

Московский Государственный Университет
имени М.В. Ломоносова
Российская Академия Наук
Международная Академия Технологических Наук
Российская Академия Естественных Наук

Интеллектуальные Системы.

Теория и приложения

ТОМ 30 ВЫПУСК 2 * 2026

МОСКВА

УДК 519.95; 007:159.955
ББК 32.81

ISSN 2411–4448
Издаётся с 1996 г.

Главный редактор: д.ф.-м.н., профессор Э. Э. Гасанов

Редакционная коллегия:

к.ф.-м.н., доц. А. В. Галатенко (зам. главного редактора)
д.ф.-м.н., проф. А. А. Часовских (зам. главного редактора)

д.ф.-м.н., проф. В. В. Александров, д.ф.-м.н., проф. С. В. Алёшин, д.ф.-м.н., проф. А. Е. Андреев, д.ф.-м.н., проф. Д. Н. Бабин, к.ф.-м.н., доц. Г. В. Боков, проф. К. Вашик, проф. Я. Деметрович, академик РАН, д.ф.-м.н., проф. Ю. Л. Ершов, к.ф.-м.н., н.с. Г. В. Калачёв, проф. Г. Килибарда, д.ф.-м.н., проф. В. Н. Козлов, к.ф.-м.н., в.н.с. В. А. Носов, д.ф.-м.н., проф. А. С. Подколзин, д.ф.-м.н., проф. Ю. П. Пытьев, д.т.н., проф. А. П. Рыжов, к.ф.-м.н., доц. Э. М. Сайдамагов, академик РАН, д.т.н., проф. А. С. Сигов, к.ф.-м.н., доц. А. С. Строгалов, проф. Б. Тальхайм, проф. Ш. Ушчумлич, д.ф.-м.н., проф. А. В. Чечкин, к.ф.-м.н. Ш. Н. Шералиев, к.ф.-м.н. Р. Шчепанович.

Секретари редакции: И. О. Бергер, Е. В. Кузнецова

В журнале «Интеллектуальные системы. Теория и приложения» публикуются научные достижения в области теории и приложений интеллектуальных систем, новых информационных технологий и компьютерных наук.

Издание журнала осуществляется под эгидой МГУ имени М.В. Ломоносова, Научного Совета по комплексной проблеме «Кибернетика» РАН, Отделения «Математическое моделирование технологических процессов» МАТН.

Учредитель журнала: ООО «Интеллектуальные системы».

Журнал входит в список изданий, включенных ВАК РФ в реестр публикаций материалов по кандидатским и докторским диссертациям по математике и механике. Входит в дополнительный перечень научных изданий, в которых могут быть опубликованы результаты диссертаций, защищаемых в МГУ.

Индекс подписки на журнал: 64559 в каталоге НТИ «Роспечать».

Адрес редакции: 119991, Москва, ГСП-1, Ленинские Горы, д. 1, механико-математический факультет, комн. 12-01.

Адрес издателя: 115230, Россия, Москва, Хлебозаводский проезд, д. 7, стр. 9, офис 9. Тел. +7 (495) 939-46-37, e-mail: mail@intsysmagazine.ru

*) Прежнее название журнала: «Интеллектуальные системы».

© ООО «Интеллектуальные системы», 2026.

ОГЛАВЛЕНИЕ

Вадим Никитович Козлов (к 80-летию со дня рождения)	5
Михаил Васильевич Носов (к 70-летию со дня рождения)	7

Часть 1. Общие проблемы теории интеллектуальных систем

<i>Колосов А. М.</i> Ординальная агрегация наборов векторных представлений слов	10
---	----

Часть 2. Специальные вопросы теории интеллектуальных систем

<i>Дробышев А. С.</i> О вычислительной сложности задачи существования предельных циклов в булевых сетях с ограничениями из решётки Поста	28
<i>Дюбанов А. В.</i> Операции над клеточными автоматами с локаторами	55
<i>Седова А. С.</i> Верхняя линейная оценка для мощности области определения универсальной функции для пар линейных	74

Часть 3. Математические модели

<i>Бирюкова В. А.</i> О K -порождаемости предполных классов линейных автоматов	82
<i>Калачев Г. В.</i> Многомерное расширение произведений кодов сильнее робастной тестируемости и тестируемости на согласованность	101
<i>Молдованов И. В.</i> Проблема полноты линейных дефинитных автоматов	120
<i>Янушкевич И. М.</i> Аналог предполного класса Слупецкого в классе полиномов по модулю четыре	142

Часть 4. Круглый стол

<i>Чечкин А. В., Плешакова Е. С.</i> Языковая радикальная сервисная платформа анализа и синтеза автоматизированных многоагентных систем искусственного интеллекта различного назначения	158
---	-----

Вадим Никитович Козлов (к 80-летию со дня рождения)

1 мая 2026 года отмечает свой 80-летний юбилей профессор механико-математического факультета МГУ, доктор физико-математических наук, заслуженный профессор Московского университета Вадим Никитович Козлов. Редакционная коллегия журнала «Интеллектуальные системы. Теория и приложения» сердечно приветствует юбиляра и выражает глубокое восхищение его многолетним служением отечественной науке и образованию.

Судьба Вадима Никитовича неразрывно связана с Московским университетом. Окончив с отличием физический факультет МГУ в 1970 году, а затем аспирантуру факультета ВМиК, он более полувека трудится на ниве просвещения и фундаментальных исследований. Пройдя путь от ассистента до профессора, В.Н. Козлов снискал авторитет крупного специалиста в области математической кибернетики, теории распознавания образов, дискретной математики и математической биологии. Его перу принадлежат около 80 научных трудов, в том числе 6 монографий, а также три патента на оригинальный принцип цифровой подписи.

Важно подчеркнуть, что Вадим Никитович всегда стремился не только добывать новое знание, но и щедро делиться им. Его педагогический стаж превышает 50 лет. Он прочитал много лекционных курсов, в том числе в филиалах МГУ в Баку и Ташкенте, а также выступал на телевидении (канал ОТР) с рассказами о работах по распознаванию образов. По приглашению организации «Универсариум» им был записан цикл интернет-лекций, который доступен в сети Интернет. Так научные идеи Вадима Никитовича выходят далеко за пределы университетских аудиторий.

Научно-организационная деятельность Вадима Никитовича также заслуживает самых тёплых слов. Он долгое время был членом диссертационного совета при Вычислительном центре РАН, учёным секретарём экспертного совета ВАК по математике и механике, награждён грамотой президиума ВАК. В 2023 году ему присвоено почётное звание «Заслуженный профессор Московского университета», а также он награждён медалью «В память 850-летия Москвы». Коллеги знают Вадима Никитовича как принципиального, доброжелательного и мудрого человека, неизменно пользующегося уважением среди коллег и студентов.

Дорогой Вадим Никитович! В день Вашего 80-летия редакционная коллегия желает Вам бодрости духа, крепкого здоровья и новых творческих успехов. Пусть Ваш опыт и энтузиазм ещё долго служат примером для молодых исследователей, а заложенные Вами традиции находят

достойное продолжение в стенах Московского университета и за его пределами.

**Редакционная коллегия журнала
«Интеллектуальные системы. Теория и приложения»**

Михаил Васильевич Носов

(к 70-летию со дня рождения)

13 апреля 2026 года исполняется 70 лет старшему научному сотруднику кафедры математической теории интеллектуальных систем механико-математического факультета МГУ, кандидату физико-математических наук, доценту Михаилу Васильевичу Носову.

Редакционная коллегия журнала «Интеллектуальные системы. Теория и приложения» тепло поздравляет Михаила Васильевича с этой знаменательной датой и выражает искреннюю признательность за его многолетний вклад в развитие отечественной школы распознавания образов.

Жизненный путь Михаила Васильевича тесно переплетён с Московским университетом. Поступив на мехмат в 1973 году и окончив его в 1978-м, он затем, после работы в различных научных организациях, вернулся в альма-матер, поступив в заочную аспирантуру, которую успешно завершил в 1988 году. С 1990 года и по настоящее время его деятельность неразрывно связана с родным факультетом, где он снискал уважение коллег ответственностью, высокой работоспособностью и неизменной добросовестностью.

Научные интересы Михаила Васильевича сформировались ещё в аспирантские годы. В 1989 году он блестяще защитил кандидатскую диссертацию, посвящённую функциональным характеристикам тестовых алгоритмов распознавания образов. Эта тема остаётся в центре его исследований на протяжении десятилетий. Им опубликовано 28 статей в ведущих журналах, а также ряд работ в сборниках и тезисов докладов. При этом Михаил Васильевич всегда стремился соединять теорию с практикой: он активно участвует в прикладных исследованиях по распознаванию образов, которые проводятся на кафедре.

Педагогическая деятельность Михаила Васильевича заслуживает самых тёплых слов. Получив в 1997 году звание доцента, он щедро передавал свои знания не только студентам мехмата, но и обучающимся в других вузах (МГАПИ, МГТУ «Станкин»), а также в Специализированном учебно-научном центре МГУ (СУНЦ). Его лекции и семинары, отличающиеся ясностью и глубиной, помогли войти в науку не одному поколению будущих математиков и кибернетиков.

Особо следует отметить организаторский талант Михаила Васильевича. Он неоднократно принимал активное участие в проведении престижной конференции «Интеллектуальные системы и компьютерные науки», а в 2021 и 2026 годах являлся председателем её Исполнительного комитета. Благодаря его усилиям форум сохраняет высокий научный уро-

вень и привлекает молодых исследователей. Также он в течении многих лет является учёным секретарём лаборатории Проблем теоретической кибернетики.

Скромность, доброжелательность и высокая требовательность к себе снискали Михаилу Васильевичу искреннее уважение всех, кто с ним работает. Коллеги ценят его за надёжность и готовность прийти на помощь, а ученики — за терпение и увлечённость своим делом.

В день Вашего 70-летия мы желаем Вам, дорогой Михаил Васильевич, крепкого здоровья, неиссякаемой энергии и новых творческих успехов. Пусть Ваш опыт и преданность науке ещё долго служат примером для молодых поколений исследователей!

**Редакционная коллегия журнала
«Интеллектуальные системы. Теория и приложения»**

Часть 1
Общие проблемы теории
интеллектуальных систем

Ординальная агрегация наборов векторных представлений слов

А. М. Колосов*

В работе исследуется задача слияния наборов векторных представлений слов от различных предобученных моделей. Поскольку прямое объединение векторных пространств сопряжено с вычислительными трудностями и проблемой локальных минимумов, предлагается переход к ординальным методам агрегации. Доказывается отсутствие циклов в индивидуальных ординальных матрицах попарных сравнений расстояний, что гарантирует эквивалентность алгоритмов Кемени и Коупленда в этом случае. Для агрегированных матриц, где возможен парадокс Кондорсе, алгоритм Коупленда выступает эффективной эвристикой. Также рассматривается метод Борда, не требующий построения турнирных графов. Проведены эксперименты на 10 моделях и 3 датасетах (WordSim-353, MEN, SimLex-999). Показано, что ординальные методы позволяют находить оптимальные комбинации моделей (тройки, четвёрки и пятёрки), превосходящие индивидуальные модели по корреляции Спирмена, при этом разница между методами Борда и Кемени/Коупленда минимальна.

Ключевые слова: векторные представления слов, агрегация моделей, метод Борда, метод Кемени, алгоритм Коупленда, турнирные графы, ординальная матрица.

1. Введение

Векторные представления слов (word embeddings) играют ключевую роль в задачах обработки естественного языка. Различные архитектуры и обучающие корпуса приводят к тому, что модели улавливают разные аспекты семантики: например, модели на основе графов знаний (ConceptNet

* *Колосов Алексей Михайлович* — научный сотрудник кафедры математической теории интеллектуальных систем механико-математического факультета Московского государственного университета имени М. В. Ломоносова, научный сотрудник лаборатории инженерии знаний института математических исследований сложных систем Московского государственного университета имени М. В. Ломоносова, e-mail: aleksei.kolosov@math.msu.ru, ORCID: 0000-0002-9474-9666.

Kolosov Alexey Mikhajlovich — Research Fellow, Department of Mathematical Theory of Intelligent Systems, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University, Research Fellow, Knowledge Engineering Lab, Institute of Complex Systems Mathematical Research, Lomonosov Moscow State University.

Numberbatch [1]) хорошо отражают строгие семантические связи, классические дистрибутивные модели (GloVe [2], Word2Vec [3], fastText [4]) улавливают статистические закономерности совместной встречаемости, модели на основе парафразных ограничений (Paragram [5]) оптимизированы для различения синонимов и антонимов, модели на основе контекста (SBERT [6], OpenAI text-embedding [7]) извлекают глубокий контекстный сигнал, а модели контрастивного обучения (SimCSE [8]) формируют представления, оптимизированные для различения семантически близких и далёких предложений.

Мотивация данной работы заключается в том, чтобы использовать готовые предобученные модели без необходимости обучать новые модели с нуля. Возникает задача: как эффективно объединить информацию из нескольких наборов векторных представлений, чтобы получить единую меру семантической близости, превосходящую каждую модель по отдельности? Прямое объединение (конкатенация или линейные преобразования) векторных пространств различной размерности и природы часто оказывается неэффективным. В данной статье предлагается подход, основанный на извлечении и объединении ординальной (порядковой) информации из различных векторных пространств.

2. Ординальная матрица для пар пар слов

Рассматривается множество слов W и множество всех пар слов $P = W \times W$. Каждая модель задаёт функцию расстояния (или сходства, например, косинусного) $d(p)$ для $p \in P$. Вместо того чтобы работать с абсолютными значениями $d(p)$, осуществляется переход к относительным сравнениям.

Для каждой пары пар слов $(p_i, p_j) \in P \times P$ фиксируется знак сравнения: $p_i \succ p_j$, если пара p_i семантически ближе, чем p_j в пространстве данной модели. Таким образом, каждая модель порождает индивидуальную ординальную матрицу (турнирный граф), где вершинами являются пары слов, а рёбра указывают направление предпочтения.

Пример турнирного графа для трёх пар слов: пусть $p_1 =$ (кошка, собака), $p_2 =$ (машина, автобус), $p_3 =$ (яблоко, груша). В таблице 1 приведён пример индивидуальной ординальной матрицы для случая, когда модель оценивает сходства как $d(p_1) = 0.9$, $d(p_2) = 0.8$, $d(p_3) = 0.7$.

Лемма 1 (Отсутствие циклов в индивидуальной матрице). *В индивидуальной ординальной матрице, порождённой функцией расстояния в метрическом пространстве, отсутствуют циклы.*

Таблица 1: Пример индивидуальной ординальной матрицы

Пара слов	p_1	p_2	p_3
p_1 (кошка, собака)	–	\succ	\succ
p_2 (машина, автобус)	\succ	–	\succ
p_3 (яблоко, груша)	\succ	\succ	–

Доказательство. Предполагается противное: существует цикл $p_1 \succ p_2 \succ \dots \succ p_k \succ p_1$. Это означает, что $d(p_1) > d(p_2) > \dots > d(p_k) > d(p_1)$. По транзитивности строгого неравенства для действительных чисел получается $d(p_1) > d(p_1)$, то есть расстояние больше самого себя. Полученное противоречие доказывает отсутствие циклов. Важно отметить, что отсутствие циклов является следствием природы происхождения турнирного графа: каждое ребро порождается сравнением значений $d(p_i)$ и $d(p_j)$, а транзитивность строгого неравенства на действительных числах гарантирует ацикличность. Произвольный турнирный граф, не порождённый функцией расстояния, может содержать циклы. \square

Для агрегированной ординальной матрицы, получаемой путём голосования большинства моделей, лемма 1 уже не выполняется. Известен парадокс Кондорсе [9]: возможна ситуация, когда большинство моделей предпочитает A перед B , большинство предпочитает B перед C , и большинство предпочитает C перед A . В таблице 2 приведён пример возникновения такого парадокса при агрегации трёх моделей.

Таблица 2: Пример возникновения парадокса Кондорсе

Модель	1-е место	2-е место	3-е место
Модель 1	A	B	C
Модель 2	B	C	A
Модель 3	C	A	B
Попарные победы (большинство 2:1):			
$A \succ B, B \succ C, C \succ A$ — цикл			

Теоретическим обоснованием возможности восстановления метрического пространства по ординальным ограничениям служит теорема Агарвала [10], утверждающая существование точного вложения в евклидово пространство при выполнении определённых условий на ординальные ограничения. К таким условиям относятся требования к размерности пространства вложения (которая должна быть достаточно большой) и

согласованности системы неравенств (отсутствие противоречивых ограничений вида $d_1 > d_2$ и $d_2 > d_1$).

3. Базовый подход: алгоритм GNMDS

Одним из способов решения задачи является восстановление векторных представлений с сохранением рангов (ординальных ограничений). Базовым подходом здесь является обобщённое неметрическое многомерное шкалирование (Generalized Non-metric Multidimensional Scaling, GNMDS) [11].

Этот алгоритм использует градиентный спуск для поиска координат векторов, которые минимизируют нарушения заданных неравенств $d(p_i) > d(p_j)$. Однако GNMDS имеет существенные недостатки:

1. Алгоритм основан на градиентном спуске и не гарантирует нахождения глобального минимума.
2. Высокая вычислительная сложность, ограничивающая масштабируемость на большие словари.

Поскольку качество векторных представлений в стандартных бенчмарках оценивается с помощью ординального показателя качества — корреляции Спирмена ρ , которая измеряет монотонную связь между предсказанными рангами пар слов и рангами экспертных оценок (то есть вычисляется как корреляция Пирсона между рангами двух переменных, принимая значения от -1 до $+1$), — восстановление полных векторов избыточно. Для решения задачи достаточно восстановить итоговые ранги пар слов.

4. Первый подход: метод Кемени и алгоритм Коупленда

Переход от ординальной матрицы непосредственно к рангам можно осуществить методами теории социального выбора. Оптимальным подходом к поиску консенсусного ранжирования по турнирному графу является метод Кемени (Kemeny-Young method) [12]. Задача Кемени состоит в поиске линейного порядка, минимизирующего число инверсий относительно рёбер турнирного графа (расстояние Кендалла).

К сожалению, задача Кемени является NP-трудной [9]. В качестве практической эвристики используется алгоритм Коупленда (Copeland's method) [13], который ранжирует вершины турнирного графа по числу попарных побед (исходящих рёбер).

Теорема 1 (Эквивалентность Кемени и Коупленда без циклов). *Если в турнирном графе отсутствуют циклы (граф является транзитивным турниром), то ранги, полученные по алгоритму Коупленда, в точности совпадают с оптимальными рангами по Кемени, и оба метода эквивалентны топологической сортировке графа.*

Доказательство. Пусть турнирный граф G на n вершинах не содержит циклов. Тогда G является транзитивным турниром: для любых трёх вершин u, v, w , если $u \succ v$ и $v \succ w$, то $u \succ w$.

В транзитивном турнире существует единственная топологическая сортировка $\sigma = (v_1, v_2, \dots, v_n)$, такая что $v_i \succ v_j$ для всех $i < j$.

Коупленд даёт σ : Вершина v_k побеждает ровно $n - k$ вершин (все v_j с $j > k$). Следовательно, число побед строго убывает: $n - 1, n - 2, \dots, 0$. Сортировка по числу побед однозначно даёт порядок σ .

Кемени даёт σ : Порядок σ согласован со всеми $\binom{n}{2}$ рёбрами графа (ни одно ребро не направлено “против” σ), поэтому число инверсий равно нулю. Это глобальный минимум расстояния Кендалла, так как число инверсий неотрицательно. Любой другой порядок $\pi \neq \sigma$ имеет хотя бы одну инверсию (хотя бы одно ребро направлено против π , поскольку σ — единственный порядок, согласованный со всеми рёбрами транзитивного турнира).

Таким образом, оба метода дают один и тот же результат — топологическую сортировку σ . \square

Из леммы 1 и теоремы 1 следует, что для индивидуальной ординальной матрицы (одной модели) алгоритм Коупленда всегда даёт оптимальное решение задачи Кемени. Для агрегированной матрицы, где циклы возможны, алгоритм Коупленда является лишь эвристикой для задачи Кемени и не гарантирует нахождения глобального оптимума, однако на практике демонстрирует высокую эффективность и вычислительную простоту ($O(N^2)$ для графа из N вершин).

5. Второй подход: метод Борда

Альтернативным подходом является метод Борда (Borda count) [14]. В отличие от Кемени и Коупленда, метод Борда работает непосредственно с рангами (позициями элементов в индивидуальных линейных порядках), а не со знаками попарных сравнений. Ординальная матрица для этого метода не строится. Каждой паре слов присваиваются баллы в зависимости от её позиции в ранжировании каждой модели: элемент на позиции k из n получает $n - k$ баллов, после чего баллы суммируются по

всем моделям. Итоговые ранги определяются сортировкой элементов по убыванию суммы баллов: элемент с наибольшей суммой получает ранг 1, следующий — ранг 2, и так далее.

Хотя метод Борда вычислительно эффективнее ($O(N \log N)$), его результаты могут отличаться от Кемени/Коупленда. В таблице 3 приведён пример, демонстрирующий это различие на четырёх элементах $\{A, B, C, D\}$.

Таблица 3: Пример различия методов Борда и Кемени/Коупленда

Модель	1-е (3 б.)	2-е (2 б.)	3-е (1 б.)	4-е (0 б.)
Модель 1	<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>
Модель 2	<i>D</i>	<i>C</i>	<i>A</i>	<i>B</i>
Модель 3	<i>D</i>	<i>A</i>	<i>B</i>	<i>C</i>
Суммы Борда: $A = 6, D = 6, B = 3, C = 3$				
Результат Борда: ничья $A \sim D$, ничья $B \sim C$				
Попарные победы: $D \succ A$ (2:1), $A \succ B$ (3:0), $D \succ B$ (2:1)				
Результат Кемени/Коупленда: $D \succ A \succ B \succ C$ (однозначно)				

Как видно из примера, два элемента (*A* и *D*) имеют одинаковую сумму баллов Борда (одинаковые средние позиции), однако в прямом попарном сравнении *D* побеждает *A* большинством голосов (2:1). Метод Борда оперирует только абсолютными позициями элементов в ранжированиях и не учитывает результаты прямых попарных сравнений, тогда как Кемени/Коупленд использует именно эту информацию для однозначного разрешения ничьих.

6. Описание моделей и датасетов

В экспериментах использовались 10 предобученных моделей, охватывающих различные подходы к получению векторных представлений:

1. **ConceptNet Numberbatch (CN)** [1] — векторы, основанные на графе знаний ConceptNet, обогащённые семантическими отношениями. Размерность: 300.
2. **Paragram-SL999 (PG)** [5] — векторы, дообученные с использованием лингвистических ограничений для улучшения различения синонимов и антонимов. Размерность: 300.
3. **OpenAI text-embedding-3-large (3L)** [7] — современная LLM-модель эмбедингов большой размерности (3072), извлекающая глубокий контекст.

4. **OpenAI text-embedding-3-small (3s)** [7] — компактная LLM-модель (1536 размерностей) нового поколения.
5. **OpenAI text-embedding-ada-002 (ada)** [7] — модель эмбедингов предыдущего поколения (1536 размерностей).
6. **Sentence-BERT (SBERT)** [6] — модель на основе архитектуры BERT, дообученная для получения семантически значимых представлений предложений. Размерность: 768.
7. **GloVe-300** [2] — классические векторы, полученные факторизацией матрицы глобальной совместной встречаемости слов. Размерность: 300.
8. **fastText** [4] — векторы, учитывающие морфологию через n-граммы подслов (subwords). Размерность: 300.
9. **Word2Vec** [3] — классические векторы, обученные с использованием архитектуры Skip-gram. Размерность: 300.
10. **SimCSE (sup-simcse-bert-base-uncased)** [8] — модель контрастивного обучения на основе BERT, дообученная на парах естественного языкового вывода (NLI) для получения семантически значимых представлений предложений. Размерность: 768.

Оценка качества проводилась на трёх стандартных датасетах:

- **WordSim-353 (WS353)** [15]: состоит из 353 пар слов. Оценивает общую ассоциативную и семантическую близость, не делая строгого различия между ними (например, пара “кофе” и “чашка” может иметь высокую оценку).
- **MEN** [16]: содержит 3000 пар слов. Оценивает визуальную и семантическую ассоциативность, полученную на основе суждений людей по изображениям и текстам.
- **SimLex-999** [17]: состоит из 999 пар слов. Строго оценивает именно семантическое сходство, отличая синонимы от связанных ассоциативно слов (например, “кофе” и “чашка” получают низкую оценку, а “кофе” и “чай” — более высокую). В датасет включены только пары с совпадающей частью речи.

7. Результаты индивидуальных моделей

В таблице 4 представлены результаты индивидуальных моделей (корреляция Спирмена ρ). Первые и вторые максимумы в каждом столбце выделены полужирным и подчёркиванием соответственно.

Таблица 4: Корреляция Спирмена для индивидуальных моделей

Модель	WS353	MEN	SimLex	Среднее
ConceptNet	0.815	0.871	0.627	0.771
Paragram	0.720	0.778	<u>0.685</u>	<u>0.728</u>
SimCSE	0.642	0.798	0.693	0.711
3L	0.733	0.793	0.566	0.698
SBERT	<u>0.744</u>	0.788	0.536	0.689
fastText	0.697	<u>0.803</u>	0.441	0.647
Word2Vec*	0.694	0.782	0.442	0.639
3s	0.650	0.754	0.502	0.635
ada	0.649	0.737	0.439	0.608
GloVe-300	0.609	0.749	0.370	0.576

ConceptNet демонстрирует лучшие результаты на WS353 и MEN, тогда как SimCSE лидирует на строго семантическом SimLex (0.693), опережая Paragram (0.685). Это объясняется тем, что контрастивное обучение SimCSE эффективно различает семантически близкие и далёкие пары. Индивидуальные результаты Word2Vec получены на усечённом наборе пар слов (в модели отсутствуют векторные представления для 5 слов). Это различие в составе оцениваемых пар слов незначительно влияет на абсолютные значения корреляций и не затрагивает результаты ансамблей (в состав рассматриваемых ансамблей Word2Vec не входит).

8. Поиск комбинаций методом Борда

Используя метод Борда, был проведён перебор комбинаций из 3, 4 и 5 моделей для поиска ансамблей, максимизирующих среднюю корреляцию на трёх датасетах. Для сравнения приведены результаты трёх лучших индивидуальных моделей (ConceptNet, Paragram и SimCSE). Все 10 исследованных ансамблей представлены в таблице 5.

Анализ результатов показывает, что комбинирование моделей позволяет превзойти лучшую индивидуальную модель (ConceptNet, 0.771) на ~ 0.032 в среднем. Особо стоит отметить синергетический эффект на датасете SimLex: тройка CN + PG + SimCSE достигает 0.722, что превышает лучшую индивидуальную модель SimCSE (0.693) на +0.029. Этот ансамбль превосходит лучшую индивидуальную модель на SimLex, что демонстрирует силу ординальной агрегации для строго семантических задач. Ключевую роль играет включение SimCSE: все четыре лучших

Таблица 5: Комбинации моделей (агрегация Борда)

Конфигурация	WS353	MEN	SimLex	Среднее
ConceptNet (индивид.)	0.815	0.871	0.627	0.771
Paragram (индивид.)	0.720	0.778	0.685	0.728
SimCSE (индивид.)	0.642	0.798	0.693	0.711
CN + PG + 3L + SimCSE	0.819	0.881	0.709	0.803
CN+SBERT+PG+3L+SimCSE	0.827	<u>0.881</u>	0.696	<u>0.801</u>
CN + PG + SimCSE	0.801	0.877	0.722	0.800
CN + PG + SimCSE + SBERT	0.819	0.878	0.705	0.800
PG + SimCSE + SBERT	0.794	0.863	<u>0.715</u>	0.791
CN + SBERT + PG + 3L	0.837	0.867	0.665	0.790
CN + PG + 3L	0.828	0.864	0.675	0.789
CN + SBERT + PG	<u>0.829</u>	0.860	0.669	0.786
CN + 3s + PG	0.810	0.861	0.669	0.780
CN + PG + ada	0.818	0.857	0.646	0.774

ансамбля по среднему содержат эту модель, что подтверждает ценность контрастного сигнала для ординальной агрегации.

9. Поиск комбинаций алгоритмом Коупленда

Аналогичный перебор комбинаций был выполнен с использованием алгоритма Коупленда для агрегации. В таблице 6 представлены все 10 комбинаций моделей. Для сравнения также приведены результаты трёх лучших индивидуальных моделей.

Результаты Коупленда демонстрируют аналогичные закономерности: четвёрка CN + PG + 3L + SimCSE лидирует по среднему (0.803), а лучший результат на SimLex делят тройки CN + PG + SimCSE и PG + SimCSE + SBERT (0.713). Алгоритм Коупленда стабильно показывает несколько более высокие результаты на ассоциативных датасетах (WS353, MEN), тогда как на строго семантическом SimLex метод Борда оказывается более устойчивым.

10. Сравнение метода Борда и алгоритма Коупленда

Для трёх лучших конфигураций (по среднему Борда) было проведено прямое сравнение метода Борда и алгоритма Коупленда (как эвристики

Таблица 6: Комбинации моделей (агрегация Коупленда)

Конфигурация	WS353	MEN	SimLex	Среднее
ConceptNet (индивид.)	0.815	0.871	0.627	0.771
Paragram (индивид.)	0.720	0.778	0.685	0.728
SimCSE (индивид.)	0.642	0.798	0.693	0.711
CN + PG + 3L + SimCSE	0.822	0.883	0.704	0.803
CN + PG + SimCSE	0.809	0.879	0.713	<u>0.800</u>
CN + PG + SimCSE + SBERT	0.822	0.880	0.700	<u>0.800</u>
CN+SBERT+PG+3L+SimCSE	0.829	<u>0.882</u>	0.689	<u>0.800</u>
CN + PG + 3L	<u>0.834</u>	0.870	0.670	0.791
CN + SBERT + PG + 3L	0.838	0.871	0.662	0.790
PG + SimCSE + SBERT	0.792	0.861	<u>0.713</u>	0.789
CN + SBERT + PG	0.830	0.867	0.663	0.786
CN + 3s + PG	0.819	0.866	0.670	0.785
CN + PG + ada	0.826	0.865	0.652	0.781

для Кемени). Результаты приведены в таблице 7. В столбце $\Delta\rho$ указано абсолютное различие, а также процентное различие относительно метода Борда.

Таблица 7: Сравнение метода Борда и алгоритма Коупленда (ρ Спирмена)

Конфигурация	Датасет	Борда	Коупленд	$\Delta\rho$ (%)
CN+PG+3L+SimCSE	WS353	0.819	0.822	+0.003 (+0.4%)
	MEN	0.881	0.883	+0.002 (+0.2%)
	SimLex	0.709	0.704	-0.005 (-0.7%)
CN+SBERT+PG+3L+SimCSE	WS353	0.827	0.829	+0.002 (+0.2%)
	MEN	0.881	0.882	+0.001 (+0.1%)
	SimLex	0.696	0.689	-0.007 (-1.0%)
CN+PG+SimCSE	WS353	0.801	0.809	+0.008 (+1.0%)
	MEN	0.877	0.879	+0.002 (+0.2%)
	SimLex	0.722	0.713	-0.009 (-1.2%)

Результаты показывают, что методы дают близкие, но не идентичные результаты. Доля инверсий между итоговыми ранжированиями — то есть доля пар элементов (p_i, p_j) , для которых порядок в методе Борда противоположен порядку в алгоритме Коупленда — составляет 2–4%. Эта величина непосредственно связана с расстоянием Кендалла τ между двумя ранжированиями: доля инверсий равна $(1 - \tau)/2$, где τ — коэффициент ранговой корреляции Кендалла между результатами двух методов.

Таким образом, 2–4% инверсий соответствуют корреляции Кендалла $\tau \approx 0.92$ – 0.96 между ранжированиями Борда и Коупленда.

Алгоритм Коупленда стабильно показывает лучшие результаты на ассоциативных датасетах (WS353, MEN), так как он лучше разрешает ничьи через попарное большинство. Метод Борда оказывается более устойчивым на строго семантическом SimLex. В целом, разница между методами невелика ($\Delta\rho \leq 0.009$, или $\leq 1.2\%$), что оправдывает использование вычислительно более простого метода Борда на практике.

11. Обсуждение: стратегия вето большинством

В рассматриваемых ансамблях присутствует неявная стратегия *вето большинством*: если одна модель даёт аномальный результат для некоторой пары слов (например, размещает её на последнем месте, тогда как остальные — на первых), большинство моделей эффективно нейтрализует эту ошибку. Эта стратегия работает в обоих методах, но с разной механикой.

В **методе Борда** вето реализуется через усреднение рангов. Если в тройке моделей одна присваивает паре слов ранг N (последнее место), а две другие — ранги, близкие к 1, то сумма Борда будет определяться преимущественно двумя согласными моделями, и пара окажется в верхней части итогового ранжирования. Однако влияние аномальной модели полностью не устраняется: её вклад в сумму смещает итоговый ранг вниз, хотя и не критически.

В **алгоритме Коупленда** вето работает более жёстко. В попарном сравнении двух пар слов решение принимается большинством голосов (например, 2:1 в тройке). Аномальный голос одной модели полностью игнорируется: независимо от того, насколько сильно одна модель отклоняется от консенсуса, результат попарного сравнения определяется только знаками предпочтений большинства, а не величинами отклонений. Это делает Коупленда более устойчивым к выбросам, но одновременно он теряет информацию о *степени* предпочтения, которую сохраняет метод Борда через суммы рангов.

Стратегия вето объясняет, почему ансамбли стабильно превосходят индивидуальные модели: ошибки отдельных моделей, как правило, некоррелированы (разные модели ошибаются на разных парах слов), и большинство ветирует каждую такую ошибку.

12. Обсуждение: переход от векторов слов к векторам текстов

Интересным наблюдением является то, что модели, оптимизированные для векторизации целых текстов и предложений (SBERT, OpenAI text-embedding-3), показывают посредственные результаты на уровне отдельных слов (особенно на SimLex) по сравнению со специализированными моделями (ConceptNet, Paragram). Исключением является SimCSE, которая, благодаря контрастивному обучению, достигает лучшего индивидуального результата на SimLex (0.693), несмотря на скромные показатели на WS353 (0.642). Тем не менее включение контекстных моделей в ансамбли (например, CN+PG+3L+SimCSE) стабильно повышает итоговое качество. Это свидетельствует о том, что LLM-эмбединги и модели контрастивного обучения содержат уникальный сигнал, который ординальные методы успешно комбинируют с графовой семантикой.

Переход от векторов отдельных слов к векторам целых текстов является логичным продолжением развития методов агрегации. Хотя данное исследование фокусируется на парах слов, предложенные ординальные подходы (Борда и Коупленд) математически не зависят от природы объектов. Они могут быть напрямую применены для агрегации оценок семантической близости целых предложений или документов, что особенно актуально для задач информационного поиска (Information Retrieval) и систем RAG (Retrieval-Augmented Generation), где объединение ранжирований от разных моделей поиска является стандартной практикой.

13. Обсуждение: от слияния векторов к слиянию моделей

Переход к ординальным методам (Борда, Кемени) открывает путь от задачи простого математического выравнивания векторных пространств к задаче ансамблирования моделей (model fusion). Вместо того чтобы пытаться найти единое пространство, модели используются как независимые “эксперты”, голосующие за семантическую близость понятий. Этот подход не требует доступа к весам моделей или обучающим данным, не подвержен проблеме локальных минимумов (как GNMDS) и легко масштабируется на любое количество новых моделей (LLM), позволяя извлекать синергетический эффект из их различных архитектур.

Важным направлением развития является слияние моделей с целью получения единых функций расстояния, применимых для получения оценок векторных представлений для новых объектов, в частности, тек-

стов. Данная задача тесно связана с областью обучения метрик (metric learning), где целью является построение функции расстояния, сохраняющей заданные ординальные ограничения на новых данных. Если ординальная агрегация на фиксированном наборе данных позволяет найти оптимальный консенсусный порядок, то обучение мета-модели (например, нейронной сети), предсказывающей этот консенсусный порядок для новых пар текстов на основе их исходных представлений, позволит обобщить результаты агрегации. Это превращает ординальные методы из инструмента оценки в инструмент создания новых, более сильных гибридных моделей векторных представлений — фактически реализуя подход metric learning на основе ансамблевых ординальных ограничений.

14. Заключение

В данной работе исследовано применение ординальных методов для агрегации наборов векторных представлений слов. Доказано, что отсутствие циклов в индивидуальных ординальных матрицах (Лемма 1) гарантирует эквивалентность алгоритмов Кемени и Коупленда (Теорема 1), что обосновывает использование вычислительно эффективного алгоритма Коупленда в качестве точного решения задачи Кемени для индивидуальных моделей и в качестве эвристики для агрегированных данных. Экспериментальное сравнение на 10 моделях и 3 датасетах продемонстрировало, что ординальные подходы (Борда и Коупленд) позволяют находить ансамбли, превосходящие лучшие индивидуальные модели. При этом разница в качестве между вычислительно простым методом Борда и более сложным алгоритмом Коупленда минимальна (не более 1.2% по корреляции Спирмена), что делает метод Борда предпочтительным выбором для практических задач. Предложенный подход открывает перспективы для ансамблирования моделей текстовых эмбеддингов без необходимости их дорогостоящего дообучения. После получения агрегированных рангов векторные представления, согласованные с консенсусным порядком, могут быть восстановлены с помощью алгоритма GNMDS [11], который минимизирует нарушения ординальных ограничений при построении евклидова вложения. Таким образом, полный конвейер включает два этапа: (а) ординальная агрегация методом Борда или алгоритмом Коупленда для получения консенсусных рангов и (б) восстановление векторных представлений алгоритмом GNMDS [11] для использования в последующих задачах.

Финансирование

Работа выполнена в рамках государственного задания МГУ имени М. В. Ломоносова «Инженерия знаний. Разработка цифровой платформы и онтологической системы фундаментальных знаний на русском языке» (№ 124020100068-4).

Список литературы

- [1] R. Speer, J. Chin, C. Havasi, “ConceptNet 5.5: An Open Multilingual Graph of General Knowledge”, *Proceedings of the 31st AAAI Conference on Artificial Intelligence*, 2017, 4444–4451. DOI: 10.1609/aaai.v31i1.11164.
- [2] J. Pennington, R. Socher, C. D. Manning, “GloVe: Global Vectors for Word Representation”, *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, 2014, 1532–1543. DOI: 10.3115/v1/D14-1162.
- [3] T. Mikolov, I. Sutskever, K. Chen, G. S. Corrado, J. Dean, “Distributed Representations of Words and Phrases and their Compositionality”, *Advances in Neural Information Processing Systems 26 (NeurIPS)*, 2013, 3111–3119. DOI: 10.48550/arXiv.1310.4546.
- [4] P. Bojanowski, E. Grave, A. Joulin, T. Mikolov, “Enriching Word Vectors with Subword Information”, *Transactions of the Association for Computational Linguistics*, **5** (2017), 135–146. DOI: 10.1162/tac1_a_00051.
- [5] J. Wieting, M. Bansal, K. Gimpel, K. Livescu, “From Paraphrase Database to Compositional Paraphrase Model and Back”, *Transactions of the Association for Computational Linguistics*, **3** (2015), 345–358. DOI: 10.1162/tac1_a_00143.
- [6] N. Reimers, I. Gurevych, “Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks”, *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, 2019, 3982–3992. DOI: 10.18653/v1/D19-1410.
- [7] A. Neelakantan, T. Xu, R. Puri, A. Radford, J. M. Han, J. Tworek, Q. Yuan, N. Tezak, J. W. Kim, C. Hallacy, J. Heidecke, P. Shyam, B. Power, T. E. Niekoul, G. Sastry, G. Krueger, D. Schnurr, F. P. Such, K. Hsu, M. Thompson, T. Khan, T. Sherbakov, J. Jang, P. Welinder, L. Weng, “Text and Code Embeddings by Contrastive Pre-Training”, *arXiv preprint arXiv:2201.10005*, 2022. DOI: 10.48550/arXiv.2201.10005.
- [8] T. Gao, X. Yao, D. Chen, “SimCSE: Simple Contrastive Learning of Sentence Embeddings”, *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, 2021, 6894–6910. DOI: 10.18653/v1/2021.emnlp-main.552.
- [9] J. J. Bartholdi, C. A. Tovey, M. A. Trick, “Voting schemes for which it can be difficult to tell who won the election”, *Social Choice and Welfare*, **6:2** (1989), 157–165. DOI: 10.1007/BF00303169.
- [10] S. Agarwal, J. Wills, L. Cayton, G. Lanckriet, D. Kriegman, S. Belongie, “Generalized Non-metric Multidimensional Scaling”, *Proceedings of the Eleventh International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2007, 11–18.

- [11] А. М. Колосов, А. И. Майсурадзе, “Улучшение качества векторных представлений слов за счёт использования нескольких источников представлений”, *Интеллектуальные системы. Теория и приложения*, **30**:1 (2026), 87–100.
- [12] J. G. Kemeny, “Mathematics without numbers”, *Daedalus*, **88**:4 (1959), 577–591.
- [13] A. H. Copeland, “A “reasonable” social welfare function”, *Seminar on Applications of Mathematics to Social Sciences, University of Michigan*, 1951.
- [14] J.-C. Borda, “Mémoire sur les élections au scrutin”, *Histoire de l’Académie Royale des Sciences*, 1781, 657–665.
- [15] L. Finkelstein, E. Gabrilovich, Y. Matias, E. Rivlin, Z. Sasson, G. Wolfman, E. Ruppin, “Placing Search in Context: The Concept Revisited”, *Proceedings of the 10th International Conference on World Wide Web*, 2001, 406–414. DOI: 10.1145/371920.372094.
- [16] E. Bruni, N.-K. Tran, M. Baroni, “Multimodal Distributional Semantics”, *Journal of Artificial Intelligence Research*, **49** (2014), 1–47. DOI: 10.1613/jair.4135.
- [17] F. Hill, R. Reichart, A. Korhonen, “SimLex-999: Evaluating Semantic Models with (Genuine) Similarity Estimation”, *Computational Linguistics*, **41**:4 (2015), 665–695. DOI: 10.1162/COLI_a_00237.

Статья поступила 15 мая 2026 г.

Ordinal Aggregation of Word Embedding Sets

A. M. Kolosov

This paper investigates the problem of merging word embedding sets from various pre-trained models. Since direct vector space alignment faces computational challenges and local minima issues, it is proposed to transition to ordinal aggregation methods. The absence of cycles in individual ordinal matrices of pairwise distance comparisons is proven, which guarantees the equivalence of the Kemeny and Copeland algorithms in this case. For aggregated matrices where the Condorcet paradox is possible, Copeland’s algorithm serves as an efficient heuristic. The Borda count method, which does not require building tournament graphs, is also considered. Experiments were conducted on 10 models and 3 datasets (WordSim-353, MEN, SimLex-999). It is shown that ordinal methods can identify optimal model combinations (triples, quads, and quints) that outperform individual models in Spearman correlation, with minimal difference between the Borda and Kemeny/Copeland methods.

Keywords: word embeddings, model aggregation, Borda count, Kemeny rule, Copeland algorithm, tournament graphs, ordinal matrix.

References

- [1] R. Speer, J. Chin, C. Havasi, “ConceptNet 5.5: An Open Multilingual Graph of General Knowledge”, *Proceedings of the 31st AAAI Conference on Artificial Intelligence*, 2017, 4444–4451. DOI: 10.1609/aaai.v31i1.11164.
- [2] J. Pennington, R. Socher, C. D. Manning, “GloVe: Global Vectors for Word Representation”, *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, 2014, 1532–1543. DOI: 10.3115/v1/D14-1162.
- [3] T. Mikolov, I. Sutskever, K. Chen, G. S. Corrado, J. Dean, “Distributed Representations of Words and Phrases and their Compositionality”, *Advances in Neural Information Processing Systems 26 (NeurIPS)*, 2013, 3111–3119. DOI: 10.48550/arXiv.1310.4546.
- [4] P. Bojanowski, E. Grave, A. Joulin, T. Mikolov, “Enriching Word Vectors with Subword Information”, *Transactions of the Association for Computational Linguistics*, **5** (2017), 135–146. DOI: 10.1162/tac1_a_00051.
- [5] J. Wieting, M. Bansal, K. Gimpel, K. Livescu, “From Paraphrase Database to Compositional Paraphrase Model and Back”, *Transactions of the Association for Computational Linguistics*, **3** (2015), 345–358. DOI: 10.1162/tac1_a_00143.
- [6] N. Reimers, I. Gurevych, “Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks”, *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, 2019, 3982–3992. DOI: 10.18653/v1/D19-1410.
- [7] A. Neelakantan, T. Xu, R. Puri, A. Radford, J. M. Han, J. Tworek, Q. Yuan, N. Tezak, J. W. Kim, C. Hallacy, J. Heidecke, P. Shyam, B. Power, T. E. Nekoul, G. Sastry, G. Krueger, D. Schnurr, F. P. Such, K. Hsu, M. Thompson, T. Khan, T. Sherbakov, J. Jang, P. Welinder, L. Weng, “Text and Code Embeddings by Contrastive Pre-Training”, *arXiv preprint arXiv:2201.10005*, 2022. DOI: 10.48550/arXiv.2201.10005.
- [8] T. Gao, X. Yao, D. Chen, “SimCSE: Simple Contrastive Learning of Sentence Embeddings”, *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, 2021, 6894–6910. DOI: 10.18653/v1/2021.emnlp-main.552.
- [9] J. J. Bartholdi, C. A. Tovey, M. A. Trick, “Voting schemes for which it can be difficult to tell who won the election”, *Social Choice and Welfare*, **6:2** (1989), 157–165. DOI: 10.1007/BF00303169.
- [10] S. Agarwal, J. Wills, L. Cayton, G. Lanckriet, D. Kriegman, S. Belongie, “Generalized Non-metric Multidimensional Scaling”, *Proceedings of the Eleventh International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2007, 11–18.

-
- [11] A. M. Kolosov, A. I. Maysuradze, “Improving the quality of vector representations of words by using several sources of representations”, *Intelligent Systems: Theory and Applications*, **30**:1 (2026), 87–100.
- [12] J. G. Kemeny, “Mathematics without numbers”, *Daedalus*, **88**:4 (1959), 577–591.
- [13] A. H. Copeland, “A “reasonable” social welfare function”, *Seminar on Applications of Mathematics to Social Sciences, University of Michigan*, 1951.
- [14] J.-C. Borda, “Mémoire sur les élections au scrutin”, *Histoire de l’Académie Royale des Sciences*, 1781, 657–665.
- [15] L. Finkelstein, E. Gabrilovich, Y. Matias, E. Rivlin, Z. Sasson, G. Wolfman, E. Ruppin, “Placing Search in Context: The Concept Revisited”, *Proceedings of the 10th International Conference on World Wide Web*, 2001, 406–414. DOI: 10.1145/371920.372094.
- [16] E. Bruni, N.-K. Tran, M. Baroni, “Multimodal Distributional Semantics”, *Journal of Artificial Intelligence Research*, **40** (2014), 1–47. DOI: 10.1613/jair.4135.
- [17] F. Hill, R. Reichart, A. Korhonen, “SimLex-999: Evaluating Semantic Models with (Genuine) Similarity Estimation”, *Computational Linguistics*, **41**:4 (2015), 665–695. DOI: 10.1162/COLI_a_00237.

Received on May 15, 2026

Часть 2
Специальные вопросы теории
интеллектуальных систем

О вычислительной сложности задачи существования предельных циклов в булевых сетях с ограничениями из решётки Поста

А. С. Дробышев*

В статье исследуется вычислительная сложность задачи существования предельных циклов фиксированной длины k в булевых сетях с локальными функциями, ограниченными классами из решётки Поста. Доказано, что задача является NP-полной для выразительных классов D_2 (монотонные самодвойственные функции), F_6^∞ и F_2^∞ , а для класса линейных функций L_1 полиномиально разрешима. Получены явные полиномиальные редукции из задачи 3-SAT с сохранением предельных циклов длины k .

Ключевые слова: булевы сети, предельные циклы, решётка Поста, вычислительная сложность, NP-полнота.

1. Введение

Булевой сетью называется дискретная динамическая система, в которой элементы, содержащие булевы функции, взаимодействуют между собой на дискретных временных шагах. Такая сеть может быть описана в виде набора булевых функций, каждая из которых определяет дискретную временную эволюцию отдельного элемента. Булеву сеть обычно представляют ориентированным графом взаимодействия. Поскольку булева сеть состоит из конечного числа элементов, общее число возможных конфигураций конечно. Следовательно, траектория любой начальной конфигурации рано или поздно попадает либо в предельный цикл, либо в неподвижную точку. Существенным аспектом булевых сетей является схема обновления, определяющая порядок обновления вершин графа взаимодействия. Основными типами схем обновления являются параллельная, последовательная, блочно-параллельная и блочно-последовательная,

* *Дробышев Александр Сергеевич* — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: drobyshev.sanya@yandex.ru, ORCID: 0009-0002-8881-8730.

Drobyshev Alexander Sergeevich — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intelligent Systems.

каждая из которых существенно влияет на динамическую траекторию системы.

Исторически булевы модели дискретной динамики восходят к логическим моделям нейронной активности Маккаллока и Питтса [4] и к моделям нейронных сетей Хопфилда [16]. В дальнейшем близкие дискретные модели активно использовались для описания генетических регуляторных сетей: ранние работы Кауффмана и Томаса показали, что булевы представления позволяют изучать устойчивые состояния и периодическое поведение биологических регуляторных систем [11–13]. Современные работы также используют дискретные и логические модели для анализа осцилляций в регуляторных сетях и молекулярных часах [9, 10].

Исследования булевых сетей можно классифицировать на два направления. Первое направление изучает структурные и алгебраические свойства динамики и графов взаимодействия. Сюда относятся результаты о влиянии структуры графа на существование и длины предельных циклов [5, 6], о поведении нейронных и хопфилдовских сетей с несколькими устойчивыми состояниями или предельными циклами [7, 8], а также работы, связывающие неподвижные точки булевых сетей с редукциями, графовой энтропией, задачами угадывания и сетевым кодированием [3, 14, 15].

Второе направление связано с вычислительной сложностью задач, возникающих при анализе динамики булевых сетей. Уже для произвольных булевых сетей задача обнаружения предельного цикла заданной длины оказывается вычислительно трудной: в работе [1] показано, что для любого фиксированного $k \geq 2$ соответствующая задача является NP-полной при основных схемах обновления, включая параллельную, последовательную и блочно-последовательную.

В работе [2] рассматривается подкласс булевых сетей — конъюнктивные сети, где каждая локальная функция определяется конъюнкцией над подмножеством компонентов сети, связанных с её вершиной. В частности, для конъюнктивных булевых сетей с параллельной схемой обновления установлена NP-полнота задачи существования предельного цикла длины k в случае, когда k является входным параметром. Вопрос о вычислительной сложности этой задачи при фиксированном k в указанной работе оставлен открытым. Кроме того, показано, что композиция конъюнктивных функций, являющаяся центральной операцией при анализе многошаговой эволюции сети, вычисляется за полиномиальное время. Этот результат позволяет свести анализ итераций конъюнктивной сети к задаче достижимости в графе взаимодействия.

В настоящей работе рассматривается задача существования предельного цикла заданной длины k при параллельной схеме обновления. Для

фиксированного класса булевых функций \mathcal{F} мы обозначаем эту задачу через $k\text{-PLCE}(\mathcal{F})$: на вход подаётся булева сеть, все локальные функции которой принадлежат замыканию класса \mathcal{F} , и требуется определить, существует ли в этой сети предельный цикл длины ровно k . Цель данной статьи — исследовать сложность задачи $k\text{-PLCE}(\mathcal{F})$ для классов булевых функций из решётки Поста. Основное внимание уделяется случаю фиксированного $k \geq 2$. Для $k = 1$ задача сводится к задаче существования неподвижной точки, которая изучалась ранее. Основные результаты работы состоят в следующем. Для фиксированного $k \geq 2$ доказана NP-полнота задачи $k\text{-PLCE}(\mathcal{F})$ для классов D_2 , F_6^∞ и F_2^∞ . Кроме того, показано, что для класса линейных функций L_1 задача решается за полиномиальное время. В совокупности с монотонностью задачи по включению классов функций эти результаты дают частичную классификацию сложности по решётке Поста. Открытыми остаются случаи конъюнктивных и дизъюнктивных классов.

Статья организована следующим образом. В разделе 2 вводятся основные определения: булевы сети, схемы обновления, предельные циклы и задача $k\text{-PLCE}$. Раздел 3 посвящён ранее известным результатам. В разделе 4 формулируются основные результаты. В разделе 5 приводятся доказательства NP-полноты и полиномиальный алгоритм для линейного случая. В заключении обсуждаются оставшиеся открытые случаи.

2. Определения

Обозначим $[n] = \{1, \dots, n\}$. Рассмотрим n булевых функций f_1, \dots, f_n , где $f_i : \{0, 1\}^n \rightarrow \{0, 1\}$.

Определение. *Булевой сетью* будем называть систему булевых функций f_1, \dots, f_n , определяемую отображением

$$f : \{0, 1\}^n \rightarrow \{0, 1\}^n,$$

где $f = (f_1, \dots, f_n)$.

Чтобы связать функциональное описание сети с её структурой, уточним понятие графа взаимодействия по аналогии с работой [1].

Определение. *Ориентированным графом взаимодействия* булевой сети f называется граф

$$G_f = (V, A),$$

где $V = [n]$, а

$$(i, j) \in A \iff \text{функция } f_j \text{ существенно зависит от переменной } x_i.$$

Далее нам понадобится язык для описания состояний системы и их эволюции.

Определение. *Пространством конфигураций* будем называть множество $\{0, 1\}^n$.

Пусть f — булева сеть, $x \in \{0, 1\}^n$ — конфигурация, $I \subseteq [n]$. *Частичным обновлением по множеству I* будем называть отображение $f^{(I)}$, заданное равенствами

$$f^{(I)}(x)_i = \begin{cases} f_i(x), & \text{если } i \in I, \\ x_i, & \text{если } i \notin I. \end{cases}$$

Теперь зафиксируем общий шаблон обновления блоками, который объединяет параллельный и последовательный случаи.

Определение. Пусть $W = (W_1, \dots, W_t)$ — упорядоченное разбиение множества $[n]$. *Булевой сетью с обновлением по схеме W* будем называть динамическую систему, реализующую отображение

$$f^{(W)} = f^{(W_t)} \circ \dots \circ f^{(W_2)} \circ f^{(W_1)}.$$

Если $W = ([n])$, то получаем синхронную (параллельную) схему обновления.

Имея механизм эволюции, перейдём к базовым аттракторам — неподвижным точкам и циклам.

Определение. Конфигурация $x \in \{0, 1\}^n$ называется *неподвижной точкой*, если

$$f^{(W)}(x) = x.$$

Определение. Конфигурация $x \in \{0, 1\}^n$ принадлежит *предельному циклу длины k* , если

$$(f^{(W)})^k(x) = x,$$

и для любого $l \in \{1, \dots, k-1\}$ выполняется

$$(f^{(W)})^l(x) \neq x.$$

Для удобства изложения введём обозначение для множества всех конфигураций, принадлежащих предельным циклам длины ровно k , то есть таких конфигураций, которые возвращаются в исходное состояние после k применений отображения $f^{(W)}$, но не возвращаются к нему после меньшего числа шагов.

Определение. Положим

$$\Phi_k(f^{(W)}) = \left\{ x \in \{0, 1\}^n \mid (f^{(W)})^k(x) = x \text{ и} \right. \\ \left. \forall l \in \{1, \dots, k-1\}, (f^{(W)})^l(x) \neq x \right\}. \quad (1)$$

Определим

$$\phi_k(f^{(W)}) = \frac{|\Phi_k(f^{(W)})|}{k},$$

то есть $\phi_k(f^{(W)})$ равно числу предельных циклов длины k .

Переходим к постановке основной вычислительной задачи и фиксации классов функций, на которых она исследуется.

Определение. Пусть \mathcal{F} — множество булевых функций. *Замыканием* множества \mathcal{F} относительно операций суперпозиции и введения фиктивных переменных будем называть множество $[\mathcal{F}]$.

Задача k-PLCE(\mathcal{F}). Существование предельного цикла в булевой сети с параллельной схемой обновления для \mathcal{F} , где $k \geq 1$ — фиксированное натуральное число.

Вход: булева сеть $f = (f_1, \dots, f_n)$ такая, что $f_i \in [\mathcal{F}]$ для всех $i \in [n]$.

Вопрос: верно ли, что $\Phi_k(f) \neq \emptyset$?

В настоящей статье доказываются результаты о вычислительной сложности задачи k-PLCE(\mathcal{F}), где \mathcal{F} — один из классов решётки Поста.

Для доказательства основных результатов используются полиномиальные редукции из задачи 3-выполнимости.

Определение. Пусть ψ — булева формула на переменных $\{x_1, \dots, x_n\}$,

$$v : \{x_1, \dots, x_s\} \rightarrow \{0, 1\}, \quad s \in [n],$$

— частичное присваивание. Через $\psi[v]$ обозначим *результат подстановки* в формулу ψ :

$$\psi[x_1 \leftarrow v(x_1), \dots, x_s \leftarrow v(x_s)].$$

Задача 3-SAT (3-выполнимость).

Вход: формула в 3-КНФ ψ на переменных $\{x_1, \dots, x_n\}$.

Вопрос: существует ли присваивание $v : \{x_1, \dots, x_n\} \rightarrow \{0, 1\}$ такое, что $\psi(v) = 1$?

Определение. Пусть f — булева сеть с множеством вершин $V = [n]$, и пусть $z \in \{0, 1\}^n$ — конфигурация. Для вершины $v \in V$ координата z_v называется *значением вершины v* в конфигурации z . Если

$$z^{(0)}, z^{(1)}, z^{(2)}, \dots$$

— траектория сети, то $z_v^{(t)}$ обозначает значение вершины v в момент времени t .

3. Известные ранее результаты

Задачи о предельных циклах булевых сетей ранее изучались для различных схем обновления и различных ограничений на локальные функции.

В работе [1] доказано, что задача определения того, допускает ли булева сеть предельный цикл длины k , является NP-полной для любого фиксированного k . Этот результат справедлив для основных схем обновления, включая параллельную, последовательную и блочно-последовательную схемы.

Для конъюнктивных булевых сетей близкие результаты получены в работе [2]. В частности, для последовательной и блочно-последовательной схем обновления NP-полнота установлена при $k > 2$, а для параллельной схемы обновления — в случае, когда k является частью входа.

В настоящей работе рассматривается другая постановка: число $k \geq 2$ фиксировано заранее, а локальные функции булевой сети ограничены классами из решётки Поста.

4. Основные результаты

Далее нас будут интересовать булевы сети, локальные функции которых ограничены определёнными классами решётки Поста [18]. Напомним используемые далее обозначения:

- F_6^∞ — класс функций, порождаемых базисом $\{x \cdot (y \vee z)\}$;
- F_2^∞ — класс функций, порождаемых базисом $\{x \vee y \cdot z\}$;
- D_2 — класс всех монотонных самодвойственных функций с базисом $\{x \cdot y \vee y \cdot z \vee x \cdot z\}$;
- L_1 — класс всех линейных функций с базисом $\{1, x \oplus y\}$.

Сначала зафиксируем простое свойство монотонности задачи по классу локальных функций.

Лемма 1. Пусть \mathcal{F}_1 и \mathcal{F}_2 — множества булевых функций, причём $\mathcal{F}_1 \subseteq \mathcal{F}_2$. Тогда $k\text{-PLCE}(\mathcal{F}_1) \leq_P k\text{-PLCE}(\mathcal{F}_2)$.

Случай $k = 1$. Для $k = 1$ задача $k\text{-PLCE}$ вырождается в задачу существования неподвижной точки.

Определение. Задачей $1\text{-FPE}(\mathcal{F})$ (Fixed Point Existence) будем называть следующую задачу:

- *Вход:* булева сеть $f = (f_1, \dots, f_n)$ такая, что $f_i \in [\mathcal{F}]$ для всех $i \in [n]$;
- *Вопрос:* существует ли неподвижная точка, то есть конфигурация $x \in \{0, 1\}^n$ такая, что $f(x) = x$?

Очевидно, что $1\text{-FPE}(\mathcal{F})$ эквивалентна задаче $1\text{-PLCE}(\mathcal{F})$.

Для общих булевых сетей (без функциональных ограничений) задача существования неподвижной точки уже является NP-полной; кроме того, известны полные дихотомии по классам функций и графов взаимодействия [17]. Следуя [17], рассмотрим пару $(\mathcal{F}, \mathcal{G})$, где \mathcal{F} — постовский класс булевых функций, а \mathcal{G} — минорно-замкнутый класс ориентированных графов.

В настоящей работе мы рассматриваем класс графов \mathcal{G}^{all} всех ориентированных графов взаимодействия. Он, очевидно, является минорно-замкнутым и, в частности, содержит все планарные графы (а также все графы с вершинным покрытием мощности 1). Поэтому к паре $(\mathcal{F}, \mathcal{G}^{\text{all}})$ применима дихотомия Косуба для задачи существования неподвижной точки $\text{FixedPoints}(\mathcal{F}, \mathcal{G})$ [17]: $\text{FixedPoints}(\mathcal{F}, \mathcal{G}^{\text{all}})$ (и, следовательно, $1\text{-PLCE}(\mathcal{F})$) NP-полна тогда и только тогда, когда \mathcal{F} содержит клон всех самодвойственных функций D_1 ; во всех остальных постовских классах \mathcal{F} эта задача решается за полиномиальное время.

Отметим также, что для монотонных классов Поста D_2 , F_6^∞ и F_2^∞ глобальное отображение $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ монотонно по покомпонентному порядку. Поскольку $\{0, 1\}^n$ является конечной полной решёткой, по теореме Кнастера–Тарского любая такая сеть имеет неподвижную точку, причём её можно найти за полиномиальное время. Следовательно, задача $1\text{-FPE}(\mathcal{F})$ для классов $\mathcal{F} \in \{D_2, F_6^\infty, F_2^\infty\}$ принадлежит классу P. Аналогично, для линейного класса L_1 задача существования неподвижной точки также полиномиально разрешима с помощью решения системы линейных уравнений над полем \mathbb{F}_2 .

В дальнейшем мы будем фокусироваться на классификации сложности задачи $k\text{-PLCE}$ для фиксированных $k \geq 2$.

Случай $k \geq 2$. Следующие результаты получены явными полиномиальными редукциями из задачи 3-SAT и показывают, что даже при сильных функциональных ограничениях задача существования предельных циклов длины больше единицы может оставаться NP-полной.

Лемма 2. Пусть фиксировано целое число $k \geq 2$. Тогда задача k -PLCE(D_2) является NP-полной.

Лемма 3. Пусть фиксировано целое число $k \geq 2$. Тогда задача k -PLCE(F_6^∞) является NP-полной.

Лемма 4. Пусть фиксировано целое число $k \geq 2$. Тогда задача k -PLCE(F_2^∞) является NP-полной.

В отличие от NP-полных случаев, для линейного класса L_1 задача k -PLCE оказывается полиномиально разрешимой благодаря алгебраической структуре линейных сетей.

Лемма 5. Пусть фиксировано целое число $k \geq 2$. Тогда задача k -PLCE(L_1) принадлежит классу P.

Полученные результаты для рассматриваемых классов Поста суммированы на рис. 1.

5. Доказательства

В настоящем разделе изложены доказательства основных результатов о вычислительной сложности задачи k -PLCE для булевых сетей с локальными функциями, ограниченными классами Поста.

Для установления NP-трудности используются явные полиномиальные редукции из задачи 3-выполнимости.

Принадлежность рассматриваемых задач классу NP отдельно не доказывается: она следует из стандартной полиномиальной проверки сертификата — конфигурации, принадлежащей предельному циклу длины k , — и уже установлена для общей задачи k -PLCE в работе [1].

Для линейного случая используется алгебраический анализ композиций функций и решение систем линейных уравнений над полем \mathbb{F}_2 .

Структура раздела следует леммам 1–5, каждая из которых касается вычислительной сложности для отдельного класса функций.

Соглашение о кратных дугах. Во всех последующих конструкциях выражения вида «проведём t дуг из вершины u в вершину v » или «добавим t петель у вершины v » используются лишь как сокращённое описание локальной функции вершины v .

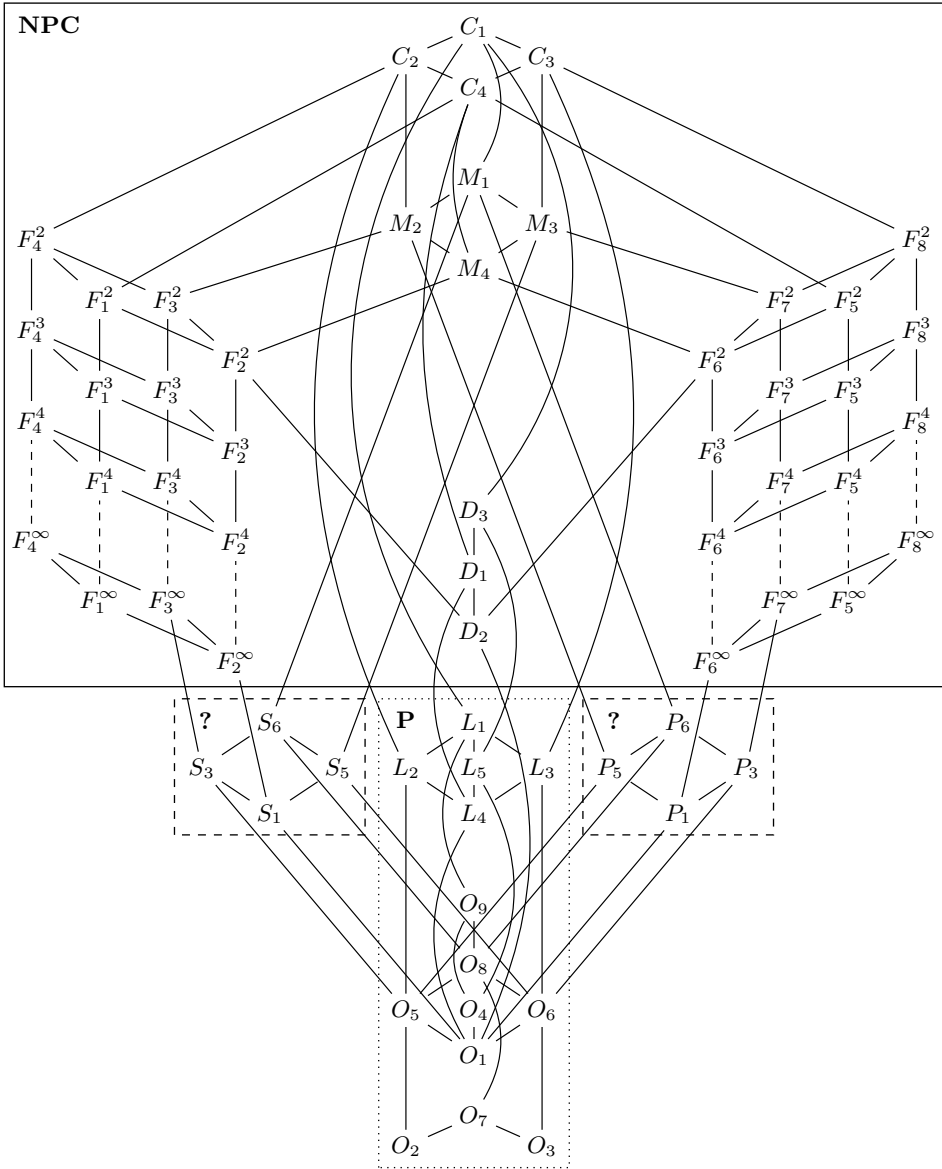


Рис. 1: Вычислительная сложность задачи $k\text{-PLCE}(F)$ для классов Поста

А именно, если при описании конструкции некоторая вершина u должна входить в локальную функцию вершины v с кратностью t , то это означает, что соответствующая переменная подставляется в выбранную базовую функцию t раз. Например, запись о двух петлях в вершине v означает, что переменная x_v участвует в локальной функции вершины v дважды.

Формально все рассматриваемые далее сети являются обычными булевыми сетями без кратных дуг. Для каждой вершины v локальная функция задаётся как булева функция от попарно различных переменных, получающаяся из указанной схемы путём отождествления одинаковых аргументов. Поскольку рассматриваемые классы функций замкнуты относительно суперпозиции и отождествления переменных, такая запись не выводит локальные функции за пределы соответствующего класса.

Таким образом, кратность дуг служит только для компактного описания того, с какими весами соответствующие переменные участвуют в локальной функции; граф взаимодействия при этом понимается в обычном смысле, то есть без кратных дуг. В частности, дополнительные вершины в конструкцию не вводятся, и пространство состояний сети определяется только исходными вершинами конструкции.

Доказательство леммы 1. Поскольку $\mathcal{F}_1 \subseteq \mathcal{F}_2$, имеем $[\mathcal{F}_1] \subseteq [\mathcal{F}_2]$. Действительно, класс $[\mathcal{F}_1]$ получается из функций множества \mathcal{F}_1 применением операций суперпозиции и введения фиктивных переменных; те же построения допустимы и для множества \mathcal{F}_2 .

Рассмотрим отображение

$$R: \text{Inst}(\text{k-PLCE}(\mathcal{F}_1)) \rightarrow \text{Inst}(\text{k-PLCE}(\mathcal{F}_2)), \quad R(f) = f,$$

где $\text{Inst}(\cdot)$ обозначает множество экземпляров соответствующей задачи.

Корректность определения R следует из включения $[\mathcal{F}_1] \subseteq [\mathcal{F}_2]$: если $f = (f_1, \dots, f_n)$ является экземпляром задачи $\text{k-PLCE}(\mathcal{F}_1)$, то $f_i \in [\mathcal{F}_1]$ для всех $i \in [n]$, а значит, $f_i \in [\mathcal{F}_2]$ для всех $i \in [n]$. Следовательно, f является также экземпляром задачи $\text{k-PLCE}(\mathcal{F}_2)$.

Кроме того, для любого экземпляра f выполнено

$$f \in \text{k-PLCE}(\mathcal{F}_1) \iff R(f) = f \in \text{k-PLCE}(\mathcal{F}_2),$$

поскольку вопрос о существовании предельного цикла длины k формулируется для одной и той же булевой сети.

Наконец, отображение R вычисляется за линейное время, так как является тождественным. Следовательно,

$$\text{k-PLCE}(\mathcal{F}_1) \leq_P \text{k-PLCE}(\mathcal{F}_2).$$

□

Теперь рассмотрим вычислительную сложность задачи k-PLCE для сетей, ограниченных классом Поста D_2 . Построение сети \mathcal{N}_ψ для этого случая схематически изображено на рис. 2.

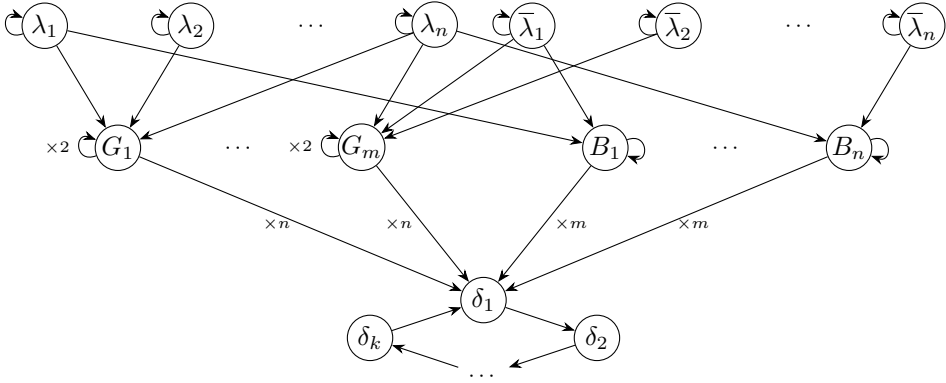


Рис. 2: Граф для случая D_2

Доказательство леммы 2. Принадлежность задачи k-PLCE(D_2) классу NP следует из общей принадлежности задачи k-PLCE классу NP, установленной в работе [1].

Докажем NP-трудность полиномиальной редукцией из задачи 3-SAT. Пусть дана формула

$$\psi = C_1 \wedge \dots \wedge C_m$$

в 3-КНФ на переменных y_1, \dots, y_n , где каждый дизъюнкт

$$C_j = (\ell_{j1} \vee \ell_{j2} \vee \ell_{j3})$$

состоит из трёх литералов, и каждый литерал ℓ_{jr} равен либо y_i , либо $\neg y_i$ для некоторого $i \in [n]$.

Предварительное упрощение. Без ограничения общности можно считать, что $\gcd(n, m) = 1$. Действительно, если $\gcd(n, m) \neq 1$, то достаточно заменить формулу ψ на эквивалентную формулу, полученную добавлением нескольких копий одного и того же дизъюнкта. Это не меняет выполнимости формулы. При этом число переменных остаётся равным n , а число дизъюнктов становится равным $m + r$, где $r \in \{1, \dots, n\}$. Среди чисел $m + 1, \dots, m + n$ найдётся число, взаимно простое с n , поэтому для подходящего r получаем $\gcd(n, m + r) = 1$. Такое преобразование

выполняется за полиномиальное время. Для простоты обозначений далее снова будем писать t для числа дизъюнктов после этой замены.

Построение сети \mathcal{N}_ψ . Построим по формуле ψ булеву сеть \mathcal{N}_ψ с параллельной схемой обновления.

1. *Слой литералов.* Для каждого $i \in [n]$ вводятся две вершины λ_i и $\bar{\lambda}_i$, соответствующие литералам y_i и $\neg y_i$. В каждой из этих вершин имеется одна петля, а локальная функция равна тождеству:

$$f_{\lambda_i}(z) = z_{\lambda_i}, \quad f_{\bar{\lambda}_i}(z) = z_{\bar{\lambda}_i}.$$

Следовательно, значения вершин λ_i и $\bar{\lambda}_i$ не изменяются вдоль любой траектории.

2. *Слой дизъюнктов и переменных.* Для каждого $j \in [m]$ вводится вершина G_j , а для каждого $i \in [n]$ вводится вершина B_i .

Если литерал y_i входит в дизъюнкт C_j , то проводится дуга $\lambda_i \rightarrow G_j$; если в C_j входит литерал $\neg y_i$, то проводится дуга $\bar{\lambda}_i \rightarrow G_j$. Кроме того, в каждой вершине G_j имеются две петли.

В вершину B_i проводятся дуги из λ_i и $\bar{\lambda}_i$, и в B_i имеется одна петля.

Локальная функция в каждой вершине G_j и B_i есть мажоритарная функция от всех её входов. Поскольку мажоритарная функция от нечётного числа аргументов является монотонной и самодвойственной, все эти функции принадлежат классу D_2 .

3. *Слой цикла.* Вводятся вершины $\delta_1, \dots, \delta_k$, образующие ориентированный цикл длины k :

$$\delta_1 \rightarrow \delta_2 \rightarrow \dots \rightarrow \delta_k \rightarrow \delta_1.$$

Для $r = 2, \dots, k$ положим

$$f_{\delta_r}(z) = z_{\delta_{r-1}}.$$

Из каждой вершины G_j проводится n дуг в вершину δ_1 , а из каждой вершины B_i проводится t дуг в вершину δ_1 . Согласно соглашению о кратных дугах, это означает, что значение каждой вершины G_j входит в локальную функцию вершины δ_1 ровно n раз, а значение каждой вершины B_i входит в неё ровно t раз.

Локальная функция в вершине δ_1 есть мажоритарная функция от всех её входов, то есть от значения δ_k , от n копий каждого значения G_1, \dots, G_m и от t копий каждого значения B_1, \dots, B_n .

Таким образом, все локальные функции сети \mathcal{N}_ψ принадлежат классу D_2 . Построение сети выполняется за полиномиальное время.

Корректность редукции.

(1) Если формула ψ выполнима, то сеть \mathcal{N}_ψ имеет предельный цикл длины k .

Пусть

$$a : \{y_1, \dots, y_n\} \rightarrow \{0, 1\}$$

— удовлетворяющее присваивание формулы ψ . Рассмотрим конфигурацию $z^{(0)}$, определённую равенствами

$$z_{\lambda_i}^{(0)} = a(y_i), \quad z_{\bar{\lambda}_i}^{(0)} = 1 - a(y_i), \quad i \in [n],$$

$$z_{G_j}^{(0)} = 1, \quad j \in [m],$$

$$z_{B_i}^{(0)} = 0, \quad i \in [n],$$

$$z_{\delta_1}^{(0)} = 1, \quad z_{\delta_2}^{(0)} = \dots = z_{\delta_k}^{(0)} = 0.$$

Покажем, что под действием глобального отображения f значения всех вершин $\lambda_i, \bar{\lambda}_i, G_j, B_i$ сохраняются.

Для вершин $\lambda_i, \bar{\lambda}_i$ это очевидно из определения:

$$f_{\lambda_i}(z) = z_{\lambda_i}, \quad f_{\bar{\lambda}_i}(z) = z_{\bar{\lambda}_i}.$$

Рассмотрим теперь вершину G_j . Её входами являются три значения, соответствующие литералам дизъюнкта C_j , и два раза её собственное значение. Так как присваивание a удовлетворяет ψ , в дизъюнкте C_j имеется хотя бы один истинный литерал. Следовательно, среди трёх литеральных входов вершины G_j хотя бы один равен 1. Так как $z_{G_j}^{(0)} = 1$, два петлевых входа также равны 1. Значит, среди пяти входов вершины G_j не менее трёх равны 1, и потому

$$f_{G_j}(z^{(0)}) = 1 = z_{G_j}^{(0)}.$$

Следовательно, значение вершины G_j остаётся равным 1.

Рассмотрим вершину B_i . Её входами являются значения $\lambda_i, \bar{\lambda}_i$ и её собственное значение. По построению

$$z_{\lambda_i}^{(0)} + z_{\bar{\lambda}_i}^{(0)} = 1$$

в обычной арифметике, то есть ровно одно из значений $z_{\lambda_i}^{(0)}, z_{\bar{\lambda}_i}^{(0)}$ равно 1. Кроме того, $z_{B_i}^{(0)} = 0$. Следовательно, среди трёх входов вершины B_i ровно одна единица, поэтому

$$f_{B_i}(z^{(0)}) = 0 = z_{B_i}^{(0)}.$$

Значит, значение вершины B_i остаётся равным 0.

Итак, на всей траектории, исходящей из $z^{(0)}$, все вершины $\lambda_i, \bar{\lambda}_i, G_j, B_i$ сохраняют свои значения.

Теперь рассмотрим вершину δ_1 . Во входах, приходящих из слоя G_1, \dots, G_m , имеется ровно mn единиц, а во входах, приходящих из слоя B_1, \dots, B_n , имеется ровно mn нулей. Следовательно, среди всех входов вершины δ_1 , кроме входа из δ_k , ровно половина равна 1, а ровно половина равна 0. Поэтому значение мажоритарной функции в δ_1 определяется значением входа из δ_k :

$$f_{\delta_1}(z) = z_{\delta_k}.$$

Для вершин $\delta_2, \dots, \delta_k$ по построению имеем

$$f_{\delta_r}(z) = z_{\delta_{r-1}}, \quad r = 2, \dots, k.$$

Следовательно, на векторе $(z_{\delta_1}, \dots, z_{\delta_k})$ глобальное отображение действует как циклический сдвиг:

$$(1, 0, \dots, 0) \mapsto (0, 1, 0, \dots, 0) \mapsto \dots \mapsto (0, \dots, 0, 1) \mapsto (1, 0, \dots, 0).$$

Значит, конфигурация $z^{(0)}$ лежит на предельном цикле длины k , то есть

$$z^{(0)} \in \Phi_k(f).$$

(2) Если сеть \mathcal{N}_ψ имеет предельный цикл длины k , то формула ψ выполнима.

Пусть $z^{(0)} \in \Phi_k(f)$, а

$$z^{(t+1)} = f(z^{(t)}), \quad t \geq 0,$$

— соответствующая траектория.

Как и выше, из тождественности локальных функций в вершинах $\lambda_i, \bar{\lambda}_i$ следует, что значения этих вершин постоянны по времени. Следовательно, литеральные входы каждой вершины G_j и B_i постоянны.

Зафиксируем вершину G_j . При фиксированных литеральных входах её динамика имеет вид

$$u^{(t+1)} = \text{Maj}(c_1, c_2, c_3, u^{(t)}, u^{(t)}),$$

где $c_1, c_2, c_3 \in \{0, 1\}$ постоянны. Это одномерное монотонное отображение множества $\{0, 1\}$ в себя, поэтому оно не имеет циклов длины больше 1. Так как рассматриваемая траектория является периодической, значение вершины G_j на ней постоянно.

Аналогично, для каждой вершины B_i при фиксированных значениях $\lambda_i, \bar{\lambda}_i$ динамика имеет вид

$$u^{(t+1)} = \text{Maj}(c_1, c_2, u^{(t)}),$$

где $c_1, c_2 \in \{0, 1\}$ постоянны. Это также одномерное монотонное отображение, а значит, на периодической траектории значение вершины B_i постоянно.

Итак, на цикле могут изменяться только вершины $\delta_1, \dots, \delta_k$.

Обозначим через p число вершин G_j , имеющих значение 1, и через q число вершин B_i , имеющих значение 1:

$$p = \#\{j \in [m] \mid z_{G_j} = 1\}, \quad q = \#\{i \in [n] \mid z_{B_i} = 1\}.$$

Тогда число единиц среди входов вершины δ_1 , приходящих из слоя G_1, \dots, G_m , равно pn , а число единиц среди входов, приходящих из слоя B_1, \dots, B_n , равно qm . Следовательно, число единиц среди всех входов вершины δ_1 , кроме входа из δ_k , равно

$$pn + qm.$$

Общее число таких входов равно

$$mn + mn = 2mn.$$

Поскольку $z^{(0)}$ лежит на цикле длины $k \geq 2$, значение вершины δ_1 не может быть постоянным. Действительно, если бы δ_1 имела постоянное значение, то из равенств

$$f_{\delta_r}(z) = z_{\delta_{r-1}}, \quad r = 2, \dots, k,$$

следовало бы, что все вершины $\delta_1, \dots, \delta_k$ также имеют постоянные значения, а значит, весь цикл имел бы длину 1, что противоречит условию $k \geq 2$.

Следовательно, значение δ_1 должно зависеть от значения вершины δ_k . Это возможно только тогда, когда среди остальных входов в δ_1 число единиц равно числу нулей, то есть

$$pn + qm = mn.$$

Из этого равенства следует

$$qm = n(m - p).$$

Так как $\gcd(n, m) = 1$, из делимости числа qm на n получаем, что q делится на n . Поскольку $0 \leq q \leq n$, заключаем, что

$$q = 0 \quad \text{или} \quad q = n.$$

Аналогично из равенства

$$pn = m(n - q)$$

получаем, что p делится на m , а значит,

$$p = 0 \quad \text{или} \quad p = m.$$

С учётом равенства $pn + qt = mn$ остаются только два случая:

$$(p, q) = (m, 0) \quad \text{или} \quad (p, q) = (0, n).$$

Рассмотрим эти два случая отдельно.

Случай 1: $(p, q) = (m, 0)$. В этом случае все вершины G_j имеют значение 1, а все вершины B_i имеют значение 0.

Определим присваивание

$$a : \{y_1, \dots, y_n\} \rightarrow \{0, 1\}, \quad a(y_i) = z_{\lambda_i}.$$

Докажем, что для каждого дизъюнкта C_j формулы ψ найдётся литерал, истинный при присваивании a . Рассмотрим произвольный дизъюнкт C_j . Так как $z_{G_j} = 1$, а вершина G_j вычисляет мажоритарную функцию от пяти входов, среди которых два петлевых входа равны 1, то среди трёх литеральных входов вершины G_j хотя бы один также должен быть равен 1.

Пусть такой литерал равен ℓ . Если $\ell = y_i$, то $z_{\lambda_i} = 1$, и поэтому $a(y_i) = 1$. Значит, литерал y_i истинен при a .

Если же $\ell = \neg y_i$, то $z_{\bar{\lambda}_i} = 1$. Так как $z_{B_i} = 0$, а вершина B_i вычисляет мажоритарную функцию от трёх входов $\lambda_i, \bar{\lambda}_i, B_i$, то не может одновременно выполняться $z_{\lambda_i} = 1$. Иначе среди трёх входов вершины B_i было бы как минимум две единицы, и тогда B_i имела бы значение 1, противоречие. Следовательно, $z_{\lambda_i} = 0$, откуда $a(y_i) = 0$, и литерал $\neg y_i$ истинен при a .

Итак, в каждом дизъюнкте C_j имеется хотя бы один литерал, истинный при присваивании a . Следовательно, формула ψ выполнима.

Случай 2: $(p, q) = (0, n)$. В этом случае все вершины G_j имеют значение 0, а все вершины B_i имеют значение 1.

Определим присваивание

$$a : \{y_1, \dots, y_n\} \rightarrow \{0, 1\}, \quad a(y_i) = 1 - z_{\lambda_i}.$$

Докажем, что для каждого дизъюнкта C_j формулы ψ найдётся литерал, истинный при присваивании a . Рассмотрим произвольный дизъюнкт C_j . Так как $z_{G_j} = 0$, а вершина G_j вычисляет мажоритарную функцию от пяти входов, среди которых два петлевых входа равны 0, то среди трёх литеральных входов вершины G_j хотя бы один должен быть равен 0. Действительно, если бы все три литеральных входа были равны 1, то среди пяти входов вершины G_j было бы три единицы, и мажоритарная функция приняла бы значение 1, что противоречит равенству $z_{G_j} = 0$.

Пусть литерал, соответствующий такому нулевому входу, равен ℓ . Если $\ell = y_i$, то $z_{\lambda_i} = 0$. Поэтому

$$a(y_i) = 1 - z_{\lambda_i} = 1,$$

и литерал y_i истинен при a .

Если же $\ell = \neg y_i$, то $z_{\bar{\lambda}_i} = 0$. Так как $z_{B_i} = 1$, а вершина B_i вычисляет мажоритарную функцию от трёх входов $\lambda_i, \bar{\lambda}_i, B_i$, то среди двух входов $\lambda_i, \bar{\lambda}_i$ хотя бы один должен быть равен 1. Поскольку $z_{\bar{\lambda}_i} = 0$, получаем $z_{\lambda_i} = 1$. Следовательно,

$$a(y_i) = 1 - z_{\lambda_i} = 0,$$

и литерал $\neg y_i$ истинен при a .

Итак, и в этом случае в каждом дизъюнкте C_j имеется хотя бы один литерал, истинный при присваивании a . Следовательно, формула ψ выполнима.

Таким образом, в обоих возможных случаях $(p, q) = (m, 0)$ и $(p, q) = (0, n)$ из существования предельного цикла длины k следует выполнимость формулы ψ .

Итак, формула ψ выполнима тогда и только тогда, когда построенная сеть \mathcal{N}_ψ имеет предельный цикл длины k . Следовательно, задача $k\text{-PLCE}(D_2)$ NP-трудна. Совместно с принадлежностью классу NP получаем, что $k\text{-PLCE}(D_2)$ NP-полна. \square

Доказательство леммы 3. Принадлежность задачи $k\text{-PLCE}(F_6^\infty)$ классу NP следует из общей принадлежности задачи $k\text{-PLCE}$ классу NP, установленной в [1].

Остаётся доказать NP-трудность. Для этого построим полиномиальную редукцию

$$k\text{-PLCE}(D_2) \leq_P k\text{-PLCE}(F_6^\infty),$$

где NP-полнота левой задачи установлена в лемме 2.

Пусть задана булева сеть

$$f = (f_1, \dots, f_n), \quad f_i \in D_2 \text{ для всех } i \in [n].$$

Рассматривается параллельная схема обновления.

Построим по сети f новую сеть

$$g = (g_0, g_1, \dots, g_n)$$

размерности $n + 1$. Добавим новую вершину 0, обозначим её переменной y , и положим

$$g_0(y, x_1, \dots, x_n) = y.$$

Для каждой исходной вершины $i \in [n]$ определим

$$g_i(y, x_1, \dots, x_n) = y \cdot f_i(x_1, \dots, x_n).$$

Покажем, что все функции g_i принадлежат F_6^∞ . Будем пользоваться следующим описанием класса F_6^∞ : булева функция принадлежит F_6^∞ , если она монотонна, сохраняет константы 0 и 1, и её значение не превосходит значения некоторой её переменной.

Сначала рассмотрим функцию g_0 . По определению

$$g_0(y, x_1, \dots, x_n) = y.$$

Она монотонна, сохраняет 0 и 1, и для всех входов выполнено

$$g_0(y, x_1, \dots, x_n) = y \leq y.$$

Следовательно, $g_0 \in F_6^\infty$.

Теперь пусть $i \in [n]$. Так как $f_i \in D_2$, функция f_i монотонна и самодвойственна. В частности, она сохраняет константы 0 и 1. Действительно, из монотонности следует

$$f_i(0, \dots, 0) \leq f_i(1, \dots, 1),$$

а из самодвойственности —

$$f_i(0, \dots, 0) = 1 - f_i(1, \dots, 1).$$

Значит,

$$f_i(0, \dots, 0) = 0, \quad f_i(1, \dots, 1) = 1.$$

Рассмотрим функцию

$$g_i(y, x_1, \dots, x_n) = y \cdot f_i(x_1, \dots, x_n).$$

Она монотонна как конъюнкция двух монотонных функций. Кроме того,

$$g_i(0, 0, \dots, 0) = 0$$

и

$$g_i(1, 1, \dots, 1) = 1 \cdot f_i(1, \dots, 1) = 1,$$

то есть g_i сохраняет 0 и 1. Наконец, для любого набора значений входов выполнено

$$g_i(y, x_1, \dots, x_n) = y \cdot f_i(x_1, \dots, x_n) \leq y.$$

Следовательно, $g_i \in F_6^\infty$.

Итак,

$$g_0, g_1, \dots, g_n \in F_6^\infty.$$

Остаётся показать эквивалентность по существованию цикла длины k .

(1) Если в сети f существует предельный цикл длины k , то такой же цикл существует в сети g . Пусть $x^{(0)} \in \Phi_k(f)$, то есть

$$f^k(x^{(0)}) = x^{(0)}, \quad f^t(x^{(0)}) \neq x^{(0)} \text{ для всех } t = 1, \dots, k-1.$$

Рассмотрим конфигурацию

$$z^{(0)} = (1, x^{(0)}).$$

Тогда при параллельном обновлении

$$y^{(t+1)} = g_0(y^{(t)}, x^{(t)}) = y^{(t)},$$

и потому $y^{(t)} \equiv 1$ для всех $t \geq 0$. Кроме того,

$$x_i^{(t+1)} = g_i(y^{(t)}, x^{(t)}) = y^{(t)} \cdot f_i(x^{(t)}) = f_i(x^{(t)}), \quad i \in [n].$$

Следовательно, если обозначить через $\pi : \{0, 1\}^{n+1} \rightarrow \{0, 1\}^n$ проекцию

$$\pi(y, x_1, \dots, x_n) = (x_1, \dots, x_n),$$

то для всех $t \geq 0$ выполняется равенство

$$\pi(z^{(t)}) = f^t(x^{(0)}).$$

Отсюда

$$z^{(k)} = (1, f^k(x^{(0)})) = (1, x^{(0)}) = z^{(0)},$$

а для всех $t = 1, \dots, k - 1$

$$z^{(t)} = (1, f^t(x^{(0)})) \neq (1, x^{(0)}).$$

Следовательно, $z^{(0)} \in \Phi_k(g)$.

(2) Если в сети g существует предельный цикл длины $k \geq 2$, то такой же цикл существует в сети f . Пусть

$$z^{(0)} = (y^{(0)}, x^{(0)}) \in \Phi_k(g), \quad z^{(t+1)} = g(z^{(t)}).$$

Из равенства $g_0(y, x) = y$ следует, что

$$y^{(t+1)} = y^{(t)} \quad \text{для всех } t \geq 0,$$

то есть $y^{(t)} \equiv y^{(0)}$.

Если $y^{(0)} = 0$, то

$$x_i^{(t+1)} = g_i(0, x^{(t)}) = 0 \quad \text{для всех } i \in [n], t \geq 0,$$

и уже через один шаг траектория попадает в конфигурацию $(0, 0, \dots, 0)$, то есть возможен только цикл длины 1. Это противоречит предположению $k \geq 2$. Значит, для цикла длины $k \geq 2$ необходимо $y^{(0)} = 1$.

Тогда $y^{(t)} \equiv 1$ для всех t , и потому

$$x_i^{(t+1)} = g_i(1, x^{(t)}) = f_i(x^{(t)}), \quad i \in [n].$$

Следовательно,

$$x^{(t+1)} = f(x^{(t)}) \quad \text{для всех } t \geq 0.$$

Из $z^{(k)} = z^{(0)}$ получаем

$$x^{(k)} = f^k(x^{(0)}) = x^{(0)},$$

а из $z^{(t)} \neq z^{(0)}$ для $t = 1, \dots, k - 1$ следует

$$x^{(t)} \neq x^{(0)} \quad \text{для тех же } t.$$

Значит, $x^{(0)} \in \Phi_k(f)$.

Тем самым по сети f за полиномиальное время строится сеть g такая, что сеть f является положительным экземпляром задачи $k\text{-PLCE}(D_2)$ тогда и только тогда, когда сеть g является положительным экземпляром задачи $k\text{-PLCE}(F_6^\infty)$. Следовательно,

$$k\text{-PLCE}(D_2) \leq_P k\text{-PLCE}(F_6^\infty).$$

Так как задача $k\text{-PLCE}(D_2)$ NP-полна по лемме 2, а задача $k\text{-PLCE}(F_6^\infty)$ принадлежит классу NP, получаем, что $k\text{-PLCE}(F_6^\infty)$ NP-полна. \square

Доказательство леммы 4. Класс F_2^∞ двойственен классу F_6^∞ . По принципу двойственности булевых функций и по лемме 3 получаем, что задача k -PLCE(F_2^∞) также является NP-полной. \square

В отличие от NP-полных случаев, для класса L_1 задача k -PLCE допускает более эффективный алгоритм: её можно решить за время $O(n^3k)$.

Доказательство леммы 5. Пусть булева сеть $f = (f_1, \dots, f_n)$ состоит из функций класса L_1 . Тогда каждая локальная функция аффинно-линейна над полем \mathbb{F}_2 , и, следовательно, глобальное отображение сети имеет вид

$$f(x) = Ax \oplus b,$$

где $A \in M_n(\mathbb{F}_2)$, $b \in \mathbb{F}_2^n$, а $x \in \mathbb{F}_2^n$.

Для каждого натурального t обозначим через $S(t)$ число неподвижных точек отображения f^t , то есть

$$S(t) = |\{x \in \mathbb{F}_2^n \mid f^t(x) = x\}|.$$

Обозначим также через $P(d)$ число конфигураций, минимальный период которых относительно f равен d .

Тогда конфигурация является неподвижной точкой отображения f^t тогда и только тогда, когда её минимальный период делит t . Следовательно, для каждого $t \geq 1$ имеем

$$S(t) = \sum_{d|t} P(d).$$

По формуле обращения Мёбиуса отсюда получаем

$$P(k) = \sum_{d|k} \mu(k/d) S(d),$$

где μ — функция Мёбиуса.

Таким образом, предельный цикл длины k существует тогда и только тогда, когда $P(k) > 0$. Поэтому достаточно вычислить все значения $S(d)$ для делителей $d \mid k$.

Шаг 1. Вычисление отображений f^t для $t = 1, \dots, k$.

Рассмотрим матрицу

$$M = \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} \in M_{n+1}(\mathbb{F}_2).$$

Непосредственной проверкой по индукции получаем, что для каждого $t \geq 1$ матрица M^t имеет вид

$$M^t = \begin{pmatrix} A_t & b_t \\ 0 & 1 \end{pmatrix},$$

где

$$f^t(x) = A_t x \oplus b_t.$$

Действительно, база $t = 1$ очевидна. Если

$$M^t = \begin{pmatrix} A_t & b_t \\ 0 & 1 \end{pmatrix},$$

то

$$M^{t+1} = M M^t = \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A_t & b_t \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} AA_t & Ab_t \oplus b \\ 0 & 1 \end{pmatrix},$$

то есть $f^{t+1}(x) = A(A_t x \oplus b_t) \oplus b$.

Следовательно, все матрицы M, M^2, \dots, M^k можно вычислить последовательно. Один шаг умножения матриц размера $(n+1) \times (n+1)$ занимает $O(n^3)$ операций, поэтому все эти матрицы вычисляются за

$$O(n^3 k).$$

Шаг 2. Вычисление чисел $S(d)$ для всех $d \mid k$.

Для каждого делителя $d \mid k$, зная матрицу

$$M^d = \begin{pmatrix} A_d & b_d \\ 0 & 1 \end{pmatrix},$$

получаем представление

$$f^d(x) = A_d x \oplus b_d.$$

Условие $f^d(x) = x$ эквивалентно системе линейных уравнений

$$(A_d \oplus I)x = b_d$$

над полем \mathbb{F}_2 . Число решений этой системы равно $S(d)$, и его можно найти методом Гаусса за $O(n^3)$ операций.

Так как число делителей числа k не превосходит k , суммарное время вычисления всех значений $S(d)$ для $d \mid k$ не превосходит

$$O(n^3 k).$$

Шаг 3. Вычисление $P(k)$.

После нахождения всех $S(d)$, $d \mid k$, значение $P(k)$ вычисляется по формуле

$$P(k) = \sum_{d \mid k} \mu(k/d) S(d).$$

Это требует не более чем $O(k)$ арифметических операций, что поглощается оценкой $O(n^3 k)$.

Итак, за время

$$O(n^3 k)$$

мы вычисляем число $P(k)$ конфигураций с минимальным периодом ровно k . Следовательно, можно за то же время проверить условие $P(k) > 0$, которое эквивалентно существованию предельного цикла длины k .

Тем самым задача k -PLCE(L_1) решается за время $O(n^3 k)$. В частности, при фиксированном k она принадлежит классу P . \square

6. Заключение

В настоящей работе исследована вычислительная сложность задачи k -Parallel Limit Cycle Existence (k -PLCE) для булевых сетей, построенных из функций различных классов решётки Поста. Доказано, что задача k -PLCE остаётся NP-полной даже при значительных функциональных ограничениях, в частности, для класса D_2 , включающего только монотонные самодвойственные функции, а также для классов F_6^∞ и F_2^∞ . В то же время установлено, что для класса линейных функций L_1 задача k -PLCE является полиномиально разрешимой.

Полученные результаты составляют основу для дальнейшего анализа вычислительной сложности динамики булевых сетей при структурных и функциональных ограничениях. Перспективными направлениями дальнейших исследований являются:

- получение полной классификации задачи k -PLCE за счёт анализа оставшихся классов S_6 и P_6 решётки Поста;
- изучение параметризованной вычислительной сложности задачи по параметрам k и/или максимальной входной степени графа взаимодействия;
- обобщение результатов на другие схемы обновления, такие как асинхронные или блочно-последовательные;
- исследование приближённых алгоритмов и эвристик для решения задачи k -PLCE в практических приложениях.

В целом, настоящая работа способствует теоретическому пониманию связи между логической структурой локальных функций и вычислительной сложностью глобальной динамики дискретных динамических систем.

Список литературы

- [1] Bridoux F., Gaze-Maillet C., Perrot K., Séné S., “Complexity of Limit-Cycle Problems in Boolean Networks”, *SOFSEM 2021: Theory and Practice of Computer Science*, Lecture Notes in Computer Science, vol. 12607, Springer, 2021, 135–146. DOI: 10.1007/978-3-030-67731-2_10.
- [2] Aracena J., Bridoux F., Gómez L., Salinas L., “Complexity of Limit Cycles with Block-Sequential Update Schedules in Conjunctive Networks”, *Natural Computing*, **22** (2023. DOI: 10.1007/s11047-023-09947-0), 411–429.
- [3] Gadouleau M., Richard A., Fanchon E., “Reduction and Fixed Points of Boolean Networks and Linear Network Coding Solvability”, *IEEE Transactions on Information Theory*, **62**:5 (2016. DOI: 10.1109/TIT.2016.2544344), 2504–2519.
- [4] McCulloch W., Pitts W., “A Logical Calculus of the Ideas Immanent in Nervous Activity”, *The Bulletin of Mathematical Biophysics*, **5**:4 (1943. DOI: 10.1007/BF02478259), 115–133.
- [5] Goles E., Ruz G.A., “Dynamics of Neural Networks over Undirected Graphs”, *Neural Networks*, **60** (2014. DOI: 10.1016/j.neunet.2014.10.013), 1–8.
- [6] Aledo J.A., Diaz L.G., Martinez S., Valverde J.C., “Coexistence of Periods in Parallel and Sequential Boolean Graph Dynamical Systems over Directed Graphs”, *Mathematics*, **8**:10 (2020. DOI: 10.3390/math8101812), 1812.
- [7] Chossat P., Krupa M., “Heteroclinic Cycles in Hopfield Networks”, *Journal of Nonlinear Science*, **26**:2 (2016), 315–344.
- [8] Ladwani V.M., Ramasubramanian V., “M-ary Hopfield Neural Network for Storage and Retrieval of Variable Length Sequences: Multi-limit Cycle Approach”, *Proceedings of the 2023 International Conference on Artificial Neural Networks (ICANN)*, Springer, 2023. DOI: 10.1007/978-3-031-44192-9_21, 255–268.
- [9] Hesse J., Czaja W., Komorowski M., Jansen R.C., “Oscillations in Gene Regulatory Networks Are Essential for a Robust Molecular Clock”, *PLoS Computational Biology*, **15**:10 (2019. DOI: 10.1371/journal.pcbi.1007361), e1007361.
- [10] Likhoshvai V.A., Golubyatnikov V.P., Khlebodarova T.M., “Limit cycles in models of circular gene networks regulated by negative feedback loops”, *BMC Bioinformatics*, **21** (2020. DOI: 10.1186/s12859-020-03598-z), 255.
- [11] Kauffman S.A., “Metabolic stability and epigenesis in randomly constructed genetic nets”, *Journal of Theoretical Biology*, **22**:3 (1969), 437–467.
- [12] Thomas R., “Boolean formalization of genetic control circuits”, *Journal of Theoretical Biology*, **42**:3 (1973), 563–585.
- [13] Thomas R., D’Ari R., *Biological Feedback*, CRC Press, Boca Raton, 1990.

- [14] Riis Søren, “Information flows, graphs and their guessing numbers”, *The Electronic Journal of Combinatorics*, **14**:1 (2007. DOI: 10.37236/962), R44.
- [15] Gadouleau M., Riis Søren, “Graph-Theoretical Constructions for Graph Entropy and Network Coding Based Communications”, *IEEE Transactions on Information Theory*, **57**:10 (2011. DOI: 10.1109/TIT.2011.2155618), 6703–6717.
- [16] Hopfield J.J., “Neural networks and physical systems with emergent collective computational abilities”, *Proceedings of the National Academy of Sciences*, **79**:8 (1982. DOI: 10.1073/pnas.79.8.2554), 2554–2558.
- [17] Kosub S., “Dichotomy Results for Fixed-Point Existence Problems for Boolean Dynamical Systems”, *Mathematics in Computer Science*, **1**:3 (2008. DOI: 10.1007/s11786-007-0038-y), 487–505.
- [18] Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Б., *Функции алгебры логики и классы Поста*, Наука, Москва, 1966 .

Статья поступила 30 апреля 2026 г.

Computational Complexity of Limit Cycle Existence in Boolean Networks Restricted by Post Classes

A. S. Drobyshev

The paper studies the computational complexity of detecting limit cycles of fixed length k in Boolean networks with local functions restricted to Post classes. It is proven that the problem is NP-complete for expressive classes D_2 (monotone self-dual functions), F_6^∞ , and F_2^∞ , while polynomial-time solvable for linear functions L_1 . Explicit polynomial reductions from 3-SAT preserving limit cycles of length k are constructed.

Keywords: Boolean networks, limit cycles, Post lattice, computational complexity, NP-completeness.

References

- [1] Bridoux F., Gaze-Maillet C., Perrot K., Séné S., “Complexity of Limit-Cycle Problems in Boolean Networks”, *SOFSEM 2021: Theory and Practice of Computer Science*, Lecture Notes in Computer Science, vol. 12607, Springer, 2021, 135–146. DOI: 10.1007/978-3-030-67731-2_10.
- [2] Aracena J., Bridoux F., Gómez L., Salinas L., “Complexity of Limit Cycles with Block-Sequential Update Schedules in Conjunctive Networks”, *Natural Computing*, **22** (2023. DOI: 10.1007/s11047-023-09947-0), 411–429.

- [3] Gadouleau M., Richard A., Fanchon E., “Reduction and Fixed Points of Boolean Networks and Linear Network Coding Solvability”, *IEEE Transactions on Information Theory*, **62**:5 (2016. DOI: 10.1109/TIT.2016.2544344), 2504–2519.
- [4] McCulloch W., Pitts W., “A Logical Calculus of the Ideas Immanent in Nervous Activity”, *The Bulletin of Mathematical Biophysics*, **5**:4 (1943. DOI: 10.1007/BF02478259), 115–133.
- [5] Goles E., Ruz G.A., “Dynamics of Neural Networks over Undirected Graphs”, *Neural Networks*, **60** (2014. DOI: 10.1016/j.neunet.2014.10.013), 1–8.
- [6] Aledo J.A., Diaz L.G., Martinez S., Valverde J.C., “Coexistence of Periods in Parallel and Sequential Boolean Graph Dynamical Systems over Directed Graphs”, *Mathematics*, **8**:10 (2020. DOI: 10.3390/math8101812), 1812.
- [7] Chossat P., Krupa M., “Heteroclinic Cycles in Hopfield Networks”, *Journal of Nonlinear Science*, **26**:2 (2016), 315–344.
- [8] Ladwani V.M., Ramasubramanian V., “M-ary Hopfield Neural Network for Storage and Retrieval of Variable Length Sequences: Multi-limit Cycle Approach”, *Proceedings of the 2023 International Conference on Artificial Neural Networks (ICANN)*, Springer, 2023. DOI: 10.1007/978-3-031-44192-9_21, 255–268.
- [9] Hesse J., Czaja W., Komorowski M., Jansen R.C., “Oscillations in Gene Regulatory Networks Are Essential for a Robust Molecular Clock”, *PLoS Computational Biology*, **15**:10 (2019. DOI: 10.1371/journal.pcbi.1007361), e1007361.
- [10] Likhoshvai V.A., Golubyatnikov V.P., Khlebodarova T.M., “Limit cycles in models of circular gene networks regulated by negative feedback loops”, *BMC Bioinformatics*, **21** (2020. DOI: 10.1186/s12859-020-03598-z), 255.
- [11] Kauffman S.A., “Metabolic stability and epigenesis in randomly constructed genetic nets”, *Journal of Theoretical Biology*, **22**:3 (1969), 437–467.
- [12] Thomas R., “Boolean formalization of genetic control circuits”, *Journal of Theoretical Biology*, **42**:3 (1973), 563–585.
- [13] Thomas R., D’Ari R., *Biological Feedback*, CRC Press, Boca Raton, 1990.
- [14] Riis Søren, “Information flows, graphs and their guessing numbers”, *The Electronic Journal of Combinatorics*, **14**:1 (2007. DOI: 10.37236/962), R44.
- [15] Gadouleau M., Riis Søren, “Graph-Theoretical Constructions for Graph Entropy and Network Coding Based Communications”, *IEEE Transactions on Information Theory*, **57**:10 (2011. DOI: 10.1109/TIT.2011.2155618), 6703–6717.
- [16] Hopfield J.J., “Neural networks and physical systems with emergent collective computational abilities”, *Proceedings of the National Academy of Sciences*, **79**:8 (1982. DOI: 10.1073/pnas.79.8.2554), 2554–2558.
- [17] Kosub S., “Dichotomy Results for Fixed-Point Existence Problems for Boolean Dynamical Systems”, *Mathematics in Computer Science*, **1**:3 (2008. DOI: 10.1007/s11786-007-0038-y), 487–505.

- [18] Yablonsky S.V., Gavrilov G.P., Kudryavtsev V.B., *Functions of Logic Algebra and Post Classes*, Nauka, Moscow, 1966 (In Russian).

Received on April 30, 2026

Операции над клеточными автоматами с локаторами

А. В. Дюбанов*

В данной работе предложены операции над клеточными автоматами с локаторами (КАСЛ). Эти операции позволяют описывать одни КАСЛ в виде формул над другими КАСЛ. В качестве примера построена формула, задающая КАСЛ, эквивалентный КАСЛ, выполняющему умножение натуральных чисел за $2n + 2$ такта.

Ключевые слова: клеточные автоматы с локаторами, суперпозиция, формула.

1. Введение

Понятие клеточного автомата с локаторами (далее КАСЛ) введено в работе Э. Э. Гасанова [1] и уточнено в работе Г. В. Калачева [5].

В настоящей работе вводятся следующие операции суперпозиции над КАСЛ:

- $B(\sigma_1, i, \sigma_2, j)$ — подстановка сигналов вещания из σ_2 в σ_1 , где σ_1 и σ_2 — КАСЛ, i и j — номера компонент эфира σ_1 и σ_2 соответственно;
- $S(\sigma_1, i, \sigma_2, j)$ — подстановка состояний из σ_2 в σ_1 , где σ_1 и σ_2 — КАСЛ, i и j — номера компонент состояний σ_1 и σ_2 соответственно;
- $C(\sigma)$ — операция введения управления, где σ — КАСЛ.

Данные операции позволяют описывать одни КАСЛ в виде формул над другими КАСЛ.

В работе Э. Э. Гасанова и Б. Ф. Хайбуллина [2] предложен алгоритм умножения натуральных n -значных чисел за $2n + 2$ тактов с помощью КАСЛ, основанный на равенстве $a \cdot b = \sum_{i=1}^n 2^{i-1} b \cdot a_i$, где $(a_n, a_{n-1}, \dots, a_1)$ — двоичное представление числа a .

Пусть КАСЛ σ_{ct} выполняет суммирование натуральных чисел, σ_{x2} — удвоение числа, σ_{12} — преобразование из унарного в двоичное представление числа, σ_m притормаживает работу КАСЛ σ_{12} . Эти КАСЛ описаны

* Дюбанов Андрей Васильевич — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: andreydyubanovpost@yandex.ru, ORCID: 0009-0009-3969-9713.

Diubanov Andrei Vasilievich — PhD student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

в работе [2]. В данной работе доказывается, что КАСЛ, задаваемый формулой

$$\mu = B(S(\sigma_{ct}, 2, \sigma_{x2}, 1), 2, B(C(\sigma_{12}), 0, \sigma_m, 1), 3),$$

эквивалентен КАСЛ из работы [2], выполняющему умножение натуральных чисел.

Автор выражает благодарность Э.Э.Гасанову за постановку задачи и помощь в работе.

2. Термины и определения

Напомним определение клеточного автомата с локаторами. Пусть $\sigma = (\mathbb{Z}^k, Q, V, G, +, L, \varphi, \psi)$ — клеточный автомат с локаторами, где:

- \mathbb{Z}^k — множество k -мерных векторов с целыми координатами; элементы \mathbb{Z}^k — ячейки клеточного автомата σ ;
- Q — некоторое конечное множество — множество состояний; $q_0 \in Q$ — состояние покоя;
- $V = \{\alpha_1, \dots, \alpha_{h-1}\}$ — упорядоченный набор попарно различных векторов из \mathbb{Z}^k ; V — шаблон соседства клеточного автомата σ ;
- $(G, +)$ — коммутативная полугруппа с нейтральным элементом e ; элементы множества G называются сигналами вещания;
- шаблон локаторов $L = \{\nu_1, \dots, \nu_m\}$ — упорядоченный набор попарно различных рациональных телесных углов в \mathbb{R}^k с вершиной в начале координат;
- локальная функция переходов $\varphi: Q^h \times G^m \rightarrow Q$, $\varphi(\mathbf{q}_0, \mathbf{e}) = q_0$, $\mathbf{q}_0 = (q_0, \dots, q_0) \in Q^h$, $\mathbf{e} = (e, \dots, e) \in G^m$;
- функция вещания $\psi: Q^h \times G^m \rightarrow G$, $\psi(\mathbf{q}_0, \mathbf{e}) = e$, $\mathbf{q}_0 = (q_0, \dots, q_0) \in Q^h$, $\mathbf{e} = (e, \dots, e) \in G^m$

В общем случае локатор — это телесный угол, границы которого являются частями гиперплоскостей, задаваемых линейными уравнениями с целыми коэффициентами. $\Omega = \mathbb{Z}^k \setminus \{(0, \dots, 0)\}$ называется полным телесным углом. Дадим наименования тем локаторам на плоскости, которые будем использовать далее в настоящей работе:

- $N = \{(x, y) : x = 0, y > 0\}$ назовём «север»;
- $NE = \{(x, y) : x > 0, y = x\}$ назовём «северо-восток»;
- $E = \{(x, y) : x > 0, y = 0\}$ назовём «восток»;

- $SE = \{(x, y) : x > 0, y = -x\}$ назовём «юго-восток»;
- $S = \{(x, y) : x = 0, y < 0\}$ назовём «юг»;
- $SW = \{(x, y) : x < 0, y = x\}$ назовём «юго-запад»;
- $W = \{(x, y) : x < 0, y = 0\}$ назовём «запад»;
- $NW = \{(x, y) : x < 0, y = -x\}$ назовём «северо-запад».

Состоянием клеточного автомата с локаторами σ назовём пару (g, f) , где g — произвольная функция, определённая на множестве \mathbb{Z}^k , принимающая значения из G , называемая состоянием эфира, f — произвольная функция, определённая на множестве \mathbb{Z}^k , принимающая значения из Q , называемая распределением состояний клеточного автомата с локаторами. Если $\alpha \in \mathbb{Z}^k$ и (g, f) — состояние клеточного автомата с локаторами σ , то значение $g(\alpha)$ назовём сигналом ячейки α , определяемым состоянием (g, f) , а значение $f(\alpha)$ — состоянием ячейки α , определяемым состоянием (g, f) .

Функции φ и ψ зависят от переменных $x_0, x_1, \dots, x_{h-1}, z_1, \dots, z_m$. Для того чтобы установить взаимно однозначное соответствие между векторами из V и телесными углами из L и переменными функций φ и ψ , воспользуемся способом, предложенным в работе [1]. Будем индексировать переменные функций φ и ψ самими векторами и телесными углами, т.е. считать, что φ и ψ зависят от переменных $x_0, x_{\alpha_1}, \dots, x_{\alpha_{h-1}}, z_{\nu_1}, \dots, z_{\nu_m}$, индекс переменной x_0 есть нулевой вектор $(0, \dots, 0) \in \mathbb{Z}^k$.

3. Операция подстановки состояния

Пусть $\sigma_D = (\mathbb{Z}^k, Q_D, V_D, G_D, +_D, L_D, \varphi_D, \psi_D)$, $\sigma_E = (\mathbb{Z}^k, Q_E, V_E, G_E, +_E, L_E, \varphi_E, \psi_E)$ — клеточные автоматы с локаторами, для которых выполнены следующие условия:

- $Q_D = Q_{D_1} \times \dots \times Q_{D_{r-1}} \times Q_{D_r} \times Q_{D_{r+1}} \times \dots \times Q_{D_n}$, $n \geq 1$,
- $Q_E = Q_{E_1} \times \dots \times Q_{E_{s-1}} \times Q_{E_s} \times Q_{E_{s+1}} \times \dots \times Q_{E_m}$, $m \geq 1$,
- $Q_{D_r} = Q_{E_s}$,
- $|V_D| = h - 1$, $|L_D| = l$, $|V_E| = p - 1$, $|L_E| = u$,
- $\varphi_D = (\varphi_{D_1}, \dots, \varphi_{D_n})$, $\varphi_{D_i} : Q_D^h \times G_D^l \rightarrow Q_{D_i}$, $i \in \{1, \dots, n\}$,
- $\varphi_E = (\varphi_{E_1}, \dots, \varphi_{E_m})$, $\varphi_{E_i} : Q_E^p \times G_E^u \rightarrow Q_{E_i}$, $i \in \{1, \dots, m\}$.

Тогда скажем, что клеточный автомат с локаторами

$$\sigma_F = (\mathbb{Z}^k, Q_F, V_F, G_F, +_F, L_F, \varphi_F, \psi_F)$$

получен из автоматов σ_D и σ_E с помощью подстановки в r -ю компоненту состояния автомата σ_D s -й компоненты состояния автомата σ_E (обозначим этот факт как $\sigma_F = S(\sigma_D, r, \sigma_E, s)$), если: $Q_F = Q_D \times Q_E$, $V_F = V_D \cup V_E$, $G_F = G_D \times G_E$, $+_F = +_D \times +_E$, $L_F = L_D \cup L_E$, $\varphi_F = (\varphi_{D_1}, \dots, \varphi_{D_{r-1}}, \varphi_{E_s}, \varphi_{D_{r+1}}, \dots, \varphi_{D_n}, \varphi_E)$, $\psi_F = (\psi_D, \psi_E)$.

Фактически результат функционирования автомата σ_F определяется следующим образом:

- автомат σ_E функционирует в соответствии со своими функциями φ_E и ψ_E ;
- автомат σ_D формирует сигналы вещания в соответствии со своей функцией вещания ψ_D ;
- все компоненты состояния автомата σ_D , кроме r -й компоненты, формируются в соответствии с функциями перехода φ_D , а r -я компонента состояния принудительно устанавливается равной s -й компоненте состояния автомата σ_E .

4. Операция подстановки сигнала вещания

Пусть $\sigma_D = (\mathbb{Z}^k, Q_D, V_D, G_D, +_D, L_D, \varphi_D, \psi_D)$, $\sigma_E = (\mathbb{Z}^k, Q_E, V_E, G_E, +_E, L_E, \varphi_E, \psi_E)$ — клеточные автоматы с локаторами, для которых выполнены следующие условия:

- $G_D = G_{D_1} \times \dots \times G_{D_{r-1}} \times G_{D_r} \times G_{D_{r+1}} \times \dots \times G_{D_n}$, $n \geq 1$,
- $G_E = G_{E_1} \times \dots \times G_{E_{s-1}} \times G_{E_s} \times G_{E_{s+1}} \times \dots \times G_{E_m}$, $m \geq 1$,
- $G_{D_r} = G_{E_s}$,
- $|V_D| = h - 1$, $|L_D| = l$, $|V_E| = p - 1$, $|L_E| = u$,
- $\psi_D = (\psi_{D_1}, \dots, \psi_{D_n})$, $\psi_{D_i} : Q_D^h \times G_D^l \rightarrow G_{D_i}$, $i \in \{1, \dots, n\}$,
- $\psi_E = (\psi_{E_1}, \dots, \psi_{E_m})$, $\psi_{E_i} : Q_E^p \times G_E^u \rightarrow G_{E_i}$, $i \in \{1, \dots, m\}$.

Тогда скажем, что клеточный автомат с локаторами

$$\sigma_F = (\mathbb{Z}^k, Q_F, V_F, G_F, +_F, L_F, \varphi_F, \psi_F)$$

получен из автоматов σ_D и σ_E с помощью подстановки в r -ю компоненту сигнала вещания автомата σ_D s -й компоненты сигнала вещания автомата σ_E (обозначим этот факт как $\sigma_F = B(\sigma_D, r, \sigma_E, s)$), если: $Q_F = Q_D \times Q_E$, $V_F = V_D \cup V_E$, $G_F = G_D \times G_E$, $+_F = +_D \times +_E$, $L_F = L_D \cup L_E$, $\varphi_F = (\varphi_D, \varphi_E)$, $\psi_F = (\psi_{D_1}, \dots, \psi_{D_{r-1}}, \psi_{E_s}, \psi_{D_{r+1}}, \dots, \psi_{D_n}, \psi_E)$.

Фактически результат функционирования автомата σ_F определяется следующим образом:

- автомат σ_E функционирует в соответствии со своими функциями φ_E и ψ_E ;
- автомат σ_D формирует состояния в соответствии со своей функцией переходов φ_D ;
- все компоненты сигнала вещания автомата σ_D , кроме r -й компоненты, формируются в соответствии с функциями вещания ψ_D , а r -я компонента сигнала вещания принудительно устанавливается равной s -й компоненте сигнала вещания автомата σ_E .

5. Операция введения управления

Пусть $\sigma = (\mathbb{Z}^k, Q, V, G, +, L, \varphi, \psi)$ — клеточный автомат с локаторами, где $|V| = h - 1$, $|L| = m$. Тогда скажем, что клеточный автомат с локаторами $\sigma_c = (\mathbb{Z}^k, Q_c, V, G_c, +_c, L_c, \varphi_c, \psi_c)$ получен из автомата σ с помощью операции введения управления (обозначим этот факт как $\sigma_c = C(\sigma)$), если $Q_c = Q \times G$, $G_c = G \times \{0, 1\}$; $+_c = +, \max$; $L_c = L \cup \{\Omega\}$; $\varphi_c : Q^h \times G^m \times G \times \{0, 1\} \rightarrow Q_c$, $\psi_c : Q^h \times G^m \times G \times \{0, 1\} \rightarrow G_c$, где для любого $\lambda \in Q^h \times G^m$ и любого $\gamma \in G$ выполняется: $\varphi_c(\lambda, \gamma, 0) = x_0$, $\varphi_c(\lambda, \gamma, 1) = (\varphi(\lambda), \psi(\lambda))$, $\psi_c(\lambda, \gamma, 0) = (\gamma, 0)$, $\psi_c(\lambda, \gamma, 1) = (\psi(\lambda), 0)$. Здесь $x_0 \in Q_c$ — состояние текущей ячейки.

Фактически результат функционирования автомата σ_c определяется следующим образом.

- К множеству состояний добавляются все компоненты множества сигналов вещания исходного автомата σ ($Q_c = Q \times G$).
- К сигналу вещания автомата σ добавляется ещё одна компонента (*компонента управления* или *компонента синхронизации*) со своим алфавитом вещания $\{0, 1\}$, заданной на нём полугрупповой функцией \max .
- К шаблону локаторов добавляется полный локатор $\{\Omega\}$, если его там не было.
- Модифицированная локальная функция переходов φ_c устроена таким образом, что, получив сигнал 0 по компоненте управления, ячейка сохраняет своё состояние. Получив сигнал 1 по компоненте управления, ячейка изменяет своё состояние: значения в исходных компонентах формируются в соответствии с исходной функцией φ , в добавленных компонентах — в соответствии с ψ (т.е. в добавленных компонентах состояния сохраняются те же значения, которые ячейка посылает в эфир).

- Похожим образом устроена модифицированная локальная функция вещания ψ_c . Получив по компоненте управления сигнал 1, ячейка осуществляет своё вещание в соответствии с исходной функцией ψ ; получив 0 — посылает в эфир тот же сигнал, который посылала в предыдущем такте (значение сигнала предыдущего такта сохранено в добавленных компонентах состояния). В эфир по компоненте управления ячейка всегда посылает сигнал 0.

6. Пример использования введённых операций для умножения чисел

В работе [2] описано решение клеточными автоматами с локаторами задачи умножения двух натуральных чисел a и b . Пусть $(a_n, a_{n-1}, \dots, a_1)$ — двоичное представление числа a , т.е. $a = \sum_{i=1}^n 2^{i-1} a_i$. Тогда $ab = \sum_{i=1}^n 2^{i-1} b a_i$.

Для вычисления произведения чисел a и b нужно одновременно выполнять три задачи, каждая из которых решается своим автоматом. С помощью автомата σ_{x2} решается задача вычисления чисел $b2^{i-1}$, $i = 1, 2, 3, \dots, n$. С помощью автомата σ_{12} находится двоичное представление числа a , т.е. получаются числа a_1, a_2, \dots, a_n . Автомат σ_{ct} накапливает суммы $S_i = \sum_{j=1}^i 2^{j-1} b a_j$, $i = 1, 2, \dots, n$, $S_0 = 0$. Также используется управляющий автомат σ_m , который синхронизирует работу этих автоматов.

Далее покажем, что автомат

$$\mu = B(S(\sigma_{ct}, 2, \sigma_{x2}, 1), 2, B(C(\sigma_{12}), 0, \sigma_m, 1), 3)$$

решает задачу умножения натуральных чисел и дадим формальные определения автоматов σ_{x2} , σ_{12} , σ_{ct} и σ_m .

6.1. Удвоение натурального числа

Зададим автомат, выполняющий удвоение заданного натурального числа. $\sigma_{x2} = (\mathbb{Z}^2, Q_{x2}, V_{x2}, G_{x2}, +_{x2}, L_{x2}, \varphi_{x2}, \psi_{x2})$, где $Q_{x2} = \{q_0, A, P, O\}$; $V_{x2} = \emptyset$; $G_{x2} = \{0, 1\}$; $+_{x2} = \max$; $L_{x2} = \{N, E, SE, S, W, NW\}$; $\psi_{x2} = 1$,

точно тогда, когда $x_0 = A \vee x_0 = P \vee x_0 = O$;

$$\varphi_{x_2} = \begin{cases} P & \text{если } x_0 = q_0 \wedge z_S = 1 \wedge z_E = 1; \\ q_0 & \text{если } (x_0 = A \wedge (z_E = 1 \vee z_N = 1)) \vee \\ & \vee (x_0 = P \wedge z_S = 1 \wedge z_W = 1); \\ A & \text{если } x_0 = q_0 \wedge ((z_{NW} = 1 \wedge z_W = 1) \vee (z_S = 1 \wedge z_{SE} = 1)); \\ x_0 & \text{во всех остальных случаях.} \end{cases}$$

Схематически функционирование автомата σ_{x_2} изображено на рисунке 1. Представлены первые 4 такта работы: в нулевом такте (начальное состояние) исходное число задано состоянием A , в первом такте строится проекция числа A , во втором такте получено удвоенное значение A . Каждые два такта автомат удваивает число. Легко заметить, что $R = 2^{\lfloor \frac{t}{2} \rfloor} x$, где R — результат работы автомата, x — исходное число, t — номер такта.

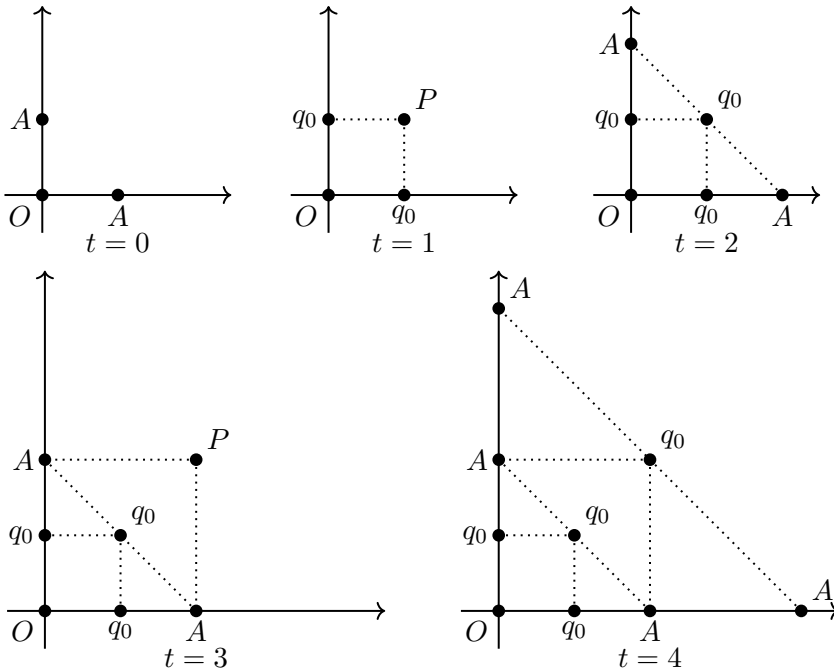


Рис. 1: Функционирование автомата σ_{x_2}

6.2. Перевод из унарного представления в двоичное

Зададим автомат σ_{12} , выполняющий перевод числа из унарного представления в двоичное. Точное решение задачи перевода числа из унарного представления в двоичное приведено в работах [3], [4]. Здесь будем использовать идейное описание такого автомата, представленное в работе [2].

Пусть a — натуральное число, $(a_n, a_{n-1}, \dots, a_1)$ — двоичное представление числа a . Задача перевода числа из унарного представления в двоичное формулируется следующим образом. В начальной конфигурации в активном состоянии находится $a + 1$ ячейка: ячейка $(0, 0)$ в состоянии «начало координат» и ячейки $(1, 0), (2, 0), \dots, (a, 0)$ в состоянии «один».

Задача состоит в том, чтобы в такты с первого по n -й выдавать в эфир сигнал «ноль», если $a_i = 0$, и сигнал «единица», если $a_i = 1$, $i \in \{1, 2, \dots, n\}$. При этом в финальной конфигурации активной остаётся только «начало координат». Здесь первым тактом считается такт, следующий после начального.

Алфавит вещания будет иметь вид $G = \{0, 1\} \times \{0, 1\} \times \{0, 1, 2, 3\}$. Полугрупповой операцией по первой компоненте будет сложение по модулю 2, а по второй и третьей — максимум. Первая компонента будет использоваться для вычисления a_i , $i \in \{1, 2, \dots, n\}$. Вторая компонента — для выявления момента окончания вычислений, а третья компонента — для передачи ответа. Состояние покоя будем обозначать как состояние «ноль». Алгоритм решения задачи будет следующий:

1. В каждый такт все ячейки, которые находятся в состоянии «один», передают в эфир сигнал $(1, 1, 0)$.
2. Ячейка в состоянии «один», которая в локатор «восток» получает сигнал $(0, *, *)$, переходит в состояние «ноль». Здесь * означает любой символ. Во всех остальных случаях ячейка не меняет состояние.
3. Если ячейка «начало координат» в локатор «восток» получает сигнал $(0, 1, 0)$, то она посылает в эфир сигнал $(0, 0, 0)$, что соответствует сигналу «ноль».
4. Если ячейка «начало координат» в локатор «восток» получает сигнал $(1, 1, 0)$, то она посылает в эфир сигнал $(0, 0, 1)$, что соответствует сигналу «единица».
5. Если ячейка «начало координат» в локатор «восток» получает сигнал $(0, 0, 0)$, то она посылает в эфир сигнал $(0, 0, 3)$, что соответствует окончанию передачи двоичного представления числа.

Строго говоря, в упомянутых работах окончанию передачи двоичного представления числа соответствует сигнал $(0, 0, 2)$. Нам же в дальнейшем потребуется различать нулевой и последний такт. Чтобы не переопределять σ_{12} , будем сразу использовать $(0, 0, 3)$.

Поскольку согласно пункту 1 каждая ячейка в состоянии «один» передаёт в эфир по первой компоненте значение «1», то «начало координат» получит в локатор «восток» по первой компоненте сумму по модулю 2 количества ячеек в состоянии «один», а это в первый момент равно a_1 . Второй пункт гарантирует, что каждый такт число ячеек в состоянии «один» будет сокращаться вдвое, поэтому во второй такт «начало координат» получит в локатор «восток» по первой компоненте значение a_2 и т.д. Если «начало координат» в локатор «восток» по второй компоненте получит значение «0», то это означает, что ячеек в состоянии «один» больше не осталось, и можно завершать работу.

В таблице 1 приведено поведение описанного выше клеточного автомата с локаторами для случая $a = 5$. Здесь символом Q обозначается строка состояний ячеек, причём O соответствует состоянию «начало координат»; 0 — состоянию «ноль»; 1 — состоянию «один»; символом S обозначается строка посылаемых «началом координат» в эфир сигналов; символом E — строка значений локатора «восток». В такты 1, 2, 3 в третьей компоненте сигнала вещания мы можем наблюдать двоичное представление числа 5 — $(1, 0, 1)$.

Дадим формальное описание:

$$\sigma_{12} = (\mathbb{Z}^2, Q_{12}, V_{12}, G_{12}, +_{12}, L_{12}, \varphi_{12}, \psi_{12}),$$

где $Q_{12} = \{q_0, O, O_1, 1\}$; $V_{12} = \emptyset$; $G_{12} = \{0, 1\} \times \{0, 1\} \times \{0, 1, 2, 3\}$; $+_{12} = +, \max, \max$; $L_{12} = \{E\}$;

$$\varphi_{12} = \begin{cases} q_0 & \text{если } x_0 = 1 \wedge z_E = (0, *, *), \text{ здесь } * \text{ означает любой символ;} \\ O_1 & \text{если } x_0 = O \vee x_0 = O_1; \\ x_0 & \text{во всех остальных случаях;} \end{cases}$$

$$\psi_{12} = \begin{cases} (1, 1, 0) & \text{если } x_0 = 1; \\ (0, 0, 0) & \text{если } x_0 = O_1 \wedge z_E = (0, 1, 0); \\ (0, 0, 1) & \text{если } x_0 = O_1 \wedge z_E = (1, 1, 0); \\ (0, 0, 3) & \text{если } x_0 = O_1 \wedge z_E = (0, 0, 0); \\ (0, 0, 2) & \text{если } x_0 = O; \\ (0, 0, 0) & \text{во всех остальных случаях.} \end{cases}$$

t		(0,0)	(1,0)	(2,0)	(3,0)	(4,0)	(5,0)
0	Q	O	1	1	1	1	1
	S	(0,0,2)	(1,1,0)	(1,1,0)	(1,1,0)	(1,1,0)	(1,1,0)
	E	(1,1,0)	(0,1,0)	(1,1,0)	(0,1,0)	(1,1,0)	(0,0,0)
1	Q	O ₁	q ₀	1	q ₀	1	q ₀
	S	(0,0,1)	(0,0,0)	(1,1,0)	(0,0,0)	(1,1,0)	(0,0,0)
	E	(0,1,0)	(0,1,0)	(1,1,0)	(1,1,0)	(0,0,0)	(0,0,0)
2	Q	O ₁	q ₀	1	q ₀	q ₀	q ₀
	S	(0,0,0)	(0,0,0)	(1,1,0)	(0,0,0)	(0,0,0)	(0,0,0)
	E	(1,1,0)	(1,1,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)
3	Q	O ₁	q ₀	q ₀	q ₀	q ₀	q ₀
	S	(0,0,1)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)
	E	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)
4	Q	O ₁	q ₀	q ₀	q ₀	q ₀	q ₀
	S	(0,0,3)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)
	E	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)

Таблица 1: Перевод числа из унарного представления в двоичное

6.3. Сложение чисел

Пусть a и b — целые числа, $a \geq 0$, $b > 0$. Автомат, выполняющий сложение $a + b$, описан в работе [2]. Идея его функционирования изображена на рисунке 2.

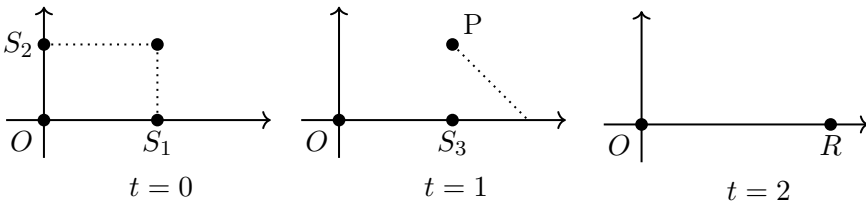


Рис. 2: Сложение целых чисел клеточным автоматом с локаторами

Внесём небольшие изменения в этот автомат и назовём σ_+ полученный автомат, выполняющий сложение $a + b$. Дадим формальное описание: $\sigma_+ = (\mathbb{Z}^2, Q_+, V_+, G_+, \max, L_+, \varphi_+, \psi_+)$, где $Q_+ = \{q_0, S_1, S_2, P_1, P_2, R\} \times \{q_0, O\}$;

$$V_+ = \emptyset; G_+ = \{0, 1, 2, 3\}; L_+ = \{W, S, NW\};$$

$$\varphi_+ = \begin{cases} (P_1, q_0) & \text{если } x_0 = (S_1, q_0); \\ (P_1, O) & \text{если } x_0 = (S_1, O); \\ (P_2, q_0) & \text{если } (x_0 = (q_0, q_0) \wedge z_S = 1 \wedge z_W = 1) \vee \\ & \vee (x_0 = (S_2, q_0) \wedge z_S = 3); \\ (q_0, O) & \text{если } x_0 = (P_1, O) \vee x_0 = (q_0, O); \\ (R, q_0) & \text{если } x_0 = (q_0, q_0) \wedge z_W = 2 \wedge z_{NW} = 2; \\ (q_0, q_0) & \text{во всех остальных случаях;} \end{cases}$$

$$\psi_+ = \begin{cases} 1 & \text{если } x_0 = (S_1, q_0) \vee x_0 = (S_2, q_0); \\ 2 & \text{если } x_0 = (P_1, q_0) \vee x_0 = (P_2, q_0) \vee x_0 = (P_1, O); \\ 3 & \text{если } x_0 = (S_1, O); \\ 0 & \text{во всех остальных случаях.} \end{cases}$$

В начальной конфигурации в отличном от (q_0, q_0) состоянии находятся ячейки:

- при $a > 0$: $(a, 0) - (S_1, q_0)$; $(0, 0) - (q_0, O)$; $(0, b) - (S_2, q_0)$;
- при $a = 0$: $(0, 0) - (S_1, O)$; $(0, b) - (S_2, q_0)$.

В финальной конфигурации в отличном от (q_0, q_0) состоянии находятся ячейки $(a + b, 0) - (R, q_0)$; $(0, 0) - (q_0, O)$.

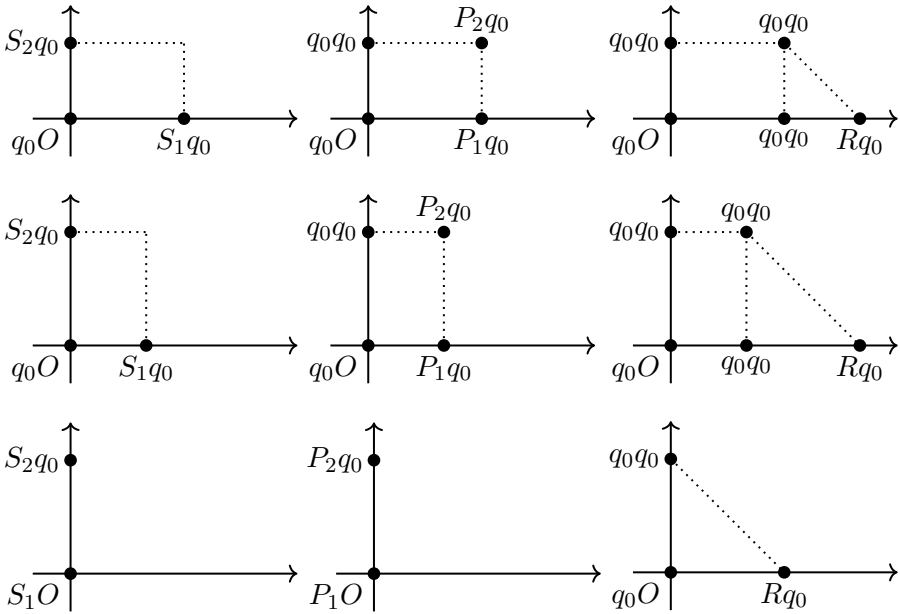
Изобразим работу автомата σ_+ на рисунке 3. В верхнем ряду рассмотрен случай для $0 < a < b$, в среднем — для $0 < b < a$, в нижнем — для $0 = a < b$.

6.4. Накопительный итог

На основе автомата σ_+ построим автомат σ_{ct} , который решает задачу расчёта накопительного итога — сложения поступившего числа с результатом предыдущего суммирования.

Добавим в шаблон локаторов автомата σ_+ полный локатор $\{\Omega\}$. К сигналу вещания автомата σ_+ добавим вторую компоненту. Алфавит вещания по этой компоненте: $\{0, 1, 2, 3\}$. Полугрупповая операция — максимум. В дальнейшем будем использовать её для подстановки сигнала вещания из σ_{12} в σ_{ct} .

К состоянию автомата σ_+ добавим компоненту: $\{q_0, A, P, O\}$. В дальнейшем будем использовать её для подстановки состояния из σ_{x2} в σ_{ct} .

Рис. 3: Диаграмма функционирования σ_+

Локальную функцию переходов зададим таким образом, чтобы ячейка $(a + b, 0)$ переходила не в состояние R , но в состояние S . Таким образом зациклим автомат — результат каждого суммирования будет сохраняться как первое слагаемое для следующего суммирования. В состоянии R ячейка будет переходить только в последнем такте работы.

Мы ввели вторую компоненту эфира с шаблоном локаторов $\{\Omega\}$. Так как Ω не включает вершину, при $S = 0$ ячейка в состоянии S не будет «слышать» значение, передаваемое в эфир «началом координат». Таким образом, приходим к тому, что нужно избежать равенства $S = 0$. Сделаем это следующим образом: в начальный момент примем $S = 1$, в последний такт работы вычтем эту единицу из результата. Кроме того, если в начальный момент времени $S = 0$, ячейка $(0, 0)$ должна одновременно принять состояние «начало координат» и S . Это требует введения дополнительной компоненты состояния или дополнительного состояния «начало координат и S одновременно». Чего мы избегаем, принимая $S = 1$ в начальный момент времени.

В начальной конфигурации в отличном от (q_0, q_0) состоянии находятся три или четыре ячейки.

- Если слагаемые не равны:

1. $(0, 0)$ в состоянии (O, O) («начало координат»);

2. $(1, 0)$ в состоянии (S, q_0) («слагаемое 1»);
 3. $(0, b)$ в состоянии (q_0, A) («слагаемое 2»).
 4. $(b, 0)$ в состоянии (q_0, A) («слагаемое 2»).
- Если слагаемые равны:
 1. $(0, 0)$ в состоянии (O, O) («начало координат»);
 2. $(1, 0)$ в состоянии (S, A) («слагаемое 1»);
 3. $(0, 1)$ в состоянии (q_0, A) («слагаемое 2»).

В финальной конфигурации в отличном от (q_0, q_0) состоянии находятся ячейки: $(x, 0)$ в состоянии (R, q_0) или (R, A) ; $(0, 0)$ в состоянии (O, O) , где x — значение накопленного итога.

Дадим формальное описание. $\sigma_{ct} = (\mathbb{Z}^2, Q_{ct}, V_{ct}, G_{ct}, \max, L_{ct}, \varphi_{ct}, \psi_{ct})$, где: $Q_{ct} = \{q_0, O, S, P, W, R\} \times \{q_0, O, A, P\}$; $V_{ct} = \{(1, 0)\}$; $G_{ct} = \{0, 1, 2\} \times \{0, 1, 2, 3\}$; $L_{ct} = \{S, W, NW, \Omega\}$;

$$\varphi_{ct} = \left\{ \begin{array}{ll} (P, q_0) & \text{если } (x_0 = (q_0, q_0) \wedge z_S = (2, *) \wedge z_W = (1, *) \wedge \\ & \wedge z_\Omega = (*, 1)) \vee (x_0 = (S, q_0) \wedge z_\Omega = (*, 1)); \\ (P, A) & \text{если } x_0 = (S, A) \wedge z_\Omega = (*, 1); \\ (q_0, q_0) & \text{если } (x_0 = (P, q_0)) \vee \\ & \vee (x_0 = (q_0, A) \wedge x_E \neq (S, *) \wedge z_\Omega = (*, 3)) \vee \\ & \vee (x_0 = (S, A) \wedge z_\Omega = (*, 3)) \vee \\ & \vee (x_0 = (S, q_0) \wedge z_\Omega = (*, 3)); \\ (q_0, A) & \text{если } x_0 = (P, A); \\ (S, q_0) & \text{если } (x_0 = (q_0, q_0) \wedge z_W = (2, *) \wedge z_{NW} = (2, *)) \vee \\ & \vee (x_0 = (W, q_0)); \\ (W, q_0) & \text{если } x_0 = (S, q_0) \wedge z_\Omega = (*, 0); \\ (W, A) & \text{если } x_0 = (S, A) \wedge z_\Omega = (*, 0); \\ (S, A) & \text{если } x_0 = (W, A); \\ (R, q_0) & \text{если } x_0 = (q_0, q_0) \wedge x_E = (S, *) \wedge z_\Omega = (*, 3); \\ (R, A) & \text{если } x_0 = (q_0, A) \wedge x_E = (S, *) \wedge z_\Omega = (*, 3); \\ x_0 & \text{во всех остальных случаях;} \end{array} \right.$$

$$\psi_{ct} = \begin{cases} (1, 0) & \text{если } x_0 = (q_0, A); \\ (2, 0) & \text{если } x_0 = (P, *) \vee x_0 = (S, *); \\ (0, 0) & \text{во всех остальных случаях.} \end{cases}$$

Рассмотрим сценарии функционирования автомата σ_{ct} . На рисунке 4 представлена работа автомата в случае значения «1» во второй компоненте эфира. Рассмотрены три случая (сверху вниз): $A > S$, $A = S$, $A < S$, где A и S - первое и второе слагаемые соответственно.

На рисунке 5 представлена работа автомата в случае значения «0» во второй компоненте эфира. Рассмотрены аналогичные три случая.

На рисунке 6 представлен последний такт работы автомата, в котором производится вычитание единицы, добавленной в первом такте. Формируется ячейка-ответ в состоянии R^* . Рассмотрены 4 случая: $S < A$, $S = A$, $S = A + 1$, $S > A + 1$, где A и S — первое и второе слагаемые соответственно.

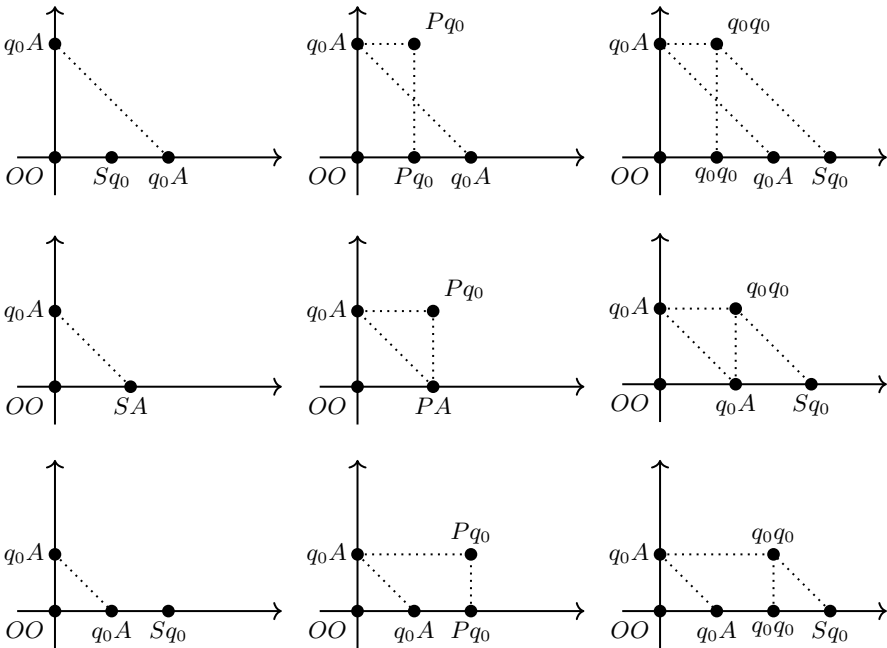


Рис. 4: Поведение автомата σ_{ct} при «1» во второй компоненте эфира

Получив значение «1» во второй компоненте эфира, автомат за два такта выполняет суммирование, где ячейка в состоянии S^* — первое сла-

гаемое, ячейка в состоянии $*A$ — второе слагаемое, результат сохраняется в ячейке с состоянием $S*$.

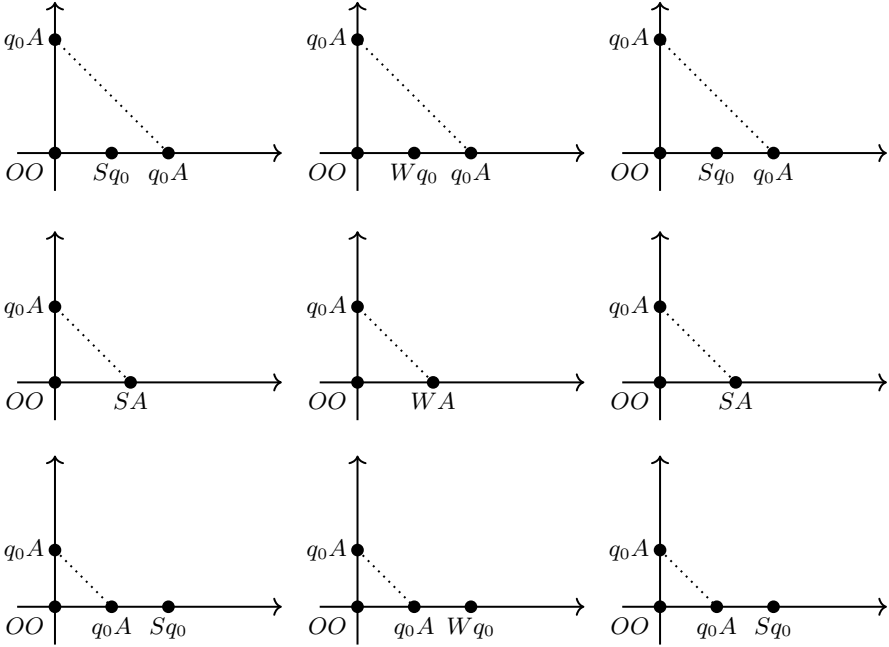


Рис. 5: Поведение автомата σ_{ct} при «0» во второй компоненте эфира

Получив значение «0» во второй компоненте эфира, автомат суммирования не производит — ячейка в состоянии $S*$ остаётся на своём месте. Для унификации с поведением при «1» во второй компоненте эфира автомат работает те же 2 такта.

Получив значение «3» во второй компоненте эфира, автомат формирует ответ в состоянии $R*$. Производится вычитание искусственно добавленной в нулевом такте единицы.

6.5. Управляющий автомат

Для формирования последовательности 1010... построим автомат σ_m . Последовательность 1010... будет передаваться в эфир ячейкой с координатами $(0, 0)$, находящейся попеременно в состояниях O_0 и O_1 . В начальный момент времени ячейка $(0, 0)$ находится в состоянии O_1 , остальные ячейки находятся в состоянии O .

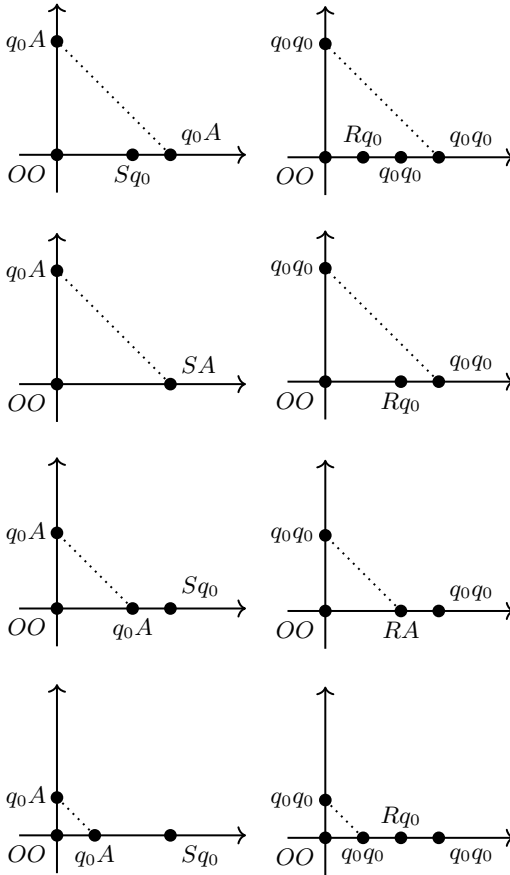


Рис. 6: Поведение автомата σ_{ct} при «3» во второй компоненте эфира

$\sigma_m = (\mathbb{Z}^2, Q_m, V_m, G_m, +_m, L_m, \varphi_m, \psi_m)$, где: $Q_m = \{O, O_0, O_1\}$; $V_m = \emptyset$; $G_m = \{0, 1\}$; $+_m = \max$; $L_m = \{\Omega\}$;

$$\begin{cases} \varphi_m = O & \text{если } x_0 = O; \\ \varphi_m = O_1 & \text{если } x_0 = O_0; \\ \varphi_m = O_0 & \text{если } x_0 = O_1; \end{cases}$$

$$\begin{cases} \psi_m = 0 & \text{если } x_0 \in \{O, O_0\}; \\ \psi_m = 1 & \text{если } x_0 = O_1. \end{cases}$$

6.6. Система клеточных автоматов с локаторами

Итак, перейдём к рассмотрению функционирования системы автоматов, заданной формулой

$$\mu = B(S(\sigma_{ct}, 2, \sigma_{x2}, 1), 2, B(C(\sigma_{12}), 0, \sigma_m, 1), 3)$$

Пусть a — натуральное число, $(a_n, a_{n-1}, \dots, a_1)$ — двоичное представление числа a . В такты с первого по n -ый автомат σ_{12} выдаёт в эфир сигнал «0», если $a_i = 0$, и сигнал «1», если $a_i = 1$, $i \in \mathbb{N}$. Автомат $B(C(\sigma_{12}), 0, \sigma_m, 1)$ формирует новое значение a_i только в нечётные такты. В последующие чётные такты в эфир выдаётся то же самое значение a_i .

В таблице 2 представлено функционирование $B(C(\sigma_{12}), 0, \sigma_m, 1)$ для перевода в двоичное представление числа 5.

Рассмотрим работу системы μ на примере умножения $3 \cdot 5$. В таблице 3 представлено функционирование системы μ .

Список литературы

- [1] Гасанов Э. Э., “Клеточные автоматы с локаторами”, *Интеллектуальные системы. Теория и приложения*, **24:2** (2020), 119–132.
- [2] Гасанов Э. Э., Хайбуллин Б. Ф., “Быстрые алгоритмы умножения и деления натуральных чисел с помощью клеточных автоматов с локаторами”, *Интеллектуальные системы. Теория и приложения*, **28:3** (2024), 103–130.
- [3] Гасанов Э. Э., “Клеточные автоматы с локаторами как модель устройств с беспроводной связью”, *Математические вопросы кибернетики*, **21** (2023), 5–51. DOI: 10.20948/mvk-2023-5.
- [4] Васильев Д. И., “Поиск ближайшего соседа на прямой с помощью клеточного автомата с локаторами”, *Интеллектуальные системы. Теория и приложения*, **24:3** (2020), 99–119.
- [5] Калачев Г. В., “Замечания к определению клеточного автомата с локаторами”, *Интеллектуальные системы. Теория и приложения*, **24:4** (2020), 47–56.

Статья поступила 27 мая 2026 г.

Operations on cellular automata with locators

A. V. Diubanov

t		$B(C(\sigma_{12}), 0, \sigma_m, 1)$						σ_m
		(0,0)	(1,0)	(2,0)	(3,0)	(4,0)	(5,0)	
0	Q	O	1	1	1	1	1	O_1
	S	(0,0,2)	(1,1,0)	(1,1,0)	(1,1,0)	(1,1,0)	(1,1,0)	1
	E	(1,1,0)	(0,1,0)	(1,1,0)	(0,1,0)	(1,1,0)	(0,0,0)	0
1	Q	O_1	0	1	0	1	0	O_0
	S	(0,0,1)	(0,0,0)	(1,1,0)	(0,0,0)	(1,1,0)	(0,0,0)	0
	E	(0,1,0)	(0,1,0)	(1,1,0)	(1,1,0)	(0,0,0)	(0,0,0)	0
2	Q	O_1	0	1	0	1	0	O_1
	S	(0,0,1)	(0,0,0)	(1,1,0)	(0,0,0)	(1,1,0)	(0,0,0)	1
	E	(0,1,0)	(0,1,0)	(1,1,0)	(1,1,0)	(0,0,0)	(0,0,0)	0
3	Q	O_1	0	1	0	0	0	O_0
	S	(0,0,0)	(0,0,0)	(1,1,0)	(0,0,0)	(0,0,0)	(0,0,0)	0
	E	(1,1,0)	(1,1,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	0
4	Q	O_1	0	1	0	0	0	O_1
	S	(0,0,0)	(0,0,0)	(1,1,0)	(0,0,0)	(0,0,0)	(0,0,0)	1
	E	(1,1,0)	(1,1,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	0
5	Q	O_1	0	0	0	0	0	O_0
	S	(0,0,1)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	0
	E	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	0
6	Q	O_1	0	0	0	0	0	O_1
	S	(0,0,1)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	1
	E	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	0
7	Q	O_1	0	0	0	0	0	O_0
	S	(0,0,3)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	0
	E	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	0
8	Q	O_1	0	0	0	0	0	O_1
	S	(0,0,3)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	1
	E	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	(0,0,0)	0

Таблица 2: Пример функционирования системы $B(C(\sigma_{12}), 0, \sigma_m, 1)$

$\mu = B(S(\sigma_{ct}, 2, \sigma_{x2}, 1), 2, B(C(\sigma_{12}), 0, \sigma_m, 1), 3)$									
Такт	0	1	2	3	4	5	6	7	8
σ_m	1	0	1	0	1	0	1	0	1
σ_{x2}	3	3	6	6	12	12	24	24	48
σ_{12}	2	1	1	0	0	1	1	3	3
σ_{ct}	S*(1,0) *A(3,0) *A(0,3)	S*(1,0) *A(3,0) *A(0,3)	P*(1,0) P*(1,3) *A(0,6) *A(6,0)	S*(4,0) *A(6,0) *A(0,6)	W*(4,0) *A(12,0) *A(0,12)	S*(4,0) *A(12,0) *A(0,12)	P*(4,0) P*(4,12) *A(0,24) *A(24,0)	S*(16,0) *A(24,0) *A(0,24)	R*(15,0) *A(48,0) *A(0,48)

Таблица 3: Пример функционирования системы автоматов μ

In this paper, operations on cellular automata with locators are proposed. These operations allow us to describe some cellular automaton with locators in the form of formulas over other cellular automaton with locators. As an example, a formula is constructed that defines a cellular automaton with locators equivalent to a cellular automaton with locators that performs multiplication of natural numbers in $2n + 2$ cycles.

Keywords: cellular automata with locators, superposition, formula.

References

- [1] Gasanov E. E., “Cellular automata with locators”, *Intelligent Systems. Theory and Applications*, **24:2** (2020), 119–132 (In Russian).
- [2] Gasanov E. E., Khaybullin B. F., “Fast algorithms for multiplication and division of natural numbers using cellular automata with locators”, *Intelligent Systems. Theory and Applications*, **28:3** (2024), 103–130 (In Russian).
- [3] Gasanov E. E., “Cellular automata with locators”, *Mathematical Problems of Cybernetics*, **21** (2023), 5–51. DOI: 10.20948/mvk-2023-5 (In Russian).
- [4] Vasilyev D. I., “The closest neighbour problem solution using the cellular automata with locators model”, *Intelligent Systems. Theory and Applications*, **24:3** (2020), 99–119 (In Russian).
- [5] Kalachev G. V., “Remarks on the Definition of Cellular Automaton with Locators”, *Intelligent Systems. Theory and Applications*, **24:4** (2020), 47–56 (In Russian).

Received on May 27, 2026

Верхняя линейная оценка для мощности области определения универсальной функции для пар линейных

А. С. Седова*

Ранее были исследованы задачи существования и оценки мощности области определения универсальных функций для различных классов функций в булевой и k -значной логиках. Для универсальной функции для пар линейных функций было доказано существование начиная с семи переменных. В данной работе, применив обобщения градиентного метода, получена верхняя линейная оценка мощности области определения универсальной функции для пар линейных функций.

Ключевые слова: линейная функция, универсальная функция, градиентный алгоритм, покрытие матрицы.

1. Введение

Понятие универсальной функции было введено в работе [1]. Далее были исследованы задачи о существовании, мощности области определения и представления в простом виде универсальных функций для различных классов. Далее в работе [2] было введено понятие универсальной функции для пар линейных. С помощью вероятностного метода доказано существование таких для линейных функций, зависящих не менее чем от семи аргументов. В настоящей работе продолжено исследование универсальных функций для пар, и получена оценка мощности области определения.

2. Постановка задачи

Далее, если особо не оговорено, будем считать функции булевыми, зависящими от переменных x_1, \dots, x_n . Далее (см., например, [3]) линейной функцией будем называть такую функцию $f(x_1, \dots, x_n)$, которая представима в виде

* Седова Анна Сергеевна — м.н.с. каф. информационной безопасности ф-та ВМК МГУ, e-mail: okuneva-anna@mail.ru, ORCID: 0009-0009-7424-0043.

Sedova Anna Sergeevna — Junior Researcher, Lomonosov Moscow State University, Faculty of Computational Mathematics and Cybernetics, Chair of Information Security.

$f(x_1, \dots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n$, где $a_i \in \{0, 1\}$. Ранее в работе [1] было введено понятие универсальной функции и поставлены основные задачи. Пусть задан некоторый класс функций K . Будем говорить, что функция f , зависящая от того же множества переменных, что и функции из класса K , порождает функцию g (при условии $g \in K$), если можно предъявить множество точек X , на котором $g(x)$ является единственной принадлежащей классу K функцией, такой, что для любого x из множества X выполняется соотношение $f(x) = g(x)$. Функция f называется универсальной для класса K , если она порождает любую функцию из данного класса. Основные задачи при исследовании универсальных функций для различных классов — это задачи существования и нахождения оценки мощности области определения и поиска представления в простой форме. В работе [1] была доказана нижняя оценка $2n + 2$ на мощность области определения универсальной функции для класса линейных функций от n переменных и верхняя, асимптотически равная $\frac{16}{5}n$. Впоследствии эти оценки были улучшены до $\frac{13}{6}n$ и $3n$ соответственно [4].

Для произвольной функции f будем обозначать функцию, принимающую противоположные значения во всех точках, через \bar{f} . Заметим, что если g_0 — произвольная булева функция, то для пары функций (g_0, \bar{g}_0) не существует точек, на которых они совпадают. Эту пару функций будем называть недопустимой. Остальные пары функций (g_0, g_1) такие, что $g_0 \in L \cap T_0$ и $g_1 \in L \cap \bar{T}_0$, будем называть допустимыми.

Функция $f(x_1, \dots, x_n)$ порождает допустимую пару линейных функций $(g_0(x_1, \dots, x_n), g_1(x_1, \dots, x_n))$, если можно предъявить множество наборов $X = \{\mathbf{x}_1, \dots, \mathbf{x}_n\}$, такое, что (g_0, g_1) является единственной допустимой парой функций, для которой при любых $i \in \{1, \dots, n\}$ выполнены соотношения $g_0(\mathbf{x}_i) = f(\mathbf{x}_i)$ и $g_1(\mathbf{x}_i) = \bar{f}(\mathbf{x}_i)$.

Заметим, что если f не порождает пару (g_0, g_1) , то для любого множества наборов $X = \{\mathbf{x}_1, \dots, \mathbf{x}_n\}$, на котором для любого $i \in \{1, \dots, n\}$ выполнено $f(\mathbf{x}_i) = g_0(\mathbf{x}_i) = g_1(\mathbf{x}_i)$, найдётся другая пара допустимых функций (g'_0, g'_1) , для которой при любых $i \in \{1, \dots, n\}$ выполнено равенство $f(\mathbf{x}_i) = g'_0(\mathbf{x}_i) = g'_1(\mathbf{x}_i)$.

Функция $f(x_1, \dots, x_n)$ называется универсальной функцией для пар линейных функций, если она порождает любую пару допустимых линейных функций.

3. Основные результаты

Теорема 1. *При $n \geq 13$ существует универсальная функция для пар линейных, имеющая мощность области определения не более $64n + 1$.*

Доказательство. Будем использовать градиентный алгоритм для решения задачи покрытия матриц (см. напр. [5], с. 136–137).

Построим $(0, 1)$ -матрицу, содержащую $N = 2^{n+1} - 2$ строк, такую, что каждому набору $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$, кроме нулевого, соответствуют две строки для $f(\alpha_1, \dots, \alpha_n) = 0$ и $f(\alpha_1, \dots, \alpha_n) = 1$. Строки, соответствующие нулевому набору, в матрице отсутствуют. Столбцы этой матрицы соответствуют упорядоченным парам различных допустимых пар функций $((g_0, g_1), (g'_0, g'_1))$. Подмножество строк матрицы, соответствующих набору $P = \{(\tilde{\alpha}_1, f(\tilde{\alpha}_1)), \dots, (\tilde{\alpha}_k, f(\tilde{\alpha}_k))\}$, является её допустимым покрытием, если в подматрице, образованной этими строками, нет нулевых столбцов и ни при каких $i \in \{1, \dots, k\}$ пары $(\tilde{\alpha}_i, f(\tilde{\alpha}_i) = 0)$ и $(\tilde{\alpha}_i, f(\tilde{\alpha}_i) = 1)$ не содержатся одновременно в P . Число различных линейных функций с фиксированным значением в нуле равно 2^n , следовательно, число столбцов M не превосходит 2^{4n} . Наличие единицы в позиции на пересечении строки, соответствующей набору $f(\alpha_1, \dots, \alpha_n) = \beta$, и столбца, соответствующего четвёрке функций $((g_0, g_1), (g'_0, g'_1))$, говорит о выполнении условия

$$\left[\begin{cases} g_0(\alpha_1, \dots, \alpha_n) = \beta, \\ g_1(\alpha_1, \dots, \alpha_n) = \beta, \\ g'_0(\alpha_1, \dots, \alpha_n) = \bar{\beta} \\ g_0(\alpha_1, \dots, \alpha_n) = \beta, \\ g_1(\alpha_1, \dots, \alpha_n) = \beta, \\ g'_1(\alpha_1, \dots, \alpha_n) = \bar{\beta}. \end{cases} \right. \quad (1)$$

Таким образом, соответствующий элемент матрицы, равный единице, показывает возможность на наборе отличить пару функций (g_0, g_1) от пары (g'_0, g'_1) . При этом покрытие матрицы обеспечивает возможность порождения любой допустимой пары линейных функций. Оценим долю единиц в столбце исходной матрицы. Зафиксируем столбец и соответствующую ему пару допустимых пар функций $((g_0, g_1), (g'_0, g'_1))$. Условие (1) на наличие единицы в позиции разобьём на две системы

$$\left\{ \begin{aligned} g_0(\alpha_1, \dots, \alpha_n) &= \beta, \\ g_1(\alpha_1, \dots, \alpha_n) &= \beta, \\ g'_0(\alpha_1, \dots, \alpha_n) \oplus 1 &= \beta. \end{aligned} \right. \quad (2)$$

$$\begin{cases} g_0(\alpha_1, \dots, \alpha_n) = \beta, \\ g_1(\alpha_1, \dots, \alpha_n) = \beta, \\ g'_1(\alpha_1, \dots, \alpha_n) \oplus 1 = \beta. \end{cases} \quad (3)$$

Оценим снизу число решений $(\alpha_1, \dots, \alpha_n, \beta)$ совокупности (1) через число решений систем (2) и (3). Заметим, что мощность множества решений системы (1) не менее, чем максимум из мощностей множеств, задаваемых одной из систем (2) или (3). Из построения для пары допустимых пар функций должно быть верно хотя бы одно из условий $g_0 \neq g'_0$ и $g_1 \neq g'_1$. Будем считать, что выполнено условие $g_0 \neq g'_0$.

Запишем систему (2) линейных уравнений относительно $(\alpha_1, \dots, \alpha_n, \beta)$.

$$\begin{cases} c_{0,1}\alpha_1 \oplus c_{0,2}\alpha_2 \oplus \dots \oplus c_{0,n}\alpha_n \oplus c_{0,0} = \beta, \\ c_{1,1}\alpha_1 \oplus c_{1,2}\alpha_2 \oplus \dots \oplus c_{1,n}\alpha_n \oplus c_{1,0} = \beta, \\ c'_{0,1}\alpha_1 \oplus c'_{0,2}\alpha_2 \oplus \dots \oplus c'_{0,n}\alpha_n \oplus c'_{0,0} \oplus 1 = \beta. \end{cases}$$

По построению, $c_{0,0} = 0, c'_{0,0} = 0, c_{1,0} = 1$.

$$\begin{cases} c_{0,1}\alpha_1 \oplus c_{0,2}\alpha_2 \oplus \dots \oplus c_{0,n}\alpha_n = \beta, \\ c_{1,1}\alpha_1 \oplus c_{1,2}\alpha_2 \oplus \dots \oplus c_{1,n}\alpha_n \oplus 1 = \beta, \\ c'_{0,1}\alpha_1 \oplus c'_{0,2}\alpha_2 \oplus \dots \oplus c'_{0,n}\alpha_n \oplus 1 = \beta. \end{cases} \quad (4)$$

Получим систему с $n + 1$ неизвестной и тремя линейно независимыми уравнениями. Следовательно, мощность множества решений системы (4) не менее, чем 2^{n-2} . Причём среди этих решений нет решения, соответствующего $(\alpha_1, \dots, \alpha_n) = (0, \dots, 0)$, так как подобная подстановка приводит к противоречию

$$\begin{cases} 0 = \beta, \\ 1 = \beta, \\ 0 = \beta. \end{cases}$$

Аналогичные рассуждения верны, если выполнено условие $g_1 \neq g'_1$. Так как число строк матрицы равно $2^{n+1} - 2$, то доля единиц в столбце не менее чем $\frac{1}{8}$.

Задача построения универсальной функции при этом сводится к задаче о покрытии матрицы с дополнительным ограничением: нельзя взять и строку, соответствующую $f(\alpha_1, \dots, \alpha_n) = 0$, и строку, соответствующую $f(\alpha_1, \dots, \alpha_n) = 1$.

Пусть в каждом столбце на каждом шаге доля единиц не меньше, чем γ' . Тогда в матрице не менее $\gamma' \cdot M_t \cdot N_t$ единиц, где N_t, M_t — число строк и столбцов на шаге t соответственно. Существует строка с не менее чем $\gamma' \cdot M_t$ единиц. Поэтому на каждом шаге число столбцов уменьшается, по крайней мере, с мультипликативной константой $(1 - \gamma')$.

При этом за t шагов при

$$(1 - \gamma')^t \leq \frac{1}{M} \quad (5)$$

градиентный алгоритм строит покрытие матрицы не более чем за $(t + 1)$ шагов.

Пусть сделано t шагов, тогда число единиц в столбце не менее чем $\frac{N}{8} - t$, так как на каждом шаге из непокрытых столбцов может быть удалено не более одной единицы, после удаления строки, соответствующей значению функции $f(\alpha_1, \dots, \alpha_n)$, противоположному взятому. При этом число строк после t шагов равно $N - 2t$, а значит, доля единиц в столбцах не менее $\frac{\frac{N}{8} - t}{N - 2t}$. Потребуем дополнительное ограничение на долю единиц в столбце после t шагов, положив $\gamma' = 1 - 2^{-\frac{1}{16}}$. Величину $(1 - \gamma')$ удобно логарифмировать. Получим неравенство

$$\frac{\frac{N}{8} - t}{N - 2t} \geq 1 - 2^{-\frac{1}{16}}. \quad (6)$$

С учётом ограничения на число столбцов из неравенства (5) получим систему

$$\begin{cases} \frac{\frac{N}{8} - t}{N - 2t} \geq 1 - 2^{-\frac{1}{16}}, \\ (1 - \gamma')^t \leq \frac{1}{2^{4n}}. \end{cases}$$

Откуда

$$(2^{-\frac{1}{16}})^t \leq \frac{1}{2^{4n}},$$

следовательно,

$$2^{-\frac{t}{16}} \leq 2^{-4n}.$$

Логарифмируя последнее неравенство, получим

$$\frac{t}{16} \geq 4n.$$

Таким образом, градиентный алгоритм при

$$t \geq 64n$$

строит покрытие матрицы при выполнении условия (6).

Для доказательства выполнения неравенства (6) воспользуемся промежуточным соотношением $0,05 \geq 1 - 2^{-\frac{1}{16}}$. При $\frac{N}{t} \geq 12$ выполняется неравенство $\frac{\frac{N}{8} - t}{N - 2t} \geq 0,05$, из которого вытекает неравенство (6).

Так как $N = 2^{n+1} - 2$, при $t \leq 64n + 1$ справедливо $\frac{N}{t} \geq \frac{2^{n+1} - 2}{64n + 1}$. При этом $\frac{2^{n+1} - 2}{64n + 1} \geq 12$ при $n \geq 13$.

Следовательно, при $n \geq 13$ функция f является универсальной для пар линейных функций. □

Список литературы

- [1] Вороненко А. А., “Об универсальных частичных функциях для класса линейных функций”, *Дискретная математика*, **24**:3 (2012. DOI: 10.4213/dm1197), 62–65.
- [2] Седова А.С., “Универсальные функции для пар линейных”, Проблемы теоретической кибернетики (Москва, 05–08 декабря 2024 года), 2024, 120–121.
- [3] Алексеев В.Б., *Дискретная математика*, М.: ИНФРА-М, 2021.
- [4] Вороненко, А.А., Вялый М.Н., “Нижняя оценка мощности области определения универсальных функций для класса линейных булевых функций”, *Дискретная математика*, **28**:4 (2016. DOI: 10.4213/dm1392), 50–57.
- [5] *Дискретная математика и математические вопросы кибернетики*, М.: Наука, **1**, ред. С.В. Яблонский, О.Б. Лупанов., 1974.

Статья поступила 30 апреля 2026 г.

Upper Linear Bound for the Cardinality of the Domain of a Universal Function for Pairs of linear

A. S. Sedova

Previously, the problems of existence and cardinality estimation of the domain of universal functions for various classes of functions in Boolean and k -valued logics were investigated. For the universal

function for pairs of linear functions, existence was proven starting from seven variables. We obtained an upper linear bound on the cardinality of the domain of the universal function for pairs of linear functions by applying generalizations of the gradient method.

Keywords: linear function, universal function, gradient algorithm, matrix covering.

References

- [1] Voronenko A.A., *Discrete Mathematics and Applications*, **22**:4 (2012. DOI: 10.1515/dma-2012-028), 421–425.
- [2] Sedova A.S., “Universal functions for pairs of linear functions”, *Problems of Theoretical Cybernetics* (Moscow, 05–08 December), 2024, 120–121 (In Russian).
- [3] Alekseev V.B., *Discrete mathematics*, M.: INFRA-M, 2021 (In Russian).
- [4] Voronenko A. A., Vyalyi M. N., “Lower estimate for the cardinality of the domain of universal functions for the class of linear Boolean functions”, *Discrete Mathematics and Applications*, **27**:5 (2017. DOI: 10.1515/dma-2017-0033), 319–324.
- [5] *Discrete Mathematics and Mathematical Issues of Cybernetics*, M.: Nauka, **1**, eds. S.V. Yablonsky, O.B. Lupanov., 1974 (In Russian).

Received on April 30, 2026

Часть 3
Математические модели

О K -порождаемости предполных классов линейных автоматов

В. А. Бирюкова*

Исследуется задача K -конечной порождаемости для предполных классов линейных автоматов над полем E_2 . Доказано, что не входящие в A -критериальную систему классы не являются K -конечнопорожденными. При этом была найдена счётная серия K -замкнутых K -конечнопорожденных классов. Также показано, что любой K -предполный класс, который не является K -конечнопорожденным, будет A -полным.

Ключевые слова: конечный автомат, линейный автомат, замкнутый класс, предполный класс, операции композиции, аппроксимационное замыкание, K -конечнопорожденность, базисы замкнутых классов.

1. Введение

Рассмотрим класс конечных автоматов $P_{O.-д.}$ с одним выходом. Для произвольного множества автоматов M обозначим через $K(M)$ его замыкание относительно операций композиции (K -замыкание): переименования входов, отождествления входов, подстановки и обратной связи [1]. Множество M будем называть K -замкнутым, если $K(M) = M$. Если $K(M) = P_{O.-д.}$, то M есть K -полное множество. Максимальное собственное K -замкнутое подмножество $P_{O.-д.}$ называется K -предполным классом.

Кольцо всех степенных рядов от ξ над полем $E_2 = \{0, 1\}$ обозначим как $R_2(\xi)$. Его подкольцо $E'_2(\xi)$ составляют ряды с периодической (с возможным предпериодом) последовательностью коэффициентов. Доказано [2], что элементы $E'_2(\xi)$ можно представить в виде дробей многочленов от ξ над E_2 , знаменатели которых не делятся на ξ .

Класс $P_{O.-д.}$ содержит в себе нетривиальный подкласс линейных автоматов L_2 [2]. Линейный автомат $f(x_1, x_2, \dots, x_n)$, имеющий n входов,

* *Бирюкова Вероника Андреевна* — аспирант кафедры Математической теории интеллектуальных систем (MaTIS), механико-математического факультета МГУ, e-mail: biryukovaveronika@mail.ru, ORCID: 0009-0006-7590-9800.

Biryukova Veronika Andreevna — PhD student at the Chair of Mathematical Theory of Intelligent Systems (MaTIS), Faculty of Mechanics and Mathematics, Lomonosov Moscow State University.

задаётся передаточными функциями $\mu_i, \mu_i \in E'_2(\xi), i = \overline{1, n}$, а также свободным членом $\mu_0 \in E'_2(\xi)$. Такой автомат ставит в соответствие каждому набору $(\alpha_1, \dots, \alpha_n)$ рядов из $R_2(\xi)$ ряд следующего вида [2]:

$$f(\alpha_1, \dots, \alpha_n) = \sum_{i=1}^n \mu_i \alpha_i + \mu_0 \tag{1}$$

Через $U(f)$ обозначим совокупность передаточных функций, ассоциированных с заданным линейным автоматом f . А через $U(\{f_1, \dots, f_p\}) = \bigcup_{i=1}^p U(f_i)$ — множество всех передаточных функций, ассоциированных хотя бы с одним автоматом из $\{f_1, \dots, f_p\}$. Свободный член (свободный ход) автомата f будем обозначать $C(f)$.

Для ряда $\alpha \in R_2(\xi)$ $\alpha(t)$ есть коэффициент при ξ^t . Если передаточная функция μ входа автомата такая, что $\mu(0) = 1$, то такой вход называется непосредственным.

Вход линейного автомата является существенным, если его передаточная функция $\mu \neq 0$. Линейный автомат без существенных переменных назовём константой.

Нетрудно видеть [3], что операции композиции задают на множестве коэффициентов μ_i переменных $x_i, i = \overline{1, n}$, линейного автомата $f(x_1, \dots, x_n)$ следующие операции:

1. Сложение элементов μ и $\tilde{\mu} : \mu + \tilde{\mu}$.
2. Умножение элементов $\mu, \tilde{\mu} : \mu \cdot \tilde{\mu}$.
3. Обратная связь, применённая к элементам μ и $\tilde{\mu}$ (при этом $\tilde{\mu}(0)$ должен равняться нулю): $Fb(\mu, \tilde{\mu}) = \frac{\mu}{1 + \tilde{\mu}}$.

Рассматривая $E'_2(\xi)$ как множество одноместных линейных автоматов, сохраняющих нулевую последовательность, к которым можно применять описанные выше операции, введём на нём оператор $K^{(1)}$ -замыкания. Аналогично K -замыканию, для $K^{(1)}$ -замыкания определяются понятия $K^{(1)}$ -замкнутого класса, $K^{(1)}$ -полного множества, $K^{(1)}$ -предполного класса, $K^{(1)}$ -конечнопорожденного класса.

Далее пронумеруем неприводимые многочлены над E_2 :

$$p_1 = \xi, p_2 = 1 + \xi, p_3 = 1 + \xi + \xi^2, \dots$$

И рассмотрим некоторые подмножества $E'_2(\xi)$:

$$R_0^{(1)} = \{ \mu \mid \mu \in E'_2(\xi), \mu = \frac{u}{v}, u, v \in E_2[\xi], (u, v) = 1, \deg u < \deg v \},$$

$$R_i^{(1)} = \{ \mu \mid \mu \in E'_2(\xi), \mu = \frac{u}{v}, u, v \in E_2[\xi], (u, v) = 1, u \vdots p_i \}, i \in \mathbb{N},$$

$$M_0^{(1)} = \{ \mu \mid \mu \in E'_2(\xi), \mu + \mu(0) = \frac{u'}{v'}, \deg u' < \deg v' \},$$

$$M_i^{(1)} = \{\mu \mid \mu \in E_2'(\xi), \mu + \mu(0) = \xi \cdot p_i \cdot \mu', \mu' = \frac{u'}{v'} \in E_2'(\xi), (v', p_i) = 1\}, i \in \mathbb{N}.$$

В статье [4] доказано, что $\mathcal{J}_2^{(1)} = \{M_i^{(1)}, R_i^{(1)} \mid i \in \mathbb{Z}_+\}$ — множество всех $K^{(1)}$ -предполных классов в $E_2'(\xi)$, которое также является $K^{(1)}$ -критериальной системой в $E_2'(\xi)$.

Определим следующие подмножества автоматов в L_2 :

$$T_0 = \{f \mid f \in L_2, \mu_0(0) = 0\},$$

$$T_1 = \{f \mid f \in L_2, \sum_{i=0}^n \mu_i(0) = 1\},$$

$$V_0 = \{f \mid f \in L_2, f \text{ имеет нечётное число непосредственных переменных}\},$$

$$V_1 = \{f \mid f \in L_2, f \text{ имеет не более 1 непосредственной переменной}\},$$

$$M_i = \{f \mid f \in L_2, \forall \mu \in U(f), \mu \in M_i^{(1)}\}, i \in \mathbb{Z}_+,$$

$$\tilde{M}_i = \{f \mid f \in L_2 : f(x_1, \dots, x_n) = \sum_{j=1}^n \mu_j x_j, \mu_j \in M_i^{(1)}, j = \overline{1, n}\} \subset M_i, i \in \mathbb{N} \setminus \{1\},$$

$$\mathbb{N} \setminus \{1\},$$

$$R_0^e = \{f \mid f \in L_2, \forall i \in \{1, \dots, n\}, \text{если } x_i \text{ — единственная существенная переменная } f, \mu_i = \frac{u_i}{v_i}, \text{то } \deg u_i \leq \deg v_i, \text{иначе } \mu_i \in R_0^{(1)}\},$$

$$R_0^d = \{f \mid f \in L_2, \forall i \in \{1, \dots, n\}, \text{если } x_i \text{ — единственная непосредственная переменная } f, \mu_i = \frac{u_i}{v_i}, \text{то } \deg u_i \leq \deg v_i, \text{иначе } \mu_i \in R_0^{(1)}\},$$

$$R_j^e = \{f \mid f \in L_2, \forall i \in \{1, \dots, n\}, \text{если } x_i \text{ — единственная существенная переменная } f, \mu_i = \frac{u_i}{v_i}, \text{то } v_i \not\sim p_j, \text{иначе } \mu_i \in R_j^{(1)}\} j \in \mathbb{N} \setminus \{1\},$$

$$R_j^d = \{f \mid f \in L_2, \forall i \in \{1, \dots, n\}, \text{если } x_i \text{ — единственная непосредственная переменная } f, \mu_i = \frac{u_i}{v_i}, \text{то } v_i \not\sim p_j, \text{иначе } \mu_i \in R_j^{(1)}\} j \in \mathbb{N} \setminus \{1\}.$$

Как показано в работе [4], $\mathcal{J}_2 = \{T_0, T_1, V_0, V_1, M_i, R_j^e, R_j^d \mid i \in \mathbb{Z}_+, j \in \mathbb{Z}_+ \setminus \{1\}\}$ есть множество всех K -предполных в L_2 классов, также это множество составляет K -критериальную систему L_2 . А в [3] доказано, что все классы, принадлежащие критериальной системе относительно -замыкания [5] $\mathcal{J}_A = \{T_0, T_1, V_0, V_1, M_1\}$ являются K -конечнопорожденными классами.

В данной статье доказываются несколько вспомогательных утверждений, K -конечнопорожденность K -замкнутых классов \tilde{M}_i , а также факт, что классы $M_i, i \in \mathbb{Z}_+ \setminus \{1\}, R_j^e, R_j^d, j \in \mathbb{Z}_+ \setminus \{1\}$ не являются K -конечнопорожденными.

2. Вспомогательные утверждения

Лемма 1. Пусть $M = \{f_1, \dots, f_p\} \subset L_2$ и каждый автомат из M сохраняет последовательность $C = c_0 c_1 \dots c_m$, $c_i \in E_2$, $i = \overline{0, m}$, $m \in \mathbb{Z}_+$. Тогда любой автомат из K -замыкания $K(M)$ также сохраняет C .

Доказательство. По условию каждый автомат из M сохраняет C . Продолжим C до формального степенного ряда

$$\tilde{C} = \sum_{s=0}^m c_s \xi^s + \sum_{s=m+1}^{\infty} d_s \xi^s \in R_2(\xi),$$

где d_s — произвольные коэффициенты (они не влияют на рассуждение, так как нас интересуют только первые $m + 1$ членов).

Из представления (1) следует, что сохранение C автоматом означает: при подаче на его входы ряда \tilde{C} выходной ряд совпадает с \tilde{C} на первых $m + 1$ членах.

Проверим, что каждая операция композиции сохраняет это свойство.

Переименование переменных не влияет на значение выхода автомата. При отождествлении переменных, если на все входы подана одна последовательность C , выходы исходного и преобразованного автоматов совпадают. Следовательно, полученный автомат также сохраняет C .

Без ограничения общности подставим f_i в n -й вход f_j . Поскольку f_i сохраняет C , на все входы f_j поступает последовательность C . Автомат f_j также сохраняет C , поэтому выход результирующего автомата на первых $m + 1$ членах совпадает с C .

Пусть в автомате $f_j \in M$ применена обратная связь по переменной x_n . Тогда $\mu_n(0) = 0$ и справедливо, что:

$$f_j(\tilde{C}, \dots, \tilde{C}) = \sum_{i=1}^{n-1} \mu_i \tilde{C} + \mu_n \tilde{C} + \mu_0 = \hat{C},$$

где \hat{C} — формальный степенной ряд, у которого первые $(m + 1)$ коэффициентов совпадают с последовательностью C .

Также верно:

$$\sum_{i=1}^{n-1} \mu_i \tilde{C} + \mu_0 = \hat{C} + \mu_n \tilde{C}.$$

По определению обратной связи [4]:

$$Fb_{x_n}(f_j) = \frac{1}{1 + \mu_n} \left(\sum_{i=1}^{n-1} \mu_i x_i + \mu_0 \right).$$

При подстановке в этот автомат на все входы \tilde{C} получаем:

$$\frac{1}{1 + \mu_n} \left(\sum_{i=1}^{n-1} \mu_i \tilde{C} + \mu_0 \right) = \frac{1}{1 + \mu_n} \left(\hat{C} + \mu_n \tilde{C} \right). \quad (2)$$

Поскольку \tilde{C} и \hat{C} совпадают на первых $(m + 1)$ членах, на этих членах ряд $\hat{C} + \mu_n \tilde{C}$ совпадает с $\tilde{C}(1 + \mu_n)$. Тогда, умножая на $\frac{1}{1 + \mu_n}$, получаем, что ряд (2) на первых $(m + 1)$ членах также совпадает с \tilde{C} , то есть с последовательностью C . Следовательно, полученный в результате применения операции обратной связи автомат также сохраняет C .

Таким образом, в K -замыкании множества M все автоматы сохраняют последовательность C . \square

Лемма 2. Пусть $p_i, i \in \mathbb{N}$, — неприводимый многочлен над E_2 , а $v \in E_2[\xi]: v(0) = 1, v \not\equiv p_i$. Тогда существует многочлен $\bar{u} \in E_2[\xi]$ такой, что $(1 + \xi \cdot p_i \cdot \bar{u}) \div v$, то есть $1 + \xi \cdot p_i \cdot \bar{u} = v \cdot \tilde{u}$ для некоторого $\tilde{u} \in E_2[\xi]$.

Доказательство. Рассмотрим остатки r_T от деления $(\xi \cdot p_i)^T$ на v для $T \in \mathbb{N}$. Поскольку множество таких остатков конечно, найдутся $T_1 < T_2$ с $r_{T_1} = r_{T_2}$. Следовательно,

$$((\xi \cdot p_i)^{T_1} + (\xi \cdot p_i)^{T_2}) \div v.$$

Вынося общий множитель, получаем

$$(\xi \cdot p_i)^{T_1} \cdot (1 + (\xi \cdot p_i)^{T_2 - T_1}) \div v. \quad (3)$$

Так как $v(0) = 1$, то $(\xi, v) = 1$, а из неприводимости p_i и условия $v \not\equiv p_i$ следует, что $(p_i, v) = 1$. Значит, $((\xi \cdot p_i)^{T_1}, v) = 1$. Отсюда и из (3) следует, что

$$(1 + (\xi \cdot p_i)^{T_2 - T_1}) \div v.$$

Заметим, что

$$1 + (\xi \cdot p_i)^{T_2 - T_1} = 1 + \xi \cdot p_i \cdot (\xi \cdot p_i)^{T_2 - T_1 - 1}.$$

Таким образом, в качестве \bar{u} можно взять $\bar{u} = (\xi \cdot p_i)^{T_2 - T_1 - 1}$. \square

Лемма 3. Пусть $p_i \in E_2[\xi], i \in \mathbb{N}$, — неприводимый многочлен степени s , а

$$M = \{1, \xi p_i \xi^m \mid m = \overline{0, s}\}.$$

Тогда $K^{(1)}(M) = M_i^{(1)}$.

Доказательство. Напомним определение класса $M_i^{(1)}$, соответствующего неприводимому многочлену $p_i = a_0 + a_1\xi + \dots + \xi^s \in E_2[\xi]$ ($i \in \mathbb{N}$):

$$M_i^{(1)} = \{ \mu \in E_2'(\xi) \mid \mu + \mu(0) = \xi p_i \mu', \mu' = u'/v' \in E_2'(\xi), (v', p_i) = 1 \}.$$

Отсюда для $\mu \in M_i^{(1)}$ возможны два случая:

- если $\mu(0) = 0$, то $\mu = \xi p_i \mu'$,
- если $\mu(0) = 1$, то $\mu = 1 + \xi p_i \mu'$.

Так как все элементы M принадлежат $M_i^{(1)}$, а сам класс $M_i^{(1)}$ $K^{(1)}$ -замкнут, то $K^{(1)}(M) \subseteq M_i^{(1)}$.

Докажем обратное включение. Сначала покажем по индукции, что $\xi p_i \xi^t \in K^{(1)}(M)$ для всех $t \in \mathbb{Z}_+$.

База индукции: для $t = \overline{0, s}$ это верно по определению M .

Индукционный переход: Пусть $t \geq s+1$ и для всех $t' < t$ уже доказано, что $\xi p_i \xi^{t'} \in K^{(1)}(M)$. Представим $t = q(s+1) + r$, где $q \in \mathbb{N}$, $0 \leq r \leq s$. Заметим, что

$$(\xi p_i)(\xi p_i) = (\xi p_i) \cdot (a_0\xi + a_1\xi^2 + \dots + \xi^{s+1}).$$

Тогда, используя, уже полученные элементы $\xi p_i \xi^{m+r}$ для $m = q, \dots, (s+1)q - 1$ (для которых $m + r < t$), получаем:

$$(\xi p_i \xi^r)(\xi p_i)^q + \sum_{m=q}^{(s+1)q-1} \xi p_i \xi^{m+r} \cdot b_m = \xi p_i \xi^{q(s+1)+r} = \xi p_i \xi^t \in K^{(1)}(M),$$

где b_m — коэффициенты многочлена p_i^q при ξ^{m-q} . Таким образом, индукционный шаг выполнен. Следовательно, $\xi p_i \xi^t \in K^{(1)}(M)$ для любого $t \in \mathbb{Z}_+$.

Для произвольного многочлена $u(\xi) = b'_0 + b'_1\xi + \dots + b'_n\xi^n \in E_2[\xi]$ имеем следующее:

$$\xi p_i \cdot u = \sum_{j=0}^n \xi p_i \xi^j b'_j \in K^{(1)}(M).$$

Далее, пусть $\mu = u/v \in E_2'(\xi)$, $u, v \in E_2[\xi]$, $(u, v) = 1$, $v \not\sim p_i$. По лемме 2, для такого v существует $\bar{u} \in E_2[\xi] : (1 + \xi p_i \bar{u}) \mid v$, т.е. $1 + \xi p_i \bar{u} = v \tilde{u}$ для некоторого $\tilde{u} \in E_2[\xi]$.

Элементы $\xi p_i u \tilde{u}$ и $\xi p_i \bar{u}$ принадлежат $K^{(1)}(M)$ по доказанному выше. Применим к ним операцию обратной связи:

$$Fb(\xi p_i u \tilde{u}, \xi p_i \bar{u}) = \frac{\xi p_i u \tilde{u}}{1 + \xi p_i \bar{u}} = \frac{\xi p_i u \tilde{u}}{v \tilde{u}} = \frac{\xi p_i u}{v} \in K^{(1)}(M).$$

Таким образом, $\xi p_i \cdot \frac{u}{v} \in K^{(1)}(M)$ для любой правильной дроби $\mu = u/v$ с $v \not\equiv p_i$.

Каждый элемент $M_i^{(1)}$ имеет вид либо $\xi p_i \mu$, либо $1 + \xi p_i \mu$ с указанными ранее свойствами. Следовательно, $M_i^{(1)} \subseteq K^{(1)}(M)$.

Из двух включений получаем $K^{(1)}(M) = M_i^{(1)}$. □

3. Основные результаты

Лемма 4. *Класс \tilde{M}_i ($i \in \mathbb{N} \setminus \{1\}$) является K -конечнопорожденным. Базис \tilde{M}_i — множество*

$$M = \left\{ x_1 + x_2, \sum_{m=0}^s \xi p_i \xi^m x_m \right\},$$

где p_i — неприводимый над E_2 многочлен степени s , соответствующий предполному классу линейных автоматов M_i .

Доказательство. Рассмотрим класс \tilde{M}_i , состоящий из всех автоматов класса M_i с нулевым свободным членом:

$$\tilde{M}_i = \left\{ f \in L_2 \mid f(x_1, \dots, x_n) = \sum_{j=1}^n \mu_j x_j, \mu_j \in M_i^{(1)} \right\}, \quad (4)$$

где $M_i^{(1)} = \{ \mu \in E_2'(\xi) \mid \mu + \mu(0) = \xi p_i \mu', \mu' = u'/v' \in E_2'(\xi), (v', p_i) = 1 \}$.

Докажем, что \tilde{M}_i K -замкнут.

1. Каждый автомат из \tilde{M}_i сохраняет нулевую последовательность. По лемме 1, в K -замыкании множества таких автоматов можно получить только автоматы, сохраняющие нулевую последовательность, т.е. с нулевым свободным членом.
2. Коэффициенты μ_j принадлежат классу $M_i^{(1)}$, который $K^{(1)}$ -замкнут. Напомним, что операции композиции над линейными автоматами индуцируют $K^{(1)}$ -операции над их коэффициентами. Следовательно, при замыкании коэффициенты остаются в $M_i^{(1)}$.

Из пунктов 1 и 2 следует, что \tilde{M}_i K -замкнут.

Покажем, что \tilde{M}_i K -конечнопорожден. Рассмотрим множество M , состоящее из следующих двух автоматов:

- $f_1 = x_1 + x_2$;
- $f_2 = \sum_{m=0}^s \xi p_i \xi^m x_m$.

Автоматы f_1 и f_2 имеют нулевые свободные члены, а коэффициенты при их переменных $U(\{f_1, f_2\}) = \{1, \xi p_i \xi^m \mid m = \overline{0, s}\}$ лежат в $M_i^{(1)}$. Следовательно, $f_1, f_2 \in \tilde{M}_i$. В силу K -замкнутости \tilde{M}_i (доказано выше) получаем $K(M) \subseteq \tilde{M}_i$.

Отождествив переменные в f_1 , получим $x_1 + x_1 = 0$, т.е. $0 \in K(M)$. Кроме того, $f_1(0, x) = 1 \cdot x \in K(M)$, следовательно, $x \in K(M)$.

Подставляя нулевой автомат в f_2 , получаем все автоматы вида $\xi p_i \xi^m x$ ($m = \overline{0, s}$). По лемме 3 множество $\{1, \xi p_i \xi^m \mid m = \overline{0, s}\}$ порождает класс $M_i^{(1)}$ относительно $K^{(1)}$ -операций. Поскольку операции композиции над автоматами индуцируют $K^{(1)}$ -операции над их коэффициентами, то в $K(M)$ можно получить любой автомат вида μx с $\mu \in M_i^{(1)}$.

При подстановке f_1 в самого себя получим сумматор от любого числа переменных. Подставляя в этот сумматор автоматы $\mu_1 x_1, \dots, \mu_n x_n$, получим произвольный автомат из \tilde{M}_i (4). Следовательно, $\tilde{M}_i \subseteq K(M)$.

Из двух включений $K(M) \subseteq \tilde{M}_i$ и $\tilde{M}_i \subseteq K(M)$ получаем $K(M) = \tilde{M}_i$.

В K -замыкании автомата f_1 получаются только сумматоры, поэтому f_1 не порождает \tilde{M}_i . В $K^{(1)}$ -замыкании коэффициентов автомата f_2 отсутствует 1, поскольку все эти коэффициенты принадлежат $K^{(1)}$ -замкнутому классу $R_1^{(1)}$, а $1 \notin R_1^{(1)}$. Следовательно, $1 \cdot x \notin K(\{f_2\})$, но $1 \cdot x \in \tilde{M}_i$. Значит, f_2 также не порождает \tilde{M}_i самостоятельно. Таким образом, M является базисом класса \tilde{M}_i . \square

Лемма 5. *K -предполный класс M_0 не может быть порождён конечным множеством линейных автоматов относительно операций композиции.*

Доказательство. Напомним, что

$$M_0 = \{f \in L_2 \mid \forall \mu \in U(f) \ \mu \in M_0^{(1)}\},$$

где $M_0^{(1)} = \{\mu \in E_2'(\xi) \mid \mu + \mu(0) = u'/v', \ u', v' \in E_2[\xi], \ \deg u' < \deg v'\}$. Следовательно, для любого $\mu \in M_0^{(1)}$ выполнено $\deg u \leq \deg v$ (в представлении $\mu = u/v$), поскольку если $\mu(0) = 0$, то $\deg u < \deg v$; если $\mu(0) = 1$, то $\deg u = \deg v$.

Любой автомат $f \in M_0$ имеет вид

$$f(x_1, \dots, x_n) = \sum_{i=1}^n \mu_i x_i + \mu_0, \quad \mu_i \in M_0^{(1)}, \mu_0 \in E_2'(\xi).$$

Предположим, что M_0 порождается конечным множеством линейных автоматов $\{f_1, \dots, f_p\} \subset M_0$. Покажем, что это приводит к противоречию.

Проанализируем, как меняется свободный член под действием операций композиции.

Переименование переменных не влияет на коэффициенты и свободный ход автомата. Отождествление переменных, хотя и изменяет коэффициенты, не затрагивает свободный член, поэтому разность степеней числителя и знаменателя свободного хода сохраняется.

Пусть $f, g \in M_0$. Тогда они имеют следующий вид:

$$f(x_1, \dots, x_n) = \sum_{i=1}^{n-1} \mu_i x_i + \mu_n x_n + \mu_0, \quad g(x'_1, \dots, x'_m) = \sum_{j=1}^m \mu'_j x'_j + \mu'_0.$$

Подставим g в f на вход x_n (без ограничения общности):

$$f(x_1, \dots, x_{n-1}, g(x'_1, \dots, x'_m)) = \sum_{i=1}^{n-1} \mu_i x_i + \sum_{j=1}^m \mu_n \mu'_j x'_j + (\mu_n \mu'_0 + \mu_0).$$

Обозначим

$$\mu_n = \frac{u}{v}, \quad \mu'_0 = \frac{u_1}{v_1}, \quad \mu_0 = \frac{u_2}{v_2}.$$

Тогда

$$\tilde{\mu}_0 = \mu_n \mu'_0 + \mu_0 = \frac{uu_1v_2 + u_2vv_1}{vv_1v_2}.$$

Степень числителя не превосходит $\max(\deg(uu_1v_2), \deg(u_2vv_1))$. В первом случае:

$$\deg(uu_1v_2) - \deg(vv_1v_2) = (\deg u_1 - \deg v_1) + (\deg u - \deg v) \leq (\deg u_1 - \deg v_1),$$

поскольку $\mu_n \in M_0^{(1)}$ и $\deg u \leq \deg v$.

Во втором случае:

$$\deg(u_2vv_1) - \deg(vv_1v_2) = \deg u_2 - \deg v_2.$$

Итак, разность степеней числителя и знаменателя свободного члена при подстановке не превосходит максимальной из соответствующих разностей для f и g .

Пусть в автомате f применена обратная связь по x_n (без ограничения общности), то есть $\mu_n(0) = 0$ (тогда $\deg u < \deg v$). Получаем:

$$Fb_{x_n}(f) = \sum_{i=1}^{n-1} \frac{\mu_i}{1 + \mu_n} x_i + \frac{\mu_0}{1 + \mu_n}.$$

Для свободного члена имеем:

$$\frac{\mu_0}{1 + \mu_n} = \frac{u_2/v_2}{1 + u/v} = \frac{u_2v}{v_2(u + v)}.$$

Так как $\deg(u + v) = \deg v$, находим:

$$\deg(u_2v) - \deg(v_2(u + v)) = \deg u_2 - \deg v_2.$$

Значит, разность степеней числителя и знаменателя свободного члена при обратной связи не увеличивается.

Таким образом, все операции композиции не увеличивают разность степеней у свободного члена автомата. Исходное конечное множество $\{f_1, \dots, f_p\}$ имеет некоторую максимальную разность степеней свободного члена k_0 . Следовательно, ни один автомат из $K(\{f_1, \dots, f_p\})$ не может иметь свободный член с разностью степеней больше k_0 . Однако в M_0 есть автоматы с любой наперёд заданной разностью. Противоречие. Значит, M_0 не является K -конечнопорожденным классом. \square

Лемма 6. K -предполный класс R_0^d не является K -конечнопорожденным.

Доказательство. По определению класса R_0^d :

$$R_0^d = \{f \mid f \in L_2, \forall i = \overline{1, n}, \text{ если } x_i \text{ — единственная непосредственная переменная } f, \mu_i = \frac{u_i}{v_i}, \text{ то } \deg u_i \leq \deg v_i, \text{ иначе } \mu_i \in R_0^{(1)}\}$$

Таким образом, для каждого автомата f из R_0^d верно следующее:

$$f(x_1, \dots, x_n) = \sum_{i=1}^n \mu_i x_i + \mu_0, \quad \mu_0 \in E_2'(\xi),$$

и для всех i имеем $\deg u_i \leq \deg v_i$ (где $\mu_i = u_i/v_i$).

Предположим, что R_0^d порождается конечным множеством автоматов $\{f_1, \dots, f_p\} \subset R_0^d$.

Проанализируем, как меняется свободный член при применении операций подстановки и обратной связи (переименование и отождествление переменных не влияют на него).

Как показано в доказательстве леммы 5, при подстановке разность степеней свободного члена не может превысить наибольшую из разностей исходных автоматов. Это рассуждение остаётся справедливым и для класса R_0^d , поскольку для любого коэффициента μ автомата из R_0^d выполнено $\deg u \leq \deg v$.

Пусть в автомате f применена обратная связь по переменной x_n . Следовательно, она не является непосредственной, и $\mu_n \in R_0^{(1)}$, то есть $\deg u < \deg v$ (в представлении $\mu_n = u/v$), а, значит $\deg(u + v) = \deg v$.

Для свободного члена имеем:

$$\frac{\mu_0}{1 + \mu_n} = \frac{u'/v'}{1 + u/v} = \frac{u'v}{v'(u + v)}.$$

Следовательно,

$$\deg(u'v) - \deg(v'(u + v)) = \deg u' + \deg v - \deg v' - \deg v = \deg u' - \deg v'.$$

Таким образом, операция обратной связи не меняет разность степеней свободного хода.

Итак, ни одна из операций композиции не позволяет превысить исходную максимальную разность степеней свободного члена. Пусть k_0 — наибольшая из разностей степеней свободных членов автоматов f_1, \dots, f_p . Тогда в $K(\{f_1, \dots, f_p\})$ все автоматы имеют разность степеней свободного хода не более k_0 . А в R_0^d существуют автоматы с разностью k для любого $k \in \mathbb{N}$. Пришли к противоречию, следовательно R_0^d не является K -конечнопорожденным. \square

Лемма 7. *K -предполный класс R_0^e нельзя породить конечным множеством автоматов относительно операций композиции.*

Доказательство. Вспомним определение класса R_0^e :

$R_0^e = \{f \mid f \in L_2, \forall i \in \{1, \dots, n\}, \text{ если } x_i \text{ — единственная существенная переменная } f, \mu_i = \frac{u_i}{v_i}, \text{ то } \deg u_i \leq \deg v_i, \text{ иначе } \mu_i \in R_0^{(1)}\}$,

Из определения следует, что каждый автомат $f \in R_0^e$ представим в виде:

$$f(x_1, \dots, x_n) = \sum_{i=1}^n \mu_i x_i + \mu_0, \quad \mu_0 \in E_2'(\xi),$$

и для всех i имеем $\deg u_i \leq \deg v_i$ (где $\mu_i = u_i/v_i$).

Пусть $\{f_1, \dots, f_p\} \subset R_0^e$ — конечное множество, порождающее R_0^e . Среди этих автоматов есть хотя бы один с более чем одной существенной переменной (иначе породить весь класс невозможно). Поскольку такой

автомат принадлежит R_0^e и имеет более одной существенной переменной, для всех его коэффициентов $\mu_i = u_i/v_i$ выполнено $\deg u_i < \deg v_i$.

Установим, что нельзя для любого $n \in \mathbb{N}$ в $K(\{f_1, \dots, f_p\})$ получить автомат от n переменных, у которого каждый коэффициент μ_i имеет разность $\deg v_i - \deg u_i = 1$.

Переименование переменных не меняет количества существенных переменных. Отождествление переменных и обратная связь уменьшают их число, поэтому для увеличения числа переменных эти операции не подходят.

Рассмотрим подстановку автомата g на q -й вход (без ограничения общности) f , где $f, g \in R_0^e$:

$$f(x_1, \dots, x_q) = \sum_{i=1}^q \mu_i x_i + \mu_0, \quad g(x'_1, \dots, x'_m) = \sum_{j=1}^m \mu'_j x'_j + \mu'_0.$$

Тогда

$$\begin{aligned} \tilde{f}(x_1, \dots, x_{q-1}, x'_1, \dots, x'_m) &= f(x_1, \dots, x_{q-1}, g(x'_1, \dots, x'_m)) = \\ &= \sum_{i=1}^{q-1} \mu_i x_i + \sum_{j=1}^m \mu_q \mu'_j x'_j + (\mu_q \mu'_0 + \mu_0). \end{aligned}$$

Число переменных результата равно $q + m - 1$. Для нашей цели достаточно рассматривать случаи $q > 1$ и $m > 1$. Тогда все коэффициенты μ_i, μ'_j принадлежат $R_0^{(1)}$, то есть $\deg u_i < \deg v_i$ и $\deg u'_j < \deg v'_j$.

Проанализируем коэффициенты полученного автомата:

1. Коэффициенты μ_i ($i = \overline{1, q-1}$) не изменились, их разность $\deg v_i - \deg u_i \geq 1$ сохранилась.
2. Коэффициенты $\mu_q \mu'_j = \frac{u_q u'_j}{v_q v'_j}$ имеют разность

$$\deg(v_q v'_j) - \deg(u_q u'_j) = (\deg v_q - \deg u_q) + (\deg v'_j - \deg u'_j) \geq 2.$$

Следовательно, у автомата \tilde{f} число коэффициентов с разностью, равной 1, не больше, чем у исходного автомата, в который производилась подстановка.

Таким образом, нельзя с помощью операций композиции из конечного множества автоматов из R_0^e получить для любого $n \geq 2$ автомат от n переменных, у которого все коэффициенты при переменных имеют

разность $\deg v_i - \deg u_i = 1$. Значит, R_0^c — не K -конечнопорожденный класс. □

Лемма 8. *K -предполные классы M_i ($i \in \mathbb{N} \setminus \{1\}$) не являются K -конечнопорожденными.*

Доказательство. Для классов M_i справедливо следующее:

$$M_i = \{f \in L_2 \mid \forall \mu \in U(f), \mu \in M_i^{(1)}\},$$

где

$$M_i^{(1)} = \{\mu \in E_2'(\xi) \mid \mu + \mu(0) = \xi p_i \mu', \mu' = u'/v' \in E_2'(\xi), (v', p_i) = 1\}.$$

Для произвольного автомата f из M_i выполнено:

$$f(x_1, \dots, x_n) = \sum_{j=1}^n \mu_j x_j + \mu_0, \quad \mu_j \in M_i^{(1)}, \mu_0 \in E_2'(\xi).$$

В классе M_i есть автоматы с любым свободным членом из $E_2'(\xi)$. В частности, существуют константы вида

$$\mu = \frac{u}{v \cdot p_i^d}, \quad u, v \in E_2[\xi], (u, v) = 1, u, v \not\sim p_i, d \in \mathbb{N}.$$

Ниже доказывается, что из конечного множества автоматов из M_i с помощью операций композиции нельзя для произвольного $d, d \in \mathbb{N}$, получить автомат, свободный член которого имеет указанный вид.

Пусть $\{f_1, \dots, f_p\} \subset M_i$ — конечное множество, порождающее M_i . Рассмотрим операции подстановки и обратной связи для $f, g \in M_i$:

$$f(x_1, \dots, x_n) = \sum_{i=1}^n \mu_i x_i + \mu_0, \quad g(x'_1, \dots, x'_m) = \sum_{j=1}^m \mu'_j x'_j + \mu'_0.$$

Подставим g на n -й вход f (без ограничения общности):

$$f(x_1, \dots, x_{n-1}, g) = \sum_{i=1}^{n-1} \mu_i x_i + \sum_{j=1}^m \mu_n \mu'_j x'_j + (\mu_n \mu'_0 + \mu_0).$$

Обозначим

$$\begin{aligned} \mu_n &= \frac{u}{v}, \quad (u, v) = 1, v \not\sim p_i, \\ \mu'_0 &= \frac{u_1}{v_1 p_i^{d_1}}, \quad \mu_0 = \frac{u_2}{v_2 p_i^{d_2}}, \end{aligned}$$

с $(u_1, v_1) = (u_2, v_2) = 1$, $v_1, v_2 \not\vdash p_i$, $d_1, d_2 \in \mathbb{Z}_+$.

Тогда, полагая $d_x = \max(d_1, d_2)$, получаем

$$\tilde{\mu}_0 = \mu_n \mu'_0 + \mu_0 = \frac{u u_1 v_2 p_i^{d_x - d_1} + u_2 v v_1 p_i^{d_x - d_2}}{v v_1 v_2 p_i^{d_x}}.$$

Следовательно, степень p_i в знаменателе свободного члена при подстановке не превосходит максимума из исходных степеней d_1 и d_2 .

Пусть к переменной x_n автомата f применима обратная связь, т.е. $\mu_n(0) = 0$. Из $\mu_n \in M_i^{(1)}$ следует, что $\mu_n = \frac{\xi p_i u}{v}$, $(u, v) = 1$, $v \not\vdash p_i$.

Операция обратной связи даёт

$$Fb_{x_n}(f) = \sum_{i=1}^{n-1} \frac{\mu_i}{1 + \mu_n} x_i + \frac{\mu_0}{1 + \mu_n}.$$

Запишем $\mu_0 = \frac{u_1}{v_1 p_i^d}$, $(u_1, v_1) = 1$, $v_1 \not\vdash p_i$, $d \in \mathbb{Z}_+$. Тогда

$$\frac{\mu_0}{1 + \mu_n} = \frac{u_1}{v_1 p_i^d} \cdot \frac{v}{\xi p_i u + v}.$$

Поскольку $(\xi p_i u + v) \not\vdash p_i$, степень p_i в знаменателе не увеличивается.

Получили, что ни одна из операций композиции не позволяет увеличить степень p_i в знаменателе свободного члена сверх максимальной степени, присутствующей в исходном конечном множестве. Значит, из конечного множества автоматов из M_i нельзя получить автомат со свободным членом $\frac{u}{v \cdot p_i^d}$ для произвольного $d \in \mathbb{N}$. Таким образом, M_i ($i \in \mathbb{N} \setminus \{1\}$) не являются K -конечнопорожденными классами. □

Лемма 9. *K -предполные классы R_i^d ($i \in \mathbb{N} \setminus \{1\}$) нельзя породить конечным множеством автоматов относительно операций композиции.*

Доказательство. Для $i \in \mathbb{N} \setminus \{1\}$

$R_i^d = \{f \mid f \in L_2, \forall j = \overline{1, n}, \text{ если } x_j \text{ — единственная непосредственная переменная } f, \mu_j = \frac{u_j}{v_j}, \text{ то } v_j \not\vdash p_i, \text{ иначе } \mu_j \in R_i^{(1)}\}$, где

$$R_i^{(1)} = \{\mu \in E'_2(\xi) \mid \mu = u/v, u, v \in E_2[\xi], (u, v) = 1, u \vdash p_i\},$$

а $p_i = a_0 + a_1 \xi + \dots + \xi^s$ — неприводимый над E_2 многочлен.

Любой автомат $f \in R_i^d$ имеет следующий вид:

$$f(x_1, \dots, x_n) = \sum_{j=1}^n \mu_j x_j + \mu_0,$$

где $\mu_j = u_j/v_j$, $(u_j, v_j) = 1$, $v_j \not\equiv p_i$, а μ_0 — произвольный элемент $E_2'(\xi)$.

Класс R_i^d содержит автоматы с любым свободным членом из $E_2'(\xi)$. Например, в нём есть константы вида

$$\mu = \frac{u}{v \cdot p_i^k}, \quad u, v \in E_2[\xi], \quad (u, v) = 1, \quad u, v \not\equiv p_i, \quad k \in \mathbb{N}.$$

Как и в лемме 8 для элементов M_i , так и в данной лемме для элементов из R_i^d выполнены следующие условия: $v_j \not\equiv p_i$ и переменные, не являющиеся непосредственными, принадлежат $R_i^{(1)}$. Поэтому рассуждение леммы 8 о том, что подстановка и обратная связь не увеличивают степень p_i в знаменателе, применимо для класса R_i^d .

Следовательно, ни одно конечное множество автоматов не порождает R_i^d . Тогда R_i^d не может быть K -конечнопорожденным классом. \square

Лемма 10. *K -предполные классы линейных автоматов R_i^e , $i \in \mathbb{N} \setminus \{1\}$ не являются K -конечнопорожденными.*

Доказательство. Для $i \in \mathbb{N} \setminus \{1\}$ класс R_i^e состоит из автоматов $f \in L_2$, у которых:

- если x_j — единственная существенная переменная, то для $\mu_j = u_j/v_j$ выполнено $v_j \not\equiv p_i$;
- иначе $\mu_j \in R_i^{(1)}$.

Произвольный автомат $f \in R_i^e$ представим в виде

$$f(x_1, \dots, x_n) = \sum_{j=1}^n \mu_j x_j + \mu_0,$$

где $\mu_j = u_j/v_j$, $(u_j, v_j) = 1$, $v_j \not\equiv p_i$, а μ_0 — произвольный элемент $E_2'(\xi)$.

Докажем, что из конечного множества автоматов из R_i^e нельзя получить автомат от n переменных (для любого $n \in \mathbb{N}$), у которого каждый коэффициент μ_j имеет вид $\mu_j = \frac{p_i u_j'}{v_j}$ с $u_j', v_j \not\equiv p_i$, т.е. ни один коэффициент не делится на p_i^2 .

Пусть $\{f_1, \dots, f_p\} \subset R_i^e$ — конечное множество, порождающее R_i^e . Поскольку иначе породить R_i^e нельзя, среди автоматов f_1, \dots, f_p есть хотя бы один с более чем одной существенной переменной. Для такого автомата все коэффициенты имеют вид $\mu_j = \frac{p_i u'_j}{v_j}$, где $v_j \not\equiv p_i$.

Для увеличения числа переменных автомата достаточно рассмотреть только операцию подстановки.

Подставим автомат g на k -й вход f (без ограничения общности), где $f, g \in R_i^e$:

$$f(x_1, \dots, x_k) = \sum_{j=1}^k \mu_j x_j + \mu_0, \quad g(x'_1, \dots, x'_m) = \sum_{q=1}^m \mu'_q x'_q + \mu'_0.$$

Тогда

$$\begin{aligned} \tilde{f}(x_1, \dots, x_{k-1}, x'_1, \dots, x'_m) &= f(x_1, \dots, x_{k-1}, g) = \\ &= \sum_{j=1}^{k-1} \mu_j x_j + \sum_{q=1}^m \mu_k \mu'_q x'_q + (\mu_k \mu'_0 + \mu_0). \end{aligned}$$

Число переменных результата равно $k + m - 1$, поэтому для увеличения числа переменных достаточно рассматривать случаи $k > 1$ и $m > 1$. Все коэффициенты μ_j, μ'_q принадлежат $R_i^{(1)}$, то есть

$$\mu_j = \frac{p_i^{t_j} \tilde{u}_j}{v_j}, \quad \mu'_q = \frac{p_i^{t'_q} \tilde{u}'_q}{v'_q},$$

где $\tilde{u}_j, v_j, \tilde{u}'_q, v'_q \not\equiv p_i, t_j, t'_q \in \mathbb{N}$.

Проанализируем коэффициенты полученного автомата:

1. Коэффициенты μ_j ($j = \overline{1, k-1}$) не изменились, их показатели t_j сохранились.
2. Коэффициенты $\mu_k \mu'_q = \frac{p_i^{t_k+t'_q} \tilde{u}_k \tilde{u}'_q}{v_k v'_q}$ имеют показатель $t_k + t'_q \geq 2$.

Следовательно, у автомата \tilde{f} число коэффициентов с показателем $t = 1$ не больше, чем у исходного автомата, в который производилась подстановка.

Таким образом, из конечного множества автоматов из R_i^e с помощью операций композиции нельзя получить автомат от произвольного числа переменных, у которого все коэффициенты имеют показатель $t = 1$ (то есть делятся на p_i , но не на p_i^2). Значит, R_i^e ($i \in \mathbb{N} \setminus \{1\}$) не являются K -конечнопорожденными классами. \square

Теорема 1. Для K -предполного класса $Q \subset L_2$ следующие утверждения равносильны:

1. Q не принадлежит A -критериальной системе \mathcal{J}_A ;
2. Q не является K -конечнопорожденным.

Доказательство. Напомним, что совокупность всех K -предполных классов в L_2 имеет вид:

$$\mathcal{J}_2 = \{T_0, T_1, V_0, V_1, M_i, R_j^e, R_j^d \mid i \in \mathbb{Z}_+, j \in \mathbb{Z}_+ \setminus \{1\}\}.$$

A -критериальная система состоит из классов

$$\mathcal{J}_A = \{T_0, T_1, V_0, V_1, M_1\}.$$

Следовательно, разность $\mathcal{J}_2 \setminus \mathcal{J}_A$ включает классы

$$\{M_i, R_j^e, R_j^d \mid i \in \mathbb{Z}_+ \setminus \{1\}, j \in \mathbb{Z}_+ \setminus \{1\}\}.$$

Докажем каждую импликацию.

(1 \Rightarrow 2). Если $Q \notin \mathcal{J}_A$, то по леммам 5–10 Q не является K -конечнопорожденным. (Эти леммы охватывают все K -предполные классы, не входящие в \mathcal{J}_A .)

(2 \Rightarrow 1). Предположим, что Q не является K -конечнопорожденным. Если бы Q принадлежал \mathcal{J}_A , то по результату [3] он был бы K -конечнопорожденным, что противоречит предположению. Следовательно, $Q \notin \mathcal{J}_A$. \square

Следствие 1. Если K -предполный класс линейных автоматов не является K -конечнопорожденным, то он является A -полным в L_2 .

Доказательство. Пусть Q — K -предполный класс, не являющийся K -конечнопорожденным. По теореме 1 $Q \notin \mathcal{J}_A$. Так как Q — K -предполный, он не может быть строгим подклассом никакого собственного K -замкнутого класса. В частности, Q не лежит ни в одном классе из \mathcal{J}_A . Тогда по теореме из [4] $A(Q) = L_2$, то есть Q является A -полным в L_2 . \square

4. Заключение

В работе изучена задача K -конечнопорожденности для всех K -предполных классов в L_2 , не входящих в A -критериальную систему.

Доказано, что классы M_i , R_i^e , R_i^d (при $i \in \mathbb{Z}_+ \setminus \{1\}$) не являются K -конечнопорожденными. Для K -замкнутых классов M_j ($j \in \mathbb{N} \setminus \{1\}$) предъявлены конечные базисы, что доказывает их K -конечнопорожденность. Также было доказано, что всё не K -конечнопорожденные предполные классы являются A -полными классами в L_2 .

Автор благодарит своего научного руководителя профессора кафедры МаТИС механико-математического факультета МГУ, д.ф.-м.н. Часовских Анатолия Александровича за предложенную тему и всестороннюю помощь в работе над проблемой.

Список литературы

- [1] Кудрявцев В. Б., Алешин С. В., Подколзин А. С., *Введение в теорию автоматов*, Наука, Москва, 1985, 320 с.
- [2] Гилл, А., *Линейные последовательностные машины*, Наука, Москва, 1974, 288 с.
- [3] Бирюкова В. А., “Задача K -конечнопорожденности для предполных классов линейных автоматов, составляющих A -критериальную систему в пространстве линейных автоматов”, *Интеллектуальные системы. Теория и приложения*, **26**:4 (2022), 109–133.
- [4] Часовских А. А., “О полноте в классе линейных автоматов”, *Математические вопросы кибернетики*, **3** (1991), 140–166.
- [5] Буевич В. А., “Об алгоритмической неразрешимости распознавания A -полноты для ограниченно-детерминированных функций”, *Матем. заметки*, **11**:6 (1972), 687–697. DOI: 10.1007/BF01093729.

Статья поступила 4 июня 2026 г.

On the K -finite generation of precomplete classes of linear automata

V. A. Biryukova

We study the problem of K -finite generation for precomplete classes of linear automata over the field E_2 . It is proved that the classes not belonging to the A -criterial system are not K -finitely generated. In addition, a countable series of K -closed classes that are K -finitely generated is found. It is also shown that any K -precomplete class which is not K -finitely generated is A -complete.

Keywords: finite automaton, linear automaton, closed class, pre-complete class, composition operations, A -closure, K -finite generation, bases of closed classes.

References

- [1] Kudryavtsev V. B., Aleshin S. V., Podkolzin A. S., *Introduction to Automata Theory*, Nauka (Science), Moscow, 1985 (In Russian), 320 pp.
- [2] Gill, A., *Linear Sequential Circuits: Analysis, Synthesis, and Applications*, McGraw-Hill, New York, 1966, 215 pp.
- [3] Biryukova V. A., “The Problem of K -Finite Generation for Precomplete Classes of Linear Automata Constituting an A -Criterion System in the Space of Linear Automata”, *Intelligent Systems. Theory and Applications*, **26**:4 (2022), 109–133 (In Russian).
- [4] Chasovskikh A. A., “On Completeness in the Class of Linear Automata”, *Mathematical Problems of Cybernetics*, **3** (1991), 140–166 (In Russian).
- [5] Buevich V. A., “On the Algorithmic Undecidability of A -Completeness for Boundedly Determinate Functions”, *Mathematical Notes*, **11**:6 (1972), 687–697. DOI: 10.1007/BF01093729.

Received on June 4, 2026

Многомерное расширение произведений кодов сильнее робастной тестируемости и тестируемости на согласованность

Г. В. Калачев*

Мы изучаем свойство кограничного расширения (coboundary expansion) для произведений кодов, называемое расширением произведения, которое сыграло ключевую роль во многих построениях хороших квантовых LDPC кодов. Ранее было показано, что это свойство эквивалентно робастной тестируемости (robust testability) и тестируемости на согласованность (agreement testability) для произведений двух кодов с линейным расстоянием. Во-первых, мы показываем, что робастная тестируемость по линиям для произведения нескольких кодов с линейным расстоянием эквивалентна тестируемости на согласованность. Во-вторых, мы приводим пример произведения трёх кодов с линейным расстоянием, которое является робастно тестируемым, но не обладает свойством расширения произведения.

Ключевые слова: тензорное произведение кодов, кограничное расширение, робастная тестируемость, тестируемость на согласованность.

1. Введение

Недавние конструкции асимптотически хороших локально тестируемых кодов (LTC) и квантовых LDPC (qLDPC) кодов [1–7] используют специальное свойство произведений кодов, которое имеет несколько названий и определений: робастная тестируемость (robust testability), тестируемость на согласованность (agreement testability) и расширение произведения (product expansion). Было показано [2, Lemma 2.9], [8, Lemma 1], что эти определения по существу эквивалентны в случае произведения двух кодов. Для всех известных конструкций хороших qLDPC кодов это свойство необходимо для обеспечения линейного расстояния и построения эффективных декодеров. Для LTC существует одно исключение: в работе [9]

* *Калачев Глеб Вячеславович* — канд. физ.-мат. наук, науч. сотр. каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: gleb.kalachev@yandex.ru, ORCID: 0000-0003-2695-3179.

Kalachev Gleb Vyacheslavovich — Candidate of Physical and Mathematical Sciences, Researcher, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

конструкция LTC кодов основывается на односторонних вершинных экспандерах и не требует локальных кодов, удовлетворяющих специальному свойству.

В [8, Appendix B] было показано, что свойство расширения произведения кодов может быть интерпретировано как форма многомерного расширения, называемая кограничным расширением¹ (coboundary expansion). Таким образом, это представляется важным свойством произведений кодов наряду с робастной тестируемостью и тестируемостью на согласованность. Более того, поскольку расширение произведения кодов является формой кограничного расширения, то вероятно, что оно будет полезно для построения многомерных аналогов кодов из [1, 2], которые потенциально могут дать хорошие квантовые локально тестируемые коды (qLTC).

В [8, Lemma 1] также было показано, что расширение произведения двух кодов совпадает с тестируемостью на согласованность с той же константой (см. также [3, Section 2.6]). Цель нашей статьи — прояснить взаимосвязь между робастной тестируемостью, тестируемостью на согласованность и расширением произведения для произведений более чем двух кодов. В частности, мы рассматриваем естественное обобщение тестируемости на согласованность для произведений нескольких кодов и показываем, что в случае произведений 3 и более кодов: 1) расширение произведения отличается от робастной тестируемости и тестируемости на согласованность; 2) тестируемость на согласованность эквивалентна робастной тестируемости для теста по осепараллельным линиям (axis-parallel line test), с точностью до константного множителя.

1.1. Расширение произведения кодов

Приведём определение расширения произведения из [8], где также представлены история и связь с другими формами этого определения. Пусть заданы линейные коды $\mathcal{C}_1, \dots, \mathcal{C}_m$ над \mathbb{F}_q . Мы можем определить (*тензорное*) *произведение кодов*

$$\mathcal{C}_1 \otimes \dots \otimes \mathcal{C}_m := \{c \in \mathbb{F}_q^{n_1 \times \dots \times n_m} \mid \forall i \in [m] \forall \ell \in \mathcal{L}_i: c|_{\ell} \in \mathcal{C}_i\},$$

где $\mathbb{F}_q^{n_1 \times \dots \times n_m}$ — это множество функций $c: [n_1] \times \dots \times [n_m] \rightarrow \mathbb{F}_q$, а \mathcal{L}_i — множество линий, параллельных i -й оси в m -мерной решётке $[n_1] \times \dots \times [n_m]$, то есть

$$\mathcal{L}_i := \{A_1 \times \dots \times A_m \subseteq [n_1] \times \dots \times [n_m] \mid A_i = [n_i], \forall j \neq i: |A_j| = 1\}.$$

¹Для двухмерного случая см. также [3, Section 2.6]

Здесь и далее мы используем обозначение $[n] := \{1, \dots, n\}$. Также для набора $\mathcal{C} = (\mathcal{C}_i)_{i \in [m]}$ линейных кодов над \mathbb{F}_q нам будет удобно использовать обозначение $\otimes \mathcal{C} := \mathcal{C}_1 \otimes \dots \otimes \mathcal{C}_m$.

Как и в [8], для линейных кодов $\mathcal{C}_1 \subseteq \mathbb{F}_q^{n_1}$, $\mathcal{C}_2 \subseteq \mathbb{F}_q^{n_2}$ мы обозначаем $\mathcal{C}_1 \boxplus \mathcal{C}_2$ как код $(\mathcal{C}_1^\perp \otimes \mathcal{C}_2^\perp)^\perp = \mathcal{C}_1 \otimes \mathbb{F}_q^{n_2} + \mathbb{F}_q^{n_1} \otimes \mathcal{C}_2 \subseteq \mathbb{F}_q^{n_1 \times n_2}$. Для набора $\mathcal{C} = (\mathcal{C}_i)_{i \in [m]}$ линейных кодов над \mathbb{F}_q мы можем определить коды

$$\mathcal{C}^{(i)} := \mathbb{F}_q^{n_1} \otimes \dots \otimes \mathcal{C}_i \otimes \dots \otimes \mathbb{F}_q^{n_m} = \{c \in \mathbb{F}_q^{n_1 \times \dots \times n_m} \mid \forall \ell \in \mathcal{L}_i: c|_\ell \in \mathcal{C}_i\}.$$

Легко видеть, что

$$\mathcal{C}_1 \otimes \dots \otimes \mathcal{C}_m = \mathcal{C}^{(1)} \cap \dots \cap \mathcal{C}^{(m)}, \quad \mathcal{C}_1 \boxplus \dots \boxplus \mathcal{C}_m = \mathcal{C}^{(1)} + \dots + \mathcal{C}^{(m)}.$$

Заметим, что каждый код $\mathcal{C}^{(i)}$ представляет собой прямую сумму $|\mathcal{L}_i| = \frac{1}{n_i} \prod_{j \in [m]} n_j$ копий кода \mathcal{C}_i . Для $x \in \mathbb{F}_q^{n_1 \times \dots \times n_m}$ обозначим $|x|_i$ и $\|x\|_i$ соответственно как количество и долю линий $\ell \in \mathcal{L}_i$, для которых $x|_\ell \neq 0$. Очевидно, что $\|x\|_i = \frac{1}{|\mathcal{L}_i|} |x|_i$. $|x|$ и $\|x\|$ обозначают соответственно *вес Хэмминга* (то есть количество ненулевых элементов) и *нормализованный вес Хэмминга* (то есть долю ненулевых элементов) в x . Легко видеть, что введённые нормы связаны неравенством $\|x\| \leq \|x\|_i$, $i \in [m]$. Мы также будем использовать следующие обозначения: нормализованное расстояние $\delta(x, y) := \|x - y\|$, нормализованное расстояние до кода $\delta(x, \mathcal{C}) := \min_{y \in \mathcal{C}} \|x - y\|$ и нормализованное минимальное расстояние $\delta(\mathcal{C}) := \min_{x \in \mathcal{C} \setminus \{0\}} \|x\|$ для кода $\mathcal{C} \subseteq \mathbb{F}_q^n$.

Определение 1 (Расширение произведения кодов [8]). Пусть задан набор $\mathcal{C} = (\mathcal{C}_i)_{i \in [m]}$ линейных кодов $\mathcal{C}_i \subseteq \mathbb{F}_q^{n_i}$. Мы говорим, что \mathcal{C} является ρ -расширяющим, если каждое кодовое слово $c \in \mathcal{C}_1 \boxplus \dots \boxplus \mathcal{C}_m$ может быть представлено как сумма $c = \sum_{i \in [m]} a_i$, где $a_i \in \mathcal{C}^{(i)}$ для всех $i \in [m]$ и выполнено следующее неравенство:

$$\rho \sum_{i \in [m]} \|a_i\|_i \leq \|c\|. \tag{1}$$

Через $\rho(\mathcal{C})$ обозначим наибольшее значение ρ , для которого \mathcal{C} является ρ -расширяющим. В [8, Appendix B] было показано, что $\rho(\mathcal{C})$ с точностью до множителя $1/m$ равен константе Чигера цепного комплекса, естественно ассоциированного с произведением кодов $\mathcal{C}_1 \otimes \dots \otimes \mathcal{C}_m$.

1.2. Робастная тестируемость и тестируемость на согласованность

Пусть X — некоторое конечное индексное множество, которое мы будем использовать для нумерации символов кода. Тогда код $\mathcal{C} \subseteq \mathbb{F}_q^X$ можно

интерпретировать как множество функций $f : X \rightarrow \mathbb{F}_q$. Если $I \subseteq X$, то $\mathcal{C}|_I := \{c|_I \mid c \in \mathcal{C}\}$ — это перфорированный код (punctured code) \mathcal{C} , состоящий из ограничений кодовых слов из \mathcal{C} на индексное множество I .

Определение 2. Тест для кода $\mathcal{C} \subseteq \mathbb{F}_q^X$ — это множество $T \subseteq 2^X$ с вероятностной мерой \mathbb{P} , определённой на нём.

В этой статье мы всегда будем использовать следующую вероятностную меру:

$$\mathbb{P}(I) = \frac{|I|}{\sum_{J \in T} |J|} \quad \text{для } I \in T. \quad (2)$$

Тестер для пары (код $\mathcal{C} \subseteq \mathbb{F}_q^X$ и тест T) работает следующим образом: для заданного слова $c \in \mathbb{F}_q^X$ мы случайным образом выбираем множество $I \in T$ и принимаем c , если $c|_I \in \mathcal{C}|_I$, и отвергаем в противном случае. Таким образом, если $c \in \mathcal{C}$, то тестер всегда принимает это слово.

Определение 3 (Робастность теста). Тест T для кода $\mathcal{C} \subseteq \mathbb{F}_q^X$ называется α -робастным, если для всех $c \in \mathbb{F}_q^X$ выполнено

$$\mathbb{E}_{I \in T} \delta(c|_I, \mathcal{C}|_I) \geq \alpha \delta(c, \mathcal{C}),$$

где \mathbb{E} обозначает математическое ожидание.

Обозначим максимальную робастность как:

$$\rho_r(T, \mathcal{C}) := \max \{ \alpha \mid \text{тест } T \text{ является } \alpha\text{-робастным для кода } \mathcal{C} \}.$$

Обычно, когда код \mathcal{C} определяется множеством локальных кодов, естественный тест содержит носители всех этих локальных кодов. Например, произведение кодов $\mathcal{C}_1 \otimes \mathcal{C}_2$ можно определить локальными кодами на линиях, параллельных осям множества $X = [n_1] \times [n_2]$:

$$\mathcal{C}_1 \otimes \mathcal{C}_2 = \left\{ f \in \mathbb{F}_q^{[n_1] \times [n_2]} \mid f(\cdot, j) \in \mathcal{C}_1 \text{ для } j \in [n_2], f(i, \cdot) \in \mathcal{C}_2 \text{ для } i \in [n_1] \right\}.$$

Таким образом, естественный тест для кода $\mathcal{C}_1 \otimes \mathcal{C}_2$ — это множество всех линий, параллельных осям:

$$T = \mathcal{L}_1 \cup \mathcal{L}_2 = \{[n_1] \times \{j\} \mid j \in [n_2]\} \cup \{\{i\} \times [n_2] \mid i \in [n_1]\},$$

и \mathbb{P} , определённое в (2), соответствует следующему процессу: выбирается случайное направление, затем случайная линия вдоль этого направления. Этот тест называется *тестом по осепараллельным линиям* (axis-parallel line test). Для произведения $m \geq 3$ кодов существуют различные естественные тесты, так как можно рассматривать подпространства, параллельные осям, различных размеров от 1 до $m - 1$. Следующее определение даёт прямое обобщение 2-flat test из [10, Algorithm 12.2].

Определение 4 (Тест по осепараллельным k -плоскостям). Пусть $X = [n_1] \times \cdots \times [n_m]$, $k \in [m-1]$. Тогда *тест по осепараллельным k -плоскостям* (*axis-parallel k -flat test*) определяется как множество T_m^k всех k -мерных параллельных координатным осям подпространств (*k -плоскостей*) в X :

$$T_m^k(X) = \bigcup_{I \subseteq [m], |I|=k} \mathcal{L}_I,$$

$$\mathcal{L}_I = \left\{ A_1 \times \cdots \times A_m \subseteq [n_1] \times \cdots \times [n_m] \mid \begin{array}{l} \forall j \in I : A_j = [n_j], \\ \forall j \in [m] \setminus I : |A_j| = 1 \end{array} \right\}.$$

Мы будем опускать аргумент T_m^k там, где это не важно или очевидно из контекста.

Здесь мы следуем терминологии из [10]. Тест T_2^1 — это стандартный тест по осепараллельным линиям, T_m^1 — его многомерная версия, а T_m^{m-1} — *тест по осепараллельным гиперплоскостям*. В [10, Theorem 12.5] было показано, что $\rho_r(T_m^2, \mathcal{C}^{\otimes m}) \geq \alpha(\delta(\mathcal{C}), m)$ для $m \geq 3$ и некоторой функции² $\alpha(\epsilon, m) > 0$. Этот результат показывает, что требование постоянной робастности теста T_m^2 для семейства кодов $(\mathcal{C}_i^{\otimes m})_{i \in \mathbb{N}}$ эквивалентно требованию линейного минимального расстояния для кодов в этом семействе: $\delta(\mathcal{C}_i) = \Omega(1)$ при $i \rightarrow \infty$. Таким образом, единственный тест, который накладывает нетривиальное ограничение на код \mathcal{C} , — это тест по осепараллельным линиям T_m^1 .

Тест T_m^1 можно рассматривать как композицию тестов T_m^2 для $\mathcal{C}^{\otimes m}$ и T_2^1 для $\mathcal{C}^{\otimes 2}$. Как будет формально показано в лемме 5,

$$\rho_r(T_m^1, \mathcal{C}^{\otimes m}) \geq \rho_r(T_m^2, \mathcal{C}^{\otimes m}) \rho_r(T_2^1, \mathcal{C}^{\otimes 2}),$$

то есть константная робастность теста T_m^1 для $\mathcal{C}^{\otimes m}$ эквивалентна константной робастности теста T_2^1 для $\mathcal{C}^{\otimes 2}$, если $\delta(\mathcal{C}) = \Omega(1)$.

Следующее определение тестируемости на согласованность для произведения нескольких кодов является непосредственным обобщением тестируемости на согласованность для произведения двух кодов [2, Definition 2.8].

Определение 5 (Тестируемость на согласованность для произведений кодов). Пусть $\mathcal{C} = (\mathcal{C}_1, \dots, \mathcal{C}_m)$ — коллекция кодов. Произведение кодов

²Из доказательства [10, Theorem 12.5] следует, что $\alpha(\epsilon, m) = \epsilon^{\frac{1}{2}(m-2)(m+3)} \cdot 24^{2-m}$.

$\otimes\mathcal{C}$ является α -тестируемым на согласованность, если для каждого $c_1 \in \mathcal{C}^{(1)}, \dots, c_m \in \mathcal{C}^{(m)}$ существует $c \in \otimes\mathcal{C}$ такое, что

$$\alpha \mathbf{E}_{i \in [m]} \|c_i - c\|_i \leq \mathbf{E}_{i, j \in [m]} \|c_i - c_j\|,$$

где предполагается равномерное распределение на $[m]$. Определим максимальную тестируемость на согласованность:

$$\rho_a(\otimes\mathcal{C}) := \max \{ \alpha \mid \otimes\mathcal{C} \text{ является } \alpha\text{-тестируемым на согласованность} \}.$$

Заметим, что $\rho_a(\otimes\mathcal{C}) \leq 2$, поскольку для любого c выполнено $\|c_i - c_j\| \leq \|c_i - c\| + \|c_j - c\| \leq \|c_i - c\|_i + \|c_j - c\|_j$.

Лемма 1 (Робастная тестируемость + линейное расстояние = тестируемость на согласованность). Пусть $\mathcal{C} = (\mathcal{C}_1, \dots, \mathcal{C}_m)$ — набор кодов $\mathcal{C}_i \subseteq \mathbb{F}_q^{n_i}$, $\rho_r := \rho_r(T_m^1, \otimes\mathcal{C})$, $\rho_a := \rho_a(\otimes\mathcal{C})$. Тогда

$$\rho_r \geq \frac{1}{4} \rho_a, \quad \rho_a \geq \frac{\rho_r}{\rho_r + 1} \min_{i \in [m]} \delta(\mathcal{C}_i).$$

Доказательство приведено в разделе 3. Оно в целом совпадает с доказательством для произведения двух кодов [2, Lemma 2.9]. Из леммы 1 следует, что робастная тестируемость и тестируемость на согласованность по существу эквивалентны.

Основной результат данной работы состоит в том, что расширение произведения набора кодов отличается от робастной тестируемости и тестируемости на согласованность произведения этих кодов.

Теорема 1. Пусть C_t — примитивный $[n_t, \frac{n_t}{3}]$ код Рида-Соломона над полем $\mathbb{F}_{2^{2t}}$, определённый проверочным многочленом $(x-1)(x-\omega) \dots (x-\omega^{\frac{n_t}{3}-1})$, где $t \in \mathbb{N}$, $n_t = 2^{2t} - 1$, ω — примитивный элемент $\mathbb{F}_{2^{2t}}$. Для каждого $m \geq 3$ существуют $\alpha_r > 0$ и $\alpha_a > 0$, такие, что для всех $t \in \mathbb{N}$ выполняются следующие неравенства:

1. $\rho(\underbrace{C_t, \dots, C_t}_{m \text{ раз}}) \leq \frac{1}{n_t}$;
2. $\rho_r(T_m^k, C_t^{\otimes m}) \geq \alpha_r$ для всех $k \in [m-1]$;
3. $\rho_a(C_t^{\otimes m}) \geq \alpha_a$.

Более того, расширение произведения влечёт робастность теста T_m^1 для кода $C^{\otimes m}$.

Утверждение 1. Пусть $\mathcal{C} \subsetneq \mathbb{F}_q^n$ и $m \geq 2$. Тогда существует функция α такая, что $\alpha(x) > 0$ при $x > 0$ и

$$\rho_r(T_m^1, \mathcal{C}^{\otimes m}) \geq \alpha(\underbrace{\rho(\mathcal{C}, \dots, \mathcal{C})}_{m \text{ раз}}).$$

Это утверждение вместе с теоремой 1 показывает, что свойство расширения произведения накладывает более сильное ограничение на код \mathcal{C} , чем робастная тестируемость. Теорема 1 и утверждение 1 доказаны в следующем разделе.

2. Доказательства

Зафиксируем $t \in \mathbb{N}$ и рассмотрим примитивный $[n, k]$ код Рида-Соломона \mathcal{C} над полем \mathbb{F}_q , где $q = 2^{2t}$, $n = q - 1$, и $k = n/3$. Этот код может быть определён проверочным многочленом $p(x) = (x - 1)(x - \omega) \dots (x - \omega^{k-1})$, где ω — примитивный элемент \mathbb{F}_q :

$$\mathcal{C} = \left\{ (a_i)_{i=0}^{n-1} \in \mathbb{F}_q^n \mid p(x) \sum_{i=0}^{n-1} a_i x^i \equiv 0 \pmod{(x^n - 1)} \right\}.$$

Сначала мы покажем, что $\rho(\mathcal{C}, \mathcal{C}, \mathcal{C}) \leq 1/n$.

Начнём с описания двойственного кода к произведению циклических кодов в терминах проверочных многочленов. Рассмотрим циклические коды $\mathcal{C}_1, \dots, \mathcal{C}_m \subseteq \mathbb{F}_q^n$, определённые соответственно проверочными многочленами $p_1, \dots, p_m \in \mathbb{F}_q[x]$ такими, что $p_i | (x^n - 1)$:

$$\begin{aligned} \mathcal{C}_i &= \left\{ (a_j)_{j=0}^{n-1} \in \mathbb{F}_q^n \mid p_i(x) \sum_{j=0}^{n-1} a_j x^j \equiv 0 \pmod{(x^n - 1)} \right\} \\ &\cong \left\{ a \in \mathbb{F}_q[x] \mid \deg a < n, p_i(x)a(x) \equiv 0 \pmod{(x^n - 1)} \right\}. \end{aligned}$$

Здесь для кодов $\mathcal{C}_1 \subseteq V_1, \mathcal{C}_2 \subseteq V_2$ мы говорим, что $\mathcal{C}_1 \cong \mathcal{C}_2$, если существует линейный изоморфизм $\varphi : V_1 \rightarrow V_2$, сохраняющий расстояние Хэмминга, такой, что $\varphi(\mathcal{C}_1) = \mathcal{C}_2$.

Лемма 2. Пусть $\mathcal{C} = \mathcal{C}_1 \boxplus \dots \boxplus \mathcal{C}_m$. Рассмотрим идеал

$$\mathcal{I} = (x_1^n - 1, \dots, x_m^n - 1) \subseteq \mathbb{F}_q[x_1, \dots, x_m].$$

Тогда

$$\begin{aligned} \mathcal{C} &= \left\{ a \in \mathbb{F}_q[x_1, \dots, x_m] \mid \deg_{x_i} a < n \text{ для всех } i \in [m] \right. \\ &\quad \left. \text{и } a(x_1, \dots, x_m) \prod_{i=1}^m p_i(x_i) \equiv 0 \pmod{\mathcal{I}} \right\}. \end{aligned}$$

Доказательство. Для многочлена $p(x_1, \dots, x_k)$ определим

$$p^*(x_1, \dots, x_k) := p(x_1^{n-1}, \dots, x_k^{n-1}) \pmod{\mathcal{I}}.$$

Поскольку $p_i(x)$ является проверочным многочленом для C_i , то $p_i^*(x)$ является порождающим многочленом для C_i^\perp , то есть

$$C_i^\perp = \{p_i^*(x)q(x) \mid \deg q < n - \deg p_i\} = \{a \in \mathbb{F}_q[x] \mid \deg a < n \text{ и } p_i^*|a\}.$$

Следовательно, тензорное произведение $C_1^\perp, \dots, C_m^\perp$ порождается полиномом

$$p_1^*(x_1) \cdots p_m^*(x_m) \in \mathbb{F}_q[x_1, \dots, x_m],$$

а именно:

$$C_1^\perp \otimes \cdots \otimes C_m^\perp = \{a \in \mathbb{F}_q[x_1, \dots, x_m] \mid \deg_{x_i} a < n \text{ и } p_i^*(x_i)|a\}.$$

Значит $(p_1^*(x_1) \cdots p_m^*(x_m))^* = p_1(x_1) \cdots p_m(x_m)$ является проверочным многочленом для $(C_1^\perp \otimes \cdots \otimes C_m^\perp)^\perp = C_1 \boxplus \cdots \boxplus C_m$. \square

Лемма 3. Пусть C — примитивный код Рида-Соломона $[n, k]$ над полем \mathbb{F}_q , определённый проверочным многочленом $p(x) = (x-1)(x-\omega) \cdots (x-\omega^{k-1})$, где $q = 2^{2t}$, $n = q-1$, $k = n/3$. Тогда

$$\rho(C, C, C) \leq 1/n.$$

Доказательство. Кодовое слово кода $C \boxplus C \boxplus C$ может быть задано как многочлен $f(x, y, z)$, такой что

$$f(x, y, z)p(x)p(y)p(z) \equiv 0 \pmod{(x^n - 1, y^n - 1, z^n - 1)}.$$

Рассмотрим многочлены

$$a'(x, y, z) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \sum_{l=0}^{n-1} a'_{ijl} x^i y^j z^l, \quad \text{и} \quad a(x, y, z) := a'(x, \omega^{-k}y, \omega^{-2k}z),$$

где

$$a'_{ijl} = \begin{cases} 1, & i + j + l \equiv 0 \pmod{n} \\ 0, & \text{иначе.} \end{cases}$$

Сначала покажем, что a — это кодовое слово кода $C \boxplus C \boxplus C$. Нам нужно показать, что

$$a(x, y, z)p(x)p(y)p(z) = 0 \pmod{(x^n - 1, y^n - 1, z^n - 1)}. \quad (3)$$

Рассмотрим многочлены

$$r(x) := p(\omega^k x) = \omega^{k^2} \prod_{i=2k}^{3k-1} (x - \omega^i), \quad s(x) := p(\omega^{2k} x) = \omega^{2k^2} \prod_{i=k}^{2k-1} (x - \omega^i).$$

Мы имеем

$$a(x, y, z)p(x)p(y)p(z) = a'(x, \omega^{-k}y, \omega^{-2k}z)p(x)r(\omega^{-k}y)s(\omega^{-2k}z), \quad \omega^n = 1,$$

таким образом, заменяя $y \mapsto \omega^{-k}y$, $z \mapsto \omega^{-2k}z$, мы можем переписать условие (3) как

$$a'(x, y, z)p(x)r(y)s(z) \equiv 0 \pmod{(x^n - 1, y^n - 1, z^n - 1)}. \quad (4)$$

Поскольку ω — примитивный элемент \mathbb{F}_q , то

$$p(x)r(x)s(x) = \underbrace{\omega^{3k^2}}_{=1} \prod_{i=0}^{n-1} (x - \omega^i) = x^n - 1.$$

Пусть $p(x) = \sum_{i=0}^{n-1} p_i x^i$, $r(x) = \sum_{i=0}^{n-1} r_i x^i$, $s(x) = \sum_{i=0}^{n-1} s_i x^i$. Из

$$p(x)r(x)s(x) \equiv 0 \pmod{(x^n - 1)}$$

следует

$$0 = \sum_{d=0}^{n-1} \sum_{i+j+l \equiv d} p_i r_j s_l x^d \implies \sum_{i+j+l \equiv d} p_i r_j s_l = 0 \text{ для всех } d \leq n-1.$$

Следовательно, по модулю $(x^n - 1, y^n - 1, z^n - 1)$ мы имеем

$$\begin{aligned} a'(x, y, z)p(x)r(y)s(z) &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \sum_{l=0}^{n-1} x^i y^j z^l \sum_{i'=0}^{n-1} \sum_{j'=0}^{n-1} \sum_{l'=0}^{n-1} p_{i-i'} r_{j-j'} s_{l-l'} a'_{i'j'l'} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \sum_{l=0}^{n-1} x^i y^j z^l \sum_{i'+j'+l' \equiv 0 \pmod n} p_{i-i'} r_{j-j'} s_{l-l'} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \sum_{l=0}^{n-1} x^i y^j z^l \underbrace{\sum_{i''+j''+l'' \equiv i+j+l \pmod n} p_{i''} r_{j''} s_{l''}}_{=0} \\ &= 0, \end{aligned}$$

где во второй строке были использованы подстановки $i'' := i - i'$, $j'' := j - j'$, $l'' := l - l'$, все индексы считаются по модулю n . Таким образом, (4) выполняется, а значит, выполняется и (3), и, следовательно, a является кодовым словом $C \boxplus C \boxplus C$ по лемме 2.

По определению выполнено $|a| = n^2$. Предположим, что $a = a_1 + a_2 + a_3$, где $a_1 \in C \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$, $a_2 \in \mathbb{F}_q^n \otimes C \otimes \mathbb{F}_q^n$, $a_3 \in \mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes C$. Поскольку каждая линия, параллельная осям в кубе $[n]^3$, покрывает только один ненулевой элемент a_{ijl} , мы имеем $|a_1|_1 + |a_2|_2 + |a_3|_3 \geq |a| = n^2$. Учитывая, что $\|a\| = \frac{1}{n^2}|a| = \frac{1}{n}$ и $\|a_i\|_i = \frac{1}{n^2}|a_i|_i$, получаем

$$\sum_{i \in [3]} \|a_i\|_i = \frac{1}{n^2} \sum_{i \in [3]} |a_i|_i \geq 1 = n\|a\|.$$

Таким образом, $\rho(C, C, C) \leq 1/n$. \square

Только что доказанная лемма 3 показывает, что расширение произведения тройки (C, C, C) стремится к нулю при $n \rightarrow \infty$. Теперь объединим известные результаты, чтобы показать, что все тесты T_m^k имеют константную робастность для кода $C^{\otimes m}$ и $k \in [m-1]$ при $n \rightarrow \infty$.

Сначала покажем, что тест T_2^1 робастный для кода $C \otimes C$. Переформулируем теорему о робастной тестируемости кодов Рида-Соломона из [11] для нашего случая.

Теорема 2 (Theorem 9 in [11]). *Пусть \mathbb{F} — поле, $X = \{x_1, \dots, x_n\} \subseteq \mathbb{F}$, $Y = \{y_1, \dots, y_n\} \subseteq \mathbb{F}$. Пусть $R(x, y)$ — полином над \mathbb{F} степени (d, n) , $C(x, y)$ — полином над \mathbb{F} степени (n, d) . Если*

$$P_{(x,y) \in X \times Y} \{R(x, y) \neq C(x, y)\} < \tau^2,$$

и $n > 2\tau n + 2d$, то существует полином $Q(x, y)$ степени (d, d) такой, что

$$P_{(x,y) \in X \times Y} \{R(x, y) \neq Q(x, y) \text{ или } C(x, y) \neq Q(x, y)\} < 2\tau^2.$$

Лемма 4 (Следствие из теоремы 2). *Пусть C — это $[n, k]$ примитивный код Рида-Соломона над \mathbb{F}_q , определённый проверочным многочленом $(x-1)(x-\omega)\dots(x-\omega^{k-1})$, где $n = q-1$, $k < n/2$, а ω — примитивный элемент \mathbb{F}_q . Тогда для любого $c_1 \in C \otimes \mathbb{F}_q^n$, $c_2 \in \mathbb{F}_q^n \otimes C$, если*

$$\delta(c_1, c_2) \leq \left(\frac{1}{2} - \frac{k}{n}\right)^2,$$

то

$$\delta(c_1, C \otimes C) \leq 2\delta(c_1, c_2), \quad \delta(c_2, C \otimes C) \leq 2\delta(c_1, c_2).$$

Доказательство. Используя дискретное преобразование Фурье (см., например, [12, Theorem 6.1.5]), можно показать, что каждое кодовое слово $c \in C$ может быть определено как вектор значений некоторого многочлена $p_c \in \mathbb{F}_q[x]$ степени не более $d = k - 1$ в точках $\{1, \omega^{-1}, \omega^{-2}, \dots, \omega^{1-n}\}$.

Применим теорему 2 к $X = Y = \{1, \omega, \dots, \omega^{n-1}\}$, $d = k - 1$, $\tau \in I$, где I — это интервал $(\sqrt{\delta(c_1, c_2)}, \frac{1}{2} - \frac{d}{n})$. Так как $\sqrt{\delta(c_1, c_2)} \leq \frac{1}{2} - \frac{k}{n} < \frac{1}{2} - \frac{d}{n}$, интервал I непуст.

Каждое кодовое слово $c_1 \in C \otimes \mathbb{F}_q^n$ (соответственно, $c_2 \in \mathbb{F}_q^n \otimes C$) определяется вектором значений на $X \times Y$ некоторого многочлена $p_{c_1}(x, y)$ от двух переменных степени не выше³ (d, n) (соответственно, $p_{c_2}(x, y)$ степени не выше (n, d)). Расстояние $\delta(c, c')$ для $c, c' \in \mathbb{F}_q^n \otimes \mathbb{F}_q^n$ можно интерпретировать как $P_{(x,y) \in X \times Y} \{p_c(x, y) \neq p_{c'}(x, y)\}$.

Поскольку $\tau \in I$, то выполнены условия теоремы 2. Применяя эту теорему к p_{c_1} и p_{c_2} , получаем, что существует многочлен p_c степени не выше (d, d) такой, что

$$P_{(x,y) \in X \times Y} \{p_{c_1}(x, y) \neq p_c(x, y) \text{ или } p_{c_2}(x, y) \neq p_c(x, y)\} \leq 2\tau^2.$$

Соответствующее слово c принадлежит произведению кодов $C \otimes C$, так как степень p_c по каждой переменной не превосходит d . Следовательно, имеем

$$\delta(c_1, C \otimes C) \leq \delta(c_1, c) = P_{(x,y) \in X \times Y} \{p_{c_1}(x, y) \neq p_c(x, y)\} \leq 2\tau^2.$$

Беря инфимум по всем $\tau \in I$, получаем $\delta(c_1, C \otimes C) \leq 2\delta(c_1, c_2)$. Аналогично $\delta(c_2, C \otimes C) \leq 2\delta(c_1, c_2)$. \square

Следствие 1. $\rho_r(T_2^1, C \otimes C) \geq \frac{1}{72}$.

Доказательство. Рассмотрим слово $x \in \mathbb{F}_q^{n \times n}$. Пусть c_1 и c_2 — ближайшие слова к x из $C \otimes \mathbb{F}_q^n$ и $\mathbb{F}_q^n \otimes C$, соответственно. Пусть $\alpha := \delta(x, c_1) + \delta(x, c_2)$. Нам нужно показать, что

$$\delta(x, C \otimes C) \leq 36 (\delta(x, C \otimes \mathbb{F}_q^n) + \delta(x, \mathbb{F}_q^n \otimes C)).$$

По определению c_1 и c_2 мы имеем $\delta(x, c_1) = \delta(x, C \otimes \mathbb{F}_q^n)$, $\delta(x, c_2) = \delta(x, \mathbb{F}_q^n \otimes C)$. Поэтому требуется доказать, что

$$\delta(x, C \otimes C) \leq 36\alpha. \tag{5}$$

Если $\alpha \geq \frac{1}{36}$, то (5) выполняется. Теперь рассмотрим основной случай $\alpha < \frac{1}{36}$. Поскольку C — это $[n, k]$ код с $k = n/3$, то по неравенству

³Мы говорим, что многочлен $p(x, y)$ от двух переменных степени не выше (a, b) , если каждый его моном имеет степень по x не выше a и степень по y не выше b

треугольника мы имеем $\delta(c_1, c_2) \leq \alpha < \frac{1}{36} = \left(\frac{1}{2} - \frac{k}{n}\right)^2$. Применяя лемму 4, получаем

$$\delta(x, C \otimes C) \leq \delta(x, c_1) + \delta(c_1, C \otimes C) \leq \alpha + 2\delta(c_1, c_2) \leq 3\alpha.$$

Таким образом, в данном случае (5) также выполняется, что завершает доказательство. \square

Лемма 5 (Робастность композиции тестов). Пусть $C \subseteq \mathbb{F}_q^n$ и $1 \leq k_1 < k_2 < m$. Тогда

$$\rho_r(T_m^{k_1}, C^{\otimes m}) \geq \rho_r(T_m^{k_2}, C^{\otimes m}) \rho_r(T_{k_2}^{k_1}, C^{\otimes k_2}).$$

Доказательство. Зафиксируем $x \in (\mathbb{F}_q^n)^{\otimes m}$. Для каждого $k \in [m-1]$ и $\pi \in T_m^k$ мы имеем $C^{\otimes m}|_\pi \cong C^{\otimes k}$. Следовательно,

$$\mathbb{E}_{\pi \in T_m^k} \delta(x|_\pi, C^{\otimes m}|_\pi) = \mathbb{E}_{\pi \in T_m^k} \delta(x|_\pi, C^{\otimes k}).$$

Таким образом,

$$\begin{aligned} \delta(x, C^{\otimes m}) \rho_r(T_m^{k_2}, C^{\otimes m}) \rho_r(T_{k_2}^{k_1}, C^{\otimes k_2}) &\leq \mathbb{E}_{\pi \in T_m^{k_2}} \delta(x|_\pi, C^{\otimes k_2}) \rho_r(T_{k_2}^{k_1}, C^{\otimes k_2}) \leq \\ &\leq \mathbb{E}_{\pi \in T_m^{k_2}} \mathbb{E}_{\pi' \in T_{k_2}^{k_1}(\pi)} \delta(x|_{\pi'}, C^{\otimes k_1}) = \mathbb{E}_{\pi' \in T_m^{k_1}} \delta(x|_{\pi'}, C^{\otimes k_1}). \end{aligned}$$

\square

Лемма 6. Пусть $C \subseteq \mathbb{F}_q^n$, $m \geq 2$. Обозначим $M := \frac{1}{2}(m-2)(m+3) = \sum_{k=3}^m k$. Тогда для $k' \in [m-1]$ выполнено

$$\rho_r(T_m^{k'}, C^{\otimes m}) \geq \frac{1}{12^{m-2}} \cdot \rho_r(T_2^1, C^{\otimes 2}) \cdot \delta(C)^M.$$

Доказательство. Заметим, что при $m=2$ утверждение леммы тавтологично. Поэтому далее рассматриваем случай $m \geq 3$. Из [13, Theorem 2.6] мы знаем нижнюю границу робастности теста T_k^{k-1} :

$$\rho_r(T_k^{k-1}, C^{\otimes k}) \geq \frac{1}{12} \delta(C)^k. \quad (6)$$

Если $k' \geq 2$, то, применяя $m-k'$ раз лемму 5, получим

$$\begin{aligned} \rho_r(T_m^{k'}, C^{\otimes m}) &\geq \prod_{k=k'+1}^m \rho_r(T_k^{k-1}, C^{\otimes k}) \geq \\ &\geq \frac{1}{12^{m-k'}} \cdot \delta(C)^{\sum_{k=k'+1}^m k} \geq \frac{1}{12^{m-2}} \cdot \delta(C)^M. \end{aligned}$$

Для T_m^1 , применяя предыдущее неравенство с $k' = 2$ и лемму 5, получаем:

$$\rho_r(T_m^1, \mathcal{C}^{\otimes m}) \geq \rho_r(T_2^1, \mathcal{C}^{\otimes 2}) \rho_r(T_m^2, \mathcal{C}^{\otimes m}) \geq \frac{1}{12^{m-2}} \cdot \rho_r(T_2^1, \mathcal{C}^{\otimes 2}) \cdot \delta(\mathcal{C})^M. \quad \square$$

Теперь мы готовы доказать основную теорему и утверждение 1.

Теорема 1. Пусть C_t — примитивный $[n_t, \frac{n_t}{3}]$ код Рида-Соломона над полем $\mathbb{F}_{2^{2t}}$, определённый проверочным многочленом $(x-1)(x-\omega) \dots (x-\omega^{\frac{n_t}{3}-1})$, где $t \in \mathbb{N}$, $n_t = 2^{2t} - 1$, ω — примитивный элемент $\mathbb{F}_{2^{2t}}$. Для каждого $m \geq 3$ существуют $\alpha_r > 0$ и $\alpha_a > 0$, такие, что для всех $t \in \mathbb{N}$ выполняются следующие неравенства:

1. $\rho(\underbrace{C_t, \dots, C_t}_{m \text{ раз}}) \leq \frac{1}{n_t}$;
2. $\rho_r(T_m^k, C_t^{\otimes m}) \geq \alpha_r$ для всех $k \in [m-1]$;
3. $\rho_a(C_t^{\otimes m}) \geq \alpha_a$.

Доказательство. Пункт 1 теоремы следует из леммы 3 и [8, Лемма 11]:

$$\rho(\underbrace{C_t, \dots, C_t}_{m \geq 3 \text{ раз}}) \leq \rho(C_t, C_t, C_t) \leq 1/n_t.$$

Пункт 2 теоремы следует из леммы 6 и следствия 1. Поскольку C_t — это $[n_t, \frac{n_t}{3}, \frac{2}{3}n_t + 1]$ код Рида-Соломона, мы имеем $\delta(C_t) = \frac{2}{3} + \frac{1}{n_t}$. Обозначим $\alpha_r := \frac{1}{72 \cdot 12^{m-2}} \cdot (\frac{2}{3})^{\frac{1}{2}(m-2)(m+3)}$. По лемме 6 и следствию 1 для всех $k \in [m-1]$ имеем

$$\begin{aligned} \rho_r(T_m^k, C_t^{\otimes m}) &\geq \rho_r(T_2^1, C_t^{\otimes 2}) \cdot \frac{1}{12^{m-2}} \cdot \delta(C_t)^{\frac{1}{2}(m-2)(m+3)} > \\ &> \frac{1}{72} \cdot \frac{1}{12^{m-2}} \cdot \left(\frac{2}{3}\right)^{\frac{1}{2}(m-2)(m+3)} = \alpha_r. \end{aligned}$$

Пункт 3 теоремы с $\alpha_a := \frac{2}{3} \frac{\alpha_r}{1+\alpha_r}$ следует из пункта 2 и леммы 1. □

Утверждение 1. Пусть $\mathcal{C} \subsetneq \mathbb{F}_q^n$ и $m \geq 2$. Тогда существует функция α такая, что $\alpha(x) > 0$ при $x > 0$ и

$$\rho_r(T_m^1, \mathcal{C}^{\otimes m}) \geq \alpha(\rho(\underbrace{\mathcal{C}, \dots, \mathcal{C}}_{m \text{ раз}})).$$

Доказательство. Пусть $\rho := \rho(\underbrace{\mathcal{C}, \dots, \mathcal{C}}_{m \text{ раз}})$. Доказательство состоит из следующих шагов:

- Из [8, Лемма 11] следует $\rho(\mathcal{C}, \mathcal{C}) \geq \rho$ и $\delta(\mathcal{C}) = \rho(\mathcal{C}) \geq \rho$.
- Используя [8, Лемма 1], мы имеем $\rho_a(\mathcal{C}^{\otimes 2}) \geq \rho(\mathcal{C}, \mathcal{C}) \geq \rho$.
- Из [2, Лемма 2.9] следует

$$\rho_r(T_2^1, \mathcal{C}^{\otimes 2}) \geq \frac{\rho_a(\mathcal{C}^{\otimes 2})}{2(1 + \rho_a(\mathcal{C}^{\otimes 2}))} \geq \frac{\rho}{2(\rho + 1)} \geq \frac{1}{4}\rho.$$

- Наконец, по лемме 6 имеем

$$\begin{aligned} \rho_r(T_m^1, \mathcal{C}^{\otimes m}) &\geq \left(\frac{1}{12}\right)^{m-2} \rho_r(T_2^1, \mathcal{C}^{\otimes 2}) \cdot \delta(\mathcal{C})^{\frac{1}{2}(m-2)(m+3)} \geq \\ &\geq \frac{1}{12^{m-2}} \cdot \frac{1}{4}\rho \cdot \rho^{\frac{1}{2}(m-2)(m+3)}. \end{aligned}$$

Таким образом, получаем требуемое неравенство с

$$\alpha(\rho) = \frac{1}{4 \cdot 12^{m-2}} \rho^{\frac{1}{2}(m-2)(m+3)+1}.$$

□

3. Связь между робастной тестируемостью и тестируемостью на согласованность

В этом разделе мы доказываем лемму 1, которая утверждает, что робастная тестируемость и тестируемость на согласованность произведений кодов эквивалентны с точностью до постоянного множителя для теста T_m^1 (тест по линиям, параллельным координатным осям).

Лемма 1 (Робастная тестируемость + линейное расстояние = тестируемость на согласованность). Пусть $\mathcal{C} = (\mathcal{C}_1, \dots, \mathcal{C}_m)$ — набор кодов $\mathcal{C}_i \subseteq \mathbb{F}_q^{n_i}$, $\rho_r := \rho_r(T_m^1, \otimes \mathcal{C})$, $\rho_a := \rho_a(\otimes \mathcal{C})$. Тогда

$$\rho_r \geq \frac{1}{4}\rho_a, \quad \rho_a \geq \frac{\rho_r}{\rho_r + 1} \min_{i \in [m]} \delta(\mathcal{C}_i).$$

Доказательство.

1. Тестируемость на согласованность влечёт робастную тестируемость. Рассмотрим произвольное $x \in \mathbb{F}_q^{n_1 \times \dots \times n_m}$. Пусть $y_i := \operatorname{argmin}_{y \in \mathcal{C}^{(i)}} \|y - x\|$ для всех $i \in [m]$. Существует $z \in \otimes \mathcal{C}$ такое, что

$$\rho_a \mathbf{E}_{i \in [m]} \|y_i - z\| \leq \mathbf{E}_{i, j \in [m]} \|y_i - y_j\|.$$

Обозначим $d_x := \mathbf{E}_{\ell \in T_m^1} \delta(x|_\ell, \otimes \mathcal{C}|_\ell)$. Мы имеем

$$d_x = \mathbf{E}_{i \in [m]} \mathbf{E}_{\ell \in \mathcal{C}_i} \delta(x|_\ell, \mathcal{C}_i) = \mathbf{E}_{i \in [m]} \delta(x, \mathcal{C}^{(i)}) = \mathbf{E}_{i \in [m]} \|x - y_i\|.$$

Следовательно,

$$\begin{aligned} \|x - z\| &\leq \mathbf{E}_{i \in [m]} (\|x - y_i\| + \underbrace{\|y_i - z\|}_{\leq \|y_i - z\|_i}) \leq d_x + \frac{1}{\rho_a} \mathbf{E}_{i, j \in [m]} \|y_i - y_j\| \\ &\leq d_x + \frac{1}{\rho_a} \cdot 2 \mathbf{E}_{i \in [m]} \|x - y_i\| = d_x \left(1 + \frac{2}{\rho_a}\right) \leq \frac{4}{\rho_a} d_x. \end{aligned}$$

Таким образом, $\rho_r \geq \rho_a/4$.

2. Робастная тестируемость влечёт тестируемость на согласованность. Рассмотрим произвольные слова $c_i \in \mathcal{C}^{(i)}$ для $i \in [m]$. Пусть

$$i_0 := \operatorname{argmin}_{i \in [m]} \mathbf{E}_{j \in [m]} \delta(c_i, c_j).$$

Тогда

$$\mathbf{E}_{j \in [m]} \|c_{i_0} - c_j\| \leq \mathbf{E}_{i, j \in [m]} \|c_i - c_j\|. \quad (7)$$

Поскольку тест T_m^1 является ρ_r -робастным для $\otimes \mathcal{C}$, то существует $c \in \otimes \mathcal{C}$ такое, что

$$\begin{aligned} \rho_r \|c_{i_0} - c\| &\leq \mathbf{E}_{\ell \in T_m^1} \delta(c_{i_0}|_\ell, \otimes \mathcal{C}|_\ell) = \mathbf{E}_{j \in [m]} \delta(c_{i_0}, \mathcal{C}^{(j)}) \leq \\ &\leq \mathbf{E}_{j \in [m]} \|c_{i_0} - c_j\| \leq \mathbf{E}_{i, j \in [m]} \|c_i - c_j\|. \quad (8) \end{aligned}$$

Пусть $\delta_* := \min_{i \in [m]} \delta(\mathcal{C}_i)$. Для $i \in [m]$, $x \in \mathcal{C}^{(i)}$ имеем $\delta(\mathcal{C}_i) \|x\|_i \leq \|x\|$. Следовательно, применяя неравенство треугольника, затем (7) и (8), получаем:

$$\begin{aligned} \delta_* \mathbf{E}_{i \in [m]} \|c_i - c\|_i &\leq \mathbf{E}_{i \in [m]} \|c_i - c\| \leq \|c_{i_0} - c\| + \mathbf{E}_{i \in [m]} \|c_i - c_{i_0}\| \leq \\ &\leq \left(1 + \frac{1}{\rho_r}\right) \mathbf{E}_{i, j \in [m]} \|c_i - c_j\|. \end{aligned}$$

Следовательно, $\rho_a(\otimes \mathcal{C}) \geq \delta_*(1 + \frac{1}{\rho_r})^{-1}$. □

Благодарности

Эта работа поддержана Министерством науки и высшего образования Российской Федерации (грант 075-15-2020-801).

Список литературы

- [1] P. Panteleev, G. Kalachev, “Asymptotically good quantum and locally testable classical LDPC codes”, *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2022, 375–388. DOI: 10.1145/3519935.3520017.
- [2] I. Dinur, S. Evra, R. Livne, A. Lubotzky, S. Mozes, “Locally testable codes with constant rate, distance, and locality”, *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2022, 357–374. DOI: 10.1145/3519935.3520024.
- [3] I. Dinur, M.-H. Hsieh, T.-C. Lin, T. Vidick, “Good Quantum LDPC Codes with Linear Time Decoders”, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2023, 905–918. DOI: 10.1145/3564246.3585101.
- [4] A. Leverrier, G. Zémor, “Quantum Tanner codes”, *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE Computer Society, Los Alamitos, CA, USA, 2022, 872–883. DOI: 10.1109/FOCS54457.2022.00117.
- [5] A. Leverrier, G. Zémor, “Efficient decoding up to a constant fraction of the code length for asymptotically good quantum codes”, *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2023, 1216–1244. DOI: 10.1137/1.9781611977554.ch45.
- [6] A. Leverrier, G. Zémor, “Decoding Quantum Tanner Codes”, *IEEE Transactions on Information Theory*, **69**:8 (2023), 5100–5115. DOI: 10.1109/TIT.2023.3267945.
- [7] S. Gu, C. A. Pattison, E. Tang, “An Efficient Decoder for a Linear Distance Quantum LDPC Code”, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2023, 919–932. DOI: 10.1145/3564246.3585169.
- [8] G. Kalachev, P. Panteleev, *Two-Sided Robustly Testable Codes*, 2022. DOI: 10.48550/arXiv.2206.09973.

- [9] T.-C. Lin, M.-H. Hsieh, “ c^3 -Locally Testable Codes from Lossless Expanders”, *2022 IEEE International Symposium on Information Theory (ISIT)*, 2022, 1175–1180. DOI: 10.1109/ISIT50566.2022.9834679.
- [10] A. Bhattacharyya, Y. Yoshida, “Linear Properties of Functions”, *Property Testing: Problems and Techniques*, Springer Singapore, Singapore, 2022, 323–368. DOI: 10.1007/978-981-16-8622-1_12.
- [11] A. Polishchuk, D. A. Spielman, “Nearly-Linear Size Holographic Proofs”, *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 1994, 194–203. DOI: 10.1145/195058.195132.
- [12] R. E. Blahut, *Algebraic codes for data transmission*, Cambridge University Press, Cambridge, 2003, ISBN: 9780521553742,0521553741. DOI: 10.1017/CB09780511800467, 482 pp.
- [13] A. Chiesa, P. Manohar, I. Shinkar, “On Axis-Parallel Tests for Tensor Product Codes”, *Theory of Computing*, **16**:5 (2020), 1–34. DOI: 10.4086/toc.2020.v016a005.

Статья поступила 6 марта 2026 г.

High-Dimensional Expansion of Product Codes is Stronger than Robust and Agreement Testability

G. V. Kalachev

We study the coboundary expansion property of product codes called product expansion, which played a key role in all recent constructions of good qLDPC codes. It was shown before that this property is equivalent to robust testability and agreement testability for products of two codes with linear distance. First, we show that robust testability for the product of many codes with linear distance is equivalent to agreement testability. Second, we provide an example of the product of three codes with linear distance that is robustly testable but not product expanding.

Keywords: tensor product code, coboundary expansion, robust testability, agreement testability.

References

- [1] P. Pantelev, G. Kalachev, “Asymptotically good quantum and locally testable classical LDPC codes”, *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2022, 375–388. DOI: 10.1145/3519935.3520017.
- [2] I. Dinur, S. Evra, R. Livne, A. Lubotzky, S. Mozes, “Locally testable codes with constant rate, distance, and locality”, *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2022, 357–374. DOI: 10.1145/3519935.3520024.
- [3] I. Dinur, M.-H. Hsieh, T.-C. Lin, T. Vidick, “Good Quantum LDPC Codes with Linear Time Decoders”, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2023, 905–918. DOI: 10.1145/3564246.3585101.
- [4] A. Leverrier, G. Zémor, “Quantum Tanner codes”, *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE Computer Society, Los Alamitos, CA, USA, 2022, 872–883. DOI: 10.1109/FOCS54457.2022.00117.
- [5] A. Leverrier, G. Zémor, “Efficient decoding up to a constant fraction of the code length for asymptotically good quantum codes”, *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2023, 1216–1244. DOI: 10.1137/1.9781611977554.ch45.
- [6] A. Leverrier, G. Zémor, “Decoding Quantum Tanner Codes”, *IEEE Transactions on Information Theory*, **69**:8 (2023), 5100–5115. DOI: 10.1109/TIT.2023.3267945.
- [7] S. Gu, C. A. Pattison, E. Tang, “An Efficient Decoder for a Linear Distance Quantum LDPC Code”, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2023, 919–932. DOI: 10.1145/3564246.3585169.
- [8] G. Kalachev, P. Pantelev, *Two-Sided Robustly Testable Codes*, 2022. DOI: 10.48550/arXiv.2206.09973.
- [9] T.-C. Lin, M.-H. Hsieh, “ c^3 -Locally Testable Codes from Lossless Expanders”, *2022 IEEE International Symposium on Information Theory (ISIT)*, 2022, 1175–1180. DOI: 10.1109/ISIT50566.2022.9834679.
- [10] A. Bhattacharyya, Y. Yoshida, “Linear Properties of Functions”, *Property Testing: Problems and Techniques*, Springer Singapore, Singapore, 2022, 323–368. DOI: 10.1007/978-981-16-8622-1_12.
- [11] A. Polishchuk, D. A. Spielman, “Nearly-Linear Size Holographic Proofs”, *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 1994, 194–203. DOI: 10.1145/195058.195132.

-
- [12] R. E. Blahut, *Algebraic codes for data transmission*, Cambridge University Press, Cambridge, 2003, ISBN: 9780521553742,0521553741. DOI: 10.1017/CB09780511800467, 482 pp.
- [13] A. Chiesa, P. Manohar, I. Shinkar, “On Axis-Parallel Tests for Tensor Product Codes”, *Theory of Computing*, **16**:5 (2020), 1–34. DOI: 10.4086/toc.2020.v016a005.

Received on March 6, 2026

Проблема полноты линейных дефинитных автоматов

И. В. Молдованов*

В работе исследуется задача полноты в классе линейных дефинитных автоматов над полем из двух элементов относительно операции суперпозиции. Основным результатом является получение критерия полноты для произвольных подмножеств класса линейных дефинитных автоматов, сформулированного в терминах системы замкнутых классов. Полученный критерий обобщает ранее известные результаты, относящиеся к конечнопорожденным подмножествам, содержащим нулевую константу. На его основе доказывается алгоритмическая разрешимость задачи распознавания полноты конечных подмножеств класса линейных дефинитных автоматов.

Ключевые слова: задача полноты, суперпозиция, линейные автоматы, дефинитные автоматы.

1. Введение

Задача исследования полноты естественным образом возникает при изучении функциональных систем. Решение данной проблемы заключается в описании алгоритмических и структурных границ распознаваемости полноты множеств функций для заданной функциональной системы, что позволяет глубже понять свойства рассматриваемых функциональных систем.

С учётом специфики проектирования электронных устройств задача полноты представляет существенный практический интерес применительно к множеству конечных детерминированных автоматов $P_{o,d}$, рассматриваемому относительно операций композиции и суперпозиции. Для класса $P_{o,d}$ с операциями композиции существуют конечные полные системы. Данный факт позволяет установить критериальность [1] континуальной системы предполных классов, содержащихся в указанном множестве [2]. При этом задача распознавания полноты конечных множеств в этом случае является алгоритмически неразрешимой [3, 4]. В то же время

* Молдованов Илья Владимирович — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: jamfr-d@mail.ru, ORCID: 0009-0004-0595-3350.

Moldovanov Ilya Vladimirovich — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

класс $P_{o.d.}$, рассматриваемый относительно операций суперпозиции, не содержит конечных полных систем.

Ввиду структурной сложности множества конечных детерминированных автоматов представляет интерес исследование его подклассов, задаваемых определёнными ограничениями на поведение автоматов. Одним из таких подклассов является класс дефинитных автоматов. Однако задача проверки полноты конечных подмножеств в данном случае также является алгоритмически неразрешимой [5].

В работах [6, 7] были исследованы классы линейных автоматов над конечными полями. Линейные автоматы представляют значительный интерес для вычислительной техники, теории кодирования и в ряде других приложений. Для данных классов были найдены все К-предполные классы [7], а также предложен алгоритм распознавания К-полноты конечных подмножеств [6]. При рассмотрении линейных автоматов относительно операций суперпозиции в [8] было установлено отсутствие конечных полных систем.

Естественным образом возникает класс линейных дефинитных автоматов, который рассматривается в [9]. Данный класс является содержательным подклассом пересечения классов линейных и дефинитных автоматов. Линейным дефинитным автоматом называется автомат, принадлежащий замыканию относительно операций суперпозиции системы, состоящей из задержек с фиксированным начальным состоянием и сумматора. Из представленного определения непосредственно следует, что класс линейных дефинитных автоматов содержит конечные полные системы относительно операций суперпозиции. В работе [10] был получен критерий полноты конечнопорожденных подмножеств данного класса, содержащих нулевую константу, сформулированный в терминах замкнутых классов. Кроме того, в [10] было показано, что на основе указанного критерия может быть построен алгоритм распознавания полноты конечных подмножеств, содержащих нулевую константу. В настоящей работе путём расширения ранее найденной системы замкнутых классов получен критерий полноты произвольных подмножеств класса линейных дефинитных автоматов. Данный критерий может быть использован для построения алгоритма распознавания полноты произвольных конечных подмножеств.

2. Обозначения

Через E_2 обозначим конечное поле из двух элементов $\{0, 1\}$. Через $E_2[\xi]$ обозначим множество многочленов по ξ с коэффициентами из E_2 , и $R_2[\xi]$

— множество формальных степенных рядов по ξ :

$$R_2[\xi] = \left\{ \sum_{t=0}^{\infty} a(t)\xi^t \mid a(t) \in E_2 \right\}.$$

В соответствии с [9], отображение $f(x_1, \dots, x_n) : R_2^n[\xi] \rightarrow R_2[\xi]$ будем называть **линейным дефинитным автоматом**, если $\exists u_0(\xi), u_1(\xi), \dots, u_n(\xi) \in E_2[\xi]$ такие, что $\forall \alpha_1, \dots, \alpha_n \in R_2[\xi]$, имеет место следующее равенство:

$$f(\alpha_1, \dots, \alpha_n) = \sum_{i=1}^n u_i(\xi)\alpha_i + u_0(\xi).$$

Множество всех линейных дефинитных автоматов над E_2 обозначим LD_2 . Для некоторого $M \subseteq LD_2$ замыкание данного множества по операциям суперпозиции будем обозначать $S(M)$.

Упорядочим счётное множество всех неприводимых в $E_2[\xi]$ многочленов p_1, p_2, \dots так, что $p_1 = \xi$. Рассмотрим произвольный неприводимый многочлен p_j степени n_j . Факторкольцо $E_2[\xi] / (p_j) = P_j$ является полем из 2^{n_j} элементов [11]. Для многочлена $u(\xi) \in E_2[\xi]$ через $\langle u(\xi) \rangle_{(p_j)}$ будем обозначать класс вычетов по модулю p_j , которому он принадлежит.

Для данного поля $P_j = E_2[\xi] / (p_j)$, $\deg(p_j) = n_j$, рассмотрим все его максимальные подполя. Пусть $n_j = d_1^{k_1} \dots d_{l_j}^{k_{l_j}}$ — разложение на простые множители. Далее через P_j^s обозначим подполе P_j , содержащее $2^{n_{j,s}}$ элементов, где $n_{j,s} = d_1^{k_1} \dots d_{s-1}^{k_{s-1}} d_s^{k_s-1} d_{s+1}^{k_{s+1}} \dots d_{l_j}^{k_{l_j}}$. Отметим, что множество $\{P_j^s, s \in 1, \dots, l_j\}$ включает все максимальные собственные подполя и только их [12].

Для пары неприводимых многочленов $p_j, p_{j'}$, $j \neq j'$, $\deg(p_j) = \deg(p_{j'})$, рассмотрим факторкольцо $E_2[\xi] / (p_j p_{j'})$. Пусть, $\{R_{j,j'}^s\}$ — все подмножества данного кольца, изоморфные P_j и $P_{j'}$. В [10] было показано существование таких множеств.

3. Класс одноместных линейных дефинитных автоматов, сохраняющих ноль

Рассмотрим подмножество LD_2 , состоящее из линейных дефинитных автоматов с одним входом, сохраняющих ноль. Обозначим данный класс

$LD_2^{(1)}$. Произвольный автомат, принадлежащий $LD_2^{(1)}$, для некоторого $u(\xi) \in E_2[\xi]$ реализует функцию

$$f(x_1) = u(\xi)x_1, \quad u(\xi) \in E_2[\xi].$$

Замыкание некоторого множества $M \subseteq E_2[\xi]$ по операциям сложения и умножения будем обозначать $S^{(1)}(M)$.

Положим $F_+(x_1, x_2) = x_1 + x_2$, автомат, реализующий сумматор. Пусть $\bar{M} \subseteq LD_2^{(1)}$ и $\bar{M}^{(1)} = \{u'(\xi) \mid u'(\xi)x_1 \in \bar{M}\}$. В [6] было показано, что произвольный автомат, содержащийся в замыкании по операциям суперпозиции множества $\bar{M} \cup \{F_+(x_1, x_2)\}$, имеет вид

$$f(x_1, \dots, x_n) = \sum_{i=1}^n v_i(\xi)x_i, \quad v_i(\xi) \in S^{(1)}(\bar{M}^{(1)}).$$

Поэтому, далее в данном разделе будем рассматривать $E_2[\xi]$ с операциями сложения и умножения.

В работе [6] были получены приведённые ниже результаты.

Определение 1. Определим семейство подмножеств $E_2[\xi]$:

$$RP_j^{(1)} = \{u(\xi) \mid u(\xi) \in E_2[\xi], u(\xi) : p_j(\xi)\}, \quad j \in \mathbb{N},$$

$$MP_j^{(1)} = \{u(\xi) \mid u(\xi) \in E_2[\xi], (u(\xi) + u(0)) : \xi p_j\}, \quad j \in \mathbb{N}.$$

Обозначим $JP^{(1)} = \{RP_j^{(1)} \mid j \in \mathbb{N}\} \cup \{MP_j^{(1)} \mid j \in \mathbb{N}\}$.

Лемма 1. Пусть $M \subseteq E_2[\xi]$. Если $M \not\subseteq \Theta$, $\forall \Theta \in JP^{(1)}$, то существует $V(\xi) \in E_2[\xi]$, $V(\xi) \neq 0$, такой, что $\forall v(\xi) \in E_2[\xi]$ многочлен $V(\xi) \cdot v(\xi) \in S^{(1)}(M)$.

На основании леммы 1 в [10] было сформулировано следующее утверждение, которое согласуется с известными результатами [13], [14], [15].

Определение 2. Определим семейство подмножеств $E_2[\xi]$:

$$L_{j,s}^{(1)} = \{u(\xi) \mid u(\xi) \in E_2[\xi], \langle u(\xi) \rangle_{(p_j)} \in P_j^s\}, \quad j \in \mathbb{N},$$

$$N_j^{(1)} = \{v^2(\xi) + p_j^2 u(\xi) \mid v(\xi), u(\xi) \in E_2[\xi], \deg(v(\xi)) < \deg(p_j)\}, \quad j \in \mathbb{N},$$

$$I_{j,j',s}^{(1)} = \{u(\xi) \mid u(\xi) \in E_2[\xi], \langle u(\xi) \rangle_{(p_j p_{j'})} \in R_{j,j',s}^s\}, \quad j \in \mathbb{N}, j' \in \mathbb{N}, j > j',$$

$$\deg(p_j) = \deg(p_{j'}).$$

Обозначим $H^{(1)} = \{L_{j,s}^{(1)}\} \cup \{N_j^{(1)}\} \cup \{I_{j,j',s}^{(1)}\}$.

Теорема 1. Пусть $M \subseteq E_2[\xi]$. $S^{(1)}(M) = E_2[\xi] \iff M \not\subseteq \Theta, \forall \Theta \in JP^{(1)} \cup H^{(1)}$.

4. Выразимость сумматора и задержки с добавками

Рассмотрим два автомата

$$\tilde{F}_+(x_1, x_2, z) = x_1 + x_2 + \tilde{F}'_+(z), \quad \tilde{F}_\xi(x_1, z) = \xi x_1 + \tilde{F}'_\xi(z),$$

где $\tilde{F}'_+(z)$, $\tilde{F}'_\xi(z)$ принадлежат LD_2 . Данные автоматы, с точностью до некоторой добавки, реализуют сумматор от двух переменных и задержку с нулевым начальным состоянием, соответственно. Обозначим через \tilde{A} множество пар $\{\{x_1 + x_2 + \tilde{F}'_+(z), \xi x_1 + \tilde{F}'_\xi(z)\} \mid \tilde{F}'_+(z), \tilde{F}'_\xi(z) \in LD_2\}$, а через $\tilde{S}(M)$ — множество $\{\{f_1, f_2\} \mid f_1, f_2 \in S(M)\}$. Если для $M \subseteq LD_2$ имеем $\tilde{S}(M) \cap \tilde{A} \neq \emptyset$, то будем говорить, что $\tilde{F}_+(x_1, x_2, z)$, $\tilde{F}_\xi(x_1, z) \in S(M)$ для некоторых добавок $\tilde{F}'_+(z)$, $\tilde{F}'_\xi(z) \in LD_2$.

Обозначим $U(f)$ — множество коэффициентов при переменных автомата $f \in LD_2$.

Определение 3. Определим семейство подмножеств LD_2 :

$$\begin{aligned} L_{j,s} &= \{ f \mid f \in LD_2, U(f) \subset L_{j,s}^{(1)} \}, \quad j \in \mathbb{N}, \\ N_j &= \{ f \mid f \in LD_2, U(f) \subset N_j^{(1)} \}, \quad j \in \mathbb{N}, \\ I_{j,j',s} &= \{ f \mid f \in LD_2, U(f) \subset I_{j,j',s}^{(1)} \}, \quad j \in \mathbb{N}, \quad j' \in \mathbb{N}, \\ &\quad j > j', \quad \deg(p_j) = \deg(p_{j'}), \\ V_j &= \{ f \mid f \in LD_2, f = \sum_{i=1}^n u_i(\xi)x_i + u_0(\xi) \text{ и среди} \\ &\quad \text{многочленов } u_i(\xi) \text{ существует не более одного такого, что} \\ &\quad p_j \nmid u_i(\xi) \}, \quad j \in \mathbb{N}, \\ P_J &= \{ f \mid f \in LD_2, f = \sum_{i=1}^n u_i(\xi)x_i + u_0(\xi) \text{ и } \forall \{j, j'\} \subset J, \\ &\quad j \neq j', \quad \nexists u_i(\xi), u_{i'}(\xi) \in U(f), \quad i \neq i', \text{ таких, что} \\ &\quad p_j \nmid u_i(\xi), \quad p_{j'} \nmid u_{i'}(\xi) \}, \quad J \subset \mathbb{N}, \quad 2 \leq |J| < \infty, \\ \bar{P} &= \{ f \mid f \in LD_2, f = \sum_{i=1}^n u_i(\xi)x_i + u_0(\xi) \text{ и } n = 1 \\ &\quad \text{или } \exists p_j \text{ такой, что } U(f) \subset \langle 0 \rangle_{(p_j)} \}. \end{aligned}$$

Обозначим $\bar{H} = \{L_{j,s}\} \cup \{N_j\} \cup \{I_{j,j',s}\} \cup \{V_j\} \cup \{P_J\} \cup \{\bar{P}\}$. Σ -замкнутость в LD_2 всех классов кроме \bar{P} показана в [10].

Лемма 2. Множество \bar{P} замкнуто в LD_2 относительно операций суперпозиции.

Доказательство. Переименование переменных и подстановка, очевидно, не выводят за пределы данного класса. Отождествление переменных применимо только в случае $n > 1$, то есть существует неприводимый многочлен p_j , который делит коэффициент при любой переменной автомата, следовательно, p_j также делит сумму произвольных коэффициентов. \square

Положим $H = \bar{H} \setminus \{\bar{P}\}$. Пусть $M \subseteq LD_2$ — конечно порождённое. В работе [10] было показано, что если $M \not\subseteq \Theta$, $\forall \Theta \in H$, то $\tilde{S}(M) \cap \tilde{A} \neq \emptyset$. Также в [10] были доказаны следующие утверждения, представленные ниже в качестве лемм.

Лемма 3. Пусть $M \subseteq LD_2$. Если $M \not\subseteq \Theta$, $\forall \Theta \in \{L_{1,0}, L_{1,1}\} \cup \{N_1\} \cup \{V_1\}$, то $\exists u_1(\xi) \in E_2[\xi]$, $Q'_1(z) \in LD_2$, что автомат

$$Q_1(x_1, z) = (\xi + \xi^2 u_1(\xi))x_1 + Q'_1(z),$$

содержится в $S(M)$.

Лемма 4. Пусть $M \subseteq LD_2$, $D = \{p_{j_1}, \dots, p_{j_K}\}$, $K > 1$, — конечное множество неприводимых многочленов и $\xi \in D$. Если $M \not\subseteq \Theta$, $\forall \Theta \in \{L_{j,s} \mid p_j \in D\} \cup \{N_j \mid p_j \in D\} \cup \{V_j \mid p_j \in D\} \cup \{I_{j,j',s} \mid \deg(p_j) = \deg(p_{j'})$, $p_j, p_{j'} \in D\} \cup \{P_{j,j'}\}$, $p_j, p_{j'} \in D\}$, то $\forall p_j \in D$, $\exists u_j(\xi) \in E_2[\xi]$, $Q'_j(z) \in LD_2$, что автомат

$$Q_j(x_1, z) = (\xi + \xi p_j u_j(\xi))x_1 + Q'_j(z),$$

содержится в $S(M)$.

Лемма 5. Пусть $M \subseteq LD_2$ и $D = \{p_{j_1}, \dots, p_{j_K}\}$, $K \geq 1$ — конечное множество неприводимых многочленов. Если $M \not\subseteq \Theta$, $\forall \Theta \in \{V_j \mid p_j \in D\} \cup \{P_J \mid J \subset \mathbb{N}, |J| > 1, p_j \in D \iff j \in J\}$, то найдутся $u_i(\xi) \in E_2[\xi]$, $p_{j_i} \nmid u_i(\xi)$, $i = 1, \dots, K$, такие что $\forall s \in \mathbb{N}$, $\exists H'_{D,s}(z) \in LD_2$, для которого

$$H_{D,s}(x_{1,1}, \dots, x_{2^s,1}, \dots, x_{1,K}, \dots, x_{2^s,K}, z) = \sum_{i=1}^K \sum_{l=1}^{2^s} u_i^{2^s-1}(\xi) x_{i,l} + H'_{D,s}(z)$$

принадлежит $S(M)$.

Покажем, что система \bar{H} , получающаяся из H добавлением класса \bar{P} , является критериальной относительно проверки соотношения $\tilde{S}(M) \cap \tilde{A} \neq \emptyset$ для подмножеств $M \subseteq LD_2$.

Пусть $u(\xi) \in E_2[\xi]$, $u(\xi) \neq 0$, тогда обозначим $D(u(\xi)) = \{p_j \mid u(\xi) : p_j\}$.

Лемма 6. Пусть $M \subseteq LD_2$. Если $M \not\subseteq \bar{P}$, то найдутся $m(\xi) \in E_2[\xi]$ и $n \in \mathbb{N}$, $\{v_i(\xi) \mid i = 1, \dots, n\} \subset E_2[\xi]$, что для произвольного $T = 2^t$, $t \in \mathbb{N}$ автомат

$$B_T(x_1, \dots, x_n, y_1, \dots, y_T, z) = \sum_{i=1}^n v_i(\xi)x_i + \sum_{l=1}^T m^T(\xi)y_l + B'_T(z),$$

$$\text{НОД}(v_i(\xi), i = 1, \dots, n) = 1, \quad D(m(\xi)) \subseteq \bigcup_{i=1}^n D(v_i(\xi)), \quad n \geq 2,$$

принадлежит $S(M)$.

Доказательство. По условию в множестве $M \setminus \bar{P}$ содержится автомат

$$B(x_1, \dots, x_n) = \sum_{i=1}^n u_i(\xi)x_i + u_0(\xi), \quad \text{НОД}(u_i(\xi), i = 1, \dots, n) = 1, \quad n \geq 2.$$

Обозначим Z^k , $k \in \mathbb{Z}_+$ — набор, состоящий из k идущих подряд переменных z , и рассмотрим подстановку

$$\begin{aligned} \bar{B}(x_1, \dots, x_n, y_1, y_2, z) &= B(B(x_1, y_1, Z^{n-2}), B(y_2, x_2, Z^{n-2}), x_3, \dots, x_n) = \\ &= u_1^2(\xi)x_1 + u_2^2(\xi)x_2 + \sum_{i=3}^n u_i(\xi)x_i + u_1(\xi)u_2(\xi)y_1 + u_1(\xi)u_2(\xi)y_2 + \bar{B}'(z) = \\ &= \sum_{i=1}^n u'_i(\xi)x_i + m(\xi)y_1 + m(\xi)y_2 + \bar{B}'(z). \end{aligned}$$

По построению автомата \bar{B} , имеем

$$\text{НОД}(\{u'_i(\xi), i = 1, \dots, n\}) = 1, \quad D(m(\xi)) \subseteq \bigcup_{i=1}^n D(u'_i(\xi)), \quad n \geq 2.$$

Индукцией по $t \in \mathbb{N}$ докажем утверждение леммы. База индукции реализуется

$$B_2 = \bar{B}(x_1, \dots, x_n, \bar{B}(Z^n, y_1, y_2, z), z, z) \in S(M).$$

В качестве шага индукции рассмотрим подстановку

$$\begin{aligned} B_{2T}(x_1, \dots, x_n, y_1, \dots, y_{2T}, z) &= \\ B_T(x_1, \dots, x_n, B_T(Z^n, y_1, \dots, y_T, z), B_T(Z^n, y_{T+1}, \dots, y_{2T}, z), Z^{T-2}, z) & \\ \in S(M). \end{aligned}$$

□

Лемма 7. Пусть $M \subseteq LD_2$. Если $\forall \Theta, \Theta \in \bar{N}$ имеем $M \not\subseteq \Theta$, то для некоторого $V(\xi) \in E_2[\xi]$, $V(\xi) \neq 0$ и произвольного $v(\xi) \in E_2[\xi]$, найдётся автомат $U_{v(\xi)}(x_1, z) \in S(M)$, что для некоторого $U'_{v(\xi)}(z) \in LD_2$ выполнено

$$U_{v(\xi)}(x_1, z) = v(\xi)V(\xi)x_1 + U'_{v(\xi)}(z) \in S(M).$$

Доказательство. По условию $M \not\subseteq \bar{P}$, следовательно по лемме 6 существуют $m(\xi) \in E_2[\xi]$ и $n \in \mathbb{N}$, $\{u_i(\xi) \mid i = 1, \dots, n\} \subset E_2[\xi]$, что автомат

$$B_T(x_1, \dots, x_n, y_1, \dots, y_T, z) = \sum_{i=1}^n u_i(\xi)x_i + \sum_{l=1}^T m^T(\xi)y_l + B'_T(z), \quad (1)$$

$$\text{НОД}(u_i(\xi), i = 1, \dots, n) = 1, \quad D(m(\xi)) \subseteq \bigcup_{i=1}^n D(u_i(\xi)), \quad n \geq 2,$$

принадлежит $S(M)$ для произвольного $T = 2^t$, $t \in \mathbb{N}$.

Многочлен $m(\xi)$, участвующий в выражении (1), имеет вид $m(0) + \xi m'(\xi)$. Если $m(0) = 0$, то положим $D_1 = \emptyset$, $S_1 = 0$, иначе $D_1 = D(m'(\xi)) \cup \{\xi\}$, $S_1 = |D_1|$. Для некоторого $T_1 \geq 2(S_1 + 1)$, $T_1 = 2^t$, $t \in \mathbb{N}$ рассмотрим автомат B_{T_1} . Обозначим $\bar{X}^{k_1}, \bar{Y}_1^{k_2}, \bar{Y}_2^{k_3}$, $k_1, k_2, k_3 \in \mathbb{N}$ — наборы идущих подряд и последовательно-пронумерованных переменных x_* и $y_{*,1}, y_{*,2}$, соответственно:

$$B_{T_1}(\bar{X}^n, \bar{Y}_1^{T_1/2}, \bar{Y}_2^{T_1/2}, z) = \sum_{i=1}^n u'_i(\xi)x_i + \sum_{l=1}^{T_1/2} m^{T_1}(\xi)y_{l,1} + \sum_{l=1}^{T_1/2} m^{T_1}(\xi)y_{l,2} + B'_{T_1}(z).$$

Имеем $D_1 = \{p_{j_1}, \dots, p_{j_{S_1}}\}$. По леммам 3 и 4 для любого $p_j \in D_1$, $\exists q_j(\xi) \in E_2[\xi]$, $Q'_j(z) \in LD_2$, что автомат

$$Q_j(x_1, z) = (\xi + \xi p_j q_j(\xi))x_1 + Q'_j(z),$$

содержится в $S(M)$.

Рассмотрим подстановку

$$\tilde{B}(\bar{X}^n, \bar{Y}_1^{S_1+1}, \bar{Y}_2^{S_1+1}, z) = B_{T_1}(\bar{X}^n, Q_{j_1}(y_{1,1}, z), \dots, Q_{j_{S_1}}(y_{S_1,1}, z), y_{S_1+1,1},$$

$$Q_{j_1}(y_{1,2}, z), \dots, Q_{j_{S_1}}(y_{S_1,2}, z), y_{S_1+1,2}, z) = \sum_{i=1}^n u'_i(\xi)x_i + \sum_{l=1}^{S_1} w_l(\xi)y_{l,1} +$$

$$+ \sum_{l=1}^{S_1} w_l(\xi)y_{l,2} + m^{T_1}(\xi)y_{S_1+1,1} + m^{T_1}(\xi)y_{S_1+1,2} + \tilde{B}'(z) \in S(M).$$

В случае если $m(0) = 1$, то $m^{2^s}(\xi) = m(0)^{2^s} + (\xi m'(\xi))^{2^s}$ в поле характеристики 2, следовательно, для произвольного p_{j_l} , $p_{j_l} \in D_1$ имеем

$$w_l(\xi) = (1 + \xi p_{j_l} m''(\xi)) \cdot (\xi + \xi p_{j_l} q_{j_l}(\xi)) = \xi(p_{j_l} w_l''(\xi) + 1) \notin MP_{j_l}^{(1)}. \quad (2)$$

Из выражений (1) и (2) следует

$$U(\tilde{B}(\bar{X}^n, \bar{Y}_1^{S_1+1}, \bar{Y}_2^{S_1+1}, z)) \not\subseteq \Theta, \forall \Theta \in JP^{(1)},$$

и все коэффициенты при переменных набора \bar{Y}_1 продублированы коэффициентами при переменных набора \bar{Y}_2 .

Положим $D_2 = \bigcup_{i=1}^n D(u_i(\xi))$, $S_2 = |D_2|$, тогда лемме 5 $S(M)$ принадлежит автомат

$$H_1(\bar{X}_1^{S_2}, \bar{X}_2^{S_2}, z) = \sum_{i=1}^{S_2} (\tilde{u}_i(\xi)x_{i,1} + \tilde{u}_i(\xi)x_{i,2}) + H_1'(z), \quad p_{j_i} \nmid \tilde{u}_i(\xi), \quad p_{j_i} \in D_2. \quad (3)$$

Рассмотрим подстановку

$$\underbrace{\tilde{B}(H_1(\bar{X}_1^{S_2}, \bar{X}_2^{S_2}, z), \dots, H_1(\bar{X}_1^{S_2}, \bar{X}_2^{S_2}, z))}_{n \text{ раз}}, \bar{Y}_1^{S_1+1}, \bar{Y}_2^{S_1+1}, z).$$

Из выражений (1) и (3) следует, что отождествлением части переменных наборов \bar{X}_1 и \bar{X}_2 в переменную z , полученный автомат можно привести к виду

$$\begin{aligned} \hat{B}(\bar{X}_1^{S_2}, \bar{X}_2^{S_2}, \bar{Y}_1^{S_1+1}, \bar{Y}_2^{S_1+1}, z) &= \sum_{i=1}^{S_2} \hat{u}_i(\xi)x_{i,1} + \sum_{i=1}^{S_2} \hat{u}_i(\xi)x_{i,2} + \\ &+ m^{\bar{S}_1}(\xi)y_{S_1+1,1} + m^{\bar{S}_1}(\xi)y_{S_1+1,2} + \sum_{l=1}^{S_1} w_l(\xi)y_{l,1} + \sum_{l=1}^{S_1} w_l(\xi)y_{l,2} + \hat{B}'(z), \\ p_{j_i} \nmid \hat{u}_i(\xi), \quad p_{j_i} \in D_2, \quad D(m(\xi)) \subseteq D_2. \end{aligned}$$

Имеем

$$\begin{aligned} \hat{B}(\bar{X}_1^{S_2}, \bar{X}_2^{S_2}, \bar{Y}_1^{S_1+1}, \bar{Y}_2^{S_1+1}, z) &\in S(M), \\ U(\hat{B}(\bar{X}_1^{S_2}, \bar{X}_2^{S_2}, \bar{Y}_1^{S_1+1}, \bar{Y}_2^{S_1+1}, z)) &\not\subseteq \Theta, \forall \Theta \in JP^{(1)} \end{aligned}$$

и все коэффициенты при переменных наборов \bar{X}_1 и \bar{Y}_1 продублированы коэффициентами при соответствующих переменных наборов \bar{X}_2 и \bar{Y}_2 . В [10] было показано, что из описанных выше условий и леммы 1 следует утверждение данной леммы. \square

Докажем основное утверждение раздела — критерий принадлежности сумматора и задержки, с точностью до некоторых добавок, Σ -замыканию произвольного подмножества LD_2 .

Теорема 2. Пусть $M \subseteq LD_2$. Если $M \not\subseteq \Theta$, $\forall \Theta \in \bar{H}$, то $\tilde{S}(M) \cap \tilde{A} \neq \emptyset$.

Доказательство. По лемме 6 автомат

$$P(\bar{X}^n, y_1, y_2, z) = \sum_{i=1}^n u_i(\xi)x_i + m(\xi)y_1 + m(\xi)y_2 + P'(z), \quad (4)$$

$$\text{НОД}(\{u_i(\xi), i = 1, \dots, n\}) = 1, \quad D(m(\xi)) \subseteq \bigcup_{i=1}^n D(u_i(\xi)), \quad n \geq 2.$$

принадлежит $S(M)$.

По лемме 7 $\exists V(\xi) \in E_2[\xi]$, такой, что $\forall v(\xi) \in E_2[\xi]$ автомат

$$U_{v(\xi)}(x_1, z) = v(\xi)V(\xi)x_1 + U'_{v(\xi)}(z) \in S(M). \quad (5)$$

Положим $D = \bigcup_{i=1}^n D(u_i(\xi)) \cup D(V(\xi)) = \{p_{j_1}, \dots, p_{j_T}\}$, $T = |D|$. Для фиксированного i , $p_{j_i} \in D$ обозначим

$$Cl_i = \{L_{j_i, k}\} \cup \{N_{j_i}\} \cup \{V_{j_i}\} \cup \{I_{j_i, j_{i'}, k} \mid \deg(p_{j_i}) = \deg(p_{j_{i'}}), p_{j_{i'}} \in D\}.$$

Пусть $T' = \max_{i=1}^T |Cl_i|$, тогда по лемме 5 для некоторого $\bar{T} \geq 4(T' + 1)$, $\bar{T} = 2^t$, $t \in \mathbb{N}$ автомат

$$H_{D, t}(\bar{X}^{T \cdot \bar{T}}, z) = \sum_{i=1}^T \sum_{k=1}^{\bar{T}} \bar{u}_i^{\bar{T}/2}(\xi)x_{(i-1)\bar{T}+k} + H'_{D, t}(z), \quad p_{j_i} \nmid \bar{u}_i(\xi), \quad p_{j_i} \in D$$

принадлежит $S(M)$. Положим $\hat{T} = \bar{T}/4$ и переименуем переменные данного автомата следующим образом

$$\begin{aligned} H(\bar{X}_1^{T\hat{T}}, \bar{X}_2^{T\hat{T}}, \bar{X}_3^{T\hat{T}}, \bar{X}_4^{T\hat{T}}, z) &= \sum_{i=1}^T \sum_{k=1}^{\hat{T}} \bar{u}_i^{\hat{T}/2}(\xi)x_{(i-1)\hat{T}+k,1} + \\ &+ \sum_{i=1}^T \sum_{k=1}^{\hat{T}} \bar{u}_i^{\hat{T}/2}(\xi)x_{(i-1)\hat{T}+k,2} + \sum_{i=1}^T \sum_{k=1}^{\hat{T}} \bar{u}_i^{\hat{T}/2}(\xi)x_{(i-1)\hat{T}+k,3} + \\ &\sum_{i=1}^T \sum_{k=1}^{\hat{T}} \bar{u}_i^{\hat{T}/2}(\xi)x_{(i-1)\hat{T}+k,4} + H'(z), \quad p_{j_i} \nmid \bar{u}_i(\xi), \quad p_{j_i} \in D. \end{aligned} \quad (6)$$

Рассмотрим подстановку

$$P(H(\bar{X}_1^{T\hat{T}}, \bar{X}_2^{T\hat{T}}, \bar{X}_3^{T\hat{T}}, \bar{X}_4^{T\hat{T}}, z), \dots, H(\bar{X}_1^{T\hat{T}}, \bar{X}_2^{T\hat{T}}, \bar{X}_3^{T\hat{T}}, \bar{X}_4^{T\hat{T}}, z), y_1, y_2, z).$$

Из выражений (4) и (6) следует, что, используя операцию отождествления переменных, из данного автомата можно получить автомат:

$$\begin{aligned} \tilde{P}(\bar{X}_1^{T\hat{T}}, \bar{X}_2^{T\hat{T}}, \bar{X}_3^{T\hat{T}}, \bar{X}_4^{T\hat{T}}, y_1, y_2, z) &= \sum_{i=1}^T \sum_{k=1}^{\hat{T}} \tilde{u}_i^{\hat{T}/2}(\xi) x_{(i-1)\hat{T}+k,1} + \\ &\sum_{i=1}^T \sum_{k=1}^{\hat{T}} \tilde{u}_i^{\hat{T}/2}(\xi) x_{(i-1)\hat{T}+k,2} + \sum_{i=1}^T \sum_{k=1}^{\hat{T}} \tilde{u}_i^{\hat{T}/2}(\xi) x_{(i-1)\hat{T}+k,3} + \\ &\sum_{i=1}^T \sum_{k=1}^{\hat{T}} \tilde{u}_i^{\hat{T}/2}(\xi) x_{(i-1)\hat{T}+k,4} + m(\xi)y_1 + m(\xi)y_2 + \tilde{P}'(z), \\ p_{j_i} \uparrow \tilde{u}_i(\xi), p_{j_i} \in D, D(m(\xi)) \cup D(V(\xi)) \subseteq D. \end{aligned} \quad (7)$$

Рассмотрим $Cl_i = \{\Theta_{1,i}^{(1)}, \dots, \Theta_{L_i,i}^{(1)}\}$, $L_i \leq \hat{T}$, $i = 1, \dots, T$. По условию теоремы и по определению классов, принадлежащих сериям $L_{j,s}, N_j, I_{j,j',s}$, для любой пары (k, i) , $i = 1, \dots, T$, $k = 1, \dots, L_i$ и некоторого $q_{k,i}(\xi) \in E_2[\xi]$, $q_{k,i}(\xi) \notin \Theta_{k,i}^{(1)}$ автомат

$$Q_{k,i}(x_1, z) = q_{k,i}(\xi)x_1 + Q'_{k,i}(z),$$

принадлежит $S(M)$. Рассмотрим симметричную относительно наборов переменных $\bar{X}_1^{T\hat{T}}, \bar{X}_2^{T\hat{T}}, \bar{X}_3^{T\hat{T}}$ и $\bar{X}_4^{T\hat{T}}$ подстановку. Опишем только преобразования переменных, входящих в $\bar{X}_1^{T\hat{T}}$. Данный набор разобьём на подгруппы $\bar{X}_{1,1}^{\hat{T}}, \dots, \bar{X}_{T,1}^{\hat{T}}$, имеем

$$\begin{aligned} \hat{P}(\bar{X}_{1,1}^{L_1}, \dots, \bar{X}_{T,1}^{L_T}, \dots, y_1, y_2, z) = \\ \tilde{P}(\sigma_{1,1,1}, \dots, \sigma_{\hat{T},1,1}, \dots, \sigma_{1,T,1}, \dots, \sigma_{\hat{T},T,1}, \dots, y_1, y_2, z). \end{aligned}$$

Внутри подгруппы с номером i , $1 \leq i \leq T$ определим подстановку по следующему правилу:

$$\sigma_{k,i,1} = \begin{cases} Q_{k,i}(x_{k,i,1}, z), & 1 \leq k \leq L_i \\ x_{k,i,1}, & k = L_i + 1 \\ z, & L_i + 1 < k \leq \hat{T} \end{cases} .$$

Таким образом, учитывая соотношение $\hat{T} \geq L_i + 1$, $i = 1, \dots, T$, каждая подгруппа заканчивается набором из $\hat{T} - L_i - 1$ переменных z . Имеем

$$\begin{aligned} & \hat{P}(\bar{X}_{1,1}^{L_1+1}, \dots, \bar{X}_{T,1}^{L_T+1}, \dots, y_1, y_2, z) = \\ & = \tilde{P}(Q_{1,1}(x_{1,1,1}, z), \dots, Q_{L_1,1}(x_{L_1,1,1}, z), x_{L_1+1,1,1}, Z^{\hat{T}-L_1-1}, \dots, \\ & \quad Q_{1,T}(x_{1,T,1}, z), \dots, Q_{L_T,T}(x_{L_T,T,1}, z), x_{L_T+1,T,1}, Z^{\hat{T}-L_T-1}, \dots, y_1, y_2, z) = \\ & = \sum_{i=1}^T \left(\sum_{k=1}^{L_i} w_{k,i}(\xi) x_{k,i,1} + x_{k,L_i+1,1} \right) + \sum_{i=1}^T \left(\sum_{k=1}^{L_i} w_{k,i}(\xi) x_{k,i,2} + x_{k,L_i+1,2} \right) + \\ & + \sum_{i=1}^T \left(\sum_{k=1}^{L_i} w_{k,i}(\xi) x_{k,i,3} + x_{k,L_i+1,3} \right) + \sum_{i=1}^T \left(\sum_{k=1}^{L_i} w_{k,i}(\xi) x_{k,i,4} + x_{k,L_i+1,4} \right) + \\ & + m(\xi)y_1 + m(\xi)y_2 + \hat{P}'(z), \quad w_{k,i}(\xi) \notin \Theta_{k,i}^{(1)}, \quad D(m(\xi)) \cup D(V(\xi)) \subseteq D. \end{aligned}$$

Для обозначенного автомата выполнено

$$\begin{aligned} U(\hat{P}(\dots)) \not\subseteq \Theta, \quad \forall \Theta \in \{L_{j,s} \mid p_j \in D\} \cup \{N_j \mid p_j \in D\} \cup \\ \cup \{V_j \mid p_j \in D\} \cup \{I_{j,j',s} \mid \deg(p_j) = \deg(p_{j'}), p_j, p_{j'} \in D\}. \end{aligned} \quad (8)$$

В работе [10] было показано, что из выражения (8) следует, что для любых $\{n_1, \dots, n_T \mid n_i \in \mathbb{N}\}$, $r(\xi) \in E_2[\xi]$, $\deg(r(\xi)) < \sum_{i=1}^T n_i \deg(p_{j_i})$, $p_{j_i} \in D$ и некоторых $w_{r(\xi)}(\xi) \in E_2[\xi]$, $B'_{r(\xi)}(z) \in LD_2$ автомат

$$\begin{aligned} B_{r(\xi)}(x_1, x_2, y_1, y_2, z) = \left(r(\xi) + w_{r(\xi)}(\xi) \prod_{i=1}^T p_{j_i}^{n_i} \right) x_1 + \\ + \left(r(\xi) + w_{r(\xi)}(\xi) \prod_{i=1}^T p_{j_i}^{n_i} \right) x_2 + m(\xi)y_1 + m(\xi)y_2 + B'_{r(\xi)}(z) \in S(M). \end{aligned}$$

Так как $D(m(\xi)) \cup D(V(\xi)) \subseteq D$ из выражения (7), то подстановкой автоматов вида (5) вместо переменных y_1 и y_2 , можно показать, что автоматы

$$\begin{aligned} \tilde{F}_+(x_1, x_2, y_1, y_2, z) = \left(1 + w_1(\xi)(\xi) \prod_{i=1}^T p_{j_i}^{n_i} \right) x_1 + \left(1 + w_1(\xi)(\xi) \prod_{i=1}^T p_{j_i}^{n_i} \right) x_2 \\ + w_1(\xi)(\xi) \prod_{i=1}^T p_{j_i}^{n_i} y_1 + w_1(\xi)(\xi) \prod_{i=1}^T p_{j_i}^{n_i} y_2 + \tilde{F}'_+(z), \\ \tilde{F}_\xi(x_1, y_1, z) = \left(\xi + w_\xi(\xi) \prod_{i=1}^T p_{j_i}^{n_i} \right) x_1 + w_\xi(\xi) \prod_{i=1}^T p_{j_i}^{n_i} y_1 + \tilde{F}'_\xi(z), \end{aligned}$$

принадлежат $S(M)$. Отождествление соответствующих пар переменных x_1, y_1 и x_2, y_2 , завершает доказательство теоремы. \square

5. Выразимость константы 0

Пронумеруем элементы поля P_j , $\deg(p_j) = n_j$ в двоичном порядке по коэффициентам их представителей в полиномиальном базисе $(1, \xi, \dots, \xi^{n_j-1})$. Для

$$s = \sum_{k=0}^{n_j-1} a_k 2^k, \quad a_k \in \{0, 1\},$$

положим

$$\langle r_s(\xi) \rangle_{(p_j)} = \left\langle \sum_{k=0}^{n_j-1} a_k \xi^k \right\rangle_{(p_j)}.$$

Определение 4. Определим семейство подмножеств LD_2 :

$$S_{j,s} = \{ f \mid f \in LD_2, f = \sum_{i=1}^n u_i(\xi)x_i + u_0(\xi) \text{ и}$$

$\forall v_1, \dots, v_n \in \langle r_s(\xi) \rangle_{(p_j)}$ имеем

$$\left(\sum_{i=1}^n u_i(\xi)v_i(\xi) + u_0(\xi) \right) \in \langle r_s(\xi) \rangle_{(p_j)} \}, j \in \mathbb{N}, s = 1, \dots, 2^{\deg(p_j)},$$

$$U_j = \{ f \mid f \in LD_2, f = \sum_{i=1}^n u_i(\xi)x_i + u_0(\xi) \text{ и } \left(\sum_{i=1}^n u_i(\xi) \right) \in \langle 1 \rangle_{(p_j)} \},$$

$j \in \mathbb{N}$.

Обозначим $H_0 = \{S_{j,s} \mid j \in \mathbb{N}, s = 1, \dots, 2^{\deg(p_j)}\} \cup \{U_j \mid j \in \mathbb{N}\}$.

Лемма 8. Для любого $\Theta \in H_0$ множество Θ замкнуто в LD_2 относительно операций суперпозиции.

Доказательство. Зафиксируем $j \in \mathbb{N}$ и рассмотрим классы $S_{j,s}$ и U_j .

Операция переименования переменных не выводит за пределы обозначенных классов, так как не изменяет коэффициенты при переменных автомата.

Рассмотрим операцию отождествления. Отображение $E_2[\xi] \rightarrow E_2[\xi] / (p_j)$,

которое ставит в соответствие многочлену его остаток по модулю неприводимого многочлена p_j , является гомоморфизмом, следовательно, сложение коэффициентов при переменных не выводит за пределы класса Θ , $\forall \Theta \in H_0$.

Рассмотрим операцию подстановки. Пусть, без ограничения общности, автомат $g(x_1, \dots, x_{n-1}, y_1, \dots, y_k)$ получается из автомата $f(x_1, \dots, x_n)$ подстановкой $h(y_1, \dots, y_k)$ вместо переменной x_n :

$$g(x_1, \dots, x_{n-1}, y_1, \dots, y_k) = \sum_{i=1}^{n-1} u_i(\xi)x_i + u_n(\xi)\left(\sum_{l=1}^k u'_l(\xi)y_l + u'_0(\xi)\right) + u_0(\xi).$$

Пусть $\Theta \in \{S_{j,s} \mid j \in \mathbb{N}, s = 1, \dots, 2^{\deg(p_j)}\}$. По определению $\forall v'_1(\xi), \dots, v'_k(\xi) \in \langle r_s(\xi) \rangle_{(p_j)}$, имеем $\langle \left(\sum_{l=1}^k u'_l(\xi)v'_l(\xi) + u'_0(\xi)\right) \rangle_{(p_j)} = \langle r_s(\xi) \rangle_{(p_j)}$, следовательно, $\forall v_1(\xi), \dots, v_{n-1}(\xi), v'_1(\xi), \dots, v'_k(\xi) \in \langle r_s(\xi) \rangle_{(p_j)}$ выполнено

$$\sum_{i=1}^{n-1} u_i(\xi)v_i(\xi) + u_n(\xi)(r_s(\xi) + p_j w(\xi)) + u_0(\xi) \in \langle r_s(\xi) \rangle_{(p_j)}.$$

Пусть $\Theta \in \{U_j \mid j \in \mathbb{N}\}$, имеем

$$\sum_{i=1}^{n-1} u_i(\xi) + u_n(\xi)\left(\sum_{l=1}^k u'_l(\xi)\right) = \sum_{i=1}^{n-1} u_i(\xi) + u_n(\xi)(1 + p_j w(\xi)) \in \langle 1 \rangle_{(p_j)}.$$

□

Как следствие одного из результатов работы [6], имеем

Лемма 9. Пусть $M \subseteq LD_2$. Если $\tilde{S}(M) \cap \tilde{A} \neq \emptyset$, то $\forall k \in \mathbb{N}$ автомат $G_k(z, \bar{X}^k, \bar{Y}^k) = z + \xi x_1 + \xi^2 x_2 + \dots + \xi^k x_k + \xi y_1 + \xi^2 y_2 + \dots + \xi^k y_k \in S(M)$.

Докажем четыре вспомогательные леммы.

Лемма 10. Пусть $M \subseteq LD_2$ и $\tilde{S}(M) \cap \tilde{A} \neq \emptyset$. Если $M \not\subseteq U_j$, то автомат

$$P_j(x_1) = p_j u_{1,j}(\xi)x_1 + u_{0,j}(\xi) \in S(M).$$

Доказательство. Рассмотрим автомат $f(x_1, \dots, x_n) \in M \setminus U_j$. Имеем

$$f'(x_1) = f(x_1, \dots, x_1) = u_1(\xi)x_1 + u_0(\xi), \quad u_1(\xi) \notin \langle 1 \rangle_{(p_j)}.$$

Если $p_j \mid u_1(\xi)$, то утверждение доказано, иначе имеем $u_1(\xi) \notin \langle 0 \rangle_{(p_j)}$ и $u_1(\xi) \notin \langle 1 \rangle_{(p_j)}$. Следовательно, существует некоторый многочлен $\tilde{u}(\xi)$, для которого верно

$$\tilde{u}(\xi) \in \langle \xi(1 + u_1(\xi)) \rangle_{(p_j)}^{-1}. \quad (9)$$

Обозначим $\deg(\tilde{u}(\xi)) = k$, тогда найдутся $a_i \in E_2$, $i = 0 \dots k$, для которых

$$\tilde{u}(\xi) = \sum_{i=0}^k a_i \xi^i.$$

По лемме 9 автомат

$$G_{k+1}(z, x_1, \dots, x_{k+1}, y_1, \dots, y_{k+1}) = z + \xi x_1 + \dots + \xi^{k+1} x_{k+1} + \xi y_1 + \dots + \xi^{k+1} y_{k+1} \in S(M).$$

Рассмотрим подстановку

$$g(x_1) = G_{k+1}(x_1, \sigma_0, \dots, \sigma_k, x_1, \dots, x_1), \quad \sigma_l = \begin{cases} x_1, & a_l = 0 \\ f'(x_1), & a_l = 1 \end{cases},$$

$$l = 0, \dots, k.$$

имеем

$$g(x_1) = (1 + \xi(1 + u_1(\xi))\tilde{u}(\xi))x_1 + u_0''(\xi) = (1 + u_1'(\xi))x_1 + u_0''(\xi).$$

Из выражения (9) следует, что многочлен $u_1'(\xi) \in \langle 1 \rangle_{(p_j)}$, следовательно, $p_j \mid (1 + u_1'(\xi))$. \square

Лемма 11. Пусть $M \subseteq LD_2$ и $\tilde{S}(M) \cap \tilde{A} \neq \emptyset$. Если для некоторого $j \in \mathbb{N}$ выполнено $M \not\subseteq \Theta$, $\forall \Theta \in \{U_j\} \cup \{S_{j,s} \mid s = 1, \dots, 2^{\deg(p_j)}\} \cup \{S_{1,s} \mid s = 1, 2\}$, то $\exists w_j(\xi) \in E_2[\xi]$, для которого автомат

$$W_j(x_1) = w_j(\xi)x_1, \quad w_j(\xi) \notin \langle 1 \rangle_{(p_j)}$$

принадлежит $S(M)$.

Доказательство. Покажем, что автоматы

$$\begin{aligned} d_0(x_1) &= p_j \tilde{w}_1(\xi)x_1 + \tilde{w}_0(\xi), & d_1(x_1) &= p_j \tilde{w}'_1(\xi)x_1 + \tilde{w}'_0(\xi), \\ \tilde{w}_0(0) &= 0, & \tilde{w}'_0(0) &= 1, & \langle \tilde{w}_0(\xi) \rangle_{(p_j)} &\neq \langle \tilde{w}'_0(\xi) \rangle_{(p_j)}. \end{aligned} \quad (10)$$

принадлежат $S(M)$. По лемме 10 автомат

$$f(x_1) = p_j u_1(\xi)x_1 + u_0(\xi) \in S(M).$$

Пусть $a = u_0(0)$. Положим $k_1 = 1$, если $a = 0$, и $k_1 = 2$, если $a = 1$. Рассмотрим автомат $f_{k_1}(x_1, \dots, x_n) \in M \setminus S_{1, k_1}$. Имеем

$$f'(x_1) = f_{k_1}(f(x_1), \dots, f(x_1)) = p_j u'_1(\xi) x_1 + u'_0(\xi), \quad u'_0(0) \neq a.$$

Если $u'_0(\xi) \notin \langle u_0(\xi) \rangle_{(p_j)}$, то $d_0(x_1), d_1(x_1) \in S(M)$, иначе имеем $\langle u_0(\xi) \rangle_{(p_j)} = \langle u'_0(\xi) \rangle_{(p_j)} = \langle r_{k_2}(\xi) \rangle_{(p_j)}$, для некоторого $r_{k_2}(\xi) \in E_2[\xi]$, $\deg(r_{k_2}(\xi)) < \deg(p_j)$. Рассмотрим автомат $f_{k_2}(x_1, \dots, x_n) \in M \setminus S_{j, k_2}$ и подстановку

$$f''(x_1) = f_{k_2}(f'(x_1), \dots, f'(x_1)) = p_j u''_1(\xi) x_1 + u''_0(\xi), \quad u''_0(\xi) \notin \langle r_{k_2}(\xi) \rangle_{(p_j)}.$$

Далее, в зависимости от значения $u''_0(0)$ одна из пар $f(x_1), f''(x_1)$ или $f'(x_1), f''(x_1)$ реализует автоматы $d_0(x_1), d_1(x_1) \in S(M)$.

Положим $k = \max(\deg(\tilde{w}_0(\xi)), \deg(\tilde{w}'_0(\xi)))$, тогда

$$\tilde{w}_0(\xi) = \sum_{l=0}^k a_l \xi^l, \quad \tilde{w}'_0(\xi) = \sum_{l=0}^k a'_l \xi^l.$$

По лемме 9 автомат

$$G_k(z, \bar{X}^k, \bar{Y}^k) = z + \xi x_1 + \dots + \xi^k x_k + \xi y_1 + \dots + \xi^k y_k \in S(M).$$

Рассмотрим подстановку

$$g(x_1) = G_k(d_0(x_1), \sigma_1, \dots, \sigma_k, \sigma'_1, \dots, \sigma'_k),$$

$$\sigma_l = \begin{cases} x_1, & a_l = 0 \\ d_1(x_1), & a_l = 1 \end{cases}, \quad \sigma'_l = \begin{cases} x_1, & a'_l = 0 \\ d_0(x_1), & a'_l = 1 \end{cases}, \quad l = 1, \dots, k.$$

Для некоторого $\bar{u}(\xi) \in E_2[\xi]$ имеем

$$g(x_1) = (\tilde{w}_0(\xi) + 1 + \tilde{w}'_0(\xi) + p_j \bar{u}(\xi)) x_1 + (\tilde{w}_0(\xi) \tilde{w}'_0(\xi) + \tilde{w}'_0(\xi) \tilde{w}_0(\xi)) =$$

$$= (1 + (\tilde{w}_0(\xi) + \tilde{w}'_0(\xi)) + p_j \bar{u}(\xi)) x_1.$$

Из выражения (10) $\langle \tilde{w}_0(\xi) \rangle_{(p_j)} \neq \langle \tilde{w}'_0(\xi) \rangle_{(p_j)}$, следовательно, $\langle 1 + (\tilde{w}_0(\xi) + \tilde{w}'_0(\xi)) \rangle_{(p_j)} \neq \langle 1 \rangle_{(p_j)}$. □

Лемма 12. Пусть $M \subseteq LD_2$ и $\tilde{S}(M) \cap \tilde{A} \neq \emptyset$. Если для некоторого $j \in \mathbb{N}$ выполнено $M \not\subseteq \Theta$, $\forall \Theta \in \{U_j\} \cup \{S_{j,s} \mid s = 1, \dots, 2^{\deg(p_j)}\} \cup \{U_1\} \cup \{S_{1,s} \mid s = 1, 2\}$, то $\exists u_j(\xi) \in E_2[\xi]$, $p_j \nmid u_j(\xi)$, такой, что $\forall w(\xi) \in E_2[\xi]$ автомат

$$f_{j,w(\xi)}(x_1, x_2) = x_1 + \xi w(\xi) u_j(\xi) x_2,$$

принадлежит $S(M)$.

Доказательство. По лемме 9 для любого $k \in \mathbb{N}$ автомат

$$G_k(z, \bar{X}^k, \bar{Y}^k) = z + \xi x_1 + \cdots + \xi^k x_k + \xi y_1 + \cdots + \xi^k y_k \in S(M).$$

По лемме 11 $S(M)$ принадлежит автомат

$$d_j(x_1) = u'_j(\xi)x_1, \quad u'_j(\xi) \notin \langle 1 \rangle_{(p_j)}. \quad (11)$$

Пусть $w(\xi) = \sum_{i=0}^K a_i \xi^i$, рассмотрим подстановку

$$f_{j,w(\xi)}(x_1, x_2) = G_{K+1}(x_1, \sigma_0, \cdots, \sigma_K, x_2, \cdots, x_2), \quad \sigma_i = \begin{cases} x_2, & a_i = 0 \\ d_j(x_2), & a_i = 1 \end{cases},$$

имеем

$$f_{j,w(\xi)}(x_1, x_2) = x_1 + \xi(1 + u'_j(\xi))w(\xi)x_2 = x_1 + \xi w(\xi)u_j(\xi)x_2 \in S(M).$$

Из выражения (11) следует, что $p_j \nmid (1 + u'_j(\xi))$.

□

Лемма 13. Пусть $M \subseteq LD_2$ и $\tilde{S}(M) \cap \tilde{A} \neq \emptyset$. Если $\exists u_1(\xi) \in E_2[\xi]$, $\xi \nmid u_1(\xi)$, такой, что $\forall w(\xi) \in E_2[\xi]$ автомат

$$f_{1,w(\xi)}(x_1, x_2) = x_1 + \xi w(\xi)u_1(\xi)x_2,$$

принадлежит $S(M)$ и выполнено $M \not\subseteq \Theta$, $\forall \Theta \in \{U_j \mid j \in D(u_1(\xi))\} \cup \{S_{j,s} \mid j \in D(u_1(\xi)), s = 1, \dots, 2^{\deg(p_j)}\} \cup \{U_1\} \cup \{S_{1,s} \mid s = 1, 2\}$, то $0 \in S(M)$.

Доказательство. По лемме 12 $\forall j \in D(u_1(\xi)) \exists u_j(\xi) \in E_2[\xi]$, $p_j \nmid u_j(\xi)$, такой, что $\forall w(\xi) \in E_2[\xi]$ автомат

$$f_{j,w(\xi)}(x_1, x_2) = x_1 + \xi w(\xi)u_j(\xi)x_2,$$

принадлежит $S(M)$. Положим $D = \{u_1(\xi)\} \cup D(u_1(\xi)) = \{u_{j_1}(\xi), \dots, u_{j_S}(\xi)\}$. Имеем $\text{НОД}(u_{j_i}(\xi) \mid u_{j_i}(\xi) \in D) = 1$, следовательно, существует набор многочленов $\{v_1(\xi), \dots, v_S(\xi)\}$ такой, что

$$\sum_{i=1}^S v_i(\xi)u_{j_i}(\xi) = 1.$$

По лемме 11 автомат $d(x_1) = \xi u''(\xi)x_1 \in S(M)$. Положим $v'_i(\xi) = u''(\xi)v_i(\xi)$, $i = 1, \dots, S$ и рассмотрим

$$\begin{aligned} & f_{j_1, v'_1(\xi)}(f_{j_2, v'_2(\xi)}(\dots f_{j_S, v'_S(\xi)}(d(x_1), x_1) \dots, x_1), x_1) = \\ & = \left(\xi u''(\xi) + \xi u''(\xi) \left(\sum_{i=1}^S v_i(\xi) u_{j_i}(\xi) \right) \right) x_1 = 0 \in S(M). \end{aligned}$$

□

Докажем основное утверждение раздела. Для произвольного подмножества $M \subseteq LD_2$, покажем, что система $\bar{H} \cup H_0$ является критериальной относительно задачи выразимости константы 0.

Лемма 14. Пусть $M \subseteq LD_2$. $0 \in S(M) \iff M \not\subseteq \Theta, \forall \Theta \in \bar{H} \cup H_0$.

Доказательство. Прямое утверждение следует из того факта, что $\forall \Theta \in \bar{H} \cup H_0$ имеем $0 \notin \Theta$ и $S(\Theta) = \Theta$.

Докажем обратное утверждение. По теореме 2 имеем $\tilde{S}(M) \cap \tilde{A} \neq \emptyset$. По лемме 12 $\exists u_1(\xi) \in E_2[\xi]$, $p_1 \nmid u_1(\xi)$, такой, что для произвольного $w(\xi) \in E_2[\xi]$ автомат

$$f_{1, w(\xi)}(x_1, x_2) = x_1 + \xi w(\xi) u_1(\xi) x_2,$$

принадлежит $S(M)$. Тогда из леммы 13 следует основное утверждение. □

Лемма 15. Пусть $M \subseteq LD_2$, M — конечное и $\tilde{S}(M) \cap \tilde{A} \neq \emptyset$. Проверка условия $0 \in S(M)$ алгоритмически разрешима.

Доказательство. Если $M \not\subseteq \Theta, \forall \Theta \in \{U_1, S_{1,1}, S_{1,2}\}$, то по лемме 12 $\exists u_1(\xi) \in E_2[\xi]$, $p_1 \nmid u_1(\xi)$, такой, что для произвольного $w(\xi) \in E_2[\xi]$ автомат

$$f_{1, w(\xi)}(x_1, x_2) = x_1 + \xi w(\xi) u_1(\xi) x_2,$$

принадлежит $S(M)$. Положим $D_1 = D(u_1(\xi))$ — множество неприводимых многочленов. По определению имеем $|D_1| < \infty$. Следовательно, если $M \not\subseteq \Theta, \forall \Theta \in \{U_j \mid j \in D(u_1(\xi))\} \cup \{S_{j,s} \mid j \in D(u_1(\xi)), s = 1, \dots, 2^{\deg(p_j)}\} \cup \{U_1\} \cup \{S_{1,s} \mid s = 1, 2\}$, то по лемме 13 имеем $0 \in S(M)$.

Поскольку M конечно, а принадлежность элемента множествам указанного вида проверяется по их определению, то каждое включение $M \subseteq \Theta$ проверяется за конечное число шагов. Следовательно, по ранее доказанному критерию условие $0 \in S(M)$ алгоритмически разрешимо. □

6. Полнота и алгоритмическая разрешимость

Определение 5. Определим семейство подмножеств LD_2 :

$$T_j = \{f \mid f \in LD_2, f = \sum_{i=1}^n u_i(\xi)x_i + u_0(\xi) \text{ и } u_0(\xi) \vdash p_j\}, j \in \mathbb{N}.$$

Обозначим $H_C = \{T_j\}$.

В работе [10] были доказаны следующие леммы.

Лемма 16. Пусть $M \subseteq LD_2$, $\tilde{S}(M) \cap \tilde{A} \neq \emptyset$ и автомат $0 \in S(M)$. Если $M \not\subseteq \Theta$, $\forall \Theta \in H_C$, то система M полна в LD_2 .

Лемма 17. Пусть $M \subseteq LD_2$, M — конечное, $\tilde{S}(M) \cap \tilde{A} \neq \emptyset$ и $0 \in S(M)$. Проверка полноты множества M в LD_2 алгоритмически разрешима.

Из представленных лемм и доказанных ранее утверждений, напрямую следует основной результат работы.

Теорема 3. Пусть $M \subseteq LD_2$. Если $M \not\subseteq \Theta$, $\forall \Theta \in \bar{H} \cup H_0 \cup H_C$, то $S(M) = LD_2$.

Теорема 4. Пусть $M \subseteq LD_2$, M — конечное. Проверка полноты множества M в LD_2 алгоритмически разрешима.

7. Заключение

В данной работе был получен критерий полноты для произвольных подмножеств класса линейных дефинитных автоматов. На основании данного критерия был построен алгоритм распознавания полноты произвольных конечных подмножеств рассматриваемого класса. Дальнейшие исследования по теме могут заключаться в обобщении полученных результатов на линейные дефинитные автоматы, построенные над произвольным конечным полем.

В заключение автор выражает особую признательность научному руководителю, д.ф.-м.н. Часовских А. А. за научное руководство, помощь и обсуждение результатов.

Список литературы

- [1] П. Кон, *Универсальная алгебра*, М.: Мир, 1968.
- [2] В. Б. Кудрявцев, “О мощностях множеств предполных классов некоторых функциональных систем, связанных с автоматами”, *Докл. АН СССР*, **151**:3 (1963), 493–496.
- [3] В. Б. Кудрявцев, С. В. Алёшин, А. С. Подколзин, *Введение в теорию автоматов*, М.: Изд-во Московского университета, 2019.
- [4] М. И. Кратко, “Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов”, *Докл. АН СССР*, **155**:1 (1964), 35–37.
- [5] Д. Н. Жук, “О неразрешимости проблемы полноты для дефинитных автоматов”, *Интеллектуальные системы. Теория и приложения*, **12** (2008), 211–228.
- [6] А. А. Часовских, “Проблема полноты в классах линейных автоматов”, *Интеллектуальные системы. Теория и приложения*, **22**:2 (2018), 151–153.
- [7] А. А. Часовских, “Об алгоритмической разрешимости проблемы полноты для линейных автоматов”, *Вестник Московского университета. Серия 1. Математика. Механика*, 1986, № 3, 82–84.
- [8] А. А. Часовских, “Линейно-автоматные функции с операциями суперпозиции”, *Нейрокомпьютеры: разработка, применение*, 2013, № 8, 3–13.
- [9] И. В. Молдованов, “Аппроксимационная полнота линейных дефинитных автоматов”, *Интеллектуальные системы. Теория и приложения*, **29**:4 (2025), 135–149.
- [10] И. В. Молдованов, “Алгоритмическая разрешимость задачи полноты конечных содержащих константу ноль множеств в классе линейных дефинитных автоматов”, *Чебышевский сборник*, **26**:5 (2025), 137–157. DOI: 10.22405/2226-8383-2025-26-5-137-157.
- [11] А. В. Чашкин, *Лекции по дискретной математике*, М., 2007.
- [12] Р. Лидл, Г. Нидеррайтер, *Конечные поля*, **1–2**, М.: Мир, 1988.

- [13] Д. Ферран, Ж.-П. Оливье, “Минимальные гомоморфизмы колец”, *Журнал алгебры*, **16**:3 (1970), 461–471. DOI: 10.1016/0021-8693(70)90020-7.
- [14] Д. Е. Доббс, Дж. Шапиро, “Классификация минимальных расширений колец целостной области”, *Журнал алгебры*, **305**:1 (2006), 185–193. DOI: 10.1016/j.jalgebra.2005.10.005.
- [15] Д. Е. Доббс, Дж. Шапиро, “Классификация минимальных расширений колец некоторых коммутативных колец”, *Журнал алгебры*, **308**:2 (2007), 800–821. DOI: 10.1016/j.jalgebra.2006.07.024.

Статья поступила 26 мая 2026 г.

The completeness problem for linear definite automata

I. V. Moldovanov

This paper studies the completeness problem under superposition in the class of linear definite automata over the finite field with two elements. Its main result is a completeness criterion for arbitrary subsets of linear definite automata, stated in terms of a family of closed classes. This criterion extends earlier results that applied only to finitely generated subsets containing the zero constant. As a consequence, the paper proves that completeness is decidable for finite subsets of the class of linear definite automata.

Keywords: completeness problem, superposition, linear automata, definite automata.

References

- [1] P. Cohn, *Universal Algebra*, Moscow: Mir, 1968.
- [2] V. B. Kudryavtsev, “On cardinalities of sets of precomplete classes of some functional systems related to automata”, *Dokl. Akad. Nauk SSSR*, **151**:3 (1963), 493–496 (In Russian).
- [3] V. B. Kudryavtsev, S. V. Aleshin, A. S. Podkolzin, *Introduction to Automata Theory*, Moscow: MSU Press, 2019.
- [4] M. I. Kratko, “Algorithmic unsolvability of the problem of recognizing completeness for finite automata”, *Dokl. Akad. Nauk SSSR*, **155**:1 (1964), 35–37 (In Russian).

- [5] D. N. Zhuk, “On the undecidability of the completeness problem for definite automata”, *Intelligent Systems. Theory and Applications*, **12** (2008), 211–228 (In Russian).
- [6] A. A. Chasovskikh, “The completeness problem in classes of linear automata”, *Intelligent Systems. Theory and Applications*, **22:2** (2018), 151–153 (In Russian).
- [7] A. A. Chasovskikh, “On algorithmic decidability of the completeness problem for linear automata”, *Moscow University Bulletin. Series 1. Mathematics. Mechanics*, 1986, №3, 82–84 (In Russian).
- [8] A. A. Chasovskikh, “Linear-automata functions with superposition operations”, *Neurocomputers: Development, Application*, 2013, №8, 3–13 (In Russian).
- [9] I. V. Moldovanov, “Approximation completeness of linear definite automata”, *Intelligent Systems. Theory and Applications*, **29:4** (2025), 135–149 (In Russian).
- [10] I. V. Moldovanov, “Algorithmic decidability of the completeness problem for finite sets containing the zero constant in the class of linear definite automata”, *Chebyshevskii Sbornik*, **26:5** (2025), 137–157. DOI: 10.22405/2226-8383-2025-26-5-137-157 (In Russian).
- [11] A. V. Chashkin, *Lectures on Discrete Mathematics*, Moscow, 2007 (In Russian).
- [12] R. Lidl, H. Niederreiter, *Finite Fields*, **1–2 (Russian translation)**, Moscow: Mir, 1988.
- [13] D. Ferrand, J.-P. Olivier, “Homomorphismes minimaux d’anneaux”, *Journal of Algebra*, **16:3** (1970), 461–471. DOI: 10.1016/0021-8693(70)90020-7.
- [14] D. E. Dobbs, J. Shapiro, “A classification of the minimal ring extensions of an integral domain”, *Journal of Algebra*, **305:1** (2006), 185–193. DOI: 10.1016/j.jalgebra.2005.10.005.
- [15] D. E. Dobbs, J. Shapiro, “A classification of the minimal ring extensions of certain commutative rings”, *Journal of Algebra*, **308:2** (2007), 800–821. DOI: 10.1016/j.jalgebra.2006.07.024.

Received on May 26, 2026

Аналог предполного класса Слупецкого в классе полиномов по модулю четыре

И. М. Янушкевич*

В работе исследуется замкнутый класс функций четырёхзначной логики, представимых в виде полинома по модулю 4. Показано, что любая такая функция единственным образом задаётся набором булевых функций той же арности. Главным результатом работы является описание предполного класса в классе полиномов, содержащего все функции-полиномы одной переменной и являющегося аналогом предполного класса Слупецкого.

Ключевые слова: функция многозначной логики, полином (многочлен), замкнутый класс.

1. Введение

Рассматривается класс Poly_4 всех полиномиальных функций четырёхзначной логики. Здесь функция k -значной логики называется полиномиальной, если её можно представить полиномом (многочленом) над кольцом вычетов по модулю k . Известно, что класс всех полиномиальных функций k -значной логики Poly_k совпадает с классом P_k всех функций k -значной логики тогда и только тогда, когда k — простое число [1]. Если k — составное число, то класс Poly_k является замкнутым, но не предполным (см., например, [1]).

И. Г. Розенбергом были описаны все предполные классы в P_k для любого $k \geq 3$ (см. [2]). Одним из таких классов является класс Слупецкого SL , построенный Е. Слупецким в работе [3]. Также в ряде работ изучается положение замкнутого класса Poly_k в решётке всех замкнутых классов функций k -значной логики, его свойства и решётка его подклассов [4–8]. В частности, были найдены все подклассы класса полиномов, содержащие все линейные функции [4] и [8].

В настоящей работе построена биекция между функциями, представимыми полиномами арности n и $n + 2$ функциями арности n из

* *Янушкевич Иван Михайлович* — студент каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: ivan13.2002@yandex.ru, ORCID: 0009-0005-6128-9519.

Yanushkevich Ivan Mikhailovich — Student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

P_2 , а также найден предполный класс в классе полиномов 4-значной логики, содержащий пересечение класса полиномов и класса Слупецкого. Насколько нам известно, это первый найденный предполный класс в классе полиномов, который содержит все полиномы одной переменной. Предикат, задающий класс Слупецкого в P_k , определяется как множество всех наборов арности k , в которых не все элементы различны [10]. Все наборы, принадлежащие предикату, задающему найденный класс, обладают тем же свойством, поэтому этот класс можно рассматривать как аналог класса Слупецкого для Poly_4 .

2. Определения

Пусть $\mathbb{N} = \{1, 2, 3, \dots\}$ — множество всех натуральных чисел; $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; $E_k = \{0, 1, 2, \dots, k-1\}$. При $n \geq 1$ определим

$$P_k^n := \{f \mid f : E_k^n \rightarrow E_k\}, P_k := \bigcup_{n \geq 1} P_k^n.$$

Элементы P_k будем называть *функциями k -значной логики*. На множестве P_k обычным образом определим оператор замыкания $[\]$ относительно операций суперпозиции. Множество $M \subseteq P_k$ называется замкнутым, если $[M] = M$. Замкнутое множество функций называется *клоном*, если в нём содержится тождественная функция.

Отображение $E_k^h \rightarrow \{0, 1\}$ будем называть *предикатом арности h* . Пусть

$$R_k^h := \{\rho \mid \rho : E_k^h \rightarrow \{0, 1\}\}, R_k := \bigcup_{h \geq 0} R_k^h.$$

В работе предикаты будем изображать в виде матриц, в которых столбцам соответствуют наборы, на которых предикат принимает значение 1. Запись

$$\rho = \begin{pmatrix} b_{11} & b_{21} & \dots & b_{n1} \\ b_{12} & b_{22} & \dots & b_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{1h} & b_{2h} & \dots & b_{nh} \end{pmatrix}$$

означает, что $\rho \in R_k^h$, $\rho(b_{i,1}, b_{i,2}, \dots, b_{i,h}) = 1$ для любого $i = 1, \dots, n$, и предикат ρ принимает значение 0 на остальных наборах. Будем

писать, что $\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_h \end{pmatrix} \in \rho$, если $\rho(b_1, b_2, \dots, b_h) = 1$.

Будем говорить, что функция $f \in P_k^n$ сохраняет предикат $\rho \in R_k^h$, если

$$f \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{h1} & a_{h2} & \dots & a_{hn} \end{pmatrix} := \begin{pmatrix} f(a_{11}, a_{12}, \dots, a_{1n}) \\ f(a_{21}, a_{22}, \dots, a_{2n}) \\ \vdots \\ f(a_{h1}, a_{h2}, \dots, a_{hn}) \end{pmatrix} \in \rho$$

для любых

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{h1} \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{h2} \end{pmatrix}, \dots, \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{hn} \end{pmatrix} \in \rho.$$

Через $\text{Pol}(\rho)$ обозначим множество всех функций $f \in P_k$, таких, что f сохраняет ρ . Для $S \subseteq R_k$ положим

$$\text{Pol}(S) := \bigcap_{\rho \in S} \text{Pol}(\rho).$$

3. Полиномы

В дальнейшем будем рассматривать только функции из P_4 и под полиномом понимать полином по модулю 4. Класс всех функций, представимых такими полиномами, обозначим через Poly_4 и назовём классом полиномов; кроме того, для каждого n положим $\text{Poly}_4^n := \text{Poly}_4 \cap P_4^n$.

Введём обозначение для операции взятия остатка по модулю 2: $x^\dagger := x \bmod 2$.

Следует отметить, что $\text{Poly}_4 = [\{1, x + y, x \cdot y\}]$, где $x + y$ и $x \cdot y$ обозначают, соответственно, сложение и умножение по модулю 4.

Рассмотрим два предиката:

$$\rho_{T_{0\sim 2,1\sim 3}} = \begin{pmatrix} 0 & 0 & 2 & 2 & 1 & 1 & 3 & 3 \\ 0 & 2 & 0 & 2 & 1 & 3 & 1 & 3 \end{pmatrix},$$

$$\rho_{\text{Poly}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 3 & 3 & 3 & 3 \\ 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 1 & 1 & 3 & 3 & 1 & 1 & 3 & 3 \\ 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 1 & 3 & 1 & 3 & 1 & 3 & 1 & 3 \\ 0 & 2 & 2 & 0 & 2 & 0 & 0 & 2 & 1 & 3 & 3 & 1 & 3 & 1 & 1 & 3 \end{pmatrix}.$$

В [5] в теореме 4 описывается предикат, задающий класс полиномов для P_{p^m} , где p — простое, $1 \leq m \leq p$. В случае $p = 2, m = 2$ полученный предикат совпадает с ρ_{Poly} . Следовательно, $\text{Pol}(\rho_{\text{Poly}}) = \text{Poly}_4$.

В [6] в теореме 9 было доказано, что для P_k , где k — квадрат простого числа, существует единственный класс, отличный от P_k и Poly_k , содержащий класс полиномов, — класс сохранения остатка по модулю \sqrt{k} . В случае $k = 4$ этот класс задаётся предикатом $\rho_{T_{0\sim 2,1\sim 3}}$.

Также в [9] было доказано, что $|\text{Poly}_4^n| = 4^{(\frac{n}{2}+1) \cdot 2^n}$, но мы предлагаем наше доказательство этого факта, так как оно напрямую связано с представлением функций-полиномов четырёхзначной логики через набор булевых функций.

Теорема 1. *Количество функций n -арности n , представимых полиномами в P_4 , не превышает $2^{(n+2) \cdot 2^n}$.*

Доказательство. Заметим, что для любой функции-полинома f , для любых наборов $(a_1, \dots, a_n) \in \{0, 1\}^n$ и $(b_1, \dots, b_n) \in \{0, 1, 2, 3\}^n$, таких, что $b_i^\dagger = a_i$ для любого i , в силу сохранения предиката $\rho_{T_{0\sim 2,1\sim 3}}$, справедливо равенство $f(a_1, \dots, a_n)^\dagger = f(b_1, \dots, b_n)^\dagger$. То есть если два набора совпадают по модулю 2 покомпонентно, то значения функции-полинома на них совпадают по модулю 2.

Также заметим, что для любого набора $(b_1, \dots, b_n) \in \{0, 1, 2, 3\}^n$ и различных $i, j \in \{1, \dots, n\}$ благодаря сохранению предиката ρ_{Poly} по значениям $c_1 = f(b_1, \dots, b_n)$, $c_2 = f(b_1, \dots, b_i + 2, \dots, b_n)$, а также значению $c_3 = f(b_1, \dots, b_j + 2, \dots, b_n)$ можно однозначно определить значение $c_4 = f(b_1, \dots, b_i + 2, \dots, b_j + 2, \dots, b_n)$. Действительно, если столбец (a, b, c, d) принадлежит предикату ρ_{Poly} , то выполняется равенство $a + b + c + d = 0$. Набор (c_1, c_2, c_3, c_4) принадлежит предикату

ρ_{Poly} и по известным значениям трёх элементов можно однозначно определить значение четвёртого: $c_4 = -c_1 - c_2 - c_3$.

Следовательно, если для всех наборов $(a_1, \dots, a_n) \in \{0, 1\}^n$ известны значения $f(a_1, a_2, \dots, a_{n-1}, a_n)$, $f(a_1 + 2, a_2, a_3, \dots, a_{n-1}, a_n)$, $f(a_1, a_2 + 2, a_3, \dots, a_{n-1}, a_n), \dots, f(a_1, \dots, a_{n-1}, a_n + 2)$, то значение функции-полинома на любом наборе $(b_1, \dots, b_n) \in \{0, 1, 2, 3\}^n$ определяется однозначно.

Для произвольного набора $(a_1, \dots, a_n) \in \{0, 1\}^n$ значение $f(a_1, \dots, a_n)$ можно выбрать не более 4 способами, количество таких наборов равно 2^n . Значение каждого из $f(a_1 + 2, a_2, \dots, a_{n-1}, a_n)$, $f(a_1, a_2 + 2, a_3, \dots, a_n)$, $\dots, f(a_1, \dots, a_{n-1}, a_n + 2)$ можно выбрать не более чем двумя способами (из-за сохранения значения по модулю 2), число таких наборов равно $n \cdot 2^n$. Остальные значения определяются однозначно.

Таким образом, число способов выбрать значения полинома на всех наборах не превышает $4^{2^n} \cdot 2^{n \cdot 2^n} = 2^{(n+2) \cdot 2^n}$.

□

Лемма 1. Пусть $g \in P_2$. Тогда функция $f \in P_4$, определяемая соотношением $f(x_1, \dots, x_n) = g(x_1^\dagger, \dots, x_n^\dagger)$, представима полиномом.

Доказательство. Заметим, что для любого набора $(a_1, a_2, a_3, a_4) \in \rho_{\text{Poly}}$ выполняется $a_1^\dagger = a_2^\dagger = a_3^\dagger = a_4^\dagger$. Следовательно, для любых наборов $(a_{11}, a_{21}, a_{31}, a_{41}), (a_{12}, a_{22}, a_{32}, a_{42}), \dots, (a_{1n}, a_{2n}, a_{3n}, a_{4n}) \in \rho_{\text{Poly}}$ справедливо равенство:

$$\begin{aligned} f \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ a_{31} & a_{32} & \dots & a_{3n} \\ a_{41} & a_{42} & \dots & a_{4n} \end{pmatrix} &= g \begin{pmatrix} a_{11}^\dagger & a_{12}^\dagger & \dots & a_{1n}^\dagger \\ a_{21}^\dagger & a_{22}^\dagger & \dots & a_{2n}^\dagger \\ a_{31}^\dagger & a_{32}^\dagger & \dots & a_{3n}^\dagger \\ a_{41}^\dagger & a_{42}^\dagger & \dots & a_{4n}^\dagger \end{pmatrix} = \\ &= g \begin{pmatrix} a_{11}^\dagger & a_{12}^\dagger & \dots & a_{1n}^\dagger \\ a_{11}^\dagger & a_{12}^\dagger & \dots & a_{1n}^\dagger \\ a_{11}^\dagger & a_{12}^\dagger & \dots & a_{1n}^\dagger \\ a_{11}^\dagger & a_{12}^\dagger & \dots & a_{1n}^\dagger \end{pmatrix} \in \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \subsetneq \rho_{\text{Poly}} \end{aligned}$$

Таким образом, функция f сохраняет предикат ρ_{Poly} и является полиномом.

□

Заметим, что функция

$$2j_3 := \begin{cases} 2, & \text{если } x = 3, \\ 0, & \text{иначе} \end{cases}$$

представима полиномом, так как $2j_3(x) = x^3 - x^2$.

Следовательно, поскольку $2j_a(x) = 2j_3(x - a + 3)$, для любого $a \in \{0, 1, 2, 3\}$ верно, что

$$2j_a(x) := \begin{cases} 2, & \text{если } x = a, \\ 0, & \text{иначе} \end{cases} \in \text{Poly}_4.$$

Теорема 2. *Отображение, сопоставляющее каждому набору из $n + 2$ функций $(g^f, g_0^f, g_1^f, \dots, g_n^f) \in (P_2^n)^{n+2}$ функцию-полином $f \in \text{Poly}_4^n$ по следующей формуле:*

$$f(x_1, \dots, x_n) = g^f(x_1^\dagger, \dots, x_n^\dagger) + \sum_{i=1}^n g_i^f(x_1^\dagger, \dots, x_n^\dagger) \cdot 2[x_i/2] + 2g_0^f(x_1^\dagger, \dots, x_n^\dagger), \quad (1)$$

устанавливает взаимно-однозначное соответствие между множеством Poly_4^n и множеством $(P_2^n)^{n+2}$.

Доказательство. Заметим, что $2[x/2] = 2j_2(x) + 2j_3(x)$, а значит, $2[x/2]$ является функцией-полиномом. Кроме того, по лемме 1 для любой $g \in P_2^n$ справедливо, что $g(x_1^\dagger, \dots, x_n^\dagger)$ является полиномом.

Следовательно, для произвольного набора $(g, g_0, g_1, \dots, g_n) \in (P_2^n)^{n+2}$ верно, что функция

$$g(x_1^\dagger, \dots, x_n^\dagger) + \sum_{i=1}^n g_i(x_1^\dagger, \dots, x_n^\dagger) \cdot 2[x_i/2] + 2g_0(x_1^\dagger, \dots, x_n^\dagger)$$

является полиномом, как сумма и произведение функций-полиномов.

Докажем инъективность отображения заданного формулой 1. Пусть два набора булевых функций $(g, g_0, g_1, \dots, g_n)$ и $(g', g'_0, g'_1, \dots, g'_n)$ задают одну и ту же функцию f .

Для любого набора $\alpha = (\alpha_1, \dots, \alpha_n) \in \{0, 1\}^n$ имеем $f(\alpha) = g(\alpha) + 2g_0(\alpha) = g'(\alpha) + 2g'_0(\alpha)$, следовательно $g(\alpha) = g'(\alpha)$ и $g_0(\alpha) = g'_0(\alpha)$.

Также для любого $i \in \{1, \dots, n\} : f(\alpha_1, \dots, \alpha_i, \dots, \alpha_n) = g(\alpha) + 2g_0(\alpha) + 2g_i(\alpha) = g'(\alpha) + 2g'_0(\alpha) + 2g'_i(\alpha)$. С учётом $g(\alpha) = g'(\alpha)$ и $g_0(\alpha) = g'_0(\alpha)$ получаем $g_i(\alpha) = g'_i(\alpha)$.

Следовательно, эти два набора функций совпадают покомпонентно и отображение инъективно.

Известно, что $|P_2^n| = 2^{2^n}$, поэтому выбрать $n + 2$ функции можно $2^{(n+2) \cdot 2^n}$ способами. Отсюда следует, что функций-полиномов арности n не менее $2^{(n+2) \cdot 2^n}$. Учитывая оценку из теоремы 1 получаем, что $|\text{Poly}_4^n| = 2^{(n+2) \cdot 2^n}$.

Так как построенное отображение $(P_2^n)^{n+2} \rightarrow \text{Poly}_4^n$ является инъекцией между равномошными множествами, то оно является биекцией. □

4. Новый класс

В этом разделе для каждой функции-полинома f также рассматривается её представление с помощью функций $g^f, g_0^f, g_1^f, \dots, g_n^f$ согласно теореме 2.

Определение 1. Будем говорить, что у функции f существует блок $0/2$, если найдутся набор $\alpha = (\alpha_1, \dots, \alpha_n) \in \{0, 1\}^n$ и индекс $i \in \{1, \dots, n\}$, для которых $g^f(\alpha) = 0$ и $g_i^f(\alpha) = 1$. То есть, $f(\alpha) \in \{0, 2\}$ и

$$f(\alpha_1, \dots, \alpha_{i-1}, \alpha_i, \alpha_{i+1}, \dots, \alpha_n) \neq f(\alpha_1, \dots, \alpha_{i-1}, \alpha_i + 2, \alpha_{i+1}, \dots, \alpha_n).$$

Эквивалентно, существуют два набора $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \{0, 1, 2, 3\}^n$, такие, что для любого $i \in \{1, \dots, n\}$ верно $a_i^\dagger = b_i^\dagger$ и $f(a_1, \dots, a_n) = 0, f(b_1, \dots, b_n) = 2$.

Определение 2. Будем говорить, что у функции f существует блок $1/3$, если найдутся набор $\alpha = (\alpha_1, \dots, \alpha_n) \in \{0, 1\}^n$ и индекс $i \in \{1, \dots, n\}$, для которых $g^f(\alpha) = 1$ и $g_i^f(\alpha) = 1$. То есть $f(\alpha) \in \{1, 3\}$ и

$$f(\alpha_1, \dots, \alpha_{i-1}, \alpha_i, \alpha_{i+1}, \dots, \alpha_n) \neq f(\alpha_1, \dots, \alpha_{i-1}, \alpha_i + 2, \alpha_{i+1}, \dots, \alpha_n).$$

Эквивалентно, существуют два набора $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \{0, 1, 2, 3\}^n$, такие, что для любого $i \in \{1, \dots, n\}$ верно $a_i^\dagger = b_i^\dagger$ и $f(a_1, \dots, a_n) = 1, f(b_1, \dots, b_n) = 3$.

Зададим следующие множества функций:

Множество I содержит функции-полиномы, у которых не существует блока 0/2, а также функции-полиномы, у которых не существует блока 1/3.

Для $n \geq 1$ определим K^n как множество функций-полиномов f степени n со следующим свойством: существует такой $i \in \{1, \dots, n\}$ (назовём i -ую переменную **выделенной**), что

- Для любых ненулевых $j \neq i$ верно $g_j^f \equiv 0$;
- Существуют константы $a_0, a_1 \in \{0, 1\}$ такие, что для любого набора $(\alpha_1, \dots, \alpha_{i-1}, k, \alpha_{i+1}, \dots, \alpha_n) \in \{0, 1\}^n$, если $g_i^f(\alpha_1, \dots, \alpha_{i-1}, k, \alpha_{i+1}, \dots, \alpha_n) = 1$, то $g^f(\alpha_1, \dots, \alpha_{i-1}, k, \alpha_{i+1}, \dots, \alpha_n) = a_k$.

Определим множество K следующим образом: $K := \bigcup_{n \geq 1} K^n$.

Кроме того, рассмотрим следующий предикат:

$$\rho = \{(a, b, c, d) \mid a, b, c, d \in \{0, 1, 2, 3\}, a^\dagger = b^\dagger, c^\dagger = d^\dagger, \{a, b, c, d\} \neq \{0, 1, 2, 3\}\}$$

Лемма 2. Все функции множества I содержатся в $\text{Pol}(\rho)$.

Доказательство. Рассмотрим функцию f из I и наборы

$$(a_{11}, a_{21}, a_{31}, a_{41}), (a_{12}, a_{22}, a_{32}, a_{42}), \dots, (a_{1n}, a_{2n}, a_{3n}, a_{4n}) \in \rho.$$

Обозначим

$$c_1 := f(a_{11}, a_{12}, \dots, a_{1n}), \quad c_2 := f(a_{21}, a_{22}, \dots, a_{2n}), \\ c_3 := f(a_{31}, a_{32}, \dots, a_{3n}), \quad c_4 := f(a_{41}, a_{42}, \dots, a_{4n}).$$

Отметим, что из определения предиката ρ для любого i выполнено $a_{1i}^\dagger = a_{2i}^\dagger$ и $a_{3i}^\dagger = a_{4i}^\dagger$. И если $c_1 = c_2 + 2$, то у функции f будет блок 0/2 или 1/3, аналогично с $c_3 = c_4 + 2$.

Поскольку f является функцией-полиномом и сохраняет предикат $\rho_{T_{0 \sim 2, 1 \sim 3}}$, верно, что $c_1^\dagger = c_2^\dagger$ и $c_3^\dagger = c_4^\dagger$. Если $c_1 \neq c_2$, $c_3 \neq c_4$ и $c_1^\dagger \neq c_3^\dagger$, то у функции f по определению существует блок 0/2 и 1/3, действительно, в этом случае одна из пар (c_1, c_2) или (c_3, c_4) образует пару $\{0, 2\}$, а другая — $\{1, 3\}$. Наличие одновременно блока 0/2 и блока 1/3 противоречит тому, что функция принадлежит множеству I. Значит, $c_1 = c_2$ или $c_3 = c_4$, или $c_1^\dagger = c_2^\dagger = c_3^\dagger = c_4^\dagger$,

то есть $\{c_1, c_2, c_3, c_4\} \neq \{0, 1, 2, 3\}$ и набор (c_1, c_2, c_3, c_4) принадлежит предикату ρ .

Следовательно, функция f сохраняет предикат ρ . □

Лемма 3. *Все функции множества K содержатся в $\text{Pol}(\rho)$.*

Доказательство. Рассмотрим функцию f из K . Без ограничения общности считаем, что выделенной является первая переменная. Рассмотрим наборы

$$(a_{11}, a_{21}, a_{31}, a_{41}), (a_{12}, a_{22}, a_{32}, a_{42}), \dots, (a_{1n}, a_{2n}, a_{3n}, a_{4n}) \in \rho,$$

и обозначим

$$\begin{aligned} c_1 &:= f(a_{11}, a_{12}, \dots, a_{1n}), & c_2 &:= f(a_{21}, a_{22}, \dots, a_{2n}), \\ c_3 &:= f(a_{31}, a_{32}, \dots, a_{3n}), & c_4 &:= f(a_{41}, a_{42}, \dots, a_{4n}). \end{aligned}$$

Заметим, что $c_1^\dagger = c_2^\dagger$, $c_3^\dagger = c_4^\dagger$, так как f является функцией-полиномом и сохраняет предикат $\rho_{T_{0 \sim 2, 1 \sim 3}}$.

Рассмотрим набор $(a_1, \dots, a_n) \in \{0, 1\}^n$ такой, что $a_i = a_{1i}^\dagger = a_{2i}^\dagger$ и набор $(a'_1, \dots, a'_n) \in \{0, 1\}^n$ такой, что $a'_i = a_{3i}^\dagger = a_{4i}^\dagger$.

Поскольку для любых ненулевых j , отличных от 1, выполнено $g_j^f \equiv 0$, то из следующей цепочки равенств

$$\begin{aligned} f(a_{11}, \dots, a_{1n}) &= g^f(a_1, \dots, a_n) + \sum_{i=1}^n g_i^f(a_1, \dots, a_n) \cdot 2 \lfloor a_{1i}/2 \rfloor + \\ 2g_0^f(a_1, \dots, a_n) &= g^f(a_1, \dots, a_n) + g_1^f(a_1, \dots, a_n) \cdot 2 \lfloor a_{11}/2 \rfloor + \\ 2g_0^f(a_1, \dots, a_n) &= f(a_{11}, a_2, a_3, \dots, a_n) \end{aligned}$$

получаем $c_1 = f(a_{11}, \dots, a_{1n}) = f(a_{11}, a_2, a_3, \dots, a_n)$. Аналогично выводятся следующие равенства:

$$\begin{aligned} c_2 &= f(a_{21}, \dots, a_{2n}) = f(a_{21}, a_2, a_3, \dots, a_n), \\ c_3 &= f(a_{31}, \dots, a_{3n}) = f(a_{31}, a'_2, a'_3, \dots, a'_n), \\ c_4 &= f(a_{41}, \dots, a_{4n}) = f(a_{41}, a'_2, a'_3, \dots, a'_n). \end{aligned}$$

Так как $(a_{11}, a_{21}, a_{31}, a_{41})$ принадлежит предикату ρ , то или $a_{11} = a_{21}$, или $a_{31} = a_{41}$, или $a_1 = a'_1$.

Значит, выполнится или $c_1 = c_2$, или $c_3 = c_4$, или, так как функция f принадлежит множеству K , $c_1^\dagger = c_2^\dagger = c_3^\dagger = c_4^\dagger = g^f(a_1, \dots, a_n)$.

Во всех указанных случаях $\{c_1, c_2, c_3, c_4\} \neq \{0, 1, 2, 3\}$ и набор (c_1, c_2, c_3, c_4) принадлежит предикату ρ . Следовательно, функция f сохраняет предикат ρ . □

Лемма 4. $(\text{Pol}(\rho) \cap \text{Poly}_4) \subseteq \text{K} \cup \text{I}$.

Доказательство. Рассмотрим $f \in \text{Pol}(\rho) \cap \text{Poly}_4$. Если у f не существует блока $0/2$ или блока $1/3$, то $f \in \text{I}$, поэтому далее мы считаем, что у f существует и блок $0/2$, и блок $1/3$. То есть существуют наборы $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \{0, 1\}^n$ и $t, s \in \{1, \dots, n\}$, что

$$\begin{aligned} g^f(a_1, \dots, a_n) &= 0, & g^f(b_1, \dots, b_n) &= 1, \\ g_s^f(a_1, \dots, a_n) &= 1, & g_t^f(b_1, \dots, b_n) &= 1. \end{aligned}$$

При этом $t = s$, так как иначе f не сохраняет предикат ρ :

$$f \begin{pmatrix} a_1 & \dots & a_s & \dots & a_t & \dots & a_n \\ a_1 & \dots & a_s + 2 & \dots & a_t & \dots & a_n \\ b_1 & \dots & b_s & \dots & b_t & \dots & b_n \\ b_1 & \dots & b_s & \dots & b_t + 2 & \dots & b_n \end{pmatrix} \in \begin{pmatrix} 0 & 0 & 2 & 2 \\ 2 & 2 & 0 & 0 \\ 1 & 3 & 1 & 3 \\ 3 & 1 & 3 & 1 \end{pmatrix}.$$

Без ограничения общности $t = s = 1$, и, следовательно, для всех $j > 1$ для любого набора $(c_1, \dots, c_n) \in \{0, 1\}^n$ выполняется $g_j^f(c_1, \dots, c_n) = 0$.

Также рассмотрим наборы $(d_2, \dots, d_n), (e_2, \dots, e_n) \in \{0, 1\}^{n-1}$, такие что $g_1^f(0, d_2, \dots, d_n) = g_1^f(0, e_2, \dots, e_n) = 1$. Тогда из сохранения предиката ρ следует:

$$f \begin{pmatrix} 0 & d_2 & \dots & d_n \\ 2 & d_2 & \dots & d_n \\ 0 & e_2 & \dots & e_n \\ 2 & e_2 & \dots & e_n \end{pmatrix} \in \begin{pmatrix} 0 & 0 & 2 & 2 & 1 & 1 & 3 & 3 \\ 2 & 2 & 0 & 0 & 3 & 3 & 1 & 1 \\ 0 & 2 & 0 & 2 & 1 & 3 & 1 & 3 \\ 2 & 0 & 2 & 0 & 3 & 1 & 3 & 1 \end{pmatrix}.$$

То есть $g^f(0, d_2, \dots, d_n) = f(0, d_2, \dots, d_n)^\dagger = f(0, e_2, \dots, e_n)^\dagger = g^f(0, e_2, \dots, e_n)$. Аналогично для наборов, начинающихся с 1. То есть существуют константы $a_0, a_1 \in \{0, 1\}$ такие, что для любого набора $(k, \alpha_2, \dots, \alpha_n) \in \{0, 1\}^n$, если $g_1^f(k, \alpha_2, \dots, \alpha_n) = 1$, то $g^f(k, \alpha_2, \dots, \alpha_n) = a_k$. Следовательно, $f \in \text{K}$, что и требовалось доказать. □

Из доказанных выше лемм выводится следующая теорема:

Теорема 3. $\text{Pol}(\rho) \cap \text{Poly}_4 = \text{I} \cup \text{K}$.

Теорема 4. $SL \cap \text{Poly}_4 \subsetneq \text{Pol}(\rho) \cap \text{Poly}_4$.

Доказательство. Класс Слупецкого SL состоит из двух типов функций: функций, существенно зависящих не более, чем от одной переменной и функций, принимающих не все значения.

Пусть функция-полином f существенно зависит не более, чем от одной переменной (без ограничения общности, если зависит, то от первой). Рассмотрим набор $(a_1, a_2, a_3, a_4) \in \rho$ и обозначим $c_1 = f(a_1, \dots)$, $c_2 = f(a_2, \dots)$, $c_3 = f(a_3, \dots)$, $c_4 = f(a_4, \dots)$.

Заметим, что $c_1^\dagger = c_2^\dagger$, так как $a_1^\dagger = a_2^\dagger$ и $f \in \text{Pol}(\rho_{T_{0 \sim 2, 1 \sim 3}})$. Аналогично, $c_3^\dagger = c_4^\dagger$, поскольку $a_3^\dagger = a_4^\dagger$ и $f \in \text{Pol}(\rho_{T_{0 \sim 2, 1 \sim 3}})$. Кроме того, $\{c_1, c_2, c_3, c_4\} \neq \{0, 1, 2, 3\}$, так как $\{a_1, a_2, a_3, a_4\} \neq \{0, 1, 2, 3\}$ и функция f отображает одинаковые значения в одинаковые. Следовательно, $(c_1, c_2, c_3, c_4) \in \rho$, и $f \in \text{Pol}(\rho)$.

Если функция f принимает не все значения, то из определения существования блоков $0/2$ и $1/3$ у неё либо не существует блока $0/2$, либо не существует блока $1/3$.

В качестве примера функции из $(\text{Pol}(\rho) \cap \text{Poly}_4) \setminus (SL \cap \text{Poly}_4)$ можно взять $h(x_1, x_2) := x_1^\dagger + 2x_2^\dagger$. Это полином, для которого $g^h(x_1, x_2) = x_1$, $g_0^h(x_1, x_2) = x_2$, $g_1^h = g_2^h \equiv 0$, принимающий все 4 значения, но у него не существует ни блока $0/2$, ни блока $1/3$. \square

Теорема 5. Класс $\text{Pol}(\rho) \cap \text{Poly}_4$ предполон в Poly_4 .

Доказательство. Рассмотрим функцию $f \in \text{Poly}_4 \setminus \text{Pol}(\rho)$. Так как f не сохраняет предикат ρ , существуют наборы $(a_{11}, a_{21}, a_{31}, a_{41})$, $(a_{12}, a_{22}, a_{32}, a_{42})$, \dots , $(a_{1n}, a_{2n}, a_{3n}, a_{4n}) \in \rho$, такие, что набор (c_1, c_2, c_3, c_4) , определённый равенствами

$$\begin{aligned} c_1 &= f(a_{11}, a_{12}, \dots, a_{1n}), & c_2 &= f(a_{21}, a_{22}, \dots, a_{2n}), \\ c_3 &= f(a_{31}, a_{32}, \dots, a_{3n}), & c_4 &= f(a_{41}, a_{42}, \dots, a_{4n}). \end{aligned}$$

не принадлежит предикату ρ .

Заметим, что $c_1^\dagger = c_2^\dagger$, $c_3^\dagger = c_4^\dagger$, так как f является функцией-полиномом и, следовательно, сохраняет предикат $\rho_{T_{0 \sim 2, 1 \sim 3}}$. Тогда $\{c_1, c_2, c_3, c_4\} = \{0, 1, 2, 3\}$ (иначе столбец принадлежал бы предикату ρ).

Далее, для любого набора $(a, b) \in \{0, 1, 2, 3\}^2$ определим две функции q_{b^*a} и q_{ab^*} следующим образом:

$$q_{b^*a}(x, y) := \begin{cases} b, & \text{если } (x, y) \in \{(0, 0), (0, 2)\}, \\ b + 2, & \text{если } (x, y) \in \{(2, 0), (2, 2)\}, \\ a, & \text{иначе} \end{cases}$$

$$q_{ab^*}(x, y) := \begin{cases} b, & \text{если } (x, y) \in \{(0, 1), (0, 3)\}, \\ b + 2, & \text{если } (x, y) \in \{(2, 1), (2, 3)\}, \\ a, & \text{иначе} \end{cases}$$

Несложно проверить, что эти функции сохраняют предикат ρ_{Poly} и, следовательно, представляются полиномами. Поскольку все эти функции представляют собой функции-полиномы, принимающие не более трёх значений, они принадлежат классу $\text{Poly}_4 \cap SL$, а следовательно, и классу $\text{Pol}(\rho)$.

Кроме того, для любых $a, b \in \{0, 1, 2, 3\}$ функции q_{b^*a} и q_{ab^*} обладают следующим свойством:

$$q_{ab^*} \begin{pmatrix} 0 & 0 \\ 2 & 0 \\ 0 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} a \\ a \\ b \\ b + 2 \end{pmatrix}, \quad q_{b^*a} \begin{pmatrix} 0 & 0 \\ 2 & 0 \\ 0 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} b \\ b + 2 \\ a \\ a \end{pmatrix}.$$

Теперь построим набор функций-полиномов h_i по следующим правилам:

1. Если $a_{1i} = a_{2i}$, $a_{3i} \neq a_{4i}$, то $h_i(x, y) = q_{a_{1i}a_{3i}^*}(x, y)$.
2. Если $a_{1i} \neq a_{2i}$, $a_{3i} = a_{4i}$, то $h_i(x, y) = q_{a_{1i}^*a_{3i}}(x, y)$.
3. Если $a_{1i} \neq a_{2i}$, $a_{3i} \neq a_{4i}$, $a_{1i} = a_{3i}$, то $h_i(x, y) = x + a_{1i}$.
4. Если $a_{1i} \neq a_{2i}$, $a_{3i} \neq a_{4i}$, $a_{1i} \neq a_{3i}$, то $h_i(x, y) = 2j_2(x) + 2j_1(y) + a_{1i}$.
5. Если $a_{1i} = a_{2i}$, $a_{3i} = a_{4i}$, то $h_i(x, y) = (a_{3i} - a_{1i}) \cdot y + a_{1i}$.

Заметим, что все функции h_i принадлежат классу $\text{Pol}(\rho)$, так как или принимают не все значения, или существенно зависят от одной переменной. Теперь рассмотрим функцию $f'(x, y) :=$

$f(h_1(x, y), \dots, h_n(x, y))$. Данная функция обладает следующим свойством:

$$f' \begin{pmatrix} 0 & 0 \\ 2 & 0 \\ 0 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix}.$$

При этом все c_i принимают разные значения и $c_1 + 2 = c_2$, $c_3 + 2 = c_4$. Рассмотрим функцию $f''(x, y) := (c_3 - c_1)(f'(x, y) - c_1)$. Она обладает следующим свойством:

$$f'' \begin{pmatrix} 0 & 0 \\ 2 & 0 \\ 0 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 1 \\ 3 \end{pmatrix}.$$

Рассмотрим ещё две функции-полинома из класса $\text{Pol}(\rho)$: $s(x, y) = x^2 + 2xy + y^2$ (принимает только значения 0 и 1) и $g(x, y) = x^2 + 2xy + y^2 + 3x + 3y$ (принимает только значения 0 и 2).

Заметим, что $x + y = f''(g(x, y), s(x, y))$. Из суммы следующим образом можно получить разность:

$$x - y = x + y + y + y.$$

С помощью суммы, разности и возведения в куб (это функция арности 1), получим функцию

$$3x^2y + 3xy^2 = (x + y)^3 - x^3 - y^3.$$

Отметим, что $x^2y^2 \in \text{Pol}(\rho)$, так как она принимает только значения 0 и 1. Также из формулы

$$(x^2 - x)(y^2 - y) = 0$$

следующим образом можно выразить умножение:

$$xy = -(x^2y + xy^2 + x^2y^2) = 3x^2y + 3xy^2 - x^2y^2.$$

Следовательно, с помощью произвольной функции-полинома $f \in \text{Poly}_4 \setminus \text{Pol}(\rho)$ и функций из $\text{Pol}(\rho)$ можно получить функции $x + y$ и xy . Константы уже принадлежат $\text{Pol}(\rho)$, а $\{1, x + y, xy\} = \text{Poly}_4$, предполнота доказана.

□

Список литературы

- [1] Яблонский С. В., “Функциональные построения в k -значной логике”, *Труды Математического института им. В. А. Стеклова*, **51** (1958), 5–142.
- [2] Розенберг И. Г., “Описание предполных классов в P_k ”, *Rozprawy Československé Akademie Věd, Série Math. Přír. Věd.*, **80** (1970), 3–93.
- [3] Слупецкий Е., “Полное трёхзначное исчисление высказываний”, *Comptes Rendus des Séances de la Société des Sciences et des Lettres de Varsovie, Classe III*, **29** (1936), 9–11.
- [4] Крохин А. А., Сафин К. Л., Суханов Е. В., “О строении решётки замкнутых классов полиномов”, *Дискретная математика*, **9:2** (1997), 24–39. DOI: 10.4213/dm469.
- [5] Селезнёва С. Н., “Описание замкнутого класса полиномиальных функций по модулю степени простого числа посредством отношения”, *Дискретная математика*, **35:4** (2023), 115–125. DOI: 10.4213/dm1803.
- [6] Мещанинов Д. Г., “О некоторых свойствах надструктуры класса полиномов в P_k ”, *Математические заметки*, **44:5** (1988), 673–681.
- [7] Ploščica M., Varga I., “Clones of compatible operations on rings \mathbb{Z}_{p^k} ”, *Journal of Multiple-Valued Logic and Soft Computing*, **36:4–5** (2021), 391–404.
- [8] Мещанинов Д. Г., “Замкнутые классы полиномов по модулю p^2 ”, *Дискретная математика*, **29:3** (2017), 54–69. DOI: 10.4213/dm1452.
- [9] Селезнёва С. Н., “О числе полиномиальных функций k -значной логики по составному модулю k ”, *Дискретная математика*, **28:2** (2016), 81–91. DOI: 10.4213/dm1371.
- [10] Марченков С. С., “Предполнота замкнутых классов в P_k : предикатный подход”, *Математические вопросы кибернетики*, 1996, № 6, 117–132 .

Статья поступила 30 марта 2026 г.

An analogue of the Slupecki maximal clone within the clone of polynomials modulo four

I. M. Yanushkevich

We study the clone of all functions on four elements that can be represented as polynomials modulo 4. We show that any such function is uniquely determined by a set of Boolean functions of the same arity. The main result of the paper is a description of a maximal clone within the clone of polynomial functions that contains all unary polynomials, and which is analogous to the Slupecky maximal clone.

Keywords: multivalued logic function, polynomial, closed class.

References

- [1] Yablonskii S. V., “Functional constructions in k -valued logic”, *Proceedings of the Steklov Institute of Mathematics*, **51** (1958), 5–142 (In Russian).
- [2] Rosenberg I. G., “Description of precomplete classes in P_k ”, *Rozprawy Československé Akademie Věd, Série Math. Přír. Věd.*, **80** (1970), 3–93 (In Russian).
- [3] Ślupecki J., “The full three-valued propositional calculus”, *Comptes Rendus des Séances de la Société des Sciences et des Lettres de Varsovie, Classe III*, **29** (1936), 9–11 (In German).
- [4] Krokhin A. A., Safin K. L., Sukhanov E. V., “On the structure of the lattice of closed classes of polynomials”, *Discrete Mathematics and Applications*, **7:2** (1997), 131–146. DOI: 10.1515/dma.1997.7.2.131.
- [5] Selezneva S. N., “Describing the closed class of polynomial functions modulo a power of a prime number by a relation”, *Discrete Mathematics and Applications*, **35:2** (2025), 125–133. DOI: 10.1515/dma-2025-0008.
- [6] Meshchaninov D. G., “Superstructures of the class of polynomials in P_k ”, *Mathematical Notes of the Academy of Sciences of the USSR*, **44** (1988), 850–854. DOI: 10.1007/BF01158427.
- [7] Ploščica M., Varga I., “Clones of compatible operations on rings \mathbb{Z}_{p^k} ”, *Journal of Multiple-Valued Logic and Soft Computing*, **36:4–5** (2021), 391–404.
- [8] Meshchaninov D. G., “Closed classes of polynomials modulo p^2 ”, *Discrete Mathematics and Applications*, **28:3** (2018), 167–178. DOI: 10.1515/dma-2018-0016.
- [9] Selezneva S. N., “On the number of functions of k -valued logic which are polynomials modulo composite k ”, *Discrete Mathematics and Applications*, **27:1** (2017), 7–14. DOI: 10.1515/dma-2017-0002.
- [10] Marchenkov S. S., “Precompleteness of closed classes in P_k : predicate approach”, *Mathematical Questions of Cybernetics*, 1996, № 6, 117–132 (In Russian).

Received on March 30, 2026

Часть 4
Круглый стол

Языковая радикальная сервисная платформа анализа и синтеза автоматизированных многоагентных систем искусственного интеллекта различного назначения

А. В. Чечкин* , Е. С. Плешакова†

В работе предложена концепция человекоцентрической архитектурно-информационной системы — Языковой Радикальной Сервисной Платформы Анализа и Синтеза (ЯРСПАС) Автоматизированных МногоАгентных Систем Искусственного Интеллекта (АМАСИИ). В условиях роста автономности интеллектуальных модулей и усложнения цифрового пространства возникает необходимость формализованного механизма их координации, адаптивной конфигурации и централизованного управления. Предлагается концептуальная модель ЯРСПАС, рассматриваемой как распределённая среда функциональных модулей с управляемыми состояниями активации и резервирования, взаимодействующих через событийно-ориентированную коммуникационную шину и общую рабочую область знаний. Обосновываются необходимые и достаточные требования к платформе ЯРСПАС для построения и сопровождения массовых умных систем типа АМАСИИ различного назначения. Используются методы радикального, математического, информационного, языкового, нейросетевого и цифрового моделирования, системного и ультрасистемного анализа и синтеза. Формулируются и обосновываются базовые требования к ЯРСПАС и АМАСИИ. Разработаны нейросетевые трансформеры нового типа.

Ключевые слова: цифровая платформа, автоматизированная многоагентная система, естественный и искусственный интеллект, трансформеры, гибридные нейронные сети..

* *Чечкин Александр Витальевич* — д.ф.-м.н., проф., Финансовый университет при Правительстве Российской Федерации, e-mail: a.checkkin@mail.ru.

Checkkin Alexander Vitalievich — Doctor of Physical and Mathematical Sciences, Professor, Financial University under the Government of the Russian Federation.

† *Плешакова Екатерина Сергеевна* — к.т.н., доцент, МИРЭА — Российский технологический университет, e-mail: pleshakova_es@mail.ru.

Pleshakova Ekaterina Sergeevna — Candidate of Technical Sciences, Associate Professor, MIREA — Russian Technological University.

1. Введение. Массовые умные системы различного назначения ноосферы Земли

Современный этап развития искусственного интеллекта характеризуется широким распространением многоагентных систем, гибридных нейросетевых архитектур и автономных цифровых сервисов, функционирующих в распределённой вычислительной среде. Такие системы применяются в задачах анализа больших данных, мониторинга цифрового пространства, обеспечения кибербезопасности, управления инфраструктурой и принятия решений в условиях неопределённости.

Рост масштабов и автономности интеллектуальных систем сопровождается возникновением ряда фундаментальных проблем, связанных с отсутствием единой архитектурной модели интеграции гетерогенных агентов, сложностью адаптивной реконфигурации систем при изменении внешней среды, недостаточной формализацией механизмов человекоцентричного управления и юридической ответственности, а также отсутствием архитектурных решений, обеспечивающих интеграцию современных когнитивных модулей — гибридных трансформеров, нейросетей Колмогорова–Арнольда и других моделей — в единую масштабируемую многоагентную платформу.

Теория многоагентных систем (Multi-Agent Systems, MAS) сформирована в работе [1]. В классическом понимании MAS представляет собой совокупность автономных агентов, взаимодействующих в общей среде и принимающих решения на основе локального восприятия и протоколов коммуникации [2]. Базовыми характеристиками агентов являются автономность и способность к кооперации. Архитектурно такие системы реализуются через модели распределённого планирования, координации задач и согласования действий.

В рамках теории MAS были разработаны модели взаимодействия агентов, механизмы распределённого поиска, протоколы переговоров, модели организационных структур, а также методы согласования стратегий в условиях частичной информации [3–5]. Однако подавляющее большинство таких архитектур ориентировано на решение прикладных задач распределённого управления или моделирования коллективного поведения и не предполагает платформенного уровня динамического синтеза и реконфигурации агентов в процессе эксплуатации системы.

Несмотря на значительное развитие теории многоагентных систем и гибридных нейросетевых архитектур, остаётся нерешённой задача построения формализованной платформенной модели, обеспечивающей адаптивное управление, когнитивную кооперацию агентов и контролируемое

сопровождение интеллектуальных систем в течение всего их жизненного цикла.

Настоящая работа направлена на устранение данного архитектурного разрыва. Авторы стремятся улучшить существующие решения за счёт разработки формализованной платформенной модели, объединяющей распределённую среду функциональных модулей, событийно-ориентированную коммуникацию, общую рабочую область знаний и уровень управления, обеспечивающий координацию и адаптивную настройку агентов. В отличие от традиционных MAS-архитектур, предлагаемый подход предусматривает механизм управляемой активации и деактивации когнитивных модулей в зависимости от изменения статистических и семантических характеристик входных данных.

В настоящей работе предлагается концептуальная архитектурная модель Языковой Радикальной Сервисной Платформы Анализа и Синтеза (ЯРСПАС), ориентированная на построение и сопровождение автоматизированных многоагентных систем искусственного интеллекта (АМАСИИ) различного назначения.

Актуальность исследования обусловлена ростом масштабов автономных интеллектуальных систем, их интеграцией в цифровые инфраструктуры и необходимостью обеспечения устойчивости, управляемости и прозрачности их функционирования. Увеличение объёма и сложности цифровых данных, а также динамичность информационной среды требуют перехода от статических архитектур к адаптивным платформенным решениям, способным координировать гетерогенные интеллектуальные агенты в единой когнитивной экосистеме. Предлагаемая модель ориентирована на решение именно этой задачи, обеспечивая структурированную интеграцию интеллектуальных модулей и их управляемое функционирование в рамках человекоцентричной цифровой платформы.

Приведем слова физиолога, академика И. П. Павлова: «...*Слово* сделало нас людьми. ...*Вторая сигнальная система* представляет собой чрезвычайную прибавку к высшей нервной деятельности человека, это наше лишнее, добавочное, социальное и есть человеческое ...» [6]. Приведем слова философа, академика В. И. Вернадского: «...Все человечество, вместе взятое, представляет ничтожную массу вещества планеты. Мощь его связана не с его массой, но с его мозгом, разумом и его трудом, направленным этим разумом. ... *Ноосфера* есть новое геологическое явление на нашей планете. В ней впервые человек становится крупнейшей геологической силой. Он может и должен перестраивать своим трудом и мыслью область своей жизни ...» [7]. Интеллектуальные системы любой архитектуры и назначения являются предметом *теоретической и прикладной информатики* [8].

Сегодня ноосфера Земли определяется умными системами искусственного интеллекта (ИИ) различного назначения в рамках разнообразных сервисных систем, таких как Infrastructure as a Service (IaaS); Software as a Service (SaaS); Platform as a Service (PaaS) [9, 10] и др.

Главная мысль авторов настоящей статьи состоит в том, что сообщество искусственных интеллектуальных систем ноосферы Земли должно формироваться и быть под жёстким контролем *человека-субъекта ПРАВА*. Для этого предлагается использовать Языковую Радикальную Сервисную Платформу Анализа и Синтеза (ЯРСПАС), с помощью которой формировать группировку исполнителей в форме Автоматизированных МногоАгентных Систем ИИ (АМАСИИ) требуемых назначений и обеспечивать высокоэффективное и юридически благоразумное сопровождение их в течение всего их жизненного цикла. В настоящей работе ЯРСПАС рассматривается не как существующий программный продукт, а как концептуальная архитектурная модель человекоцентричной многоагентной цифровой платформы, формализуемая впервые. Ниже сформулируем и обсудим базовые требования к сервисной платформе и к её многоагентным системам ИИ:

1.1. Радикальность архитектуры платформы ЯРСПАС и ее АМАСИИ

Платформа строится на базе математической модели проблемной области — расширенный театр действий ЯРСПАС и АМАСИИ в форме среды радикалов [11–15].

Определение. *Среда радикалов* — это тип распределённого информационно-системного избыточного ресурса, когда каждая целостность (модуль) этого ресурса является *радикалом*.

Определение. *Радикал* — это гетерогенная функциональная система любой архитектуры, которая имеет предназначение и два внешне доступных типа состояния: *активен* (включен) и *пассивен* (выключен).

Определение. *Активный радикал* — когда радикал функционирует, действует по своему назначению.

Определение. *Пассивный радикал* — когда радикал не функционирует по назначению, но готов к активации и находится в резерве, в запасе, в хранении. Пассивные радикалы определяют скрытый *потенциал* среды радикалов, предназначенный для преодоления нештатных, неопределённых ситуаций в театре действий ЯРСПАС и АМАСИИ. Наличие пассивных радикалов для ЯРСПАС и АМАСИИ — это эффективная

форма информационно-системной избыточности, которая обеспечивает их *Информационно-Системную Безопасность* (ИСБ) [11, 12].

Среда радикалов — иерархическая сеть взаимосвязанных и взаимосогласованных гетерогенных радикалов разной архитектуры. Структура среды радикалов имеет эффективную дружественную человеку форму *Координатной Навигационной Семантической Сети (КНСС)*, обладающей:

Во-первых, единой, глобальной семантической стандартизацией и согласованностью радикалов. В результате активные радикалы при функционировании не конфликтуют между собой. Пассивные радикалы выключены и не мешают функционированию активных радикалов.

Во-вторых, автономностью радикалов, когда доступно внешнее для ЯРСПАС или АМАСИИ управление активным радикалом, когда пассивный радикал доступен для *автономного обновления и модификации, с соблюдением* семантической согласованности и глобальной бесконфликтности среды радикалов.

В-третьих, оптимальной активацией среды радикалов, когда из многовариантной, многофункциональной возможности активации среды радикалов выбирается оптимальная, наиболее эффективная конфигурация, когда выбирается оптимальный кластер радикалов, целевая рабочая сеть активных радикалов, целевой системоквант.

Целью настоящего исследования является разработка и формализация архитектурной модели человекоцентричной многоагентной цифровой платформы — Языковой Радикальной Сервисной Платформы Анализа и Синтеза (ЯРСПАС), предназначенной для построения и координации автоматизированных многоагентных систем в динамически изменяющемся цифровом пространстве. В рамках достижения поставленной цели осуществляется формализация распределённой среды функциональных модулей (радикалов) как среды гетерогенных вычислительных компонентов с управляемыми состояниями активации и резервирования, объединённых в единую архитектуру взаимодействия. Разрабатывается модель межмодульной коммуникации на основе событийно-ориентированной шины (Event Bus), обеспечивающей асинхронный обмен сигналами и метаданными, и общей рабочей области (Shared Blackboard), реализующей согласованное хранение и агрегацию промежуточных когнитивных представлений. Предусматривается интеграция гибридных нейросетевых архитектур (включая трансформерные и KAN-ориентированные модели) в качестве вычислительных ядер агентов, выполняющих задачи семантического анализа, классификации и прогнозирования. Также формализуются механизмы динамического синтеза новых агентов и их конфигурацион-

ной адаптации в ответ на изменение статистических и семантических характеристик входных потоков данных.

1.2. Человекоцентричность платформы ЯРСПАС и её АМАСИИ

ЯРСПАС задумана как лаборатория для проведения экспериментально-исследовательских работ с целью построения элементной базы будущих АМАСИИ различного назначения. В частности, эффективных массовых стандартных радикалов, схем радикалов вплоть до штатных агентов АМАСИИ. При этом АМАСИИ всегда является автоматизированной системой, где главным является социально и юридически ответственный человек — (координатор, оператор, начальник, командир, хозяин). Платформа ЯРСПАС должна оперативно отвечать на динамику изменений в своей проблемной области, использовать свои инновации для создания, формирования, адаптации, управления, модификации сообщества социально ответственных АМАСИИ различного назначения под жёстким контролем человека. Координатор АМАСИИ должен соблюдать закон и быть юридическим или физическим субъектом ПРАВА. Действует правило: «Смочь АМАСИИ сможет, но кто ей позволит?».

ЯРСПАС организует, с учётом общего *Стратегического Технического Задания (общее СТЗ)* на дальнесрочный период для каждой АМАСИИ группировки индивидуальное *частное* Тактико-Техническое Задание (*ТТЗ*), включая (*частные ТТЗ*) для каждого агента. Имея стратегическую цель, как *общее СТЗ*, с учётом модели расширенного театра действий ЯРСПАС и АМАСИИ, координатор распределяет подцели, нагрузку между АМАСИИ. При этом каждому агенту АМАСИИ выдаётся своё *частное ТТЗ*. Без частного ТТЗ агенты не функционируют, находятся в резерве, в запасе в ожидании своего частного ТТЗ. *Координатор контролирует* исполнение общего и частных технических заданий и может в любой момент времени скорректировать любое частное ТТЗ своих агентов [13–16]. Кроме этого, ЯРСПАС обеспечивает успешное сервисное сопровождение всех подсистем АМАСИИ в течение всего их жизненного цикла. *Пример*, пусть для ЯРСПАС имеем:

общее СТЗ = «Анализ и оценки *Корректности ЦП*».

Здесь *ЦП* — это *Цифровое Пространство* — Выделенная часть Больших Данных (*ВчБД*) и Выделенная часть Умных Технологий (*ВчУТ*). *Корректность ЦП* — это когда *ВчБД* о точке [5], о чём-либо или о ком-либо зарегистрированы, формализованы и ещё, когда *ВчУТ* воздействия на данные, или на материал, или на энергию для достижения

разумной и закономерной цели, тоже *зарегистрированы, формализованы*. Анализ и оценки *корректности ЦП* — значит *обеспечить* для всех тех элементов ЦП, которые являются *активными (используемыми) в данное время в рамках ЯРСПАС* достоверную оценку корректности этого элемента.

1.3. Языковое общение в ЯРСПАС и в АМАСИИ

Языковое общение в ЯРСПАС и в АМАСИИ происходит на естественном языке человека. Координатор каждой АМАСИИ должен подчиняться закону и быть юридическим или физическим субъектом ПРАВА. Агентами АМАСИИ выступают отдельные умные системы ИИ различного назначения: сенсоры, датчики, роботы, цифровые двойники, нейросетевые трансформеры, классификаторы, системы поддержки выбора решений, планировщики и другие эффективные исполнители. Элементной базой платформы ЯРСПАС является сеть гетерогенных когнитивных радикалов, взаимодействующих через событийно-ориентированную шину (Event Bus) и общую рабочую область (Shared Blackboard).

Далее рассмотрим методические примеры успешных разработок в рамках ЯРСПАС трёх новых нейросетевых трансформеров: *Hyb-KAN* (см. раздел 2), *KAN-BiLSTM* (см. раздел 3) и *Hyb-TKAN* (см. раздел 4), являющихся прототипами будущих агентов АМАСИИ соответствующего назначения.

2. Hyb-KAN в многоагентной системе

Автоматизированная Многоагентная Система ИИ является прикладной реализацией ЯРСПАС. Каждый агент АМАСИИ является автономной функциональной системой — схемой радикалов, выполняющей конкретную задачу в рамках частного ТТЗ, утверждённого координатором. В рамках ЯРСПАС ключевое значение приобретает вопрос выбора и организации вычислительного «ядра» для радикалов, реализующих функции интеллектуального анализа, прогнозирования и принятия оценок корректности ЦП. Отдельные агенты АМАСИИ могут быть реализованы в виде специализированных гибридных нейросетевых структур.

Наиболее перспективной является новая архитектура *Hyb-KAN* (*Hybrid Kolmogorov–Arnold Network*), интегрирующая принципы рекуррентных сетей (BiLSTM), трансформеров (RoBERTa), многодоменного динамического внимания (MD-DAN, Multi-Domain Dynamic Attention) и функциональных аппроксиматоров Колмогорова–Арнольда (KAN). Универсальная архитектура *Hyb-KAN* разработана для интеллектуального

анализа и оценок корректности ЦП, для выявления деструктивного контента ЦП, в том числе проблем социальной инженерии.

Гибридная нейросетевая архитектура нового поколения *Hyb-KAN* обеспечивает интерпретируемость, адаптивность, устойчивость вычислений и применяется для задачи классификации текстовых данных цифрового пространства, рис. 1.

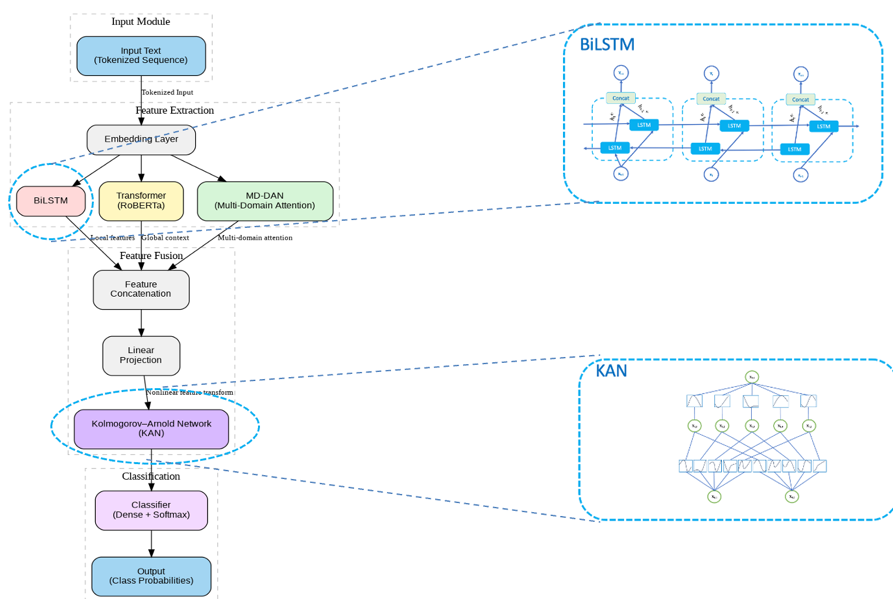


Рис. 1: Архитектура *Hyb-KAN*

Архитектура *Hyb-KAN*, рис. 1, объединяет несколько уровней:

- *уровень локальных зависимостей*, моделируемый модулем BiLSTM, который фиксирует синтаксические и временные связи последовательностей;
- *уровень глобального контекста*, реализуемый специализированным трансформером RoBERTa для извлечения семантических корреляций между токенами и предложениями;
- *уровень многодоменного динамического внимания (MD-DAN)*, обеспечивающий селективное выделение трёх взаимосвязанных доменов признаков — семантического, контекстного и временного;
- *уровень функциональной аппроксимации (KAN)*, моделирующий нелинейные взаимодействия между признаками, которые извлечены

предыдущими модулями, в соответствии с теоремой Колмогорова–Арнольда о суперпозиции многомерных функций.

Каждый радикал *Hyb-KAN* в платформе ЯРСПАС функционирует как интеллектуальный модуль, способный к адаптивной самокалибровке и контекстной переработке входных данных. При активации радикал подключается к событийно-ориентированной шине платформы и общей доске знаний, обмениваясь результатами анализа с другими агентами-радикалами.

В процессе работы *Hyb-KAN* формирует многоуровневое представление входного текста X , преобразуя его в интегрированное пространство признаков F_{MD-DAN} .

Предлагаемая модель *Hyb-KAN* интегрирует преимущества сети *KAN*, сети *BiLSTM*, многодоменной динамической сети внимания *MD-DAN* и *Transformer*.

Ниже представлена символьная формализация основных модулей модели.

Входное пространство и этап восприятия. Рассмотрим входной текст X в виде последовательности эмбедингов: $x_i, i = 1, \dots, T$

$$X = \{x_1, x_2, \dots, x_T\}, \quad x_i \in \mathbb{R}^{d_i},$$

где T — длина последовательности, d_i — размерности эмбедингов, $i = 1, \dots, T$. Для моделирования локального синтаксического контекста используется *BiLSTM*:

$$\begin{aligned} \vec{h}_i &= \text{LSTM}_f(x_i, \vec{h}_{i-1}), \\ \overleftarrow{h}_i &= \text{LSTM}_b(x_i, \overleftarrow{h}_{i+1}), \\ h_i &= [\vec{h}_i; \overleftarrow{h}_i], \quad H_{\text{BiLSTM}} = \{h_1, \dots, h_T\}, \quad h_i \in \mathbb{R}^{2h}. \end{aligned}$$

Для глобального контекстного кодирования используется предварительно обученный трансформер *RoBERTa*:

$$H_{\text{Trans}} = \text{RoBERTa}(X) = \{r_1, \dots, r_T\}, \quad r_i \in \mathbb{R}^{d_r}.$$

Таким образом, радикал *Hyb-KAN* сочетает линейные зависимости *BiLSTM* с глобальной контекстуальной структурой *Transformer*, обеспечивая многомерное восприятие смыслов.

Многодоменная динамическая сеть внимания. Для интеграции разных доменов внимания используется многодоменная динамическая сеть внимания (*MD-DAN*). Модуль *MD-DAN* описывает семантическое, контекстное и временное внимание. Пусть E_i — общий вектор признаков для i -го токена, полученный через объединение скрытых состояний:

$$E_i = [h_i; r_i] \in \mathbb{R}^{2h+d_r}.$$

Семантическое внимание:

$$\alpha_i = \text{softmax}(E_i^\top W_s), \quad S = \sum_{i=1}^T \alpha_i E_i.$$

Контекстуальное self-внимание:

$$\begin{aligned} Q_i &= E_i W_q, & K_j &= E_j W_k, & V_j &= E_j W_v, \\ A_{ij} &= \frac{Q_i K_j^\top}{\sqrt{d_k}}, \\ C_i &= \sum_{j=1}^T \text{softmax}(A_{ij}) V_j. \end{aligned}$$

Временное внимание (при наличии t_i):

$$\beta_i = \text{softmax}(t_i^\top W_t), \quad \mathcal{T} = \sum_{i=1}^T \beta_i E_i.$$

Агрегация доменных признаков:

$$F_{\text{MD-DAN}} = w_s S + w_c C + w_t \mathcal{T}, \quad w_s, w_c, w_t \in \mathbb{R}.$$

Интеграция признаков. Объединение всех модулей:

$$\tilde{H} = [H_{\text{BiLSTM}}; H_{\text{Trans}}; F_{\text{MD-DAN}}] \in \mathbb{R}^{T \times d_f}, \quad X_f = W_f \tilde{H} + b_f \in \mathbb{R}^{T \times d_x}.$$

Завершающий когнитивный этап. Завершающий когнитивный этап работы радикала реализуется посредством *сети Колмогорова–Арнольда (KAN)*, формализующей рассуждение как суперпозицию функций и реализующей обобщённую модель *КАН* аппроксимации:

$$\begin{aligned} f(X_f) &= \sum_{i=1}^m \varphi_i \left(\sum_{j=1}^n \omega_{ij} g_j(x_j) + b_i \right), \\ g_j(x_j) &= a_{j0} + \sum_{k=1}^p a_{jk} x_j^k, \end{aligned}$$

где $\varphi_i(\cdot)$ — обучаемая активация.

В контексте ЯРСПАС этот уровень отражает процесс интерпретации и принятия решения — формирование нового смыслового состояния на основании накопленных представлений.

Далее результат от *KAN* передаётся в двухслойный классификатор:

$$\begin{aligned} z &= \text{ReLU}(W^{(1)}f(X_f) + b^{(1)}), \\ z' &= \text{Dropout}(z), \\ \hat{y} &= \text{Softmax}(W^{(2)}z' + b^{(2)}). \end{aligned}$$

В качестве функции потерь используется кросс-энтропия:

$$\mathcal{L} = - \sum_{i=1}^T y_i \log(\hat{y}_i),$$

где y_i — истинная метка, \hat{y}_i — предсказанная вероятность класса i .

Таким образом, радикал *Hyb-KAN* обучается минимизировать расхождение между предсказанным и истинным смысловым классом, формируя устойчивую когнитивную реакцию на входной стимул. Такая многоуровневая структура обеспечивает интерпретируемое и человекоцентричное функционирование радикала: каждый вычислительный этап соответствует наблюдаемому когнитивному процессу, а результат его работы подлежит контролю и правовой ответственности человека-координатора.

Было проведено *сравнительное экспериментальное исследование* её качества по отношению к широко используемым моделям глубокого обучения. Сравнение проводилось на корпусе текстов цифрового пространства, включающем категории корректного и деструктивного контента. Обучение моделей осуществлялось при одинаковых условиях разбиения данных и параметрах оптимизации. Предложенная авторами в исследовании модель сравнивалась с тремя базовыми моделями классификации: свёрточные нейронные сети *CNN*, сети с долговременной краткосрочной памятью *LSTM*, *BiLSTM* и двунаправленные кодирующие представления от трансформеров *RoBERTa*. Полученные результаты демонстрируют, что интеграция многодоменного динамического внимания и функционального слоя Колмогорова–Арнольда позволяет повысить качество классификации по сравнению с традиционными рекуррентными и трансформерными архитектурами, рис. 2.

Представленные тестовые результаты подтверждают, что модуль *Hyb-KAN* в рамках концепции ЯРСПАС создаёт основу для построения человекоцентричных многоагентных систем различного назначения, обладающих устойчивостью к контекстному искажению данных, необходимой

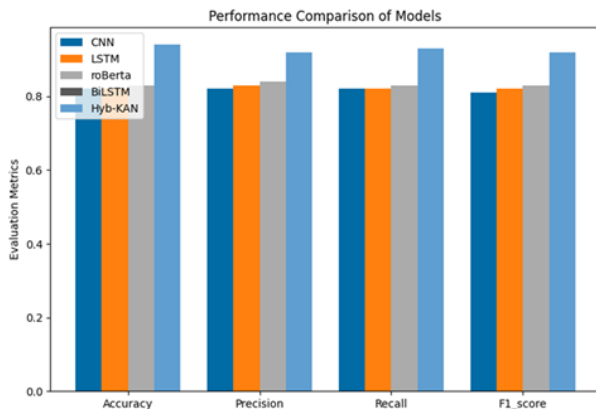


Рис. 2: Сравнительный анализ производительности моделей

адаптивностью и высокой интерпретируемостью. В частности, систем классификации текстов, систем интеллектуального анализа и оценок коррекции цифрового пространства.

Развитие гибридных архитектур искусственного интеллекта открывает возможности реализации интеллектуальных агентов нового типа: интерпретируемых, адаптивных и этически контролируемых [13–17]. Синтез концепции ЯРСПАС и нейросетей типа *Hyb-KAN* позволяет сформировать метауровневую систему АМАСИИ, в которой человек выступает субъектом права и координатором, а нейросетевые агенты с подчинёнными им функциональными радикалами реализуют задачи интеллектуального анализа и оценок корректности ЦП.

В Языковой Радикальной Сервисной Платформе Анализа и Синтеза (ЯРСПАС) каждый радикал функционирует не изолированно, а как элемент распределённой когнитивной экосистемы. Управление взаимодействием радикалов и координация их когнитивных циклов осуществляется посредством событийно-ориентированной шины (Event Bus) и общей рабочей области (Shared Blackboard), формирующих коммуникационное ядро платформы (рис. 3).

Событийно-ориентированная шина реализует асинхронный обмен данными и сигналами между активными радикалами.

Каждый *Hyb-KAN*-радикал может: *публиковать* события, отражающие результаты анализа контента; *подписываться* на события от других радикалов, инициируя собственный когнитивный цикл при появлении новых данных; передавать управляющие мета-сигналы в сторону координатора. Таким образом, *Event Bus* выступает как проводящая система

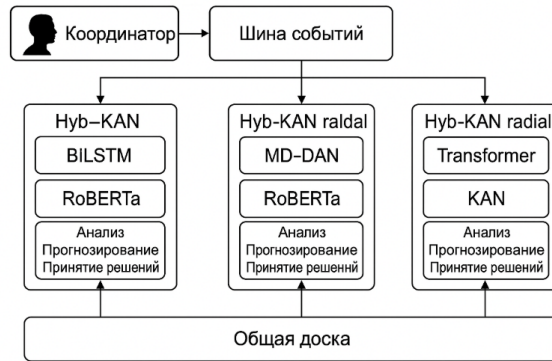


Рис. 3: Архитектура Гиб-KAN в ЯРСПАС–АМАСИИ

ЯРСПАС, обеспечивающая живой обмен смысловыми импульсами между интеллектуальными модулями-радикалами.

Общая рабочая область (*Shared Blackboard*) представляет собой *глобальную память платформы*, содержащую структурированные представления текущего состояния среды радикалов, их гипотез и промежуточных выводов. В отличие от событийной шины, которая передаёт мгновенные сигналы, доска знаний аккумулирует долгоживущие артефакты анализа.

Гиб-KAN-радикалы взаимодействуют с доской в трёх режимах:

1. *Запись* — публикация новых интерпретаций и вероятностных оценок в виде векторов \hat{y}_i , сопровождаемых метаданными (дата, источник, контекст).
2. *Чтение* — получение результатов других радикалов для контекстного обогащения собственного анализа.
3. *Резонанс* — совместная обработка записей с разными уровнями доверия, что формирует когнитивный консенсус между радикалами.

Эта структура реализует принцип *когнитивной кооперации*: радикалы не просто обмениваются данными, но синтезируют общее представление ситуации ЦП.

В надсистемном уровне ЯРСПАС функционирует *Метамодуль-диспетчер*, который координирует работу всех деятельных радикалов, распределяет тактико-технические задания (ТТЗ) и контролирует нагрузку. При поступлении в *Event Bus* нового класса угроз или изменении статистики входных сигналов диспетчер инициирует создание нового радикала, используя шаблон *Гиб-KAN* как *архитип когнитивного ядра*.

В этом заключается процесс настраивания АМАСИИ на новое семантическое состояние ЦП. Процесс синтеза нового радикала включает:

1. *Копирование* базовой архитектуры *Hyb-KAN* и загрузку предварительно обученных параметров.
2. *Инициализацию домена внимания D^** , соответствующего новому типу угрозы (например, речевая агрессия, фейковый контент, манипулятивная реклама).
3. *Регистрацию радикала* в среде и установку связей с *Blackboard* и другими модулями ЯРСПАС.
4. *Включение механизма обратного обучения* на новых данных, поступающих через шину событий.

Таким образом, система демонстрирует *адаптивный синтез модулей* — формирование новых когнитивных радикалов, настроенных по требованию ЦП без нарушения глобальной семантической согласованности.

В основе всей событийно-ориентированной архитектуры сохраняется принцип человекоцентризма: любой радикал, даже синтезированный автоматически, подчинён координатору-человеку, являющемуся субъектом права. Только человек может авторизовать активацию радикала и подтвердить его решения. В результате формируется человеко-машинная когнитивная система, способная адаптивно реагировать на угрозы, синтезировать новые формы интеллектуальной активности и при этом оставаться под полным юридическим и этическим контролем субъекта-координатора.

3. Новый гибридный нейросетевой трансформер KAN-BiLSTM для анализа и оценок корректности ЦП

В рамках ЯРСПАС была разработана новая архитектура нейросети с высокими показателями многоуровневой обработки текстовых данных: от локального синтаксического анализа до функционального синтеза смысловых данных. Новая гибридная нейросетевая архитектура *Hyb-KAN* (Hybrid Kolmogorov–Arnold Network). Модуль *Hyb-KAN* интегрирует преимущества известных механизмов: BiLSTM, Transformer (RoBERTa), Multi-Domain Dynamic Attention (MD-DAN) и функциональных аппроксиматоров Колмогорова-Арнольда (KAN).

Автоматизированная Многоагентная Система (АМАСИИ) выступает прикладной реализацией ЯРСПАС. Каждый агент является автономной функциональной системой — схемой радикалов, выполняющей

конкретную задачу в рамках общей цели, определённой координатором. В рамках ЯРСПАС ключевое значение приобретает вопрос выбора и организации вычислительного «ядра» для радикалов, реализующих функции интеллектуального анализа, прогнозирования и принятия решений об оценках корректности ЦП. В этой роли естественным образом выступают гибридные нейросетевые архитектуры нового поколения, обеспечивающие интерпретируемость, адаптивность и устойчивость вычислений. Наиболее перспективным решением является новая архитектура *Hyb-KAN (Hybrid Kolmogorov–Arnold Network)*, интегрирующая принципы рекуррентных сетей (*BiLSTM*), трансформеров (*RoBERTa*), многодоменного динамического внимания (*MD-DAN*) и функциональных аппроксиматоров Колмогорова–Арнольда (*KAN*) (см. раздел 2).

С точки зрения платформы ЯРСПАС, такая архитектура выступает интеллектуальным агентом, трансформером *KAN-BiLSTM* (см. раздел 3), способным к многоуровневому семантическому анализу и синтезу решений в составе распределённой среды радикалов. При этом модуль *BiLSTM* обеспечивает моделирование локальных зависимостей и временных закономерностей текстовых потоков, трансформерный блок *RoBERTa* извлекает глобальный контекст и скрытые связи в языке, модуль *MD-DAN* выделяет семантические, контекстные и временные домены внимания, а сеть *KAN* выполняет функциональную аппроксимацию сложных нелинейных зависимостей между признаками. В совокупности эти компоненты формируют *гибридное ядро радикала*, которое может быть внедрено в любую Автоматизированную МногоАгентную Систему ИИ (АМАСИИ) как автономный элемент среды радикалов ЯРСПАС. При активации такой радикал выполняет интеллектуальные функции анализа ЦП, распознавания деструктивных воздействий и формирования сигналов для управляющих агентов.

С точки зрения платформы ЯРСПАС, аналогичная архитектура выступает как интеллектуальный агент, трансформер *KAN-BiLSTM* [18], способный к многоуровневому семантическому анализу и синтезу решений в составе распределённой среды радикалов. В этом случае модуль *BiLSTM* обеспечивает моделирование локальных зависимостей и временных закономерностей текстовых потоков, трансформерный блок *RoBERTa* извлекает глобальный контекст и скрытые связи в языке, модуль *MD-DAN* выделяет семантические, контекстные и временные домены внимания, а сеть *KAN* выполняет функциональную аппроксимацию сложных нелинейных зависимостей между признаками.

Ключевой особенностью предлагаемой новой архитектуры является замена стандартного полносвязного классификационного блока на функциональный аппроксиматор *KAN*. Такой подход позволяет моделировать

нелинейные зависимости между признаками через суперпозицию одномерных функций, что повышает структурированность нелинейности и снижает параметрическую избыточность модели. В результате достигается баланс между выразительной способностью и вычислительной устойчивостью.

Дополнительным эффектом является повышение *интерпретируемости*, при которой вклад отдельных признаков и их функциональных преобразований может быть проанализирован на уровне компонент *KAN*, что было бы затруднительно при использовании стандартных плотных слоёв.

Снижение параметрической сложности делает модель менее чувствительной к дисбалансу классов, а также обеспечивает стабильность при обработке текстов с вариативной лексикой и синтаксическими перестановками. Благодаря линейной масштабируемости и умеренным требованиям к вычислительным ресурсам архитектура пригодна для работы в режиме непрерывного анализа потоковых данных, где критическим фактором является скорость обработки. Таким образом, слой *KAN* позволяет повысить точность модели и структурировать её нелинейность без существенного увеличения вычислительной нагрузки, обеспечивая практическую применимость при решении задач анализа и получения оценок корректности цифрового пространства.

При активации новый трансформер *KAN-BiLSTM* [18] (см. раздел 3) выполняет функции интеллектуального анализа и оценок корректности ЦП с учетом распознавания очередных новых деструктивных воздействий и формирования сигналов для управляющих агентов. При деактивации он сохраняет свою конфигурацию и знания в составе пассивного резерва платформы, обеспечивая информационно-системную избыточность и безопасность среды радикалов. При этом модуль *Hyb-KAN* используется в ЯРСПАС как универсальный вычислительный модуль синтеза смыслов и распознавания паттернов, обеспечивающий технологическую основу для человекоцентричных, юридически контролируемых и этически ответственных автоматизированных многоагентных систем интеллектуального анализа и оценок корректности ЦП.

4. Новый гибридный нейросетевой трансформер Hyb-TKAN для классификации ЦП

Кроме трансформера *KAN-BiLSTM* (см. раздел 3) в рамках Языковой Радикальной Сервисной Платформы Анализа и Синтеза (ЯРСПАС) получена ещё одна новая гибридная нейросетевая архитектура трансформер

Hyb-TKAN (Hybrid Kolmogorov–Arnold Network Transformer), [19], который является агентом АМАСИИ. Он обеспечивает классификацию ЦП, семантический анализ, идентификацию угроз и адаптивную обработку потоковых данных в коллективном ЦП.

Гибридная архитектура нейросетевого преобразователя *Hyb-TKAN* сочетает ключевые преимущества моделей *BiLSTM*, *Transformer*, многодоменной динамической сети внимания (*MD-DAN*) и сети *KAN*. Предлагаемая структура сочетает способность *BiLSTM* эффективно фиксировать локальные взаимосвязи внутри последовательностей с возможностями *Transformera* учитывать глобальные контекстные зависимости. Дополнительный модуль *MD-DAN* повышает производительность модели, подчёркивая семантические, контекстные и временные характеристики данных.

Гибридная структура *Hyb-TKAN* позволяет дополнять преимущества *Transformera* и *BiLSTM* при обработке последовательных текстовых данных, в то время как сеть *KAN* расширяет возможности модели в плане учёта меняющихся во времени зависимостей. Это делает её особенно эффективной в сценариях динамического распространения деструктивного контента, например, в рамках скоординированных кампаний по дезинформации.

Архитектура *Hyb-TKAN* состоит из нескольких модулей, включая модуль *BiLSTM*, модуль *Transformer*, многодоменную динамическую сеть внимания (*MD-DAN*), сеть *KAN* и финальный классификатор. Ключевые особенности *Hyb-TKAN* включают многоуровневый анализ, в котором *BiLSTM* фиксирует локальные синтаксические и последовательные зависимости, *Transformer* обрабатывает глобальную контекстную информацию, *MD-DAN* обеспечивает семантическое, контекстное и временное внимание, а сеть *KAN* явно моделирует нелинейные временные зависимости, улучшая способность системы обнаруживать динамические и скрытые закономерности в данных.

Синергия *BiLSTM*, *Transformer*, *MD-DAN* и сети *KAN* обеспечивает гибкость, адаптивность и точность анализа текста и последовательностей. Модель *Hyb-TKAN* [19] легко применима в различных областях и задачах благодаря гибридной архитектуре и внедрению сети *KAN*. Она позволяет эффективно обрабатывать временные и нелинейные зависимости. Модель легко применима в различных областях и задачах благодаря гибридной архитектуре и внедрению сети *KAN*, обеспечивает эффективную обработку временных и нелинейных зависимостей.

5. Заключение

Обоснована необходимость создания человекоцентрической архитектурно-информационной платформы нового типа Языковой Радикальной Сервисной Платформы Анализа и Синтеза (ЯРСПАС), обеспечивающей управляемое, юридически ответственное и этически согласованное функционирование систем искусственного интеллекта типа АМАСИИ ноосферы Земли. Показано, что предложенная структура радикалов, объединённых через событийно-ориентированную шину и общую рабочую область, формирует когнитивную экосистему, способную к адаптивному синтезу новых функциональных элементов и поддержанию информационно-системной безопасности в динамически изменяющемся цифровом пространстве.

Интеграция радикала *Hyb-KAN* (см. раздел 2) в рамках ЯРСПАС в многоагентную среду АМАСИИ убедительно продемонстрировала возможность построения самоорганизующихся систем, где взаимодействие между агентами осуществляется через Event Bus и Shared Blackboard, а метаагент управляет синтезом новых радикалов на основе текущего контекста. Тем самым реализуется принцип когнитивной кооперации и создаётся человеко-машинная экосистема, способная к автономному развитию под полным правовым и этическим контролем координатора, субъекта права.

Результаты демонстрационных примеров (см. разделы 3 и 4) подтверждают, что объединение философских основ ноосферного подхода к ЦП с современными новыми гибридными нейросетевыми архитектурами формирует теоретическую и технологическую базу для построения эффективных Автоматизированных Многоагентных Систем анализа и оценок корректности ЦП, обеспечивающих безопасность, устойчивость и интерпретируемость когнитивных процессов искусственного интеллекта в рамках человекоцентричной цифровой сервисной платформы.

Список литературы

- [1] M. Wooldridge, N.R. Jennings, “Intelligent agents: Theory and practice”, *The Knowledge Engineering Review*, **10:2** (1995), 115–152. DOI: 10.1017/S0269888900008122.
- [2] J. Huang et al., “Foundation models and intelligent decision-making: Progress, challenges, and perspectives”, *The Innovation*, **6:6** (2025), 100948. DOI: 10.1016/j.xinn.2025.100948.
- [3] W. Zhao et al., “A Survey on Computing Power Networks: Architecture, Resource Allocation, and AI Services Enablement”, *IEEE Transactions on Network Science and Engineering*, 2026.

- [4] S. Gupta, “AI agents collaboration under resource constraints: Practical implementations”, *International journal of artificial intelligence research and development*, **3**:1 (2025), 51–63. DOI: 10.34218/IJAIRD_03_01_004.
- [5] Nguyen-Thi-Mai A. et al., “A Survey on Challenges and Emerging Frontiers of Multi-Agent Systems”, *SOICT 2025 (The 14th International Symposium on Information and Communication Technology)*, 2025.
- [6] И. П. Павлов, *Лекции о работе больших полушарий головного мозга. Полное собрание трудов*, т. **1, 2, 5**, 1973.
- [7] В. И. Вернадский, *Биосфера и ноосфера*, Наука, М., 1989.
- [8] А. В. Чечкин, *Математическая информатика*, Наука, М., 1991.
- [9] *Яндекс 360*, <https://360.yandex.ru/>.
- [10] S. Russell, P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed., Pearson, 2021.
- [11] А. В. Чечкин, “Тезис о наличии искусственного интеллекта”, *Интеллектуальные системы. Теория и приложения.*, **25**:1 (2021), 29–49.
- [12] А. В. Чечкин, “Когнитивный уровень ИИ”, *Интеллектуальные системы. Теория и приложения.*, **26**:2 (2022), 5–24.
- [13] А. В. Чечкин, “Математические основы теоретической информатики. Теория нечёткой семантической информации о точке. Семантика естественного языка”, *Интеллектуальные системы. Теория и приложения.*, **29**:1 (2025), 5–16.
- [14] L. Floridi, J. Cowsls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, E. Vayena, “AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations”, *Minds and Machines*, **28**:4 (2018), 689–707. DOI: 10.1007/s11023-018-9482-5.
- [15] B. Shneiderman, “Human-centered artificial intelligence: Reliable, safe & trustworthy”, *International Journal of Human-Computer Interaction*, **36**:6 (2020), 495–504. DOI: 10.1080/10447318.2020.1741118.
- [16] F. Chen, S. Li, J. Han, F. Ren, Z. Yang, “Review of Lightweight Deep Convolutional Neural Networks”, *Archives of Computational Methods in Engineering*, **31**:4 (2024), 1915–1937. DOI: 10.1007/s11831-023-10032-z.
- [17] A. V. Chechkin, E. S. Pleshakova, S. T. Gataullin, “A Hybrid KAN-BiLSTM Transformer with Multi-Domain Dynamic Attention Model for Cybersecurity”, *Technologies*, **13**:6 (2025), 223. DOI: 10.3390/technologies13060223.
- [18] A. V. Chechkin, E. S. Pleshakova, S. T. Gataullin, “Мультиагентная система мониторинга цифрового пространства на основе гибридного нейросетевого трансформера KAN-BiLSTM”, *Свидетельство о государственной регистрации программы на ЭВМ № 2025696035*, 2025.
- [19] A. V. Chechkin, E. S. Pleshakova, S. T. Gataullin, “Гибридный нейросетевой трансформер Нуб-ТКАН для обнаружения и классификации деструктивного контента в цифровом пространстве”, *Свидетельство о государственной регистрации программы на ЭВМ № 2025697450*, 2025.

Language Radical Service Platform for Analysis and Synthesis of Automated Multi-Agent Artificial Intelligence Systems for Various Purposes

A. V. Chechkin, E. S. Pleshakova

This paper proposes the concept of a human-centric architectural information system — the Language Radical Service Platform for Analysis and Synthesis (YARSPAS) of Automated Multi-Agent Artificial Intelligence Systems (AMASII). In the context of the growth of autonomous intelligent modules and the increasing complexity of digital spaces, the need arises for a formalized mechanism for their independence, adaptive configuration, and centralized control. A conceptual model of YARSPAS is proposed, considered as a distributed environment created by modules with controlled activation and redundancy states, interacting through an event-oriented communication bus and a conducting knowledge area. The necessary and sufficient requirements for the YARSPAS platform for the construction and maintenance of mass-scale smart systems like AMASII for various purposes are substantiated. Methods of radical, mathematical, information, language, neural network, and digital modeling, as well as system and ultra-system analysis and synthesis are used. Basic requirements for YARSPAS and AMASII are formulated and substantiated. A new type of neural network transformers is developed.

Keywords: digital platform, automated multi-agent system, natural and artificial intelligence, transformers, hybrid neural networks..

References

- [1] M. Wooldridge, N. R. Jennings, “Intelligent agents: Theory and practice”, *The Knowledge Engineering Review*, **10**:2 (1995), 115–152. DOI: 10.1017/S0269888900008122.
- [2] J. Huang et al., “Foundation models and intelligent decision-making: Progress, challenges, and perspectives”, *The Innovation*, **6**:6 (2025), 100948. DOI: 10.1016/j.xinn.2025.100948.
- [3] W. Zhao et al., “A Survey on Computing Power Networks: Architecture, Resource Allocation, and AI Services Enablement”, *IEEE Transactions on Network Science and Engineering*, 2026.
- [4] S. Gupta, “AI agents collaboration under resource constraints: Practical implementations”, *International journal of artificial intelligence research and development*, **3**:1 (2025), 51–63. DOI: 10.34218/IJAIRD_03_01_004.
- [5] Nguyen-Thi-Mai A. et al., “A Survey on Challenges and Emerging Frontiers of Multi-Agent Systems”, *SOICT 2025 (The 14th International Symposium on Information and Communication Technology)*, 2025.

- [6] I. P. Pavlov, *Lectures on the Work of the Large Hemispheres of the Brain. Complete Works, Vols. 1, 2, 5*, 1973.
- [7] V. I. Vernadsky, *The Biosphere and the Noosphere*, Nauka, Moscow, 1989.
- [8] A. V. Chechkin, *Mathematical Informatics*, Nauka, Moscow, 1991.
- [9] *Yandex 360*, <https://360.yandex.ru/>.
- [10] S. Russell, P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed., Pearson, 2021.
- [11] A. V. Chechkin, “Thesis on the Existence of Artificial Intelligence”, *Intelligent Systems. Theory and Applications.*, **25**:1 (2021), 29–49.
- [12] A. V. Chechkin, “Cognitive Level of AI”, *Intelligent Systems. Theory and Applications.*, **26**:2 (2022), 5–24.
- [13] A. V. Chechkin, “Mathematical Foundations of Theoretical Informatics. Theory of Fuzzy Semantic Information About a Point of a Set. Semantics of Natural Language”, *Intelligent Systems. Theory and Applications.*, **29**:1 (2025), 5–16.
- [14] L. Floridi, J. Cowsls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, E. Vayena, “AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations”, *Minds and Machines*, **28**:4 (2018), 689–707. DOI: 10.1007/s11023-018-9482-5.
- [15] B. Shneiderman, “Human-centered artificial intelligence: Reliable, safe & trustworthy”, *International Journal of Human-Computer Interaction*, **36**:6 (2020), 495–504. DOI: 10.1080/10447318.2020.1741118.
- [16] F. Chen, S. Li, J. Han, F. Ren, Z. Yang, “Review of Lightweight Deep Convolutional Neural Networks”, *Archives of Computational Methods in Engineering*, **31**:4 (2024), 1915–1937. DOI: 10.1007/s11831-023-10032-z.
- [17] A. V. Chechkin, E. S. Pleshakova, S. T. Gataullin, “A Hybrid KAN-BiLSTM Transformer with Multi-Domain Dynamic Attention Model for Cybersecurity”, *Technologies*, **13**:6 (2025), 223. DOI: 10.3390/technologies13060223.
- [18] A. V. Chechkin, E. S. Pleshakova, S. T. Gataullin, “Multiagent System for Monitoring Digital Space Based on the Hybrid Neural Network Transformer KAN-BiLSTM”, *Certificate of State Registration of Computer Program No. 2025696035*, 2025.
- [19] A. V. Chechkin, E. S. Pleshakova, S. T. Gataullin, “Hybrid Neural Network Transformer Hyb-TKAN for Detecting and Classifying Destructive Content in Digital Space”, *Certificate of State Registration of Computer Program No. 2025697450*, 2025.

К сведению авторов публикаций в журнале «Интеллектуальные системы. Теория и приложения»

В соответствии с требованиями ВАК РФ к изданиям, входящим в перечень ведущих рецензируемых научных журналов и изданий, в которых могут быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук, статьи в журнал «Интеллектуальные системы. Теория и приложения» предоставляются авторами в следующей форме:

1. Статьи, набранные в пакете \LaTeX , предоставляются к загрузке через WEB-форму <https://intsysmagazine.ru/submit>.
2. В преамбуле статьи должны содержаться название статьи на русском и английском языках, аннотация на русском и английском языках (не более 150 слов), список ключевых слов на русском и английском языках (не более 12 слов), информация об авторах: Ф.И.О. полностью, место работы, должность, ученая степень и/или звание (если имеется), для аспирантов ФИО научного руководителя, e-mail, ORCID.
3. Список литературы оформляется в едином формате, установленном системой Российского индекса научного цитирования. Списки на русском и английском языках приводятся в конце файла с текстом статьи, и должны быть оформлены с помощью пакета `amsbib`.
4. За публикацию статей в журнале «Интеллектуальные системы. Теория и приложения» с авторов (в том числе аспирантов высших учебных заведений) статей, рекомендованных к публикации, плата не взимается. Авторам бесплатно предоставляется номер журнала, в котором вышла статья. Журнал распространяется по подписке, экземпляры журнала рассылаются подписчикам наложенным платежом. Условия подписки публикуются в каталоге НТИ «Роспечать», индекс журнала 64559.
5. Электронная версия журнала находится в открытом доступе. Все материалы распространяются на условиях лицензии Creative Commons Attribution 4.0 International (CC BY 4.0). Электронные версии всех выпущенных номеров размещаются на сайте

<https://intsysmagazine.ru>

и доступны для свободного чтения и скачивания. Авторы сохраняют авторские права на свои статьи.

Подписано в печать: 12.06.2026

Дата выхода: 22.06.2026

Тираж: 200 экз.

Цена свободная

Свидетельство о регистрации СМИ: ПИ № ФС77-58444 от 25 июня
2014 г., выдано Федеральной службой по надзору в сфере связи,
информационных технологий и массовых коммуникаций
(Роскомнадзор).