \sigma(\tilde{r})$, $\tilde{x} \in E_k^n$ определим величины

$$\Delta^R(\tilde{r})f(\tilde{x}) = \sum_{s_1=0}^{r_1} \cdots \sum_{s_n=0}^{r_n} (-1)^{R-\sigma(\tilde{r})} \binom{r_1}{s_1} \cdots \binom{r_n}{s_n} f(\tilde{x} + d\tilde{s}).$$

Они называются *d-разностями типа $\tilde{r}$ и порядка R функции f в точке $\tilde{x}$.*

Если $\sigma(\tilde{b}) = B$, $\sigma(\tilde{c}) = C$, то $\Delta^B(\tilde{b})(\Delta^C(\tilde{c})f(\tilde{x})) = \Delta^{B+C}(\tilde{b}+\tilde{c})f(\tilde{x})$.

При фиксированном $\tilde{\mu} \in E_d^n$ под *d-разностями d-сеточного ограничения* $f^{\tilde{\mu}}$ функции $f(\tilde{x})$ будем иметь в виду ее d-разности только в таких точках $\tilde{x}$, что $\tilde{x} \equiv \tilde{\mu} \pmod{d}$.

Будем говорить, что *функция* $f(\tilde{x})$ *сохраняет* d*-разности порядка* R, если для каждого фиксированного $\tilde{r}$, $\sigma(\tilde{r}) = R$, и каждого фиксированного $\tilde{\mu} \in E_d^n$ величины $\Delta^R(\tilde{r}) f^{\tilde{\mu}}(\tilde{x})$ равны при всех $\tilde{x}$, $\tilde{x} \equiv \tilde{\mu} \pmod{d}$.

Если функция сохраняет d-разности некоторого порядка, то все ее d-разности больших порядков равны 0.

4.3 Случай $k = p^m$

Утверждение 4.1. *При* $k = p^m$ *любая* p*-периодическая функция представима полиномом.*

Действительно, она является линейной комбинацией функций $g_p(\tilde{x} - \tilde{a})$, $\tilde{a} \in E_p^n$. С помощью теорем Эйлера и Ферма нетрудно проверить, что

$$g_p(\tilde{x}) = \prod_{j=1}^{n} \left(1 - x_j^{p-1}\right)^{\varphi(p^m)}. \tag{4.1}$$

где $\varphi(N)$ — функция Эйлера.

Очевидны также следующие факты.

Утверждение 4.2. *Функция* $f(\tilde{x})$ *представима полиномом в том и только том случае, когда полиномами представимы все ее* p*-сеточные ограничения* $f^{\tilde{\mu}}(\tilde{x})$.

Если $\tilde{\mu} \in E_p^n$, *то функция* $f^{\tilde{\mu}}(\tilde{x})$, *т. е.* p*-сеточное ограничение функции* $f(\tilde{x})$, *представляется полиномом в том и только том случае, когда она представляется полиномом вида*

$$f^{\tilde{\mu}}(\tilde{x}) = g_p(\tilde{y}) \cdot \sum_{\tilde{t}:\ 0 \le \sigma(\tilde{t}) \le R} a(\tilde{y}) y_1^{t_1} \cdots y_n^{t_n}, \quad \text{где } \tilde{y} = \tilde{x} - \tilde{\mu},\ R \le m-1,\ a(\tilde{y}) \in E_k. \tag{4.2}$$

Теорема 4.1. *Пусть* $f(\tilde{x}) \in Polyn$, *тогда выполняются следующие условия*:

$(R1)$ *если набор* $\tilde{r}$ *имеет сумму компонент* R, *то все* p*-разности типа* $\tilde{r}$ *функции* f *кратны* $p^R r_1! \cdots r_n!$;

$(R2)$ *функция* f *сохраняет* p*-разности порядка* $m - 1$.

Доказательство. Фиксируем R, $R \le m-1$, и возьмем набор $\tilde{r}$ с суммой компонент R. Пусть $D = \Delta^R(\tilde{r}) f^{\tilde{\mu}}(\tilde{x})$. Положим, не ограничивая общности, $\tilde{\mu} = \tilde{0}$. Тогда

$$D = \sum_{\tilde{s}} (-1)^{R-\sigma(\tilde{s})} \binom{r_1}{s_1} \cdots \binom{r_n}{s_n} \sum_{\tilde{t}:\ 0 \le \sigma(\tilde{t}) < m} a(\tilde{t}) \prod_{j=1}^{n} (x_j + s_j p)^{t_j} = \sum_{\tilde{t}} \prod_{j=1}^{n} S_j,$$

где

$$S_j = \sum_{s=0}^{r_j} (-1)^{r_j - s} \binom{r_j}{s} \sum_{i=0}^{t_j} \binom{t_j}{i} x_j^{t_j - i} (sp)^i = \sum_{i=0}^{t_j} x_j^{t_j - i} p^i \binom{t_j}{i} S(i, r_j).$$

Здесь величины

$$S(i, r_j) = \sum_{s=0}^{r_j} (-1)^{r_j - s} \binom{r_j}{s} s^i$$

обращаются в 0 при $i < r_j$, равны $r_j!$ при $i = r_j$ и кратны r_j при $i > r_j$ [1], поэтому

$$D = \sum_{\tilde{t}} a(\tilde{t}) \prod_{j=1}^{n} \sum_{i=r_j}^{t_j} x_j^{t_j - i} p^i \binom{t_j}{i} S(i, r_j), \tag{4.3}$$

где внешняя сумма берется по наборам $\tilde{t}$ с суммой компонент R и $t_1 \geq r_1, \ldots, t_n \geq r_n$. Отсюда следует первое утверждение теоремы.

Если $R = m - 1$, то в сумме (4.3) остается единственное слагаемое, оно соответствует $\tilde{t} = \tilde{r}$:

$$D = a(\tilde{t}) p^R r_1! \cdots r_n!.$$

Величина D не зависит от $\tilde{x}$, доказано второе утверждение теоремы. □

Пример 4.1. Пусть $k = p^3$. Рассмотрим снова функцию, построенную А. В. Кузнецовым [86, §16] (пример 2.2):

$$f(x_1 + l_1 p,\ x_2 + l_2 p) = l_1 l_2 p, \quad f \in K, \quad Polyn \subseteq K \subset M(p^3).$$

При $k = 2^3$ возьмем любое 2-сеточное ограничение, например, при $\mu_1 = \mu_2 = 0$, $f^{00}(x_1, x_2)$:

x_1 / x_2	0	2	4	6
0	0	0	0	0
2	0	2	4	6
4	0	4	0	4
6	0	6	4	2

.

Показано, что $f(x_1, x_2) \notin R(2)$. Функция не сохраняет первые 2-разности, но сохраняет 2-разности порядка $R = 2 = 3 - 1 = m - 1$, однако для смешанной 2-разности в точке $(0, 0)$ имеем

$$\Delta^2(1,1) f(0,0) = 0 + 2 - 0 - 0 = 2 \not\equiv 0 \pmod{2^{1+1} 1!1!}.$$

Таким образом, не выполняется условие (R2), функция не представима полиномом по модулю 8, $f \in K \setminus Polyn$. В этом можно убедиться также, составив систему линейных уравнений для коэффициентов полинома. (Подробнее об этом будут дальнейшие теоремы.)

[1] Сачков В. Н. Введение в комбинаторные методы дискретной математики — М.: Наука, 1982, с. 39–40

Лемма 4.1. *Если функция $f(\tilde{x})$ сохраняет p-разности порядка R, то для всех $\tilde{\mu}$ из E_p^n и всех $\tilde{M}$ из $\mathbb{Z}_+^n$ выполняется равенство*

$$f(\tilde{\mu}+\tilde{M}p)=\sum_{\tilde{t}:\ 0\le T=\sigma(\tilde{t})\le R}\binom{M_1}{t_1}\cdots\binom{M_n}{t_n}\Delta^T(\tilde{t})f(\tilde{\mu}). \tag{4.4}$$

Доказательство. Применим индукцию по числу переменных функции.

При $n=1$ необходимо показать, что для всех $\mu\in E_p$, $M\ge 0$ справедливо равенство

$$f(\mu+Mp)=\sum_{t=0}^{R}\binom{M}{t}\Delta^t f(\mu), \tag{4.5}$$

где

$$\Delta^R f(\mu)=\sum_{s=0}^{R}(-1)^{R-s}\binom{R}{s}f(\mu+sp) \tag{4.6}$$

для $R=0,1,2,\ldots$. Формулы (4.5) и (4.6) взаимно обратны, поэтому базис индукции обоснован.

Пусть, далее, утверждение леммы выполнено для n-местных функций. Рассмотрим $(n+1)$-местную функцию $f(\tilde{x},\ y)$ и покажем, что для всех $(\tilde{\mu},\nu)\in E_p^{n+1}$, $(\tilde{M},N)\in\mathbb{Z}_+^{n+1}$ справедливо равенство

$$f(\tilde{\mu}+\tilde{M}p,\ \nu+Np)=\sum_{0\le\sigma(\tilde{t})+u\le R}\binom{M_1}{t_1}\cdots\binom{M_n}{t_n}\binom{N}{u}\Delta^{\sigma(\tilde{t})+u}(\tilde{t},\ u)f(\tilde{\mu},\nu). \tag{4.7}$$

Для фиксированных $\tilde{\mu},\nu,N$ рассмотрим n-местную функцию $h(\tilde{x})=f(\tilde{x},\ \nu+Np)$ и одноместную функцию $H(y)=f(\tilde{\mu},\ y)$. По предположению индукции имеем

$$h(\tilde{\mu}+\tilde{M}p)=\sum_{0\le T=\sigma(\tilde{t})\le R}\binom{M_1}{t_1}\cdots\binom{M_n}{t_n}\Delta^T(\tilde{t})h(\tilde{\mu}), \tag{4.8}$$

$$H(\nu+Np)=\sum_{u=0}^{R}\binom{N}{u}\Delta^u H(\nu). \tag{4.9}$$

При этом $h(\tilde{\mu})=f(\tilde{\mu},\nu+Np)=H(\nu+Np)$. Подставляя (4.9) в (4.8) и используя свойства разностей, получаем:

$$f(\tilde{\mu}+\tilde{M}p,\ \nu+Np)=h(\tilde{\mu}+\tilde{M}p)=\sum_{\tilde{t}}\sum_{u=0}^{R}\binom{M_1}{t_1}\cdots\binom{M_n}{t_n}\binom{N}{u}\Delta^T(\tilde{t})(\Delta^u H(\nu)),$$

где

$$\Delta^T(\tilde{t})(\Delta^u H(\nu))=\Delta^T(\tilde{t},\ 0)(\Delta^u(\tilde{0},\ u)f(\tilde{\mu},\ \nu))=\begin{cases}\Delta^{T+u}(\tilde{t},u)f(\tilde{\mu},\ \nu), & T+u\le R,\\ 0, & T+u>R.\end{cases},$$

откуда и следует (4.7). Индуктивный переход завершен. □

Теорема 4.2. *Если функция $f(\tilde{x})$ принадлежит классу $M(k)$ и удовлетворяет условиям $(R1)$ и $(R2)$ теоремы 1, то $f \in Polyn$.*

Доказательство. Фиксируем $\tilde{\mu} \in E_p^n$. Пусть R — максимальный порядок ненулевых p-разностей функции $f\tilde{\mu}$, при этом $R \leq m-1$ в силу условия (R2). Покажем, что $f^{\tilde{\mu}}$ можно представить в виде (4.2).

Положим $\tilde{x} = \tilde{\mu} + \tilde{M}p$ в (4.2), получим

$$f^{\tilde{\mu}}(\tilde{\mu} + \tilde{M}p) = \sum_{\tilde{t}:\ 0 \leq T = \sigma(\tilde{t}) \leq R} a(\tilde{t}) p^T M_1^{t_1} \cdots M_m^{t_n}. \tag{4.10}$$

Используя условие и 4.1, получаем:

$$f(\tilde{\mu} + \tilde{M}p) = \sum_{\tilde{t}:\ 0 \leq T = \sigma(\tilde{t}) \leq R} \binom{M_1}{t_1} \cdots \binom{M_n}{t_n} \Delta^T(\tilde{t}) f(\tilde{\mu}) =$$

$$= \sum_{\tilde{t}} \frac{\Delta^T(\tilde{t}) f(\tilde{\mu})}{t_1! \cdots t_n!} (M_1)_{t_1} \cdots (M_n)_{t_n} = \sum_{\tilde{t}} \frac{\Delta^T(\tilde{t}) f(\tilde{\mu})}{t_1! \cdots t_n!} \prod_{j=1}^{n} \sum_{r=0}^{t_j} s(t_j, T) M_j^T =$$

$$= \sum_{\tilde{t}} \sum_{r_1=t_1}^{R} \sum_{r_2=t_2}^{R-t_1} \cdots \sum_{r_n=t_n}^{R-t_1-\cdots-t_{n-1}} \frac{\Delta^R(\tilde{r}) f(\tilde{\mu})}{r_1! \cdots r_n!} \prod_{j=1}^{n} \sum_{r=0}^{t_j} s(r_j, t_j) M_j^{r_j},$$

где $(M)_t = M(M-1)\cdots(M-t+1)$ и $s(i,j)$ — числа Стирлинга первого рода. Сопоставляя последнее выражение с (4.10), получаем уравнения для коэффициентов полинома (4.2):

$$a(\tilde{t}) p^T = \sum_{\tilde{r}} \frac{\Delta^R(\tilde{r}) f(\tilde{\mu})}{r_1! \cdots r_n!} \prod_{j=1}^{n} s(r_j, t_j). \tag{4.11}$$

В силу условия (R2) эти уравнения разрешимы в кольце вычетов по модулю p^m. □

4.4 Алгоритм для распознавания полиномиальности и построения полинома

Алгоритмы реализуются машиной с произвольным доступом к памяти.

Теорема 4.3. *Существует алгоритм с временной сложностью $O(n^m p^{mn})$, который для произвольной n-местной функции f из P_k определяет, представима ли функция f полиномом и (если $f \in Polyn$) строит один из представляющих ее полиномов.*

Доказательство. Алгоритм состоит из следующих шагов.

1. Проверка условия $f \in M(k)$. Если оно не выполняется, то $f \notin Polyn$, Выход.

2. Для каждого $\tilde{\mu} \in E_p^n$ осуществить следующее.

2a. Для $R = 0, 1, \ldots, m-1$ и всех $\tilde{r}$ с суммой компонент R вычислить p-разности $\Delta^R(\tilde{r})f(\tilde{\mu})$ и проверить, кратны ли они $p^R r_1! \cdots r_n!$. Если при этом все разности некоторого порядка равны 0, то разности высших порядков можно не вычислять. Если для некоторого $\tilde{r}$ с суммой компонент R оказалось, что разность $\Delta^R(\tilde{r})f(\tilde{\mu})$ не кратна $p^R r_1! \cdots r_n!$, то $f \notin Polyn$, Выход.

2b. Для каждого $\tilde{M} \in E^n_{p^{m-1}}$ проверить условие (4.4). Если для некоторого $\tilde{M}$ оно не выполняется, то $f \notin Polyn$, Выход.

2c. Из уравнений (4.11) найти коэффициенты полинома (4.2).

3. Полином, представляющий функцию f, записать в виде суммы сеточных ограничений (4.2).

Шаг 1 требует $O(mp^{mn})$ операций. Оценим трудоемкость шага 2a.

Пусть $D(n)$ — количество p-разностей, которые должны быть вычислены для n-местной функции, из них $D(n, R)$ количество разностей порядка R. Тогда

$$D(n, R) = \binom{n + R - 1}{R}$$

— число разбиений R в сумму n неотрицательных слагаемых. Далее,

$$D(n) = \sum_{R=1}^{m-1} D(n, R) \le \sum_{R=0}^{m-1} \binom{n + R - 1}{R} = \binom{n+m}{m-1}.$$

Оценим теперь сложность вычисления разности $\Delta^R(\tilde{r})f(\tilde{\mu})$ по формуле в ее определении.

В сумме $(r_1 + 1) \cdots (r_n + 1)$ слагаемых. Учитывая, что $r_1 + \cdots + r_n = R$, получим оценку

$$(r_1 + 1) \cdots (r_n + 1) \le \left(\frac{R+n}{n}\right)^n = \left(\frac{m-1}{n} + 1\right)^n = O\left(\frac{m^n}{n^n}\right).$$

Для вычисления каждого слагаемого достаточно $O(n)$ операций сложения и умножения. Таким образом, разность $\Delta^R(\tilde{r})f(\tilde{\mu})$ вычисляется со сложностью $O(m^n/n^{n-1})$. Следовательно, сложность всего шага 2a есть

$$D(n)O\left(\frac{m^n}{n^{n-1}}\right) = O\left(n^{m-1}\frac{m^n}{n^{n-1}}\right) = O(m^n n^{m-n}).$$

Далее, для оценки трудоемкости шага оценим сложность вычисления суммы (4.4) при фиксированных μ и $\tilde{M}$. Число слагаемых в сумме есть $O(n^{m-1})$. Каждое слагаемое требует для своего вычисления $O(n)$ операций. Следовательно, для вычисления суммы (4.4) достаточно $O(n^m)$ операций.

Далее, имеется $p^{(m-1)n}$ векторов $\tilde{M}$, для каждого из них вычисляется сумма (4.4). Следовательно, сложность шага 2b есть $O(n^m p^{(m-1)n})$.

Наконец, шаг 2c требует $O(n^{m-1})$ операций (так оценивается число уравнений).

Суммарная сложность шагов 2a, 2b, 2c есть, таким образом,

$$O(m^n n^{m-n}) + O(n^m p^{(m-1)n}) + O(n^{m-1}) = O(n^m p^{(m-1)n}).$$

Далее, имеется p^n векторов $\tilde{\mu}$, поэтому для выполнения всего этапа 2 достаточно $O(n^m p^{mn})$ операций. Сложность реализации этапов 1 и 3 также удовлетворяет этой оценке. □

Пример 4.2. Пусть $k = 3^4$, рассмотрим 9-периодическую функцию $f(x, y) = f^{00}(x, y)$, заданную на множестве E_9^2 следующей таблицей:

y \ x	0	3	6
0	0	0	0
3	0	27	27
6	0	54	54

Применим более короткое обозначение $D(r_1, r_2) = \Delta^R(r_1, r_2) f(0, 0)$. Имеем:

$D(1,0) = D(0,1) = D(2,0) = D(0,2) = D(3,0) = D(0,3) = 0,$

$D(1,1) = f(0,0) - f(3,0) - f(0,3) + f(3,3) = 27,$

$D(2,1) = -f(0,0) + f(0,3) + 2f(3,0) - 2f(3,3) - f(6,0) + f(6,3) = -27 = 54,$

$D(1,2) = 0.$

Тогда соотношение (4.4) принимает вид

$$f(3M_1, 3m_2) = \binom{M_1}{1}\binom{M_2}{1}27 + \binom{M_1}{2}\binom{M_2}{1}54,$$

откуда

$$f(3M_1, 3M_2) \equiv 27M_1^2 M_2 \pmod{81}.$$

В силу 9-периодичности последние соотношения достаточно проверить лишь для $M_1, M_2 = 1, 2$. Они выполняются на каждом из этих четырех наборов (M_1, M_2), условия (R1) и $(R2)$ удовлетворены. Система уравнений для коэффициентов полинома (4.2) при $k = p^4$, $n = 2$, $\mu_1 = \mu_2 = 0$ такова:

$$a(0,0) = 0,$$

$$a(1,0)p = D(1,0) - \frac{1}{2}D(2,0) + \frac{2}{3!}D(3,0),$$

$$a(0,1)p = D(0,1) - \frac{1}{2}D(0,2) + \frac{2}{3!}D(0,3),$$

$$a(2,0)p^2 = \frac{1}{2}D(2,0) - \frac{3}{3!}D(3,0), \quad a(0,2)p^2 = \frac{1}{2}D(0,2) - \frac{3}{3!}D(0,3),$$
$$a(1,1)p^2 = D(1,1) - \frac{1}{2}D(2,1) - \frac{1}{2}D(1,2),$$
$$a(3,0)p^3 = \frac{1}{3!}D(3,0), \quad a(0,3)p^3 = \frac{1}{3!}D(0,3),$$
$$a(2,1)p^3 = \frac{1}{2}D(2,1), \quad a(1,2)p^3 = \frac{1}{2}D(1,2).$$

Уравнения принимают вид сравнений по модулю 81:

$a(0,0) = 0$,

$3a(1,0) \equiv 3a(0,1) \equiv 9a(2,0) \equiv 9a(0,2) \equiv 0$,

$9a(1,1) =\equiv 27 - 54/2$,

$27a(3,0) \equiv 27a(0,3) \equiv 0, \quad 27a(2,1) \equiv 54/2, \quad 27a(1,2) \equiv 0.$

Решением является, например, набор из $a(2,1) = 1$ и всех остальных коэффициентов, равных 0. Следовательно,

$$f(x,y) = g_3(x,y)x^2y = (1-x^2)^{54}(1-y^2)^{54}x^2y.$$

4.5 Случай произвольного составного k

Теорема 4.4. *Если $p|k$, то любая p-периодическая функция класса $M(k)$ представима полиномом.*

Доказательство. Пусть $k = p^m Q$, $m \geq 1$, $Q \geq 1$, НОД$(p,Q) = 1$.

Случай $Q = 1$ описан утверждением 4.1.

Пусть $Q > 1$, $f(\tilde{x})$ есть p-периодическая функция класса $M(k)$, и пусть $F(\tilde{x}) = f(\tilde{x}) - f(\tilde{0})$. Тогда $F(\tilde{0}) = 0$. Из условия $F \in C(Q)$ следует, что p-периодическая функция $F(\tilde{x})$ кратна Q и является линейной комбинацией функций $Qg_p(\tilde{x} - \tilde{a})$, $\tilde{a} \in E_p^n$. В силу теорем Эйлера и Ферма получаем полином

$$Qg_p(x_1, \ldots, x_n) = Q \cdot \prod_{i=1}^{n} \left(1 - x_i^{p-1}\right)^{\varphi(p^m)}. \tag{4.12}$$

□

Теорема 4.5. *Если $Q|k$, $Q = q_1 \cdots q_s$, где $q_1, \ldots, q_s$ — попарно различные простые делители числа k и $s \geq 1$, то любая Q-периодическая функция класса $M(k)$ представима полиномом.*

Доказательство. Согласно леммам 1.4 и 1.5 такую функцию можно представить в виде

$$f(\tilde{x}) = f(\tilde{0}) + \sum_{j=1}^{s} f_j(\tilde{x}),$$

где каждая функция f_j принадлежит классу $M(k)$, является q_j-периодической и кратна k/q_j. В силу теоремы 4.4 она представима полиномом. □

Далее в данном разделе предполагаются условия

$$s \geq 2, \quad k = k_1 \cdots k_s, \quad k_i = p_i^{m_i}, \quad d_i = k/k_i, \quad i = 1, \ldots, s. \tag{4.13}$$

Утверждение 4.3. *Пусть $f(\tilde{x}) \in M(k)$. Тогда функцию f можно представить в виде*

$$f(\tilde{x}) = f(\tilde{0}) + \sum_{i=1}^{s} h_i(\tilde{x}), \tag{4.14}$$

где $h_i(\tilde{x})$ — это k_i-периодические кратные d_i функции класса $M(k)$,

$$h_i(\tilde{x}) = c_i d_i F(c_i d i \tilde{x}), \quad \text{где} \quad c_i = d_i^{-1} \pmod{k_i}, \quad F(\tilde{x}) = f(\tilde{x}) - f(\tilde{0}). \tag{4.15}$$

Такой способ построения функций $h_i(\tilde{x})$ проще использованного в выводе леммы 1.4, он предложен А. А. Нечаевым. При этом справедливость разложения (4.14) следует из теоремы 1.3 (теорема 1 в [3]).

Следствие 4.1. *Функция $f(\tilde{x})$ класса $M(k)$ представима полиномом в том и только том случае, когда представимы полиномами все k_i-периодические функции формулы* (4.14).

Легко проверить следующие факты.

Лемма 4.2. *Пусть $h(\tilde{x})$ есть k_i-периодическая функция класса $M(k)$. Тогда*:

1) *справедливо p_i-сеточное представление*

$$h(\tilde{x}) = \sum_{\tilde{\mu} \in E_{p_i}^n} h^{\tilde{\mu}}(\tilde{x});$$

2) *функция $h(\tilde{x})$ представима полиномом в том и только том случае, когда представимы полиномами все ее p_i-сеточные ограничения $h^{\tilde{\mu}}(\tilde{x})$*;

3) *функция $h^{\tilde{\mu}}(\tilde{x})$ представима полиномом в том и только том случае, когда она выражается полиномом*

$$h^{\tilde{\mu}}(\tilde{x}) = d_i g_{p_i}(\tilde{y}) \cdot \left(\sum_{\tilde{t}:\ 0 \leq \sigma(\tilde{t}) < m_i} a(\tilde{t}) y_1^{t_1} \cdots y_n^{t_n} \right),$$

где $\tilde{y} = \tilde{x} - \tilde{\mu}$, $a(\tilde{t}) \in E_k$.

Аналогично случаю $k = p^m$ выводится следующий результат.

Теорема 4.6. *Если $h(\tilde{x})$ есть k_i-периодическая функция класса $M(k)$, то она представима полиномом в точности при одновременном выполнении двух условий*:

$(R1')$ *для всех $\tilde{r}$ с суммой компонент R, $R \le m_i - 1$, все p_i-разности типа $\tilde{r}$ функции $h(\tilde{x})$ кратны $p_i^R r_1! \cdots r_n!$;*

$(R2')$ *функция $h(\tilde{x})$ сохраняет p_i-разности порядка $m_i - 1$.*

Пример 4.3. Пусть $k = 360 = 2^3 \cdot 3^2 \cdot 5$. Тогда

$$k_1 = 8, d_1 = 45, \quad k_2 = 9, d_2 = 40, \quad k_3 = 5, d_3 = 72.$$

Рассмотрим одноместную функцию $f(x)$, все ненулевые значения которой заданы следующей матрицей:

$$f = \begin{pmatrix} 30 & 60 & 90 & 120 & 150 & 180 & 210 & 240 & 270 & 300 & 330 \\ 250 & 20 & 270 & 160 & 290 & 180 & 70 & 200 & 90 & 340 & 310 \end{pmatrix}$$

(в первой строке значения x, во второй — значения $f(x)$). Выясним, представима ли эта функция полиномом. Имеем $f(0) = 0$, $F(x) = f(x)$. Построим 8-периодическую функцию $h_1(x)$, а также 9-периодическую функцию $h_2(x)$ и 5-периодическую функцию $h_3(x)$ так, чтобы $f(x) = h_1(x) + h_2(x) + h_3(x)$:

$$h_1(x) = 45F(45x), \quad h_2(x) = 40F(40x), \quad h_3(x) = 72F(72x).$$

Получаем $h_3(x) = 0$,

$$h_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 270 & 0 & 180 & 0 & 90 & 0 \end{pmatrix}, \quad h_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 0 & 0 & 160 & 0 & 0 & 80 & 0 & 0 \end{pmatrix}.$$

Функция $h_1(x)$ сохраняет 2-разности порядка 1, $\Delta h_1(0) = 270$, она представима полиномом

$$h_1(x) = 45g_2(x) \cdot 3x = 45(1-x)^4 \cdot 3x \pmod{360},$$

а функция $h_2^0(x)$ не сохраняет 3-разности порядка $2-1$ и, следовательно, не представима полиномом. Итак, $f \notin Polyn$.

4.6 Критерии полиномиальности в терминах первых разностей

Рассмотрим числа k, свободные от кубов (не кратные кубу простого).

Пусть $p_1, \ldots, p_s, q_1, \ldots, q_t$ — попарно различные простые,

$$k = p_1^2 \cdots p_s^2 q_1 \cdots q_t, \quad s \geq 0, t \geq 0, \quad k \geq 2. \tag{4.16}$$

Рассмотрим делители числа k вида

$$Q_i = k/p_i^2, \quad d_i = k/p_i \ (i = 1, \ldots, s), \quad d_0 = p_1 \cdots p_s q_1 \cdots q_t. \tag{4.17}$$

Имеем $\text{НОД}(p_i^2, Q_i) = 1, \ d_i^2 \equiv 0 \pmod{k}$.

Теорема 4.7. *При условиях* (4.16) *и* (4.17) *справедливо включение* $Polyn \subseteq R(d_0)$.

Доказательство. Пусть $f \in Polyn$. На основании лемм 2.1, 2.2, 2.5 и следствия 2.1 получаем условие $f \in R(d_1) \cap \cdots \cap R(d_s)$. Согласно утверждению 2.10, $R(d_1) \cap \cdots \cap R(d_s) = R(\text{НОД}(d_1, \ldots, d_s)) = R(d_0)$. □

Итак, $Polyn \subseteq R(d_0)$. Кроме того, $Polyn \subseteq M(k)$. Это два необходимых условия полиномиальности.

Рассмотрим разложение (4.14) функции класса $M(k)$ в сумму периодических, соответствующую разложению k на простые множители (теорема 4.4):

$$f(\tilde{x}) = f(\tilde{0}) + \sum_{i=1}^{s} F_i(\tilde{x}) + \sum_{l=1}^{t} h_l(\tilde{x}), \tag{4.18}$$

где $F_i(\tilde{x}) = Q_i G_{p_i^2}(\tilde{x}), \ h_l(\tilde{x}) = (k/q_l) G_{q_l}(\tilde{x})$. При этом

$$F_i(\tilde{x}) = c_i Q_i F(c_i Q_i \tilde{x}), \ F(\tilde{x}) = f(\tilde{x}) - f(\tilde{0}), \quad c_i = Q_i^{-1} \pmod{p_i^2}.$$

Из этих формул и замкнутости класса $R(d_0)$ заключаем, что и функция F, и все функции F_i принадлежат $R(d_0)$. Функция F_i является p_i^2-периодической, $\text{НОД}(p_i^2, d_0) = p_i$, следовательно, по лемме 2.12, $F_i \in R(p_i)$.

Тем самым доказана

Теорема 4.8. *Если* $f \in Polyn$, *то в сумме* (4.18) *каждая* p_i^2*-периодическая функция* F_i *сохраняет* p_i*-разности.*

Это еще одно необходимое условие полиномиальности. Покажем его достаточность вместе с условием $f \in M(k)$.

Теорема 4.9. *Пусть* $f(\tilde{x}) \in M(k)$ *при условиях* (4.16) *и* (4.17), *и каждая* p_i^2*-периодическая функция* F_i *в разложении* (4.18) *сохраняет* p_i*-разности. Тогда* $f \in Polyn$.

Доказательство. При фиксированном $\tilde{\mu}$ из $E_{p_i}^n$ рассмотрим p_i-сеточное ограничение $F_i^{\tilde{\mu}}(\tilde{x})$. Эта функция кратна Q_i. Как и в случае $k = p^m$, нетрудно построить реализующий ее полином:

$$F_i^{\tilde{\mu}}(\tilde{x}) = Q_i g_{p_i}(\tilde{y}) \cdot \left(a_0(\tilde{\mu}) + \sum_{j=1}^{n} a_j(\tilde{\mu}) y_j \right),$$

где

$$\tilde{y} = \tilde{x} - \tilde{\mu},\ a_0(\tilde{\mu}), a_j(\tilde{\mu}) \in E_k, \quad Q_i g_{p_i}(\tilde{x}) = Q_i \prod_{j=1}^{n} \left(1 - x_j^{p_i - 1}\right)^{\varphi(p_i^2)}.$$

□

Достаточное условие полиномиальности при любом k дает следующая теорема.

Теорема 4.10. *Пусть* $k = p_1^{m_1} \cdots p_s^{m_s}$, $m_1 \geq 1, \ldots, m_s \geq 1$, $d_0 = p_1 \cdots p_s$. *Если* $f \in M(k) \cap R(d_0)$, *то* $f \in Polyn$.

Доказательство. Представим функцию f в виде суммы (4.14) $p_i^{m_i}$-периодических функций h_i. Каждая функция h_i сохраняет d_0-разности, НОД$(p_i^{m_i}, d_0) = p_i$, поэтому $h_i \in R(p_i)$. Кроме того, функция h_i кратна $d_i = k/p_i^{m_i}$. Тогда для каждого $\tilde{\mu}$ из $E_{p_i}^n$ функция $h_i^{\tilde{\mu}}(\tilde{x})$ представляется полиномом

$$h_i^{\tilde{\mu}}(\tilde{x}) = d_i g_{p_i}(\tilde{y}) \cdot \left(a_0(\tilde{\mu}) + \sum_{j=1}^{n} a_j(\tilde{\mu}) y_j \right),$$

где

$$\tilde{y} = \tilde{x} - \tilde{\mu},\ a_0(\tilde{\mu}), a_j(\tilde{\mu}) \in E_k, \quad d_i g_{p_i}(\tilde{x}) = d_i \prod_{j=1}^{n} \left(1 - x_j^{p_i - 1}\right)^{\varphi(p_i^{m_i})}.$$

□

Теорема 4.11. *При условиях* (4.16) *и* (4.17) *функция класса* $M(k)$ *представима полиномом в том и только том случае, когда она сохраняет* d_i*-разности для всех* $i = 1, \ldots, s$.

Доказательство. Необходимость сохранения всех d_i-разностей вытекает из лемм 2.1, 2.2, 2.5 и следствия 2.5.

Обратно: пусть $f \in M(k) \cap R(d_1) \cap \cdots \cap R(d_s)$. Тогда $f \in R(d_0)$, так как $d_0 =$ НОД$(d_1, \ldots, d_s)$. Следовательно, и все p_i^2-периодические функции F_i в разложении (4.18) сохраняют d_0-разности. Имеем НОД$(d_0, d_i) = p_i$, поэтому каждая функция F_i сохраняет p_i-разности и в силу теоремы 4.9 представима полиномом. Тогда и функция f представима полиномом в силу (4.18). □

4.7 Заключение к главе 4

Основные результаты главы следующие.

1. Достаточное условие полиномиальности при любом k — функция принадлежит классу $M(k)$ и является p-периодической, где $p|k$ (теорема 4.4). Канонический вид полинома, представляющего p-периодическую функцию, формулы (4.1), (4.12). Применение p-сеточных ограничений функции произвольной k-значной логики и p-периодических полиномов для построения канонического полинома функции как суммы p-сеточных ограничений.

2. Необходимые (теорема 4.1) и достаточные (теорема 4.2) условия полиномиальности функции p^m-значной логики.

3. Алгоритм распознавания полиномиальности и построения полинома функции p^m-значной логики. Оценка (полиномиальная) временной сложности алгоритма (теорема 4.3).

4. Обобщение условий полиномиальности при $k = p^m$ на случай произвольного составного k с использованием разложения функций в суммы $p_i^{m_i}$-периодических (теоремы 4.5–4.10, следствие 4.1). Критерий полиномиальности в терминах первых d_i-разностей ($d_i|k$) для всех k, не кратных кубу простого (теорема 4.11).

Глава 5

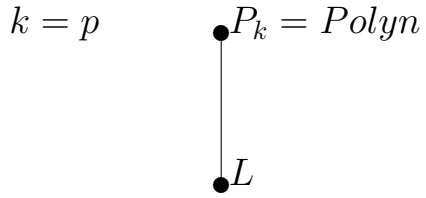
Решетка замкнутых классов

В этой главе мы рассматриваем фрагменты решетки $\mathcal{L}(P_k)$ замкнутых классов в P_k, определяемых введенными аддитивными представлениями, в частности, классов, содержащих все линейные функции, т. е. интервал $I(L; P_k)$.

При всех $k \geq 2$ имеют место включения

$$L \subset Polyn \subseteq M(k) \subseteq P_k.$$

Если $k = p$, то справедливы равенства $Polyn = M(k) = C(p) = P_k$, а класс L является предполным в P_k, т. е. весь интервал $I(L; P_k)$ состоит из одного ребра:



Исторически первыми в этой области следует признать результаты А. В. Кузнецова [86]:

1) при простом k класс полиномов равен P_k, при составном — $Polyn$ есть собственный подкласс в P_k, не являющийся максимальным (предполным);

2) при простом k класс линейных функций L является предполным в классе всех полиномов (т. е. в P_k).

Эти результаты порождают проблему описания решетки классов, содержащих все полиномы (интервал $I(Polyn; P_k)$), и классов, содержащих все линейные функции (более обширный интервал $I(L; P_k)$, включающий предыдущий), в решетке $\mathcal{L}(P_k)$ всех замкнутых классов при составных k.

Решение проблемы зависит от разложения k на простые множители.

Для описания интервала $I(Polyn; P_k)$ полезны условия полиномиальности функций в P_k, как необходимые (некоторые из них формулируются довольно

просто), так и достаточные. Необходимые условия, сохраняемые суперпозициями функций, определяют замкнутые классы.

Несложное необходимое и достаточное условие сформулировано Н. Н. Айзенбергом и И. В. Семйоном в 1971 г. для k, не кратных квадрату простого числа: оно состоит в сохранении сравнений (эквивалентностей на множестве E_k) по каждому из простых множителей, образующих число k. В связи с этим было начато изучение интервала $I(M(k); P_k)$ не только при $k = p_1 \cdots p_s$ (когда $Polyn = M(k)$), но и в более общих случаях. В 1983 г. А. Н. Черепов описал этот интервал для всех k, свободных от квадратов, он же в 1986 г. решил эту задачу для произвольного k. Описание ввиду его большой общности получилось довольно сложным, многие частные эффекты не выделялись.

Особое внимание многие исследователи (А. Н. Черепов [84] , Г. П. Гаврилов [54, 55], М. В. Заец [58], А. А. Нечаев [67], А. Б. Ремизов [73], L. Carlitz [90] и др. уделили случаю $k = p^m$. В частности, А. Н. Черепов в 1986 г. показал, что интервал $I(M(k); P_k)$ в таком случае изоморфен m-мерному кубу. В дальнейшем выяснилось, что m-мерному кубу изоморфен и интервал $I(Polyn; M(k))$ при $k = p_1^2 \cdots p_m^2 p_{m+1} \cdots p_t$, $1 \le m \le t$, [6, 24, 73].

В 1980 г. А. А. Нечаев нашел критерий полноты относительно класса полиномов при $k = p^n$ [67], эта же задача для $k = p_1 \cdots p_s$ решена А. Н. Череповым в 1983 г. [83].

Большие ожидания связаны со значением $k = 4$ (наименьшее составное число, важность в практичесих вычислениях). Используя специфику полиномов по модулю 4, в [60] полностью построен интервал $I(L; Polyn)$ решетки $\mathcal{L}(P_4)$.

Ранее, в 1989 г., важнейший результат получен А. Б. Ремизовым [73]: если k кратно кубу простого, то интервал $I(Polyn; M(k))$ бесконечен, он содержит бесконечно возрастающую цепь замкнутых классов. Мощность его, как и мощность множества бесконечных цепей, выяснить не удалось. При этом А. Б. Ремизов, как и другие авторы (Н. Н. Айзенберг и И. В. Семйон, А. А. Нечаев, А. Н. Черепов, Г. П. Гаврилов, М. В. Заец), применял метод координатных функций при $k = p^m$ — функций p-значной логики, которые, домноженные на последовательные степени p, однозначно определяют p^m-значную функцию. Этот метод известен в алгебре и теории чисел, он оказался плодотворным и в функциональных системах k-значной логики, однако его применимость ограничивается значениями $k = p^m$.

В связи с результатом А. Б. Ремизова в p^3-значной логике с помощью критерия полиномиальности в терминах p-разностей второго порядка (см. гл. 4) соискателю удалось выделить максимальный подкласс в интервале $I(Polyn; M(p^3))$, отличный от $M(p^3)$ [4]. Его лаконичное описание — в разделе 4 данной главы. Выяснилось (замечание 5.1), что этот класс описывается и другими способами [54, 58]. (Различные авторы используют различные языки, проблема перевода,

отыскания эквивалентностей и аналогий типична для математического творчества.)

В работах Г. П. Гаврилова [54, 55] описаны конечные множества классов из интервала $I(Polyn; M(p^m))$. Они определяются аддитивными формулами, в качестве слагаемых берутся координатные функции. Специальные критерии полиномиальности не применяются, возможность или невозможность полиномиальной реализации функции выясняется анализом системы уравнений для коэффициентов полинома.

М. В. Заец, В. Г. Никонов и А. Б. Шишков [57, 58] используют координатные функции и особые системы уравнений для их последовательного вычисления, при этом уравнения над кольцом вычетов по модулю p^m сводятся к уравнениям над $\mathbb{Z}_p$ (так называемая варионно-координатная полиномиальность, заимствована из алгебры). Им удалось описать конечное множество классов, некоторые из которых совпадают с нашими.

Во многих указанных работах проявляется отличие случаев $p = 2$ и $p \geq 3$.

Материал главы разбит на пять разделов.

В первом описан интервал $I(Polyn; P_k)$ при всех k, не кратных кубу простого числа.

Во втором разделе анализируется интервал $I(L; Polyn)$ для всех k, свободных от квадратов (при этом $Polyn = M(k)$).

В разделе 5.3 описан интервал $I(L; P_k)$ при $k = pq$.

В разделе 5.4 характеризуется максимальный подкласс в интервале $I(Polyn; M(k))$ при $k = p^3$.

Раздел 5.5 содержит описание интервала $I(L; P_k)$ при всех $k = p^2$, оно обобщает результаты [60].

Наконец, в разделе 5.6 приведен фрагмент интервала $I(L; P_k)$ при $k = p^3$, содержащий классы, рассмотренные в предыдущих главах.

5.1 Классы, содержащие все полиномы

Рассмотрим интервал $I(Polyn; P_k)$. Его часть, интервал $I(M(k); P_k)$, полностью описан А. Н. Череповым, поэтому уделим основное внимание интервалу $I(Polyn; M(k))$, а также классам, не сравнимым с $M(k)$.

Рассмотрим числа k, свободные от кубов (не кратные кубу простого).

Пусть $p_1, \ldots, p_s, q_1, \ldots, q_t$ — попарно различные простые,

$$k = p_1^2 \cdots p_s^2 q_1 \cdots q_t, \quad s \geq 0, t \geq 0, \quad k \geq 2. \tag{5.1}$$

Будем иметь дело с делителями числа k вида

$$Q_i = k/p_i^2, \quad d_i = k/p_i \ (i = 1, \ldots, s), \quad d_0 = p_1 \cdots p_s q_1 \cdots q_t. \tag{5.2}$$

Имеем $\text{НОД}(p_i^2, Q_i) = 1,\ d_i^2 \equiv 0 \pmod{k}$.

Сначала рассмотрим наиболее простой случай $s = 1,\ t = 0$.

Теорема 5.1. *При $k = p^2$ класс $Polyn$ является предполным в $M(k)$.*

Доказательство. Имеем $M(k) = C(p)$, $Polyn = R(p)$. Пусть $d = p$, тогда $k = pd$ и в силу теоремы 2.2 класс $R(d)$ является предполным в $C(d)$. □

Теперь рассмотрим общий случай, описываемый условиями (5.1) и (5.2). Пусть

$$S = \{1, \ldots, s\}, \quad I \subseteq S, \quad MR(I) = M(k) \cap \left(\bigcap_{i \in I} R(d_i) \right).$$

Следствие 5.1. *Справедливы следующие соотношения.*

1. *Если $I = \{i_1, \ldots, i_t\}$, то $MR(I) = M(k) \cap R(НОД(d_{i_1}, \ldots, d_{i_t}))$.*
2. *$MR(S) = Polyn, \quad MR(\emptyset) = M(k)$.*
3. *Если $I_1 \subseteq I_2$, то $MR(I_1) \supseteq MR(I_2)$.*

Утверждение 5.1. *Если $f(\tilde{x}) \in MR(I)$, то функцию f можно представить в виде*

$$f(\tilde{x}) = \pi(\tilde{x}) + \sum_{j \notin I} F_i(\tilde{x}),$$

где

$$\pi(\tilde{x}) \in Polyn, \quad F_j(\tilde{x}) = Q_j G_{p_j^2}(\tilde{x}).$$

Доказательство. Рассмотрим сумму (4.18), представляющую такую функцию f. Все слагаемые h_l представимы полиномами как периодические с простыми периодами. Представимы полиномами также все слагаемые F_i, для которых $i \in I$, они сохраняют d_i-разности. Остаются слагаемые с номерами $j, j \notin I$. □

Следствие 5.2. *Полной в классе $MR(I)$ является система функций*

$$\{1,\ x + y,\ xy\} \cup \left(\bigcup_{j \notin I} \{Q_j g_{p_j^2}(x, y)\} \right).$$

Следствие 5.3. *Классы $MR(I)$ образуют решетку, изоморфную решетке всех подмножеств множества S.*

Особо выделим случай $s = 0$.

Следствие 5.4. *Если $k = q_1 \cdots q_t$, то $Polyn = M(k) = C(q_1, \ldots, q_t)$.*

Следствие 5.5. *Если $k = q$, то $Polyn = P_k$.*

Теорема 5.2. *Равенство $Polyn = M(k)$ имеет место в точности при $k = q_1 \cdots q_t$.*

Доказательство. Справедливость равенства при $k = q_1 \cdots q_t$ следует из теоремы 3.4 и утверждения 3.3.

Обратно: пусть k кратно p^2, т. е. $k = p^m Q$, $m \geq 2$, НОД$(p, Q) = 1$, $Q \geq 1$, и пусть $d = p^{m-1}Q$. Тогда d^2 кратно k, функция $dg_{p^m}(x, y)$ не сохраняет d-разности и принадлежит $M(k) \setminus Polyn$. □

Следствие 5.6. *Равенство $Polyn = P_k$ справедливо только при $k = q$.*

5.2 Интервал $I(L; Polyn)$ для k, свободного от квадратов

Всюду в данном разделе простые числа $p_1, \ldots, p_s$ попарно различны,

$$k = p_1 \cdots p_s,\ s \geq 2, \quad d_i = k/p_i,\ i = 1, \ldots, s. \tag{5.3}$$

При этих условиях имеют место равенства $Polyn = M(k) = C(p_1, \ldots, p_s)$, базисом этого класса является система функций $\{x+y,\ d_1 g_{p_1}(x, y), \ldots, d_s g_{p_s}(x, y)\}$, причем для каждого $p_i \neq 2$ базисную функцию $d_i g_{p_i}(x, y)$ можно заменить на одноместную $d_i g_{p_i}(x)$.

В разделе 2.10 введены классы

$$L_{d_i} M_k = L(d_i) \cap M(k),\ i = 1, \ldots, s,$$

для каждого из них найдена каноническая формула функций, ее можно записать как

$$f(x) = \ l_i(\tilde{x}) + p_i G_{d_i}(\tilde{x}).$$

Применим к каждому слагаемому $p_i G_{d_i}(\tilde{x})$ леммы 1.4 и 1.5 о разложении функций в сумму периодических, получим каноническую формулу

$$f(\tilde{x}) = l(\tilde{x}) + \sum_{j \neq i} h_j(\tilde{x}), \quad \text{где } h_j(\tilde{x}) = d_j G_{p_j}(\tilde{x}), \tag{5.4}$$

для элементов класса $L_{d_i} M_k$.

Следствие 5.7. *Базис в классе $ML(d_i)$ образует система функций*

$$\{1, x + y\} \cup \left(\bigcup_{j \neq i} \{d_j g_{p_j}(x, y)\} \right),$$

и для каждого $p_j \neq 2$ базисную функцию $d_j g_{p_j}(x, y)$ можно заменить на одноместную функцию $d_j g_{p_j}(x)$.

Пусть

$$S = \{1, \ldots, s\}, \quad I \subseteq S, \quad ML(I) = \bigcap_{i \in I} ML(d_i).$$

Следствие 5.8. *Справедливы следующие соотношения.*

1. *Если* $I = \{i_1, \ldots, i_t\}$, *то* $ML(I) = ML(d_0)$, *где* $d_0 = НОД(d_{i_1}, \ldots, d_{i_t})$.
2. $ML(S) = L, \quad ML(\emptyset) = Polyn.$
3. *Если* $I_1 \subseteq I_2$, *то* $ML(I_1) \supseteq ML(I_2)$.

Следствие 5.9. *Если* $f \in ML(I)$, *то функцию* f *можно представить в виде*

$$f(\tilde{x}) = l(\tilde{x}) + \sum_{j \notin I} F_i(\tilde{x}), \quad \text{где} \quad F_j(\tilde{x}) = d_j G_{p_j}(\tilde{x}). \tag{5.5}$$

Следствие 5.10. *Полной в классе* $ML(I)$ *является система функций*

$$\{1, x + y\} \cup \left(\bigcup_{j \notin I} \{d_j g_{p_j}(x, y)\} \right),$$

и для каждого $p_j \neq 2$ *базисную функцию* $d_j g_{p_j}(x, y)$ *можно заменить на одноместную функцию* $d_j g_{p_j}(x)$.

Теорема 5.3. *Пусть* $k = p_1 \cdots p_s, \quad s \geq 2, \quad d | k, d \neq k,$ *и пусть* p *— одно из чисел* $p_1, \ldots, p_s$, *не входящее в разложение* d. *Тогда класс* $ML(d)$ *является предполным в классе* $ML(pd)$.

Доказательство. Введем обозначение $Q = k/p$.

Пусть $f \in ML(pd) \setminus ML(d)$. Покажем, что замыкание $[ML(d) \cup \{f\}]$ содержит функцию $Qg_p(x, y)$ и, следовательно, весь класс $ML(pd)$. Представим функцию f в виде, аналогичном (5.5). Вычитая функции класса $ML(d)$, получим p-периодическую кратную Q функцию, она также не принадлежит $ML(d)$. Кроме того, она нелинейна, не сохраняет 1-разности, поэтому из нее с помощью линейных функций можно получить двухместную и (только при $p \neq 2$) одноместную функцию (назовем ее H) с теми же свойствами.

Если $p = 2$, **то** имеем 2-периодическую кратную Q нелинейную функцию $H(x, y)$. Линейными преобразованиями добьемся, чтобы

$$H(0, 0) = H(1, 0) = H(0, 1) = 0.$$

Тогда $H(1, 1) = Q$, $H(x, y) = Qg_2(x - 1, y - 1)$ и $Qg_2(x, y) = H(x + 1, y + 1)$.

Если $p > 2$, **то** имеем 2-периодическую кратную Q функцию $H(x)$. Достаточно показать, что $Qg_p(x) \in [ML(d) \cup \{H\}]$. Линейными преобразованиями добьемся, чтобы $H(0) = H(1) = 0$. Введем обозначения:

$$H(i) = y_i = a_i Q, \ i \in E_p, \ \text{НОД}(a_i, p) = 1;$$

при этом $y_0 = y_1 = 0$, не ограничивая общности полагаем $y_2 = Q$ (иначе умножим функцию $H(x)$ на константу);
$W(H)$ (*вес* функции H) — количество ненулевых значений y_i, при этом $1 \le W(H) \le p-2$;
$\sigma(H) = y_0 + \cdots + y_{p-1}$ (сумма в кольце целых чисел).

Если $p = 3$, то $H(x) = a_2 Q g_3(x-2)$, для получения $Qg_3(x)$ остается выполнить линейные преобразования функции H (умножение на константу и сдвиг аргумента).

Если $p > 3$, то возможны следующие случаи.

Случай 1: $W(H) = 1$ и $H(x) \ne 0$ при $x = i_0$. Тогда $H(x) = a_{i_0} Q g_p(x - i_0)$, остается выполнить линейные преобразования функции H.

Случай 2: $W(H) > 1$ и НОД$(\sigma(H), p) = 1$. Рассмотрим функцию

$$F(x) = H(x) + H(2x) + \cdots + H((p-1)x).$$

Она является p-периодической, $F(0) = 0$, а если $1 \le i \le p-1$, то $F(i) = \sigma(H)$. Тогда $\sigma(H) - F(x) = \sigma(H) g_p(x)$. Остается только умножить полученную функцию на константу.

Случай 3: $W(H) > 1$ и $\sigma(H)$ кратно p. Будем последовательно уменьшать вес рассматриваемой функции, пока не получим вес 1.

Подслучай 3а: для некоторого $j \in E_p$ выполняется условие $H(y_j) \ne y_j$.

Если при этом $H(Q) = 0$, то для некоторого j_1, $2 < j_1 \le p-1$ имеем $y_{j_1} = H(y_{j_1}) \ne 0$. Рассмотрим функцию $F(x) = H(H(x))$. Если $H(x_0) = 0$ в некоторой точке x_0, то и $F(x_0) = 0$, кроме того, $F(Q) = 0$, $F(j_1) \ne 0$, поэтому $1 \le W(F) < W(H)$.

Если же $H(Q) = Q$, то рассмотрим функцию $F(x) = H(H(x)) - H(x)$. Если $H(x_0) = 0$ в некоторой точке x_0, то и $F(x_0) = 0$, кроме того, $F(Q) = 0$, $F(j) \ne 0$, поэтому $1 \le W(F) < W(H)$.

Подслучай 3: для всех $j \in E_p$ выполняется условие $H(y_j) = y_j$ (назовем это свойство *стабильностью*). Приведем примеры стабильных функций и их преобразований.

Пример 1. $k = 15$, $p = 5$, $Q = 3$,

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$H(x)$	0	0	3	3	9	0	0	3	3	9	0	0	3	3	9
$H(-x)$	0	9	3	3	0	0	9	3	3	0	0	9	3	3	0

Пример 2. $k = 14$, $p = 7$, $Q = 2$,

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$H(x)$	0	0	2	10	0	0	2	0	0	2	10	0	0	2
$H(-x)$	0	2	0	0	10	2	0	0	2	0	0	10	2	0

Теперь продолжим доказательство теоремы. Рассмотрим функцию $F(x) = H(-x)$. Она p-периодична и принимает те же значения, что $H(x)$, но в других точках, поэтому $W(F) = W(H)$, $\sigma(F) = \sigma(H)$. Покажем, что функция F не стабильна.

Положим $z_j = F(j)$, $j = 0, \ldots, p-1$. Допустим, что $\forall j \in E_p\ (F(z_j) = z_j)$, т. е. $\forall j \in E_p\ (H(-H(j)) = H(-j))$. Обозначим $i = -j \pmod p$. Тогда $\forall i \in E_p\ (H(-H(i) = H(i))$. Учтем, что $H(i) = y_i = H(y_i)$, получим

$$\forall i \in E_p\ (H(y_i) = y_i = H(-y_i)).$$

Следовательно, значения $y_2, \ldots, y_{p-1}$ (их количество $p-2$ нечетно) разбиваются на пары одинаковых, т. е. их количество четно, противоречие. Итак, случай стабильности сводится к предыдущему. Во всех случаях $[ML(d) \cup \{f\}] = ML(pd)$. $\square$

Следствие 5.11. *При условиях* (5.3) *замкнутые классы полиномов, содержащие все линейные функции, образуют решетку, изоморфную s-мерному кубу. Они имеют вид $ML(I)$, $I \subseteq \{1, \ldots, s\}$. Атомы решетки — классы $ML(p_i)$, коатомы — классы $ML(d_i)$.*

5.3 Интервал $I(L; P_k)$ для $k = pq$

При $k = pq$, $p \neq q$, имеют место равенства $Polyn = M(k) = C(p, q)$, интервал $(L; Polyn)$ есть двухмерный куб (квадрат). Классы $C(p)$ и $C(q)$ являются предполными в P_k. Класс $C(p, q)$ является предполным в каждом из классов $C(p)$ и $C(q)$ в силу утверждения 1.18. Дополним этот фрагмент.

1. Имеются классы $C_p(p)$ и $C_q(q)$, они являются предполными в $C(p)$ и $C(q)$ соответственно согласно теореме 1.2.

2. Имеются классы $R(p)$ и $R(q)$, они являются предполными в $C(p)$ и $C(q)$ соответственно согласно теореме 2.2.

3. Имеются классы $L(p)$ и $L(q)$, они являются предполными в $R(p)$ и $R(q)$ соответственно согласно теореме 2.3.

4. Имеются классы $S(p)$ и $S(q)$. Согласно теоремам 2.4 и 2.5 класс $S(p)$ является предполным в классах $R(p)$ и $C_p(p)$, а $S(q)$ — предполным в $R(q)$ и $C_q(q)$.

5. Имеются классы $K(p)$ и $K(q)$, они являются предполными в $L(p)$ и $L(q)$ соответственно согласно теореме 3.1, класс L является предполным в $K(p)$ и $K(q)$ согласно теореме 3.2.

6. В предыдущем разделе определены класс

$$ML(p) = M(k) \cap R(p) = [1,\ x + y,\ qg_p(x, y)]$$

всех функций вида

$$l(\tilde{x}) + qG_p(\tilde{x})$$

и класс

$$ML(q) = M(k) \cap R(q) = [1,\ x + y,\ pg_q(x, y)]$$

всех функций вида

$$l(\tilde{x}) + pG_q(\tilde{x}).$$

Следствие 5.12. *Имеют место равенства*

$$ML(p) = C(p) \cap C_q(q), \quad ML(q) = C(q) \cap C_p(p).$$

Утверждение 5.2. *Класс $ML(p)$ является предполным в $C_q(q)$, класс $ML(q)$ — предполным в $C_p(p)$.*

Доказательство. Если $f \in C_q(q) \setminus ML(p)$, то $f \in C(q) \setminus C(p)$. Далее все так же, как при выводе утверждений 1.17 и 1.18 с применением леммы 1.12. □

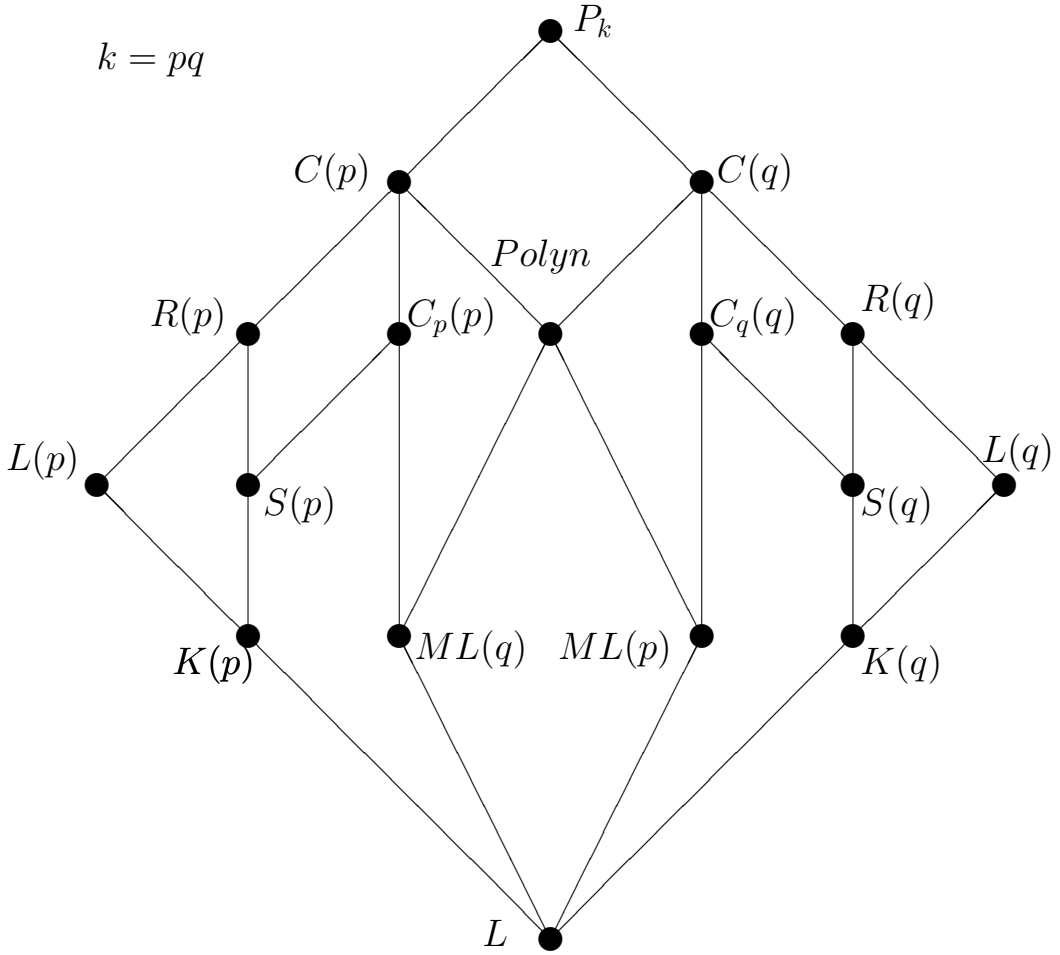
Из теоремы 5.3 получаем

Следствие 5.13. *Классы $ML(p)$ и $ML(q)$ являются предполными в $M(k)$, класс*

$$L = ML(p) \cap R(1) = ML(q) \cap R(1)$$

— предполным в каждом из классов $ML(p)$ и $ML(q)$.

Изобразим диаграмму решетки всех рассмотренных классов.



Резюмируем важнейшие сведения о каждом классе.

Класс	Канонические формулы	Базис
P_k	$f(\tilde{x}) = \sum_{\tilde{a} \in E_k^n} f(\tilde{a}) j(\tilde{x} - \tilde{a})$	$\{x + y,\ j(x)\}$
$C(p)$	$l(\tilde{x}) + G_p(\tilde{x}) + pF(\tilde{x})$	$\{x + y,\ g_p(x, y),\ pj(x, y)\}$; $\{x + y,\ g_p(x, y),\ pg_q(x, y)\}$
$Polyn = C(p, q)$	$f(\tilde{x}) = f(\tilde{0}) + qG_p(\tilde{x}) + pG_q(\tilde{x})$	$\{x + y,\ qg_p(x, y),\ pg_q(x, y)\}$
$C_p(p)$	$l(\tilde{x}) + pF(\tilde{x})$	$\{1,\ x + y,\ pj(x, y)\}$
$R(p)$	$l(\tilde{x}) + G_p(\tilde{x}) + H_p(\tilde{x})$	$\{x + y,\ g_p(x, y),\ \chi_p(x)\}$
$S(p)$	$l(\tilde{x}) + pG_p(\tilde{x}) + H_p(\tilde{x})$	$\{1,\ x + y,\ \chi_p(x)\}$
$L(p)$	$l(\tilde{x}) + G_p(\tilde{x})$	$\{x + y,\ g_p(x, y)\}$
$K(p)$	$l(\tilde{x}) + pG_p(\tilde{x})$	$\{1,\ x + y,\ pg_p(x)\}$
$ML(p)$	$l(\tilde{x}) + qG_p(\tilde{x})$	$\{1,\ x + y,\ qg_p(x, y)\}$
L	$l(\tilde{x})$	$\{1,\ x + y\}$

Точно такие же классы получаются при взаимной замене p на q.

5.4 Максимальный подкласс в $M(k)$, содержащий все полиномы при $k = p^3$

При $k = p^3$ согласно [73] интервал $I(Polyn; M(k))$ бесконечен. Найдем в этом интервале максимальный подкласс класса $M(k)$.

Имеем $M(k) = C(p, p^2)$. Согласно следствию 1.2 функции этого класса представляются в виде (1.5). Полагая $d = p^2, e = p$, получаем следующую формулу:

$$f(\tilde{x}) = l(\tilde{x}) + G_p(x) + pG_{p^2}(\tilde{x}) + p^2F(\tilde{x}).$$

Здесь функция G_p в силу p-периодичности представима полиномом.

Следствие 5.14. *Функции класса $M(p^3)$ представляются в виде*

$$f(\tilde{x}) = \pi(\tilde{x}) + pG_{p^2}(\tilde{x}) + p^2F(\tilde{x}), \quad \pi(\tilde{x}) \in Polyn. \tag{5.6}$$

Полной в классе $M(p^3)$ является система функций

$$\{1,\ x + y,\ xy,\ pg_{p^2}(x, y),\ p^2j(x, y)\}.$$

Если $p \neq 2$, то полной является также система $\{1,\ x+y,\ xy,\ pg_{p^2}(x),\ p^2j(x)\}$.

Определим M_1 как подкласс в $M(p^3)$, состоящий из всех функций вида

$$f(\tilde{x}) = \pi(\tilde{x}) + p^2F(\tilde{x}), \quad \pi(\tilde{x}) \in Polyn. \tag{5.7}$$

Следствие 5.15. *Класс M_1 замкнут и порождается системой функций*

$$\{1,\ x + y,\ xy,\ p^2j(x, y)\}.$$

Если $p \neq 2$, то функцию $p^2j(x, y)$ в этой системе можно заменить на $p^2j(x)$.

Теорема 5.4. *Класс M_1 является предполным в $M(p^3)$.*

Доказательство. Пусть $f \in M(p^3) \setminus M_1$. Представим функцию f в виде (5.6) Вычтем слагаемые $\pi(\tilde{x})$, $p^2F(\tilde{x})$, они принадлежат M_1. Получим функцию $h(\tilde{x}) = = pG_{p^2}(\tilde{x})$, $h \notin M_1$, при этом $h \in C(p) \setminus R(p)$. Тогда имеем полную аналогию со случаем $k = p^2$, $h \in C(p) \setminus R(p)$. Так же, как при выводе теоремы 2.2, убеждаемся, что замыкание $[M_1 \cup \{f\}]$ (оно включает в себя $[M_1 \cup \{h\}]$) содержит функцию $pg_{p^2}(x, y)$ и, следовательно, весь класс $M(p^3)$. □

Замечание 5.1. В [54] Г. П. Гавриловым для $k = p^m$ построена цепь классов $V_m(l)$, $l = 1, \ldots, m-1$, состоящих из функций вида

$$f(\tilde{x}) = \pi(\tilde{x}) + p^l F(\tilde{x}), \quad \pi(\tilde{x}) \in Polyn.$$

При этом $M_1 = V_3(2)$. Свойства такого класса и теорема 5.4 получены автором в [4].

Также в работе М. В. Заеца [58] описан класс $\mathcal{CP}_{p^m}$ так называемых *вариационно-координатно-полиномиальных* над кольцом $\mathbb{Z}_{p^m}$ функций. Он оказался равен классу $V_m(m-1)$ Г. П. Гаврилова. Таким образом,

$$M_1 = V_3(2) = \mathcal{CP}_{p^3}.$$

5.5 Интервал $I(L; P_k)$ при $k = p^2$

При $k = p^\alpha$ одна и та же функция класса $Polyn$ как отображение $E_k^n \mapsto E_k$ может быть реализована несколькими полиномами над $\mathbb{Z}_k$. Всегда будут рассматриваться только *приведенные полиномы*, т. е. такие, в которые каждая переменная входит в степени не выше $p\alpha - 1$, однако и приведенный полином не единствен, например, $px^p \equiv px \pmod{p^2}$.

5.5.1 Классы K_m

Положим $K_1 = L$. Для каждого $m \in \mathbb{N}$, $m \geq 2$, определим K_m как класс функций, представимых приведенными полиномами следующего вида:

$$l(\tilde{x}) + \sum_{r=1}^{n} \sum_{j_1,\ldots,j_r;\ m_1,\ldots,m_r} a(j_1, \ldots, j_r;\ m_1, \ldots, m_r) \cdot p x_{j_1}^{m_1} \cdots x_{j_r}^{m_r}, \tag{5.8}$$

где

$$1 \leq j_1 < j_2 < \cdots < j_r \leq n, \quad m_1, \ldots, m_r \in \{1, 2, \ldots, 2p-1\},$$
$$a(j_1, \ldots, j_r;\ m_1, \ldots, m_r) \in E_p,$$
$$2 \leq m_1 + \cdots + m_r \leq m \tag{5.9}$$

(сумма в кольце целых чисел). Другими словами, каждый нелинейный моном имеет степень не выше m и коэффициент, кратный p.

Легко проверяемые свойства классов K_m следуют из их определения.

Утверждение 5.3. *Классы K_m обладают следующими свойствами.*

1. *Если $m \geq 2$, $m_1 < m$, то $K_{m_1} \subset K_m$. Включение строгое, так как полином*

$$\phi_m(x_1, \ldots, x_m) = px_1 \cdots x_m$$

принадлежит разности классов $K_m \setminus K_{m_1}$.

2. *Класс K_m замкнут относительно введения и удаления фиктивных переменных функций, а также относительно линейных операций над функциями.*

3. *Если $f(\tilde{x}) \in K_1$, то $\phi_1(f(\tilde{x})) \in K_1$. Если $m \geq 2$ и $f(\tilde{x}) \in K_m$, то $\phi_m(f(\tilde{x}), y_2, \ldots, y_m) \in K_m$.*

Утверждение 5.4. *Для каждого $m \geq 2$ класс K_m замкнут и система функций*

$$A_m = \{1,\ x + y,\ \phi_m(x_1, \ldots, x_m)\}$$

является базисом этого класса.

Доказательство. Покажем, что $K_m \subseteq [A_m]$. Если функция $f(x_1, \ldots, x_n)$ из K_m реализуется приведенным полиномом (5.8), то каждый нелинейный моном можно получить из функции $\phi_m(y_1, \ldots, y_m)$ подстановкой переменных $x_1, \ldots x_n$ и констант. Складывая такие мономы, получим нелинейную часть полинома (5.8), его линейная часть порождается подсистемой $\{1, x + y\}$. Таким образом, $f(x_1, \ldots, x_n) \in [A_m]$ и требуемое включение выполнено.

Обратное включение легко проверяется индукцией по сложности формулы над A_m, задающей функцию из $[A_m]$. Индуктивный переход осуществляется с применением свойств, перечисленных в утверждении 5.3.

Полнота системы A_m в классе K_m установлена. Покажем, что любая ее собственная подсистема не полна в K_m. Подсистема $A_m \setminus \{1\}$ порождает только функции, сохраняющие константу 0, подсистема $A_m \setminus \{x + y\}$ — только мономы, подсистема $A_m \setminus \{\phi_m\}$ — только собственный подкласс L в K_m. Таким образом, A_m есть базис в K_m. □

Из леммы 2 статьи [60] получаем

Следствие 5.16. *Если полином f над $\mathbb{Z}_p$ имеет степень $m \geq 2$, то система $\{1,\ \ x + y \pmod p,\ \ f\}$ порождает полином $x_1 \cdots x_m$.*

Для полиномов над $\mathbb{Z}_{p^2}$ совершенно аналогично выводится

Утверждение 5.5. *Если $m \geq 2$ и полином f над $\mathbb{Z}_{p^2}$ принадлежит разности классов $K_m \setminus K_{m-1}$, то система $\{1,\ x+y,\ f\}$ порождает полином $\phi_m(x_1, \ldots, x_m)$.*

Следствие 5.17. *Если $m \geq 2$, то каждый класс K_{m-1} является предполным в K_m и существует неуплотняемая бесконечная возрастающая цепь*

$$L = K_1 \subset K_2 \subset \cdots \subset K_{m-1} \subset K_m \subset \cdots$$

Предел этой цепи — замкнутый класс

$$K_\infty = \bigcup_{m=1}^{\infty} K_m,$$

состоящий из функций, представимых приведенными полиномами (5.8), *но при этом неравенства* (5.9) *заменяются одним неравенством*

$$m_1 + \cdots + m_r \geq 2.$$

Он не имеет базиса и порождается системой

$$A_\infty = \{1, x+y\} \cup \left(\bigcup_{m=1}^{\infty} \{\phi_m\} \right).$$

5.5.2 Классы Λ_m

Для каждого $m \in \mathbb{N}$, $m \geq p$, определим Λ_m как класс функций, представимых приведенными полиномами

$$l(\tilde{x}) + \sum_{r=1}^{n} \sum_{j_1,\ldots,j_r;\ m_1,\ldots,m_r} a(j_1,\ldots,j_r;\ m_1,\ldots,m_r) \cdot p x_{j_1}^{m_1} \cdots x_{j_r}^{m_r} + \sum_{j=1}^{n} b_j x_j^p, \quad (5.10)$$

где

$$1 \leq j_1 < j_2 < \cdots < j_r \leq n, \quad m_1,\ldots,m_r \in \{1,2,\ldots,2p-1\},$$
$$a(j_1,\ldots,j_r;\ m_1,\ldots,m_r), b_j \in E_p,$$

и выполняются неравенства (5.9). (Другими словами, каждый моном либо принадлежит классу K_m, либо имеет вид bx^p, НОД$(b,p) = 1$.) Легко проверяемые свойства классов Λ_m следуют из их определения.

Следствие 5.18. *Классы Λ_m обладают следующими свойствами.*

1. *Справедливо включение $\Lambda_m \subset K_m$.*
2. *Если $p \leq m_1 < m$, то $\Lambda_{m_1} \subset \Lambda_m$.*
3. *Класс Λ_m замкнут относительно введения и удаления фиктивных переменных функций, а также относительно линейных операций над функциями.*
4. *Если $f(\tilde{x}) \in \Lambda_m$, то $\phi_m(f(\tilde{x}), y_2, \ldots, y_m) \in \Lambda_m$.*
5. *Если $f(\tilde{x}) \in \Lambda_m$, то $(f(\tilde{x}))^p \in \Lambda_m$.*

Последнее свойство проверяется с помощью тождеств

$$px^p \equiv px, \quad x^{p^2} \equiv x^p \pmod{p^2}. \tag{5.11}$$

Утверждение 5.6. *Для каждого $m \geq p$ класс Λ_m порождается системой функций*

$$B_m = \{1,\ x+y,\ \phi_m(x_1,\ldots,x_m),\ x^p\}.$$

Эта система является базисом класса Λ_m при $m \geq p+1$, а базис класса Λ_p составляет система

$$C = \{1, x+y, x^p\}.$$

Доказательство. Включение $\Lambda_m \subseteq [B_m]$ обосновывается так же, как при доказательстве утверждения 1. Обратное включение доказывается индукцией по сложности формулы над B_m, задающей функцию из $[B_m]$; индуктивный переход проводится с использованием свойств, перечисленных в следствии 5.18. Таким образом, $\Lambda_m = [B_m]$ при всех $m \geq p$.

Рассмотрим собственные подсистемы системы B_m.

Подсистема $B_m \setminus \{1\}$ порождает только функции, сохраняющие константу 0;
подсистема $B_m \setminus \{x+y\}$ — только мономы;
подсистема $B_m \setminus \{x^p\} = A_m$ порождает не весь класс Λ_m, а только его собственный подкласс K_m.

Рассмотрим подсистему $B_p \setminus \{\phi_p\} = C$. Покажем, что $[C] \subseteq \Lambda_p$, индукцией по сложности формулы над C, задающей функцию из $[C]$. Базис индукции составляет очевидное включение $C \subseteq \Lambda_p$. Индуктивный переход осуществляется с помощью свойств 3–5 следствия 5.18.

Таким образом, любая собственная подсистема системы B_m не является полной в Λ_m, система B_m — базис этого класса.

Установлено, что $[C] \subseteq \Lambda_p$. Докажем обратное включение, выразив полином $\phi_p(x_1,\ldots,x_p)$ через элементы системы C. Сделаем это по аналогии с утверждением 5.5. Рассмотрим полином

$$f(x_1,\ldots,x_p) = (x_1+\cdots+x_p)^p - x_1^p - \cdots - x_p^p,$$

принадлежащий $[C]$. Представим его в виде

$$f(x_1,\ldots,x_p) = p!x_1\cdots x_p + g(x_1,\ldots,x_p),$$

где каждый моном суммы $g(x_1,\ldots,x_p)$ не содержит хотя бы одну из переменных $x_1,\ldots,x_p$. Тогда

$$p!x_1\cdots x_p = f(x_1,\ldots,x_p) -$$
$$-f(0,x_2,\ldots,x_p) - f(x_1,0,x_3,\ldots,x_p) - \cdots - f(x_1,\ldots,x_{p-1},0).$$

Имеем

$$p! = ap,\ a = (p-1)!,\ \text{НОД}(a,p) = 1.$$

Складывая $a^{-1} \pmod p$ одинаковых слагаемых $p!x_1 \cdots x_p$, получим

$$px_1 \cdots x_p = \phi_p(x_1, \ldots, x_p).$$

Итак, система C полна в классе Λ_p. Легко проверить, что она является и базисом этого класса. □

Следствие 5.19. *Если $m \geq p+1$, то каждый класс Λ_{m-1} является предполным в Λ_m и существует неуплотняемая бесконечная возрастающая цепь*

$$\Lambda_p \subset \Lambda_{p+1} \subset \cdots \subset \Lambda_{m-1} \subset \Lambda_m \subset \cdots .$$

Предел этой цепи — замкнутый класс

$$\Lambda_\infty = \bigcup_{m=p}^{\infty} \Lambda_m,$$

состоящий из функций, представимых приведенными полиномами (5.10)*, но при этом неравенства* (5.9) *заменяются одним неравенством*

$$m_1 + \cdots + m_r \geq 2.$$

Он не имеет базиса и порождается системой

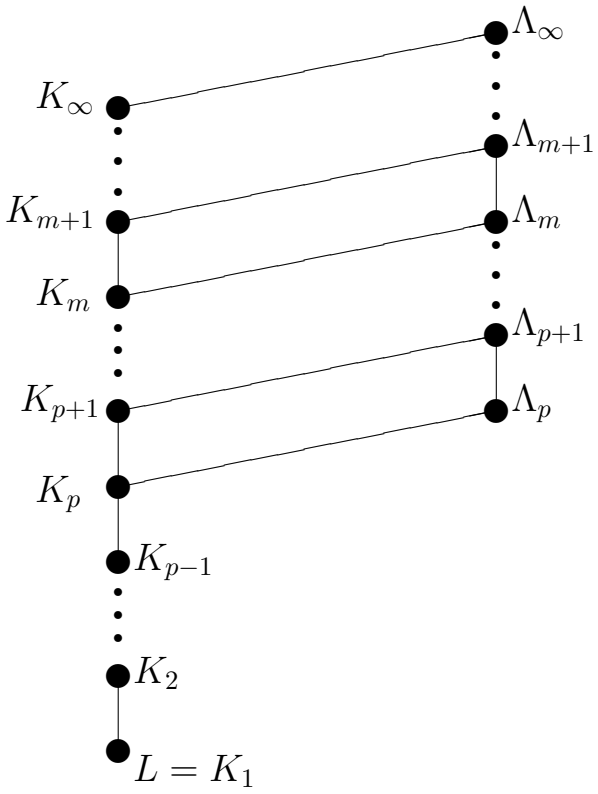
$$B_\infty = \{1, x+y, x^p\} \cup \left(\bigcup_{m=1}^{\infty} \{\phi_m\} \right).$$

Следствие 5.19 аналогично следствию 5.17.

Легко проверить справедливость следующего утверждения.

Утверждение 5.7. *При $m = p, p+1, \ldots, \infty$ класс K_m является предполным в классе Λ_m.*

Следствие 5.20. *Классы K_m и Λ_m образуют следующую решетку.*



5.5.3 Порождающие системы классов K_m, Λ_m, K_∞, Λ_∞ и $L(p)$

Утверждение 5.8. *Для всех $n \in \mathbb{N}$ справедливы включения*

$$\phi_n(x_1, \dots, x_n) \in [1,\ x + y,\ pg_p(x_1, \dots, x_n)], \quad pg_p(x_1, \dots, x_n) \in K_{n(p-1)}.$$

Доказательство. Полином $\phi_n(\tilde{x})$ является p-периодической кратной p функцией p^2-значной логики, поэтому его можно представить как

$$\phi_n(\tilde{x}) = l(\tilde{x}) + pG_p(\tilde{x}).$$

С другой стороны, имеем

$$pg_p(x_1, \dots, x_n) = p \prod_{j=1}^{n} \left(1 - x_j^{p-1}\right).$$

При раскрытии скобок в произведении в правой части получим линейную комбинацию мономов

$$px_{j_1}^{p-1} \cdots x_{j_r}^{p-1}, \quad 1 \le j_1 < j_2 < \cdots < j_r \le n.$$

Каждый из них получается из функции $\phi_{n(p-1)}(\tilde{y}^{n(p-1)})$ переименованием с отождествлением переменных и подстановкой констант 1. □

Следствие 5.21. *При любом $m \in \mathbb{N}$ класс K_m имеет базис*

$$\{1,\ x+y,\ pg_p(x_1,\ldots,x_{m(p-1)})\}.$$

Класс K_∞ порождается бесконечной системой функций

$$\{1,\ x+y,\}\cup\left(\bigcup_{n=1}^{\infty}\{pg_p(x_1,\ldots,x_n)\}\right).$$

Для всех k и всех d, $d|k$, в разделе 2.2 введена функция

$$\delta_d(x) = d\cdot\lfloor x/d\rfloor.$$

Легко проверить справедливость равенства

$$dg_d(x) = \delta_d(x) - \delta_d(x-1).$$

Также непосредственно проверяются следующие факты.

Утверждение 5.9. *Пусть*

$$g(x) = \begin{cases} 0, & x\equiv 0 \pmod p \ \text{ или } \ x\equiv 1 \pmod p,\\ \mu^p-\mu, & x\equiv\mu \pmod p,\ \mu\in E_p\setminus\{0,1\},\end{cases}$$

Тогда $g(x)\in[1,\ x+y,\ pg_p(x)]$ и справедливы соотношения

$$x^p = x+g(x)+(p-1)\delta_p(x), \qquad \delta_p(x)\in\Lambda_\infty.$$

Замечание 5.2. Для любых k и его делителя d функция $\delta_d(x)$ принадлежит классу $L(d)$.

Следствие 5.22. *При $m\geq p+1$ класс Λ_m порождается системой функций*

$$\{1,\ x+y,\ pg_p(x_1,\ldots,x_{m(p-1)}),\ \delta_p(x)\}.$$

Базисы в классе Λ_p образуют системы функций

$$\{1,\ x+y,\ x^p\} \quad и \quad \{1,\ x+y,\ \delta_p(x)\}.$$

Класс Λ_∞ порождается системой

$$\{1,\ x+y,\ \delta_p(x)\}\cup\left(\bigcup_{n=1}^{\infty}\{pg_p(x_1,\ldots,x_n)\}\right).$$

Утверждение 5.10. *Справедливо включение $\Lambda_\infty\subset L(p)$.*

Доказательство. Нелинейная часть полинома класса Λ_∞ является p-периодической функцией p^2-значной логики и поэтому принадлежат классу $L(p)$. Включение строгое, так как, например, $x^p y^p \in L(p) \setminus \Lambda_\infty$. □

Мы часто будем использовать следующие простые факты.

Лемма 5.1. *Если* $k = p^2$, *то* $g_p(x) = 1 - x^{p(p-1)}$.

Это следствие малой теоремы Ферма.

Лемма 5.2. *Если* $k = p^2$ *и*

$$\psi_n(x_1, \ldots, x_n) = x_1^p \cdots x_n^p \text{ при } n \in \mathbb{N},$$

то любой полином $\psi_n(x_1, \ldots, x_n)$ *порождается системой* $\{1, \psi_2(x_1, x_2)\}$.

Это следует из соотношений $\psi_1(x) = \psi_2(x, 1)$ и

$$\psi_{n+1}(\tilde{x},\ y) = \psi_2(\psi_n(\tilde{x}),\ y) \text{ при } n \geq 2.$$

Утверждение 5.11. *При* $k = p^2$ *система*

$$C_p = \{1,\ x + y,\ \psi_2(x, y)\}$$

является базисом класса $L(p)$.

Доказательство. С учетом известных базисов в классе $L(d) = [x + y,\ g_d(x, y)]$ достаточно установить, что $g_p(x, y) \in [C_p]$.

При $p = 2$ имеем $g_2(x, y) = \psi_2(1 + x, 1 + y)$.

Если $p \geq 3$, то

$$g_p(x, y) = g_p^{(1)}\left(g_p^{(1)}(x) + g_p^{(1)}(y) - 2\right)$$

и $g_p^{(1)}(x) = 1 - \psi_{p-1}(x, x, \ldots, x)$. Тогда $g_p(x, y) \in [1,\ x + y,\ \psi_2(x, y)] = [C_p]$. Нетрудно проверить, что любая собственная подсистема системы C_p не является полной в $L(p)$. □

5.5.4 Классы Λ_∞ и $L(p)$ при $k = p^2$

Напомним, что класс $L(p)$ абсолютного сохранения p-разностей состоит из функций вида

$$l(\tilde{x}) + G_p(\tilde{x}) + \sum_{j=1}^{n} c_j \delta_p(x_j),$$

класс Λ_∞ — из функций (5.10)

$$l(\tilde{x}) + \sum_{r=1}^{n} \sum_{j_1,\dots,j_r;\ m_1,\dots,m_r} a(j_1,\dots,j_r;\ m_1,\dots,m_r) \cdot p x_{j_1}^{m_1} \cdots x_{j_r}^{m_r} + \sum_{j=1}^{n} b_j x_j^p,$$

что эквивалентно

$$l'(\tilde{x}) + \sum_{r=1}^{n} \sum_{j_1,\dots,j_r;\ m_1,\dots,m_r} a'(j_1,\dots,j_r;\ m_1,\dots,m_r) \cdot p x_{j_1}^{m_1} \cdots x_{j_r}^{m_r} + \sum_{j=1}^{n} b'_j \delta_p(x_j),$$

где $1 \le j_1 < j_2 < \cdots < j_r \le n$, $m_1,\dots,m_r \in \{1,2,\dots,2p-1\}$, $a(j_1,\dots,j_r;\ m_1,\dots,m_r), b_j, a'(j_1,\dots,j_r;\ m_1,\dots,m_r), b'_j \in E_p$, $m_1+\cdots+m_r \ge 2$; класс $C_p(p)$ — из функций

$$l(\tilde{x}) + pF(\tilde{x}).$$

В разделе 3.3 для произвольных k, d, $d|k$, определены классы $K(d)$, задаваемые каноническими формулами (3.9). Из этого определения, следствия 3.2 и теоремы 3.1 выводим такие факты.

Следствие 5.23. *При $k = p^2$ имеют место равенства*

$$\Lambda_\infty = K(p) = L(p) \cap C_p(p).$$

Замечание 5.3. Для любых k и его делителя d справедливо включение

$$\delta_d(x) \in L(d).$$

Утверждение 5.12. *Класс Λ_∞ является предполным в классе $L(p)$.*

Доказательство. Если $f \in L(p) \setminus \Lambda_\infty$, то $f \in C(p) \setminus C_p(p)$. Как следует из теоремы 1.2 и ее доказательства, суперпозицией функции f и элементов класса $C_p(p)$, причем принадлежащих Λ_∞, можно получить функцию $g_p(x,y)$ и, таким образом, весь класс $L(p)$. □

Утверждение 5.13. *Если при $k = p^2$ функция $g(\tilde{x})$ является p-периодической и $g(\tilde{x}) \equiv 0 \pmod p$, то $g(\tilde{x}) \in \Lambda_\infty$.*

Доказательство. Это следует из соотношений

$$g(\tilde{x}) = \sum_{\tilde{\mu} \in E_p^n} c(\tilde{\mu}) p g_p(\tilde{x} - \tilde{\mu}), \quad c(\tilde{\mu}) \in E_p, \quad p g_p(\tilde{x}) = p \prod_{j=1}^{n} (1 - x_j^{p-1}),$$

$$p x_1^{m_1} \cdots x_n^{m_n} = \phi_{m_1+\cdots+m_n}(\underbrace{x_1,\dots,x_1}_{m_1},\dots,\underbrace{x_n,\dots,x_n}_{m_n}), \quad \phi_m(\tilde{x}^m) \in \Lambda_\infty,$$

справедливых для всех $m, m_1, \dots, m_n \in \mathbb{Z}_+$. □

5.5.5 Классы $S(p)$, $C_p(p)$, $R(p)$ и $C(p)$

В разделе 2.9 для произвольных k и его делителя d определены классы

$$S(d) = C_d(d) \cap R(d)$$

всех функций канонического вида

$$l(\tilde{x}) + dG_d(\tilde{x}) + H_d(\tilde{x}),$$

с базисом $\{1,\ x+y,\ \chi_d(x)\}$.

Построим другой базис в этом классе при $k = p^2$.

Лемма 5.3. *Если $k = p^2$, то*

$$\chi_p(x) = x - x^{(2p-1)^2}.$$

Доказательство. Если $p|x$, то $p^2|x^{(2p-1)^2}$, так как $(2p-1)^2 > 2$. Если же $НОД(x,p) = 1$, из тождеств (5.11) получаем $x^{p^2} \equiv x^p,\ x^{4p^2-4p} \equiv 1,\ x - x^{(2p-1)^2} \equiv 0 \pmod{p^2}$. □

Лемма 5.4. *Если $k = p^2$, то $x^p \in [\{x^{2p-1}\}]$.*

Доказательство. Положим $f(x) = (x^{2p-1})^{2p-1} = x^{(2p-1)^2}$. Покажем, что полином x^p можно выразить p-кратной итерацией полинома $f(x)$:

$$x^p = \underbrace{f(f(\cdots f(x)\cdots))}_{p}.$$

Правая часть последней формулы есть $x^{(2p-1)^{2p}}$. Если $p|x$, то $x^{(2p-1)^{2p}} \equiv x^p \equiv 0 \pmod{p^2}$, так как $p \geq 2$ и $(2p-1)^{2p} > 2$. Если же $НОД(x,p) = 1$, то $x^{(2p-1)^2} \equiv x$, $x^{(2p-1)^{2p}} \equiv x^p \pmod{p^2}$. Таким образом, $x^p \in [x^{2p-1}]$. □

Лемма 5.5. *Если $k = p^2$, то $\quad pg_p(\tilde{x}) \in [\{1, x+y, x^{2p-1}\}]$.*

Доказательство. Согласно лемме 5.4 имеем $x^p \in [\{x^{2p-1}\}]$. Из полиномов $1,\ x+y$, x^p можно получить все полиномы $\phi_n(x_1, \ldots, x_n)$ (см. доказательство утверждения 5.6) и, следовательно, все полиномы $pg_p(\tilde{x})$ (доказательство утверждения 5.13). □

Следствие 5.24. *При $k = p^2$ базисами в классе $S(p)$ являются системы функций*

$$\{1,\ x+y,\ \chi_p(x)\}, \quad \{1,\ x+y,\ x^{2p-1}\}$$

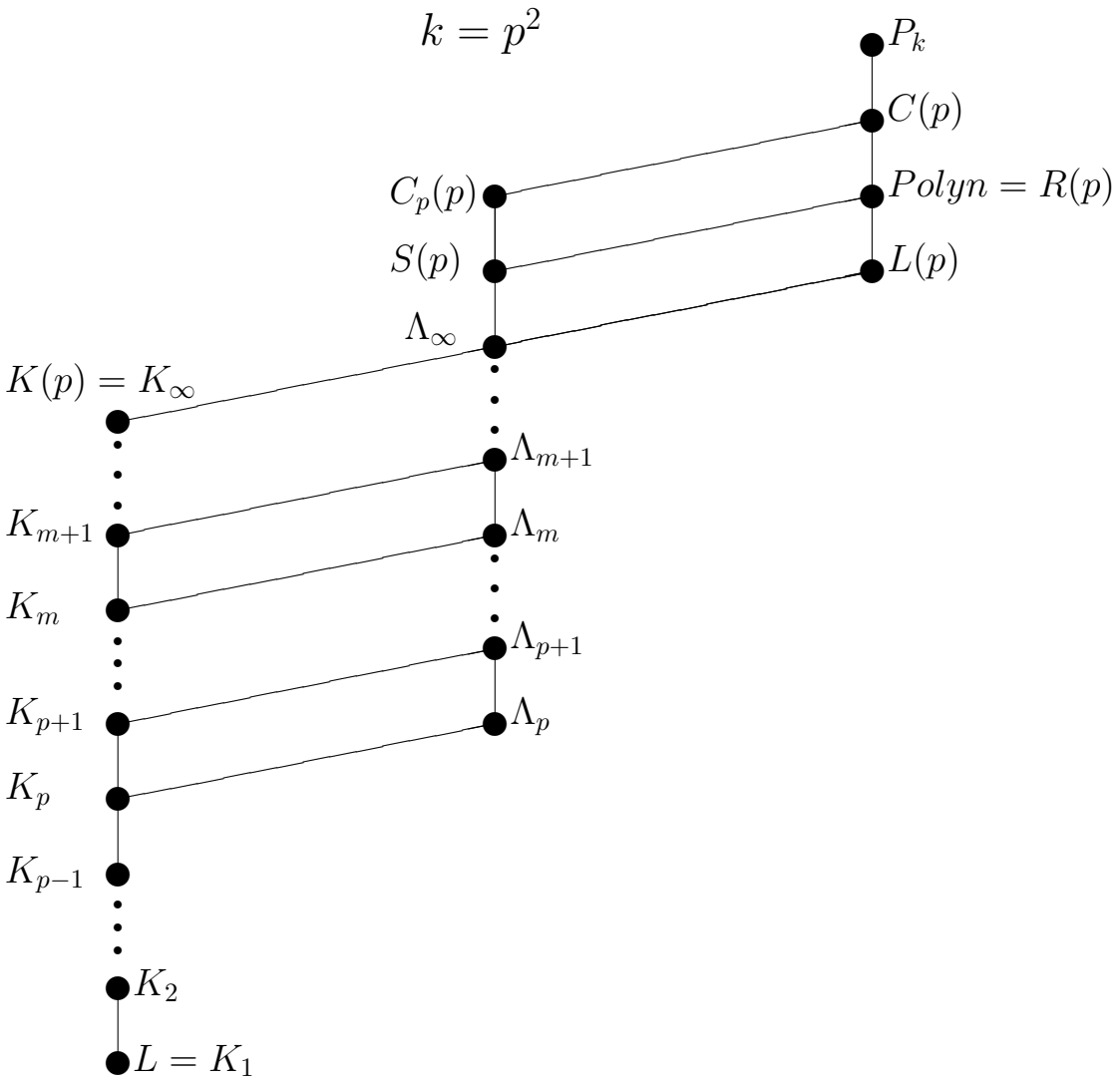
Второй базис сводится к первому в силу лемм 5.3–5.5.

Классы $S(p)$, $C_p(p)$, $R(p)$ и $C(p)$ образуют квадрат, описанный в следствии 2.10. При $k = p^2$ справедливо равенство $C(p) = M(k)$, откуда следует равенство $R(p) = Polyn$ в силу теорем 4.1 и 4.2.

5.5.6 Интервал $I(L; P_k)$ при $k = p^2$

Объединяя результаты предыдущих разделов, строим решетку всех рассмотренных классов.

Теорема 5.5. *При $k = p^2$ замкнутые классы, находящиеся между P_k и L, образуют следующую решетку.*

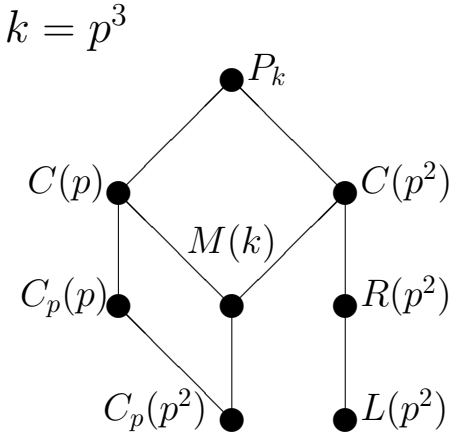


Резюмируем важнейшие сведения о каждом классе. Отметим, что для каждого класса каноническая формула, полная система и базис не являются единственными, возможны и другие.

Класс	Канонические формулы	Полная система
$K_m,\ m \geq 1$	(5.8) с условием (5.9)	базисы $\{1,\ x+y,\ px_1 \cdots x_m\}$; $\{1,\ x+y,\ pg_p(\tilde{x}^{m(p-1)})\}$
$\Lambda_m,\ m \geq p+1$	(5.10) с условием (5.9)	базисы $\{1,\ x+y,\ px_1 \cdots x_m,\ x^p\}$; $\{1,\ x+y,\ pg_p(\tilde{x}^{m(p-1)}),\ \delta_p(x)\}$
Λ_p	(5.10) с условием (5.9), $m=p$	базисы $\{1,\ x+y,\ x^p\}$; $\{1,\ x+y,\ \delta_p(x)\}$
$K_\infty = K(p)$	$l(\tilde{x}) + pG_p(\tilde{x})$	$\{1,\ x+y\} \cup (\cup_{n=1}^{\infty}\{px_1 \cdots x_n\}) = A$, $\{1,\ x+y\} \cup (\cup_{n=1}^{\infty}\{pg_p(\tilde{x}^n\}) = B$
Λ_∞	$l(\tilde{x}) + pG_p(\tilde{x}) + + \sum_{j=1}^{n} b_j x_j^p$	$A \cup \{x^p\}, B \cup \{\delta_p(x)\}$
$S(p)$	$l(\tilde{x}) + pG_p(\tilde{x})H_p(\tilde{x})$	базисы $\{1,\ x+y,\ \chi_p(x)\}$; $\{1,\ x+y,\ x^{2p-1}\}$
$L(p)$	$l(\tilde{x}) + G_p(\tilde{x})$	базисы $\{1,\ x+y,\ g_p(x,y)\}$; $\{1,\ x+y,\ x^p y^p\}$
$R(p)$	$l(\tilde{x}) + G_p(\tilde{x}) + H_p(\tilde{x})$	базисы $\{1,\ x+y,\ xy\}$; $\{1,\ x+y,\ g_p(x,y),\ \chi_p(x)\}$
$C_p(p)$	$l(\tilde{x}) + pF(\tilde{x})$	базис $\{1,\ x+y,\ pj(x,y)\}$
$C(p)$	$l(\tilde{x}) + G_p(\tilde{x}) + pF(\tilde{x})$	базис $\{1,\ x+y,\ g_p(x,y),\ pj(x,y)\}$

5.6 Фрагмент интервала $I(L; P_k)$ для $k = p^3$

Построим фрагмент решетки, образованный определенными в предыдущих главах классами при $k = p^3$.



5.7 Заключение к главе 5

Основные результаты главы следующие.

1. Описание интервала $I(Polyn; M(k))$ для всех k, свободных от кубов (следствие 5.3). Независимое получение известных результатов А. В. Кузнецова (1958), Н. Н. Айзенберга и И. В. Семйона (1971), А. Н. Черепова (1983, 1986), А. Б. Ремизова (1989) — теорема 5.1, следствие 5.3.

2. Вытекающие из строения решетки критерии полиномиальной реализуемости функций при $k = p$ (следствие 5.5), $k = p_1 \cdots p_s$ (следствие 5.4). Доказательство невозможности их распространения на другие разложения числа k (теорема 5.2, следствие 5.6).

3. Описание интервала $I(L; Polyn)$ при всех k, свободных от квадратов (следствие 5.11).

4. Описание интервала $I(L; P_k)$ при $k = pq$ (теорема 5.3, следствия 5.11–5.13).

5. Выделение максимального подкласса в бесконечном интервале $I(Polyn; M(k))$ при $k = p^3$ (теорема 5.4), установление его тождества с классами, найденными другими авторами (замечание 5.1).

6. Описание интервала $I(L; P_k)$ при $k = p^2$ (теорема 5.5). Независимое получение и усиление результата А. А. Крохина, К. Л. Сафина и Е. В. Суханова 1997 г. для $k = 4$.

Глава 6

Некоторые результаты о функциях счетнозначной логики

Введенные аддитивные представления и замкнутые классы можно аналогичным образом определить и в счетнозначной логике с множеством значений $\mathbb{Z}$. Мы рассматриваем класс P_ω всех функций

$$f:\ \mathbb{Z}^n \to \mathbb{Z}, \quad n = 0, 1, 2, \ldots,$$

и функциональную систему $(P_\omega;\ C)$ с операциями суперпозиции. Если свойство функций k-значной логики зависит от делителя d числа k, то оно имеет аналоги в P_ω для всех натуральных d.

В частности, для функций из P_ω и произвольного натурального d можно определить свойства d-периодичности, сохранения сравнения по модулю d, сохранения и абсолютного сохранения d-разностей.

В данной главе рассмотрены некоторые замкнутые классы в функциональной системе $(P_\omega;\ C)$, в частности, классы $P(\mathbb{Z})$ и $L(\mathbb{Z})$ функций, представимых всеми полиномами с целыми коэффициентами и полиномами только первой степени. Не стремясь к полноте изложения всех имеющихся результатов, мы выбрали лишь те, которые аналогичны полученным в предыдущих главах результатам о k-значных функциях.

В разделе 6.1 приведены некоторые простые факты о реализации счетнозначных функций полиномами. Отмечена необходимость сохранения сравнений по всем натуральным модулям d (аналогично конечнозначной логике), невозможность полиномиальной реализации d-периодических функций и функций, абсолютно сохраняющих d-разности, $d \geq 2$ (отличие от конечнозначной логики).

В разделе 6.2 определяются функциональные системы $P(\mathbb{Z})$ и $L(\mathbb{Z})$, указываются их конечные базисы.

В разделе 6.3 вводятся классы $F(d)$ в $P(\mathbb{Z})$ и классы $LF(d)$ в $L(\mathbb{Z})$, состоящие из полиномов, у которых свободный коэффициент кратен фиксированному натуральному d, строятся решетки этих классов, антиизоморфные решетке $\mathbb{N}$ с

отношением делимости. Из них выделяются классы, предполные в $P(\mathbb{Z})$ и $L(\mathbb{Z})$, соответствующие $d = 1$.

В разделах 6.4 и 6.5 анализируются семейства классов $SV(k)$ и $U(a, b)$ в $L(\mathbb{Z})$, также образующие решетки, антиизоморфные $(\mathbb{N}; |)$. Находятся базисы этих классов, выделяются классы, предполные в $L(\mathbb{Z})$.

В разделе 6.6 кратко описываются все предполные в $L(\mathbb{Z})$, их множество оказалось счетно-бесконечным. Они позволяют установить критерий полноты и алгоритм распознавания полноты в $L(\mathbb{Z})$, главные из таких результатов получены и опубликованы совместно с А. И. Мамонтовым [11, 12]. Соискателю в этих работах принадлежит выделение и анализ семейств $F(d)$, $LF(d)$, $SV(k)$, $U(a, b)$, постановка и решение особых задач, требующих применения критериев и методов (алгоритмов) проверки некоторых свойств функций. Одна из таких задач в виде вопроса "Существует ли класс $U(b, p)$, содержащий фиксированную функцию?" рассмотрен в разделе 6.6. Решение такой задачи особым способом дает утверждение 6.8. Следствие 6.7 дает оценку алгоритмической сложности такой проблемы, при этом общая оценка сложности улучшена.

Другие особые задачи, поставленные и решенные лично соискателем, — выяснение полноты в $L(\mathbb{Z})$ относительно некоторых классов K функций (полнота системы, содержащей данный класс K):

— класс K_0 нечетных функций $(f(x_1, \ldots, x_n) = -f(-x_1, \ldots, -x_n))$;

— класс K_E функций со свободным коэффициентом, кратным E, $E \in \mathbb{N}$);

— класс K_1 унарных функций;

— класс K_M функций, сохраняющих модуль (если $|x_1| = |y_1|, \ldots, |x_n| = |y_n|$, то $|f(\tilde{x})| = |f(\tilde{y})|$;

— класс K_S всех сюръекций на $\mathbb{Z}$.

Критерии полноты относительно этих классов содержатся в разделе 6.7, они опубликованы в совместных с А. И. Мамонтовым работах [12, 23]. В них лично соискателю принадлежит постановка задачи и получение результатов, изложенных в диссертации как утверждения 6.1, 6.2, 6.4, 6.5, 6.7, 6.8, 6.12, следствия 6.11–6.12 и леммы 6.2–6.4.

В разделе 6.8 приведены семейства замкнутых классов в $L(\mathbb{Z})$, образующих бесконечные цепи: возрастающую с пределом, не имеющим базиса (леммы 6.2, 6.3 и следствие 6.11) и убывающую (лемма 6.4 и следствие 6.12). Эти результаты изложены в совместной с И. В. Никитиным работе [14], где лично соискателю принадлежит раздел 2, содержащий указанные результаты диссертации.

6.1 О реализации функций счетнозначной логики целочисленными полиномами

Рассмотрим в качестве множества значений функций и переменных $\mathbb{Z}$. Полиномы с целыми коэффициентами будем называть *целочисленными*. Отметим следующие факты.

1. *Необходимое условие реализации функции целочисленным полиномом — сохранение сравнений по всем натуральным модулям d.*

2. *Функция $j(x)$ не представима целочисленным полиномом*, так как она не сохраняет сравнения по модулям $d \geq 2$.

3. *Не представима целочисленным полиномом любая функция, отличная от константы и принимающая одинаковые значения в бесконечном множестве точек*, так как любой полином имеет лишь конечное множество корней.

4. *Не представимы целочисленными полиномами d-периодические функции при любом $d \geq 2$.* Функция $g_d(x)$ не сохраняет сравнение по модулю $d+1$.

5. *Не представимы полиномами функции*

$$f(x) = a\lfloor x/d \rfloor,\ d \geq 2,$$

абсолютно сохраняющие d-разности.

Если a не кратно d, то функция не сохраняет сравнение по модулю a.

Пусть $a = Nd$, тогда $f(x) = N\delta_d(x)$, такая функция не сохраняет сравнение по модулю $Nd+1$.

6.2 Функциональные системы $P(\mathbb{Z})$ и $L(\mathbb{Z})$

Замкнутыми классами в P_ω являются, в частности, функциональные системы $P(\mathbb{Z})$ и $L(\mathbb{Z})$ всех полиномов с целыми коэффициентами и полиномов только первой степени [9-10, 32–35, 39, 56–59].

Основными объектами нашего рассмотрения являются функции $f : \mathbb{Z}^n \to \mathbb{Z}$, задаваемые полиномами

$$f(x_1, \ldots, x_n) = \sum_{(j_1,\ldots j_n)\in\mathbb{Z}_+^n} a(j_1, \ldots j_n) x_1^{j_1} \cdots x_n^{j_n},\quad a(j_1, \ldots, j_n) \in \mathbb{Z}. \tag{6.1}$$

Каждый такой полином полностью определяется упорядоченным набором коэффициентов $a(j_1, \ldots, j_n)$ (он имеет конечную длину) и представляет ровно одну функцию. Мы отождествляем функцию f, реализующий ее полином вида (6.1) и все конгруэнтные и равные f функции (т. е. получаемые из f переименованием

переменных, а также введением и изъятием фиктивных переменных). Множество всех таких функций мы обозначаем как $P(\mathbb{Z})$. Такое же обозначение применяем и для функциональной системы (алгебры) $P(\mathbb{Z}) = (P(\mathbb{Z}); C)$ с операциями суперпозиции.

Частным случаем формулы (6.1) являются линейные функции

$$f(x_1, \ldots, x_n) = a_0 + a_1 x_1 + \cdots + a_n x_n, \quad a_0, a_1, \ldots, a_n \in \mathbb{Z}. \tag{6.2}$$

Они образуют функциональную систему полиномов первой степени $L(\mathbb{Z})$.

Понятие наибольшего общего делителя несколько модифицируем, вводя обозначение $\Delta(c_1, \ldots, c_k)$ для наибольшего общего делителя лишь ненулевых из чисел $c_1, \ldots, c_k$ и полагая $\Delta(0, \ldots, 0) = 0$.

Алгебры $(P(\mathbb{Z}); C)$ и $(L(\mathbb{Z}); C)$ являются конечно-порожденными. Базисами в $P(\mathbb{Z})$ являются системы

$$\{1,\ -x,\ x+y,\ xy\}, \quad \{1,\ x-y,\ xy\},$$

базисами в $L(\mathbb{Z})$ — системы

$$\{1,\ -x,\ x+y\}, \quad \{1,\ x-y\}.$$

Построим решетки замкнутых классов в $P(\mathbb{Z})$ и $L(\mathbb{Z})$, антиизоморфные решетке $\mathbb{N}$ с отношением делимости.

6.3 Семейства классов $F(d)$ и $LF(d)$

Для каждого $d \in \mathbb{N}$ определим $F(d)$ как класс всех полиномов (6.1) из $P(\mathbb{Z})$ со свободным коэффициентом $a(\tilde{0})$, кратным d.

Легко проверить

Утверждение 6.1. *Классы $F(d)$ замкнуты и обладают следующими свойствами.*

1. *Справедливо равенство $F(1) = P(\mathbb{Z})$.*

2. *Системы функций $\{d,\ x+y,\ ,-x,\ xy\}$ и $\{d,\ x-y,\ xy\}$ являются базисами в классе $F(d)$.*

3. *Условия $d_1 | d_2$ и $F(d_1) \supseteq F(d_2)$ равносильны.*

4. *Если $d_0 = НОД(d_1, d_2)$, $d_3 = НОК(d_1, d_2)$, то $[F(d_1) \cup F(d_2)] = F(d_0)$, $F(d_1) \cap F(d_2) = F(d_3)$.*

Утверждение 6.2. *Класс $F(d_2)$ является предполным в классе $F(d_1)$ в точности при $d_2 = pd_1$.*

Доказательство. Если $d_2 = abd_1,\ a > 1, b > 1$, то $F(d_2) \subset F(ad_1) \subset F(d_1)$. Включения строгие, так как $d_1 \in F(d_1) \setminus F(ad_1)$, $ad_1 \in F(ad_1) \setminus F(d_2)$.

Пусть $d_2 = pd_1$, $f(\tilde{x}) \in F(d_1) \setminus F(d_2)$. Покажем, что $[F(d_2) \cup \{f\}] = F(d_1)$. Действительно, $a_0 = f(\tilde{0}) \in [F(d_2) \cup \{f\}]$, так как $0 \in F(d_2)$. Заметим, что $НОД(a_0, d_2) = d_1$, так как $f \notin F(d_2)$. Рассмотрим функцию $g(x, y) = Mx + Ny$ класса $F(d_2)$ такую, что $Ma_0 + Nd_2 = d_1$. Тогда $d_1 = g(a_0, d_2)$, поэтому $[F(d_2) \cup \{f\}]$ содержит полную в $F(d_1)$ систему $\{d_1,\ x - y,\ xy\}$. □

Аналогично в $L(\mathbb{Z})$ определяются классы

$$LF(d) = F(d) \cap L(\mathbb{Z}) = [\{d,\ -x,\ x + y, \}] = [\{d,\ x - y, \}].$$

Они обладают теми же свойствами из утверждений 6.1 и 6.2, только базисы иные.

Следствие 6.1. *Все классы $F(d)$ образуют в $P(\mathbb{Z})$ решетку, антиизоморфную решетке $\mathbb{N}$ с отношением делимости; такую же решетку образуют в $L(\mathbb{Z})$ все классы $LF(d)$.*

Следствие 6.2. *Класс $F(d)$ является предполным в $P(\mathbb{Z})$ в точности при $d = p$. В точности при том же условии класс $LF(d)$ является предполным в $L(\mathbb{Z})$.*

Следствие 6.3. *[11] Существуют по крайней мере счетные множество классов, предполных в $P(\mathbb{Z})$, и множество классов, предполных в $L(\mathbb{Z})$.*

6.4 Семейство классов $SV(k)$

Для линейной функции (6.2) рассмотрим сумму ее коэффициентов при переменных

$$SC(f) = a_1 + \cdots + a_n.$$

Для каждого $k \in \mathbb{N}$ определим $SV(k)$ как класс всех функций с условием

$$SC(f) \equiv 1 \pmod{k}.$$

Для всех $n \in \mathbb{N}$ введем функции

$$h_n(\tilde{x}^{n+1}) = x_1 - x_2 - x_3 - \cdots - x_{n+1}, \quad g_n(\tilde{x}^{n+1}) = x_1 + x_2 + x_3 + \cdots + x_{n+1}.$$

Положим также $h_0(x) = g_0(x) = x$.

Лемма 6.1. *[11] Для всех $r, n \in \mathbb{Z}_+$ справедливы включения*

$$h_{rn}(\tilde{x}^{rn+1}), g_{rn}(\tilde{x}^{rn+1}) \in [h_n(x^{n+1})].$$

Доказательство. При $n = 0$ это очевидно. Далее нетрудно проверить, что

$$g_1(x_1, x_2) = h_1(x_2,\ h_1(h_1(x_2, x_1), x_2)),$$

$$g_2(x_1, x_2, x_3) = h_2(x_1,\ h_2(x_2, x_2, x_3),\ h_2(x_3, x_2, x_3));$$

если $m \geq 3$, то

$$g_m(\tilde{x}^{m+1}) = h_m(x_1,\ h_m(x_2, x_2, x_3, \ldots, x_{m+1}),\ h_m(x_3, x_2, x_3, \ldots x_{m+1}),\ x_4, \ldots, x_{m+1}),$$

а если $r \geq 2$, то

$$h_{rn}(\tilde{x}^{rn+1}) = h_{(r-1)n}(h_n(\tilde{x}^{n+1}),\ x_{n+2}, \ldots, x_{rn+1}).$$

□

Утверждение 6.3. *[11] Каждый класс $SV(k)$ замкнут. Система функций*

$$B(k) = \{1 + x,\ h_k(\tilde{x}^{k+1})\}$$

является его базисом.

Доказательство.

1. Замкнутость класса $SV(k)$ легко проверяется.
2. В силу леммы 6.1 имеем $g_k(\tilde{x}^{k+1}) \in [B(k)]$. Из тождества

$$x = g_k(h_k(x, x_2, \ldots, x_{k+1}),\ x_2, \ldots, x_{k+1})$$

следует, что и $x \in [B(k)]$.

3. Докажем полноту системы $B(k)$ в $SV(k)$. Рассмотрим произвольную функцию $f(\tilde{y})$ класса $SV(k)$ и выразим ее как суперпозицию элементов системы $B(k)$.

Пусть N — сумма модулей всех отрицательных коэффициентов функции f. Применяя лемму 6.1, построим функции $h_{rk}(\tilde{x}^{rk+1})$ для $r = 1, 2, \ldots, m$. Число m выберем так, чтобы $(m-1)k < N \leq mk$. Положим $t = (m+1)k + 1$, тогда построим функцию

$$g_k(h_{mk}(\tilde{x}^{mk+1}),\ x_{mk+2}, \ldots, x_t) = x_1 - x_2 - \cdots - x_{mk+1} + x_{mk+2} + \cdots + x_t.$$

Отождествим часть переменных этой функции с коэффициентами 1 и -1 так, чтобы число коэффициентов -1 стало равно N, и переименуем остальные переменные. Получим функцию

$$H(x_1, \ldots, x_N, \ldots, x_l) = -x_1 - \cdots - x_N + x_{N+1} + \cdots + x_l.$$

Построив суперпозицию $g_k(H(\tilde{x}^l),\ x_{l+1}, \ldots, x_{l+k})$, увеличим сумму коэффициентов на k. Будем повторять эту процедуру, пока не получим сумму коэффициентов $SC(f)$ (при этом все коэффициенты равны ± 1).

Отождествим a_1 переменных, коэффициенты при которых имеют тот же знак, что a_1, обозначим результат как y_1. Аналогично отождествим другие $a_2, \ldots, a_n$ групп переменных. Изменяя свободный коэффициент с помощью функций $1+x$, $-1+x$, получим $f(\tilde{y})$. При этом функция $-1+x$ строится следующим образом: если $k \geq 2$, то

$$h_k(g_k(\tilde{x}^{k+1}),\ x_3, x_3, x_4, \ldots, x_{k+1}) = \varphi(x_1, x_2, x_3) = x_1 + x_2 - x_3,$$

$$\varphi(x, x, 1+x) = -1 + x;$$

если $k = 1$, то $h_1(x, x) = 0,\ 1 + 0 = 1,\ h_1(x, 1) = -1 + x$.

4. Полнота системы $B(k)$ в классе $SV(k)$ доказана. Далее нетрудно проверить, что эта система является и базисом. □

Утверждение 6.4. *Классы $SV(k)$ обладают следующими свойствами.*

1. *Имеет место равенство $SV(1) = L(\mathbb{Z})$.*
2. *Условия $k_1 | k_2$ и $SV(k_1) \supseteq SV(k_2)$ равносильны.*
3. *Если $НОК(k_1, k_2) = k_3$, то $SV(k_1) \cap SV(k_2) = SV(k_3)$.*
4. *Если $k_0 = НОД(k_1, k_2)$, то $[SV(k_1) \cup SV(k_2)] = SV(k_0)$.*

Доказательство. Первые три свойства легко проверяются. Докажем четвертое. Из свойств 1 и 2 следует, что $SV(k_0) \supseteq [SV(k_1) \cup SV(k_2)]$. Установим обратное включение, выразив базисную функцию $h_{k_0}(\tilde{x}^{k_0+1})$ через функции классов $SV(k_1)$ и $SV(k_2)$. Пусть целые неотрицательные A и B таковы, что $Ak_1 - Bk_2 = k_0$. Тогда

$$h_{k_0}(\tilde{x}^{k_0+1}) = g_{Bk_2}(h_{Ak_1}(\tilde{x}^{Ak_1+1}),\ x_{k_0+2}, \ldots, x_{Ak_1+1}).$$

В силу леммы 6.1 функции $g_{Bk_2}(\tilde{x}^{Bk_2+1})$, $h_{Ak_1}(\tilde{x}^{Ak_1+1})$ принадлежат $[SV(k_1) \cup SV(k_2)]$. □

Утверждение 6.5. *Класс $SV(k_2)$ является предполным в классе $SV(k_1)$ в точности при $k_2 = pk_1$.*

Доказательство. Если $k_2 = abk_1,\ a > 1, b > 1$, то $SV(k_2) \subset SV(ak_1) \subset SV(k_1)$. Включения строгие, так как

$$(k_1 + 1)x \in SV(k_1) \setminus SV(ak_1), \qquad (ak_1 + 1)x \in SV(ak_1) \setminus SV(k_2).$$

Пусть $k_2 = pk_1,\ f(\tilde{x}^n) \in SV(k_1) \setminus SV(k_2)$. Покажем, что $[SV(k_2) \cup \{f\}] = SV(k_1)$.

Если $n \geq 2$, то, отождествив все переменные функции f, получим функцию $Ax + B$ с условиями $A \equiv 1 \pmod{k_1},\ A \not\equiv 1 \pmod{k_2}$. С помощью функций $x + k_2 y,\ x - k_2 y$ класса $SV(k_2)$ получим из $Ax + B$ функцию $Cx + D$ с условиями $C \equiv A \pmod{k_2},\ C \in \{2, 3, \ldots, k_2\}$. Далее, используя функцию $x + y - z$ класса

$SV(k_2)$, строим $x+(C-1)y+D$, $x-(C-1)y-D$, а из них, применяя $1+x$, $-1+x$, получим $\varphi_1(x,y)=x+(C-1)y$, $\varphi_2(x,y)=x-(C-1)y$. При этом $НОД(C-1,k_2)=1$. Пусть целые M и N таковы, что $(C-1)M+k_2N=k_1$. Тогда из $\varphi_1(x,y)$, $\varphi_2(x,y)$ получим функцию $x+(C-1)My$, а из последней, применяя $x+k_2y$, $x-k_2y$, — функцию

$$\psi(x,y)=x+(C-1)My+k_2Ny=x+k_1.$$

Наконец, используя функцию $u(\tilde{x}^{k_1+1},\ y)=h_{k_1}(\tilde{x}^{k_1+1})+k_1y$ класса $SV(k_2)$, получим $u(x_1,\ \psi(x_2,y),\ x_3,\dots,x_{k_1+1},\ y)=h_{k_1}(\tilde{x}^{k_1+1})$. Построен базис $B(k_1)$ класса $SV(k_1)$. □

Следствие 6.4. *Все классы $SV(k)$ образуют решетку, антиизоморфную решетке $\mathbb{N}$ с отношением делимости.*

Следствие 6.5. *Класс $SV(k)$ является предполным в $L(\mathbb{Z})$ в точности при $k=p$.*

6.5 Семейство классов $U(a,b)$

Для $b\in\mathbb{N}$, $a\in\{0,1,\dots,b-1\}$ определим $U(a,b)$ как класс всех линейных функций в $L(\mathbb{Z})$, сохраняющих множество

$$\mathbb{Z}(a,b)=\{c\in\mathbb{Z}:\ c\equiv a\pmod b\}.$$

Эти классы замкнуты как классы сохранения множеств, кроме того,

$$U(0,d)=LF(d),\qquad U(0,1)=L(\mathbb{Z}).$$

Утверждение 6.6. *[11] Система функций*

$$\Omega(a,b)=\{a,\ x+b,\ x+y-z\}$$

является базисом класса $U(a,b)$.

Доказательство.

1. Положим $g(x,y,z)=x+y-z$, тогда $g(x,x,x+b)=x-b$.
2. Последовательно получаем функции $2x-a=g(x,x,a)$, $3x-2a=g(2x-a,\ x,\ a)$, $\dots$, $bx-(b-1)x=g((b-1)x-(b-2)a,\ x,\ a)$.
3. Образуем $bx+y-ab=g(bx-(b-1)a,\ y,\ a)$.
4. Из последней функции с помощью $x+b$ получим $bx+y$.
5. Строим $y-bx=g(y,y,bx+y)$.

6. Итак, получены все функции $Ax + B$, $A = 0, 1, \ldots, b-1$, сохраняющие множество $\{a\}$, и функции $y \pm bx$. Функция $x+b$ есть изначально. Суперпозициями этих функций выражаются все остальные унарные функции класса $U(a,b)$, так как они имеют вид $f(x) = Ax + (1-A)a + Nb$, $A, N \in \mathbb{Z}$.

7. Будем далее строить произвольную функцию (6.2) класса $U(a,b)$ нескольких переменных. Для нее выполняется условие $a_0 + S(f)a \equiv a \pmod{b}$.

8. С помощью функции $\alpha(x) = a_0 + SC(f)x$ построим

$$\alpha_1(x_1, x_2) = a_0 + a_1 x_1 + (SC(f) - a_1)x_2.$$

Если $a_1 > 0$, то последовательно получаем

$$g(\alpha(x_2),\ x_1,\ x_2) = a_0 + x_1 + (SC(f) - 1)x_2,$$

$$g(a_0 + x_1 + (SC(f) - 1)x_2,\ x_1,\ x_2) = a_0 + 2x_1 + (SC(f) - 2)x_2$$

и так далее, пока не придем к функции $\alpha_1(x_1, x_2)$.

Если $a_1 < 0$, то последовательно строим

$$g(\alpha(x_2),\ x_2,\ x_1) = a_0 - x_1 + (SC(f) + 1)x_2,$$

$$g(a_0 - x_1 + (SC(f) + 1)x_2,\ x_2,\ x_1) = a_0 - 2x_1 + (SC(f) + 2)x_2$$

и так далее до получения функции $\alpha_1(x_1, x_2)$.

9. Имея $\alpha_1(x_1, x_2)$, аналогично строим функции

$$\alpha_m(\tilde{x}^{m+1}) = a_0 + a_1 x_1 + \cdots + a_m x_m + (SC(f) - a_1 - \cdots - a_m)x_{m+1}$$

для $m = 2, 3, \ldots, n-1$. На последнем шаге получим требуемую функцию n переменных.

10. Итак, система $\Omega(a,b)$ полна в классе $U(a,b)$. Покажем, что она является базисом. Подсистема $\{a,\ x+b\}$ не полна, так как порождает только одноместные функции и константы. Подсистема $\{a,\ x+y-z\}$ сохраняет множество $\{a\}$. Наконец, $\{x+b,\ x+y-z\} \subset SV(b)$, но $a \notin SV(b)$. □

Замечание 6.1. Можно обобщить классы $U(a,b)$ на случай всех $a \in \mathbb{Z}_+$. Под классом $U(a,b)$ будем понимать определенный ранее класс $U(c,b)$, где c — наименьший неотрицательный вычет числа a по модулю b.

Утверждение 6.7. *При фиксированном a классы $U(a,b)$ обладают следующими свойствами.*

1. *Условия $b_1 | b_2$ и $U(a,b_1) \supseteq U(a,b_2)$ равносильны.*

2. *Если $b_0 = НОД(b_1, b_2)$, $НОК(b_1, b_2) = b_3$, то $[U(a,b_1) \cup U(a,b_2)] = U(a,b_0)$, $U(a,b_1) \cap U(a,b_2) = U(a,b_3)$.*

3. *Класс $U(a,b_2)$ является предполным в $U(a,b_1)$ в точности при $b_2 = pb_1$.*

4. *Все классы $U(a,b)$ образуют решетку, антиизоморфную решетке $\mathbb{N}$ с отношением делимости.*

Доказательство. Первые два свойства очевидны. Докажем третье.

Если $b_2 = b_1cd,\ c > 1, d > 1$, то $U(a, b_2) \subset U(a, b_1c) \subset U(a, b_1)$. Включения строгие, так как $a + b_1 \in U(a, b_1) \setminus U(a,\ b_1c),\ \ a + b_1c \in U(a, b_1c) \setminus U(a,\ b_2)$.

Пусть $b_2 = pb_1,\ f(\tilde{x}) \in U(a, b_1) \setminus U(a, b_2)$. Тогда для некоторых $e_1, \ldots, e_n$ из $\mathbb{Z}(a, b_2)$ имеем $f(\tilde{e}) = k$ и $\ k \equiv a \pmod{b_1},\ $ но $\ k \not\equiv a \pmod{b_2}$. С помощью функций $a,\ x \pm b_2$ класса $U(a, b_2)$ и функции f построим константы $e_1, \ldots, e_n,\ k$. Образуем также функции $x \pm (k - a)$, а из последних — функции $x \pm r$, где r — наименьший неотрицательный вычет числа $a - k$ по модулю b_2. Пусть целые M, N таковы, что $b_2M + rN = b_1$. За $|M|$ итераций функций $x + b_2$ получим $x + b_2M$, аналогично построим $x + rN$. Далее получаем $x + b_2M + rN = x + b_1$. Итак, $[U(a, b_2) \cup \{f\}]$ содержит базис $\Omega(a, b_1)$ класса $U(a, b_1)$.

Свойство 4 непосредственно следует из предыдущих. □

Следствие 6.6. *Для всех p и для $a = 0, 1, \ldots, p - 1$ классы $U(a, p)$ являются предполными в $L(\mathbb{Z})$.*

6.6 Алгоритм распознавания полноты в функциональной системе $L(\mathbb{Z})$

В [11] найдены все предполные в $L(\mathbb{Z})$ классы, они позволили сформулировать критерий полноты в конечно-порожденной функциональной системе $L(\mathbb{Z})$. Перечислим предполные классы.

1. Класс L^+ функций, у которых все коэффициенты при переменных неотрицательны.

2. Класс D, содержащий все константы и унарные функции, а также все n-местные $(n \geq 2)$ функции, имеющие $\Delta(a_1, \ldots, a_n) > 1$.

3. Классы $C(p_1 \cdots p_r)$, где $p_1, \ldots, p_r$ — различные простые числа, $r \geq 1$, состоят из функций, у которых все коэффициенты $a_1, \ldots, a_n$ кратны некоторому p_i, $1 \leq i \leq r$, или все коэффициенты $a_1, \ldots, a_n$ кроме, возможно, одного кратны $p_1 \cdots p_r$. Каждый класс $C(p_1 \cdots p_r)$ содержит все константы и унарные функции.

4. Классы $SV(p)$.

5. Классы $U(b, p),\ b = 0, 1, \ldots, p - 1$.

На основе критерия полноты в терминах всех предполных классов в [12] сформулирован и проанализирован алгоритм распознавания полноты. (Алгоритмическая разрешимость проблемы не очевидна, так как множество всех предполных классов бесконечно.)

Уточним проблему. Дана конечная система мощности m, состоящая из функций

$$f_i(\tilde{x}) = a_{i0} + a_{i1}x_{i1} + \cdots + a_{in}x_{in}, \quad i = 1, \ldots, m,$$

зависящих от одних и тех же переменных $\tilde{x} = (x_1, \ldots, x_n)$. Она полностью определяется $(m, n+1)$-матрицей коэффициентов a_{ij}. Пусть все коэффициенты ограничены по абсолютной величине натуральным числом t. Тогда за *размер задачи* примем $N = mnt$. Требуется выяснить, является ли система полной в $L(\mathbb{Z})$.

Теорема [12] *Существует алгоритм распознавания полноты конечной системы размера N в функциональной системе $L(\mathbb{Z})$. Он имеет временную сложность $O(N^2 \log^2 N)$ (двоичных операций) и емкостную сложность $O(N \log N)$ (битов).*

Вопрос. Существует ли класс $U(b, p)$, содержащий некоторую фиксированную функцию f?

Утверждение 6.8. *Функция $f(x_1, \ldots, x_n) = a_0 + a_1 x_1 + \cdots + a_n x_n$ не содержится ни в одном классе $U(b, p)$ тогда и только тогда, когда $a_0 \in \{1, -1\}$ и $SC(f) = 1$.*

Доказательство. Если $a_0 \notin \{1, -1\}$, то существует простой делитель p числа a_0, и для него $f \in U(0, p)$.

Пусть $x_1 \equiv \cdots \equiv x_n \equiv b \pmod{p}$ для некоторых p и b. Условие $f(x_1, \ldots, x_n) \equiv b \pmod{p}$ в этом случае эквивалентно

$$(SC(f) - 1)b \equiv -a_0 \pmod{p}. \tag{6.3}$$

Если $SC(f) = 1$ и $a_0 \in \{1, -1\}$, то такое сравнение невозможно.

Если $SC(f) \neq 1$, то найдется простое p, не делящее $SC(f) - 1$. Для такого p и $b \equiv -a_0 \cdot SC(f)^{-1} \pmod{p}$ получим класс $U(b, p)$, содержащий f. □

Следствие 6.7. *Нахождение ответа на поставленный вопрос для функции n переменных имеет временную сложность $O(n \log t)$ и емкостную сложность $O(1)$.*

6.7 Распознавание относительной полноты в функциональной системе $L(\mathbb{Z})$

Проблема *полноты относительно* заданного *класса* K (не обязательно замкнутого) состоит в выяснении полноты системы, содержащей класс K. Рассмотрим эту проблему в $L(\mathbb{Z})$ для классов $K = K_0, K_1, K_E, K_M, K_S$, где
K_0 — класс всех функций с коэффициентом $a_0 = 0$ (класс всех нечетных функций $f(x_1, \ldots, x_n) = -f(-x_1, \ldots, -x_n)$);
K_E — классы всех функций с коэффициентом a_0, кратным E, $E \geq 2$;
K_1 — класс всех функций, зависящих не более чем от одной переменной;
K_M — класс всех функций, сохраняющих модуль, т. е. эквивалентность $x \sim y \Leftrightarrow$

$|x| = |y|$ на $\mathbb{Z}$;
K_S — класс всех сюръекций.

Утверждение 6.9. *[12] Если $K_0 \subseteq F$, то система F полна в $L(\mathbb{Z})$ тогда и только тогда, когда она не содержится ни в одном из классов $U(0,p)$.*

Нетрудно проверить, что из всех предполных в $L(\mathbb{Z})$ классов только классы $U(0,p)$ содержат K_0.

Условие $f \in U(0,p)$ равносильно делимости на p коэффициента a_0.

Следствие 6.8. *Проверка полноты конечной системы размера N относительно класса K_0 имеет временную сложность $O(N)$ и емкостную сложность $O(1)$.*

Утверждение 6.10. *[12] Если $K_E \subseteq F$, то система F полна в $L(\mathbb{Z})$ тогда и только тогда, когда она не содержится ни в одном из классов $U(0,p)$, где $p|E$.*

Доказательство. Функция $x - y$ из K_E не принадлежит ни одному из классов $L^+, D, C(p_1 \cdots p_r), SV(p)$, поэтому система F не содержится ни в одном из указанных классов. Далее, пусть $f(x_1, \ldots, x_n) \in K_E$. Если $E \not\equiv 0 \pmod p$, то для любого b функция f не принадлежит классу $U(b,p)$. Если $p|E$, то $p|a_0$ и условие $f \in U(b,p)$ эквивалентно сравнению (6.3). Класс K_E содержит функции f, для которых $SC(f) \not\equiv 1 \pmod p$. Тогда из условия (6.3) следует $b = 0$. Таким образом, из всех предполных в $L(\mathbb{Z})$ классов только классы $U(0,p)$, где $p|E$, содержат K_E. Для полноты системы F необходимо и достаточно, чтобы она не содержалась ни в одном из таких классов $U(0,p)$. □

Следствие 6.9. *Проверка полноты конечной системы размера N относительно класса K_E имеет временную сложность $O(N)$ и емкостную сложность $O(1)$.*

Утверждение 6.11. *[12] Если $K_1 \subseteq F$, то система F полна в $L(\mathbb{Z})$ тогда и только тогда, когда она не содержится ни в одном из классов D и $C(p_1 \cdots p_r)$.*

Доказательство. Класс K_1 содержит все константы, функции $-x$ и $x + 1$. При этом константы не принадлежат классам $SV(p)$, $-x \notin L^+$, функция $x + 1$ не входит в классы $U(b,p)$. С другой стороны, $K_1 \subset D$ и $K_1 \subset C(p_1 \cdots p_r)$ для всех $r, p_1, \ldots, p_r$. Таким образом, система F не содержится ни в одном из классов $SV(p)$, $U(b,p)$, L^+, и ее полнота зависит только от включения в классы D и $C(p_1 \cdots p_r)$. □

Рассмотрим проблему полноты относительно класса K_M.

В [13] доказан (лично соискателем) следующий критерий сохранения модуля в более общих функциональных системах $P(A)$ полиномов как функций

$$f:\ A^n \to A, \qquad n = 0, 1, 2, \ldots,$$

при $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

Утверждение 6.12. *Полином произвольной степени с целыми, рациональными или вещественными коэффициентами сохраняет модуль тогда и только тогда, когда каждая его переменная имеет либо только четное, либо только нечетное число вхождений в каждое слагаемое полинома.*

Следствие 6.10. *Замкнутый класс K_M в функциональной системе $L(\mathbb{Z})$ состоит в точности из всех констант и всех функций вида ax, $a \in \mathbb{Z}$.*

Утверждение 6.13. *[12] Если $K_M \subseteq F$, то система F полна в $L(\mathbb{Z})$ тогда и только тогда, когда она не содержится ни в одном из классов D и $C(p_1 \cdots p_r)$.*

Доказательство. Функция $-x$ из K_M не принадлежит классу L^+, любая константа не принадлежит классам $SV(p)$; константы C такие, что $C \not\equiv b \pmod p$, не входят в классы $U(b, p)$. Таким образом, K_M не содержится в классах $L^+, SV(p)$, $U(b, p)$, но $K_M \subset D$ и $K_M \subset C(p_1 \cdots p_r)$ для всех $r \geq 1, p_1 \ldots, p_r$. Для полноты системы F необходимо и достаточно, чтобы она не содержалась в классах D и $C(p_1 \cdots p_r)$. □

Проблема полноты относительно K_S решается просто.

Утверждение 6.14. *[12] Если $K_S \subseteq F$, то система F полна в $L(\mathbb{Z})$.*

Доказательство. Сюръекция $x - y$ не входит ни в один из классов L^+, D, $C(p_1 \cdots p_r)$, $SV(p)$, сюръекция $x+1$ не принадлежит ни одному из классов $U(b, p)$. Следовательно, класс K_S не содержится ни в одном из предполных в $L(\mathbb{Z})$ классов, поэтому $[K_S] = L(\mathbb{Z})$. □

Тем самым найдено достаточное условие полноты.

Для применения критериев полноты относительно K_0, K_E, K_M, K_1 полезно знать базисы в этих классах. Нетрудно проверить

Утверждение 6.15. *Системы $\{x - y\}$ и $\{E, x - y\}$ есть базисы в классах K_0 и K_E соответственно. Системы*

$$\{0, 1, -x\} \cup \left(\bigcup_p \{px\}\right), \quad \{0, -x, x - 1\} \cup \left(\bigcup_p \{px\}\right)$$

являются базисами бесконечно-порожденных классов K_M и, соответственно, K_1.

6.8 Бесконечные цепи замкнутых классов в $L(\mathbb{Z})$

Рассмотрим в $L(\mathbb{Z})$ замкнутый класс $L(\mathbb{Z}_+)$ сохранения множества $\mathbb{Z}_+$. Он состоит в точности из всех полиномов вида (6.2) с неотрицательными коэффициентами. Такие полиномы реализуют отображения $f:\ \mathbb{Z}_+^n \to \mathbb{Z}_+$.

Для фиксированного $m \geq 2$ и $n = 0, 1, 2, \ldots$ рассмотрим функции

$$s_m^{(n)} = m + x_1 + \cdots + x_n$$

и замкнутые классы $\Sigma_n(m) = [\mathbb{Z}_+ \cup \{x,\ s_m^{(n)}\}]$.

Введем на $\mathbb{Z}_+$ эквивалентность S_m, разбивающую $\mathbb{Z}_+$ на два класса $\{x < m\}$ и $\{x \geq m\}$, а также замкнутый класс $U(S_m)$ сохранения этого отношения.

Лемма 6.2. *При фиксированном m для всех $n \geq 0$ справедливы включения*

$$\Sigma_n(m) \subset \Sigma_{n+1}(m) \subseteq U(S_m).$$

Доказательство. Включения $\Sigma_n(m) \subseteq U(S_m)$ легко проверяются.

Пусть $k \geq 0,\ n \geq 0,$ тогда $s_m^{(n)}(\tilde{x}^n) = s_m^{(n+k)}(\tilde{x}^n, \tilde{0}^k),$ поэтому $\Sigma_n(m) \subseteq$ $\subseteq \Sigma_{n+k}(m)$. Покажем невозможность равенства $\Sigma_n(m) = \Sigma_{n+1}(m)$. Если функция (6.2) принадлежит классу $\Sigma_r(m)$ и $n > r$, то свободный коэффицент этой функции удовлетворяет неравенству $a_0 \geq 2m$, так как формула над базисной системой $\mathbb{Z}_+ \cup \{x, \sigma_m^{(r)}\}$, реализующая функцию $f,$ должна в силу условия $n > r$ содержать элемент $\sigma_m^{(r)}$ как минимум дважды. Таким образом, $\sigma_m^{(n+1)}(\tilde{x}^n,\ y) \in \Sigma_{n+1}(m) \setminus \Sigma_n(m)$. □

Положим

$$\Sigma_*(m) = \bigcup_{n=0}^{\infty} \Sigma_n(m).$$

Лемма 6.3. *Справедливо равенство $\Sigma_*(m) = U(S_m)$.*

Доказательство. Уже установлено, что $\Sigma_*(m) \subseteq U(S_m)$. Докажем обратное включение. Пусть функция вида (6.2) принадлежит $U(S_m)$, и пусть $a_1 \cdots a_n \neq 0$, $a_0 = m + k$. Положим $N = a_1 + \cdots + a_n + k$. Тогда

$$f(x_1, \ldots, x_n) = s_m^{(N)}(\underbrace{x_1, \ldots, x_1}_{a_1}, \ldots, \underbrace{x_n, \ldots, x_n}_{a_n}, \underbrace{1, \ldots, 1}_{k}).$$

Таким образом, $f(x_1, \ldots, x_n) \in \Sigma_*(m)$. □

Следствие 6.11. *В функциональной системе $L(\mathbb{Z}_+)$ для каждого $m \geq 2$ существует бесконечно возрастающая цепь замкнутых классов*

$$\Sigma_0(m) \subset \Sigma_1(m) \subset \cdots \subset \Sigma_n(m) \subset \Sigma_{n+1}(m) \subset \cdots \subset U(S_m).$$

Система функций $\{0, 1, \ldots, m-1, s_m^{(n)}\}$ *образует базис класса* $\Sigma_n(m)$. *Каждый класс* $U(S_m)$ *бесконечно порождаем и не имеет базиса, полной в нем является система функций*

$$\{0, 1, \ldots, m-1\} \cup \left(\bigcup_{n=0}^{\infty} \{\sigma_m^{(n)}\} \right).$$

Классы $U(S_m)$ образуют бесконечную убывающую цепь.

Нетрудно проверить следующие факты.

Лемма 6.4. *Если* $m_1 < m_2$, *то* $U(S_{m_1}) \supseteq U(S_{m_2})$. *Равенство* $U(S_{m_1}) = U(S_{m_2})$ *имеет место только при* $m_1, m_2 \in \{0, 1\}$.

Следствие 6.12. *В функциональной системе* $L(\mathbb{Z}_+)$ *существует бесконечная убывающая цепь замкнутых классов*

$$U(S_1) \supset U(S_2) \supset \cdots \supset U(S_m) \supset U(S_{m+1}) \supset \cdots,$$

причем

$$\bigcap_{m=0}^{\infty} U(S_m) = [\mathbb{Z}_+ \cup \{x\}] = \mathbb{Z}_+ \cup \{x\}.$$

6.9 Заключение к главе 6

Укажем основные результаты главы (повторим, что они получены лично соискателем, но опубликованы в совместных работах [11, 12, 23, 13]).

1. Следствия 6.1 и 6.2 о решетках классов $F(d)$ в $P(\mathbb{Z})$ и классов $LF(d)$ в $L(\mathbb{Z})$.

2. Следствия 6.4 и 6.5 о решетках классов $SV(k)$ в $L(\mathbb{Z})$.

3. Утверждение 6.7 и следствие 6.6 о классах $U(a, b)$ в $L(\mathbb{Z})$.

4. Утверждение 6.8 о проверке существования класса $U(b, p)$, содержащего фиксированную функцию из $L(\mathbb{Z})$, следствие 6.7 об алгоритмической сложности этой проблемы.

5. Следствия 6.8 и 6.9 об алгоритмической сложности распознавания относительной полноты.

6. Следствия 6.11 и 6.12 о бесконечных цепях замкнутых классов в $L(\mathbb{Z})$.

ЗАКЛЮЧЕНИЕ

Укажем основные результаты всей диссертации.

1. Определены замкнутые классы следующих семейств:

$C(d), R(d), L(d), S(d), \quad d|k;$
$C(d_1, \ldots, d_l), \quad d_1|d_2,\ d_2|d_3, \ldots, d_{l-1}|d_l,\ d_l|k;$
$C(k_1, \ldots, k_s), \quad k = k_1 \cdots k_s$, числа $k_1, \ldots, k_s$ попарно взаимно простые, $s \geq 2;$
$C_e(d), \quad e|d,\ d|k;$
$K(d_1, d), \quad d|k,\ d_1|k;$
$R_d C_e, \quad k = de,\ \text{НОД}(d, e) = 1.$

Каждый класс состоит из всех функций, представимых аддитивной формулой

$$l(\tilde{x}) + G_d(\tilde{x}) + d \cdot F(\tilde{x})$$

с однозначно определенными слагаемыми. Для каждого класса найдена задающая его аддитивная формула, а также базис или полная система.

Класс	Каноническая формула	Базис
$C(d)$	$l(\tilde{x}) + G_d(\tilde{x}) + d \cdot F(\tilde{x})$	$\{x + y,\ g_d(x, y),\ dj(x, y)\}$
$C(d_1, \ldots, d_l)$	$l(\tilde{x}) + G_{d_1}(\tilde{x}) + d_1 G_{d_2}(\tilde{x}) +$ $+ \cdots + d_{l-1} G_{d_l}(\tilde{x}) + d_l F(\tilde{x})$	$\{x + y,\ g_{d_1}(x, y),\ d_1 g_{d_2}(x, y),$ $\ldots, d_{l-1} g_{d_l}(x, y),\ d_l j(x, y)\}$
$C_e(d)$	$l(\tilde{x}) + eG_d(\tilde{x}) + d \cdot F(\tilde{x})$	$\{1,\ x + y,\ eg_d(x, y),\ dj(x, y)\}$
$C(k_1, \ldots, k_s)$	$l(\tilde{x}) + (k/k_1) G_{k_1}(\tilde{x}) +$ $+ \cdots + (k/k_s) G_{k_s}(\tilde{x})$	$\{1,\ x + y,\ (k/k_1) g_{k_1}(x, y),$ $\ldots, (k/k_s) g_{k_s}(x, y)\}$
$R(d)$	$l(\tilde{x}) + G_d(\tilde{x}) + H_d(\tilde{x})$	$\{x + y,\ g_d(x, y),\ \chi_d(x)\}$
$S(d)$	$l(\tilde{x}) + dG_d(\tilde{x}) + H_d(\tilde{x})$	$\{1,\ x + y,\ \chi_d(x)\}$
$L(d)$	$l(\tilde{x}) + G_d(\tilde{x})$	$\{x + y,\ g_d(x, y)\}$
$R_d C_e$	$l(\tilde{x}) + eG_d(\tilde{x})$	$\{1,\ x + y,\ eg_d(x, y)\}$
$K(d_1, d)$	$l(\tilde{x}) + d_1 G_d(\tilde{x})$	полная система $\{1,\ x + y\} \cup (\cup_{n=1}^{\infty} \{d_1 g_d(\tilde{x}^n)\})$

2. Для пар классов одного семейства и для пар, образованных классами разных семейств, выявлены отношения включения. Найдены условия, необходимые и достаточные для того, чтобы меньший класс был предполным в большем. Описаны и построены подрешетки, образованные введенными классами в решетке $\mathcal{L}(P_k)$ всех замкнутых классов k-значных функций по отношению включения.

3. Найдены критерии полиномиальной реализации функций k-значной логики. Предложен метод построения полинома, представляющего фиксированную функцию; при этом использованы введенные аддитивные формулы и условия принадлежности функций замкнутым классам, содержащим класс $Polyn$ всех полиномов и класс L линейных функций. Оценена временная сложность алгоритма для распознавания полиномиальности и построения полинома.

4. Описаны и построены следующие подрешетки в $\mathcal{L}(P_k)$:

интервал $I(Polyn;\ M(k))$ для всех k, не кратных кубу простого числа;
интервал $I(L;\ Polyn)$ для всех k, не кратных квадрату простого числа;
интервал $I(L; P_k)$ для $k = pq$, где p и q — различные простые числа;
бесконечный интервал $I(L; P_k)$ для $k = p^2$ (обобщение результата А. А. Крохина, К. Л. Сафина и Е. В. Суханова 1997 г.).

Найден максимальный подкласс класса $M(k)$ в бесконечном интервале $I(Polyn;\ M(k))$ при $k = p^3$.

5. Найдены аналоги построенных решеток замкнутых классов k-значных функций в счетнозначной логике. Некоторые из них выявляют предполные классы в функциональной системе $L(\mathbb{Z})$ полиномов первой степени с целыми коэффициентами. Выведены критерии полноты в $L(\mathbb{Z})$ систем, содержащих некоторые классы линейных функций (критерии относительной полноты).

Некоторые направления дальнейших исследований

1. Рассмотрение других значений составного k, в частности, $k = p_1 \cdots p_m,\ m \geq 3,\ \ k = p^2 q,\ \ k \equiv 0 \pmod{p^3}$.

2. Объяснение факта бесконечности интервала $I(Polyn; M(k))$ при $p^3|k$, обнаруженного А. Б. Ремизовым. Уточнение мощности бесконечной цепи, поиск других бесконечных семейств замкнутых классов.

3. Рассмотрение не всюду определенных функций и их замкнутых классов, содержащих введенные классы отображений в P_k.

4. Применение других, более "сильных" операторов замыкания.

5. Рассмотрение и классификация мультифункций.

Литература

[1] Мещанинов Д. Г. Некоторые условия представимости функций из P_k полиномами по модулю k // Доклады АН СССР. — 1988. — Т. 299, №1. — С. 50–53. (Перевод: Meshchaninov D. G. Some conditions for representability of functions from P_k by polynomials modulo k // Soviet Math. Doklady — 1988. — V. 37, No 2. — Pp. 338–341.)

[2] Мещанинов Д. Г. О некоторых свойствах надструктуры класса полиномов в P_k // Математические заметки. — 1988. — Т. 44, №5. — С. 673–681. (Перевод: Meshchaninov D. G. Superstructure of the closed class of polynomials in P_k // Mathematical Notes —- V. 44, No 5. — Pp. 950–954.)

[3] Мещанинов Д. Г. Перестановочные представления функций k-значной логики // Вестник Московского ун-та. Сер. 15. Вычислительная математика и кибернетика. — 1988, №3. — С. 61–66.

[4] Мещанинов Д. Г. О вторых p-разностях функций p^α-значной логики // Дискретная математика. — 1992. — Т. 4, вып. 4.— С. 131–139. (Перевод: Meshchaninov D. G. On the secondary p-differences of functions of p^α-valued logic // Discrete Mathematics and Applications — 1993. — V. 3, No 6. — Pp. 611–621.)

[5] Мещанинов Д. Г. Метод построения полиномов для функций k-значной логики // Дискретная математика — 1995. — Т. 7, №3. — С. 48–60. (Перевод: Meshchaninov D. G. A method for constructing polynomials for functions of k-valued logic // Discrete Mathematics and Applications — 1995. — V. 5, No 4. — Pp. 333–346.)

[6] Мещанинов Д. Г. О первых d-разностях функций k-значной логики // Математические вопросы кибернетики. Вып. 7. — М.: Наука, 1998. — С. 265–280.

[7] Мещанинов Д. Г. О замкнутых классах k-значных функций, сохраняющих первые d-разности // Математические вопросы кибернетики. Вып. 8. — М.: Наука, 1999. — С. 219–230.

[8] Мещанинов Д. Г. Замкнутые классы полиномов по модулю p^2 // Дискретная математика. — 2017. — Т. 29, №3. — С. 54–69. (Перевод: Meshchaninov

D. G. Closed classes of modulo p^2 polynomials // Discrete Mathematics and Applications — 2017. — V. 28, No 3. — Pp. 167—178.)

[9] Мещанинов Д. Г. Об одном семействе замкнутых классов в k-значной логике // Вестник Московского университета. Сер. 15. Вычислительная математика и кибернетика. — 2019, №1. — С. 44–53. (Перевод: Meshchaninov D. G. A family of closed classes in k-valued logic // Moscow University Computational Mathematics and Cybernetics — 2019. — V. 43, No 1. — Pp. 25–31.)

[10] Мещанинов Д. Г. Некоторые семейства замкнутых классов в P_k, задаваемых аддитивными формулами // Дискретная математика. — 2021. — Т. 33, №2. — С. 100–116. (Перевод: Meshchaninov D. G. Some families of closed classes in P_k defined by additive formulas // Discrete Mathematics and Applications — 2022. — V. 32, No 2. — Pp. 115—128.)

[11] Мамонтов А. И., Мещанинов Д. Г. Проблема полноты в функциональной системе линейных полиномов с целыми коэффициентами // Дискретная математика — 2010. — Т. 22, №4. — С. 64–82. (Перевод: Mamontov A. I., Meshchaninov D. G. The completeness problem in the function algebra of linear integer-coefficient polynomials // Discrete Mathematics and Applications — 2010. — V. 20, No 5-6. — Pp. 621–641.)

[12] Мамонтов А. И., Мещанинов Д. Г. Алгоритм распознавания полноты в функциональной системе $L(Z)$ // Дискретная математика — 2014 — Т. 26, №1. — С. 85–95. (Перевод: Mamontov A. I., Meshchaninov D. G. The algorithm for completeness recognizing in function algebra $L(Z)$ // Discrete Mathematics and Applications — 2014. — V. 24, No 1. — Pp. 21–28.)

В совместных работах [11,12] лично соискателю принадлежат постановки задач и получение результатов, изложенных в диссертации: утверждений 6.1, 6.2, 6.4, 6.5, 6.7, 6.8, 6.12, следствий 6.1–6.12 и лемм 6.2–6.4.

[13] Мещанинов Д. Г., Никитин И. В. Функционально замкнутые классы полиномов, сохраняющие некоторые эквивалентности на числовых множествах // Вестник МЭИ — 2011, №6. — С. 14–23.

В этой работе лично соискателю принадлежат постановки задач, окончательные формулировки результатов, вывод утверждений о полиномах, сохраняющих модуль (последние представлены в диссертационной работе как утверждение 6.12 и следствие 6.10).

[14] Мещанинов Д. Г., Никитин И. В. Классы сохранения пороговых разбиений в функциональных системах полиномов // Вестник МЭИ — 2012, №6. — С. 132–141.

В этой работе лично соискателю принадлежит постановка задачи и весь параграф 2 (он использован в разделе 6.7 диссертационной работы).

Публикации [1–14] — из перечня ВАК.

[15] Галкин П. А., Мещанинов Д. Г. Аналитический метод решения уравнений в k-значной логике // Вестник МЭИ. — 2002, №6. — С. 28–33.

[16] Галкин П. А., Мещанинов Д. Г. Аналитический метод решения уравнений на конечных множествах // Материалы VIII Междунар. сем. "Дискретная математика и ее приложения" (2–6 фев. 2004 г.) — М.: Изд. мех.-мат. факультета МГУ, 2004. — С. 127–129.

[17] Галкин П. А., Мещанинов Д. Г. Метод решения системы уравнений над кольцом вычетов, содержащей неопределенность в коэффициентах // Вестник МЭИ — 2005, №6. — С. 121–128.

В совместных работах [15-17] лично соискателю принадлежит постановка задачи и окончательные формулировки результатов.

[18] Крахмалева О. А., Мещанинов Д. Г. Метод оптимального доопределения частичной трехзначной функции // Вестник МЭИ — 2009, №6. — С. 94–102.

В этой работе лично соискателю принадлежит постановка задачи и формулировки результатов.

[19] Кузьмина О. Л., Мещанинов Д. Г. Метод доопределения частичной булевой функции до кратчайшего полинома // Вестник МЭИ — 2004, №6. — С. 73–80.

В этой работе лично соискателю принадлежит постановка задачи и формулировки результатов.

[20] Мамонтов А. И., Мещанинов Д. Г. Проблема полноты в функциональной системе линейных полиномов с целыми коэффициентами // Труды VI Международной конференции "Дискретные модели в теории управляющих систем" (Москва, 7–11 декабря 2004 г.) — М.: Изд. отдел ВМиК МГУ им. М. В. Ломоносова. — С. 50–52.

[21] Мамонтов А. И., Мещанинов Д. Г. Функционально-замкнутые классы полиномов, сохраняющих подмножества бесконечной области определения // Труды XIX Международ. научно-техн. конф. "Информ. средства и технологии" (Москва, 18–20 окт. 2011 г.). — М.: Изд. дом МЭИ, 2011. — Т. 3. — С. 272–277.

[22] Мамонтов А. И., Мещанинов Д. Г. Алгоритм распознавания полноты в алгебре $L(\mathbb{Z})$ // Тез. докл. Междунар. конф. "Дискретная математика, теория графов и их приложения". Минск, 11-14 ноября 2013 г. — Мн.: Ин-т математики НАН Беларуси, 2013. — С. 30–32.

[23] Мамонтов А. И., Мещанинов Д. Г. Алгоритмические проблемы, связанные с полнотой в функциональной системе $L(Z)$ // Проблемы теоретической кибернетики. Материалы XVII международной конференции (Казань, 16–20 июня 2014 г.) — Казань: Отечество, 2014. — С. 192–194.

В совместных работах [20–23] лично соискателю принадлежат постановки задач и получение результатов, изложенных в диссертации: утверждений 6.1, 6.2, 6.4, 6.5, 6.7, 6.8, 6.12, следствий 6.1–6.12 и лемм 6.2–6.4.

[24] Мещанинов Д. Г. О полиномиальной реализации функций k-значной логики / Деп. ВИНИТИ 23.10.1987, №7441-В87. — М., 1987. — 9 с.

[25] Мещанинов Д. Г. О классе Кузнецова в p^α-значной логике // Проблемы теоретической кибернетики. Тезисы докладов XI Международной конференции. Ульяновск, 10–14 июня 1996 г. — С. 142–143.

[26] Мещанинов Д. Г. Периодические функции k-значной логики // Труды VI Международной конференции "Дискретные модели в теории управляющих систем" (Москва, 7–11 декабря 2004 г.) — М.: Изд. отдел ВМиК МГУ им. М. В. Ломоносова. — С. 55–57.

[27] Мещанинов Д. Г. О надструктуре класса полиномов в частичной k-значной логике // Труды VII Международной конференции "Дискретные модели в теории управляющих систем". Покровское, 4–6 марта 2006 г. — М: Макс-Пресс, 2009. — С. 248–250.

[28] Мещанинов Д. Г. Классификация аддитивных представлений частичных и всюду определенных функций k-значной логики // Труды VIII Международной конференции "Дискретные модели в теории управляющих систем". 6–9 апреля 2009 г. — М: Макс-Пресс, 2009. — С. 214–218.

[29] Мещанинов Д. Г. Замкнутые классы в P_k^*, определяемые значениями функций на параллелограммах // Материалы XI Международного семинара «Дискретная математика и ее приложения», посвященного 80-летию со дня рождения академика О. Б. Лупанова (Москва, 18–23 июня 2012 г.) — М.: Изд. мех.-мат. ф-та МГУ, 2012. — С. 202–204.

[30] Мещанинов Д. Г. Периодические функции и замкнутые классы в P_k^* // Синтаксис и семантика логических систем: Материалы IV российской школы-семинара, посвященной 80-летию Бурятского государственного университета

(Улан-Удэ, 14–19 августа 2012 г.) — Иркутск, Изд-во ФГБОУ ВПО "Восточно-Сибирская государственная академия образования", 2012. — С. 74–77.

[31] Мещанинов Д. Г. О замкнутых классах полиномов над кольцом Z_k // Труды VIII Международной конференции "Дискретные модели в теории управляющих систем". Москва и Подмосковье, 20–22 мая 2015 г. — М: Макс Пресс, 2015. — С. 161–163.

[32] Мещанинов Д. Г. Семейства замкнутых классов в P_k, определяемые аддитивными и полиномиальными представлениями функций // Материалы XII Международного семинара «Дискретная математика и ее приложения» им. академика О. Б. Лупанова (Москва, МГУ, 20–25 июня 2016 г.) — М.: Изд. мех.-мат. ф-та МГУ, 2016. — С. 96–106.

[33] Мещанинов Д. Г. Три семейства замкнутых классов в P_k, определяемых d-разностями функций // Материалы XII Международного семинара «Дискретная математика и ее приложения» им. академика О. Б. Лупанова (Москва, МГУ, 20–25 июня 2016 г.) — М.: Изд. мех.-мат. ф-та МГУ, 2016. — С. 207–209.

[34] Мещанинов Д. Г. Некоторые замкнутые классы в P_k и их гомоморфизмы в P_d при $d|k$ // Труды XVIII Международной конференции "Проблемы теоретической кибернетики" (Пенза, 19–23 июня 2017 г.) — М: МАКС Пресс, 2017. — С. 161–163.

[35] Мещанинов Д. Г. Функции, обобщающие полиномы по модулю k // Труды X Международной конференции "Дискретные модели в теории управляющих систем". Москва и Подмосковье, 23–25 мая 2018 г. — М: Макс Пресс, 2018. — С. 198–200.

[36] Мещанинов Д. Г. Классификация k-значных функций на основе аддитивных формул // Синтаксис и семантика логических систем: материалы 6 -й Международной школы-семинара, Монголия, Ханх, 11–16 августа 2019 г.; ФГБОУ ВО «ИГУ». — Иркутск: Изд. ИГУ, 2019. — С. 68–72.

[37] Мещанинов Д. Г. О решетке некоторых классов в P_k // Проблемы теоретической кибернетики. Материалы заочного семинара XIX международной конференции — Казань: Отечество, 2020. — С. 82–84.

[38] Мещанинов Д. Г. Отношения делимости чисел и включения замкнутых классов многозначных функций // Проблемы теоретической кибернетики. Материалы XIX международной конференции — Казань: Казанский федеральный ун-т, 2021. — С. 109–112.

[39] Мещанинов Д. Г., Никитин И. В. Классы полиномов, сохраняющих разбиения области определения на промежутки равной длины // Вестник МЭИ — 2013, №6. — С. 147–153.

[40] Мещанинов Д. Г., Никитин И. В. Классы полиномов, сохраняющих обобщенные точечные разбиения бесконечной области определения // Международный научно-исследовательский журнал — 2015, 9-3(40). — С. 75–79.

В совместных работах [39–40] лично соискателю принадлежат постановки задач и окончательные формулировки результатов, вывод некоторых утверждений.

[41] Айзенберг Н. Н., Семйон И. В. Некоторые критерии представимости функций k-значной логики полиномами по модулю k — В кн.: Многоустойчивые элементы и их применение — М.: Сов. радио, 1971. — С. 84–88.

[42] Айзенберг Н. Н., Семйон И. В., Циткин А. И. Мощность класса функций k-значной логики от n переменных, представимых полиномами по модулю k — В кн.: Многоустойчивые элементы и их применение — М.: Сов. радио, 1971. — С. 79–83.

[43] Алексеев В. Б. О замкнутых классах в частичной k-значной логике, содержащих все полиномы // Дискретная матем. — 2021. — Т. 33, №2. — С. 6–19.

[44] Алексеев В. Б., Вороненко А. А. О некоторых замкнутых классах в частичной двузначной логике // Дискрет. матем. — 1994. — Т. 6, №4. — С.58–79.

[45] Алексиадис Н. Ф. Функциональная система полиномов с натуральными коэффициентами // Вестник МЭИ. — 2013, №6. — С. 109–111.

[46] Алексиадис Н. Ф. Алгоритмическая неразрешимость проблемы полноты для полиномов с целыми коэффициентами // Вестник МЭИ. — 2015, №3. — С. 110–117.

[47] Алексиадис Н. Ф. Алгоритмическая неразрешимость задачи о нахождении базиса конечной полной системы полиномов с целыми коэффициентами // Интеллектуальные системы. Теория и приложения. — 2016. — Т. 20, №3. — С. 19–23.

[48] Алексиадис Н. Ф. О функциональной системе полиномов с рациональными коэффициентами // Интеллектуальные системы. Теория и приложения. — 2019. — Т. 23, №4. — С. 93–114.

[49] Башов М. А., Селезнева С. Н. О длине функций k-значной логики в классе полиномиальных нормальных форм по модулю k // Дискретная математика — 2014. — Т. 26, №3. — С. 3–9.

[50] Вороненко А. А. Об универсальных частичных функциях для класса линейных функций // Дискрет. матем. — 2012. — Т. 24, №3. — С. 62–65.

[51] Вороненко А. А., Воронова Н. К., Ильютко В. П. О существовании универсальной функции для класса линейных k-значных функций при небольших k // Прикладная математика и информатика. — 2016, вып. 51. — С. 100–108.

[52] Вороненко А. А., Окунева А. С. Универсальные функции для классов линейных функций двух переменных // Дискрет. матем. — 2020. — Т. 32, №1. — С. 3–7.

[53] А. А. Вороненко А. А. Об универсальности произведения для классов линейных функций двух переменных// Дискретная математика. — 2022. — Т. 34, №1. — С. 20–22.

[54] Гаврилов Г. П. О надструктуре класса полиномов в многозначных логиках // Дискретная математика.— 1996. — Т. 8, №3. — С. 90–97.

[55] Гаврилов Г. П. О замкнутых классах многозначной логики, содержащих класс полиномов // Дискретная математика.— 1997. — Т. 9, №2. — С. 12–23.

[56] Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по дискретной математике — М.: ФИЗМАТЛИТ, 2004. — 416 с.

[57] Заец М. В., Никонов В. Г., Шишков А. Б. Класс функций с вариационно-координатной полиномиальностью над кольцом Z_{2^m} и его обобщение // Математические вопросы криптографии — 2013. — Т. 4, № 3. — С. 21–47.

[58] Заец М. В. О классе вариационно-координатно-полиномиальных функций над примарным кольцом вычетов // Прикладная дискретная математика — 2014. — №3(25). — С. 12–27.

[59] Зинченко А. С., Пантелеев В. И. Полиномиальные операторные представления функций k-значной логики // Дискретн. анализ и исслед. опер., сер. 1. — 2006. — Т. 13, №3. — С. 13–26.

[60] Крохин А. А., Сафин К. Л., Суханов Е. В. О строении решетки замкнутых классов полиномов // Дискретная математика.— 1997. — Т. 9, №2. — С. 24–39.

[61] Марченков С. С. Об операторе замыкания по перечислению в многозначной логике // Вестник Московского ун-та. Сер. 15. Выч. математика и кибернетика. — 2015, №2. — С. 33–39.

[62] Марченков С. С. Сильные операторы замыкания — М.: МАКС Пресс, 2017. — 94 с.

[63] Марченков С. С. Расширения оператора позитивного замыкания с помощью логических связок // Дискрет. анализ и исслед. операций. — 2018. — Т. 25, №4. — С. 46–58.

[64] Марченков С. С. Критерий полноты в классе экспоненциально-полиномиальных функций // Вестник Московского ун-та. Сер. 15. Выч. математика и кибернетика. — 2020, №2. — С. 37–44.

[65] Марченков С. С., Простов В. А. Критерий полноты относительно оператора замыкания по перечислению в трехзначной логике // Дискретная матем. — 2021. — Т. 33, №2. — С. 86–89.

[66] Марченков С. С. О проблеме равенства конечно-порожденных классов экспоненциально-полиномиальных функций // Дискретная матем. — 2022. — Т. 34, №1. — С. 64–75.

[67] Нечаев А. А. Критерий полноты систем функций p^n-значной логики, содержащих операции сложения и умножения по модулю p^n // Методы дискретного анализа в решении комбинаторных задач. — Вып. 34. — Новосиб.: Изд-во ИМ СО АН СССР, 1980. — С. 74–89.

[68] Пантелеев В. И. Полиномиальное разложение k-значных функций по невырожденным функциям — Матем. заметки. — 1994. — Т. 55, №1. — С.144–149.

[69] Пантелеев В. И. Полиномиальные разложения k-значных функций по операторам дифференцирования и нормализации // Изв. вузов. Матем. — 1998, №1. — С. 82–85.

[70] Пантелеев В. И., Перязев Н. А. О представлении функций k-значной логики суммой произведений остаточных подфункций // Дискретная математика. — 2007. — Т. 19, №2. — С. 94–100.

[71] Пантелеев В. И., Тагласов Э. С. ES_I-замыкание мультифункций ранга 2: критерий полноты, классификация и типы базисов // Интеллектуальные системы. Теория и приложения. — 2021. — Т. 25, №2. — С. 55–80.

[72] Перязев Н. А. Тождества в алгебрах мультиопераций фиксированной размерности — Известия Иркутского государственного университета. Серия Математика. — 2019. — Т. 29. — С. 86–97.

[73] Ремизов А. Б. О надструктуре замкнутого класса полиномов по модулю k // Дискретная математика. — 1989. Т. 1, №1. — С. 3–15.

[74] Рябов В. Г. О степени ограничения функций q-значной логики на линейные многообразия // Прикладная дискретная математика. — 2019, №45. — С. 13–25.

[75] Селезнева С. Н. Полиномиальный алгоритм для распознавания принадлежности представленной полиномом функции k-значной логики предполным классам линейных функций // Материалы четвертой молодежной научной школы по дискретной математике и ее приложениям (Москва, 18–23 сент. 2000 г.) — М.: Изд. мех.-мат. факультета МГУ, 2000. — С. 69–73.

[76] Селезнева С. Н. О приближении с заданной точностью функций k-значных логик полиномами // Дискрет. матем. — 2008. — Т. 20, №2. — С. 32–45.

[77] Селезнева С. Н. О сложности задания k-значных функций обобщенно-поляризованными полиномами // Дискрет. матем. — 2009. — Т. 21, №4. — С. 20–29.

[78] Селезнева С. Н. Быстрый алгоритм построения для k-значных функций полиномов по модулю k при составных k // Дискретная математика. — 2011. — Т. 23, №3. — С. 3–22.

[79] Селезнева С. Н. О числе полиномиальных функций k-значной логики по составному модулю k // Дискрет. матем. — 2016. — Т. 28, №2. — С. 81–91.

[80] Селезнева С. Н. О свойствах мультиаффинных предикатов на конечном множестве // Дискрет. матем., — 2021. — Т. 33, №4. — С. 141–152.

[81] Селезнева С. Н., Маркелов Н. К. Быстрый алгоритм построения векторов коэффициентов поляризованных полиномов k-значных функций // Учён. зап. Казан. гос. ун-та. Сер. Физ.-матем. науки. — 2009. — Т. 151, №2. — С. 147–153.

[82] Семигродских А. П., Суханов Е. В. О замкнутых классах полиномов над конечными полями // Дискретная математика.— 1997. — Т. 9, №4. — С. 50–62.

[83] Черепов А. Н. Описание структуры замкнутых классов в P_k, содержащих класс полиномов // Проблемы кибернетики. Вып. 40. — М.: Наука, 1983. — С. 5–18.

[84] Черепов А. Н. Надструктура класса сохранения отношений сравнения в k-значной логике по всем модулям-делителям k. / Автореф. дисс. канд. физ.-мат. н. — М., 1986.

[85] Черемушкин А. В. Аддитивный подход к определению степени нелинейности дискретной функции // Прикладная дискретная матем. // 2010, №2(8). — С. 22–33.

[86] Яблонский С. В. Функциональные построения в k-значной логике // Труды МИАН СССР. — Т. 51. — М.: МИАН СССР, 1958. — С. 5–142.

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

[88] Bagyinszki J., Demetrovics J. The lattice of linear classes in prime-valued logics — Banach Center Publ., 7. — 1982. — Pp. 105–123.

[89] Bulatov A. A. Polynomial reducts of modules, I. Rough classification // Mult.-Valued Log. — 1998.— V. 33, No 2. — Pp. 135–154.

[90] Carlitz L. Functions and polynomials $(\mathrm{mod}\ p^n)$ // Acta Arithmetica. — 1964, No 9. — Pp. 66–78.

[91] Couceiro M., Haddad L., Scholzel K., Waldhauser T. A solution to a problem of D. Lau: complete classiffication of intervals in the lattice of partial boolean clones // J. Mult.-Val. Logic Soft Comput. — 2017. — V. 28. — Pp. 47–58.

[92] Hermit Ch. Sur les fonctions des sept lettres // C. R. Acad. Sci. Paris. — 1863. — 57. — Pp. 750–757.

[93] Keller G, Olson F. R. Counting polynomial functions $(\mathrm{mod}\ p^n)$ // Duke Math. J. — 1968. — V. 35, No 4. — Pp. 835–838.

[94] Kempner A. J. Polynomials and their residue systems // Transactions of AMS. — 1921. — V. 22. — Pp. 240-288.

[95] Lau D. Function algebras on finite sets. — Berlin, Heidelberg, New York: Springer-Verlag, 2006. — 668 pp.

[96] Peryazev N. A., Peryazeva Yu. V., Sharankhaev I. K. Minimal algebras of unary multioperations // Журн. СФУ. Сер. Матем. и физ. — 2016. — Т.9, №2 — С. 220–224.

[97] Peryazev N. A., Sharankhaev I. K. On some sufficient condition for the equality of multi-clone and super-clone // Журн. СФУ. Сер. Матем. и физ. — 2018. — Т.11, №1. — С. 97–102.

[98] Peryazev N. A. Systems of inclusions with unknowns in multioperations // Известия Иркутского государственного университета. Серия Математика.— 2021. — Т. 38. — С. 112–123.

[99] Post E. L. Introduction to a general theory of elementary propositions // Amer. J. Math. — 1921. — V. 43, No 3. — Pp. 163–185.

[100] Post E. L. The two-valued iterative systems of mathematical logic // Annals of Math. Stud. Vol. 5. — Princeton-London: Princeton Univ. Press, 1941.

[101] Redei L., Szele T. Algebraisch-Zahlentheoretisch Betrachtungen über Ringe, II // Acta Math. — 1950. — V. 82. — Pp. 240–291.

[102] Reed I. S., Truong T. K. The use of finite fields to compute convolations // IEEE Trans. on Inform. Theory — 1975. — V. IT-21, No 3. — Pp. 208–213. (Перевод: Рид И. С., Труонг Т. К. Применение конечных полей для вычисления сверток // В кн.: Макклеллан Дж. Х., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов — М.: Радио и связь, 1983. — С. 207–216.)

[103] Rosenberg I. G. Polynomial functions over finite rings // Glasnik Matematiki. — 1975. — V. 10, No 1. — Pp. 25–33.

[104] Salomaa A. A. On infinitely generated sets of operations in finite algebra, I // Ann. Univ. Turku. — 1964. — Ser. A, 74. — Pp. 1–12.

[105] Selezneva S. N. Constructing polynomials for functions over residue rings modulo a composite number in linear time // Lect. Notes Comput. Sci. — 2012.— **7353**. — Pp. 303–312.

[106] Singmaster D. On polynomial functions $\pmod m$ // J. Number Theory. — 1974. — V. 6, No 5. — Pp. 345–352.

[107] Szendrei Á. On closed sets of linear operations over a finite set of square-free cardinality // Elektr. Inform. Kybern., 14 — 1978. — Pp. 547–559.

[108] Szendrei Á. On closed classes of quasilinear functions // Czechoslov. Math. J. — 1980, No 80. — Pp. 498–509.