

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

# **Интеллектуальные Системы. Теория и приложения**

**ТОМ 22 ВЫПУСК 2 \* 2018**  
**МОСКВА**

**Главный редактор:** д.ф.-м.н., профессор В. Б. Кудрявцев

**Редакционная коллегия:**

д.ф.-м.н., проф. А. Е. Андреев (зам. главного редактора)  
д.ф.-м.н., проф. Э. Э. Гасанов (зам. главного редактора)  
к.ф.-м.н., доц. А. С. Строгалов (зам. главного редактора)  
к.ф.-м.н., м.н.с. В. В. Осокин (ответственный секретарь)  
д.ф.-м.н., проф. В. В. Александров, д.ф.-м.н., проф. С. В. Алешин, д.ф.-м.н., проф. Д. Н. Бабин, д.ф.-м.н., проф. В. А. Бувеч, академик РАН, д.ф.-м.н., проф. Ю. Л. Ершов, академик РАН, д.ф.-м.н., проф. Ю. И. Журавлев, д.ф.-м.н., проф. В. Н. Козлов, чл.-корр. РАН, д.ф.-м.н., проф. А. В. Михалев, к.ф.-м.н., проф. В. А. Носов, д.ф.-м.н., проф. А. С. Подколзин, д.т.н., проф. Д. А. Поспелов, д.ф.-м.н., проф. Ю. П. Пытгев, академик РАН, д.т.н., проф. А. С. Сигов, д.э.н., проф. Ю. Н. Черемных, д.ф.-м.н., проф. А. В. Чечкин

**Международный научный совет журнала:**

С. Н. Васильев (Россия), К. Вашик (Германия), В. В. Величенко (Россия), А. И. Галушкин (Россия), И. В. Голубятников (Россия), Я. Деметрович (Венгрия), Л. Заде (США), Г. Килибарда (Сербия), Ж. Кнап (Словения), П. С. Краснощеков (Россия), А. Нозаки (Япония), В. Н. Редько (Украина), И. Розенберг (Канада), А. П. Рыжов (Россия) — ученый секретарь совета, А. Саломая (Финляндия), С. Саксида (Словения), Б. Тальхайм (Германия), Ш. Ушчумлич (Сербия), Фан Дин Зиеу (Вьетнам), А. Шайб (Сирия), Р. Шчепанович (США), Г. Циммерман (Германия)

**Секретари редакции:** И. О. Бергер, М. А. Ильгова, А. А. Коровин

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, Секции «Информатики и кибернетики» РАЕН.

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.

Спонсором издания является:

**ООО «Два Облака»**

Разработка корпоративных информационных систем  
<http://www.dvaoblaka.ru>

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@intsysjournal.org](mailto:mail@intsysjournal.org)

\*) Прежнее название журнала: «Интеллектуальные системы».  
© ООО «Интеллектуальные системы», 2018.

## ОГЛАВЛЕНИЕ

### Часть 1. Общие проблемы теории интеллектуальных систем

*Михалевич И.Ф., Рыжов А.П.* Оценка устойчивости развития критической инфраструктуры Российской Федерации на базе технологии оценки и мониторинга информационной безопасности ..... 7

*И.Н.Молодцов, Д.О.Бабаева.* Некоторые математические модели упругопластических процессов сложного нагружения ..... 19

### Часть 2. Специальные вопросы теории интеллектуальных систем

*Дергач П.С.* О языках, устойчивых относительно операций выпадения, вставки ..... 39

*Казаков И.Б.* Структура графа на множестве перестановок  $S_n$ , задаваемая моделью ошибки в скрытом канале перестановки пакетов ..... 53

### Часть 3. Математические модели

*Моисеев С. В.* Решётка клонов трёхзначной логики, содержащих функции 0, 1, 2, *min*, *max* ..... 83

*Самоненко И.Ю.* О количестве регулярных языков, представимых в групповых гиперавтоматах ..... 113

### Часть 4. Материалы семинара «Теория автоматов»

Доклады семинара «Теория автоматов» ..... 125

*Рыжов А. П.* Оценка и мониторинг процессов в социотехнических системах и связанные с ними задачи ..... 129

*Соколов А. П., Межов И. В.* О ранковой флеш памяти ..... 141

*Часовских А.А.* Проблема полноты в классах линейных автоматов ..... 151



**Часть 1.**  
**Общие проблемы теории**  
**интеллектуальных систем**



# Оценка устойчивости развития критической инфраструктуры Российской Федерации на базе технологии оценки и мониторинга информационной безопасности

Михалевич И.Ф., Рыжов А.П.

В работе рассмотрены возможности применения технологии оценки и мониторинга сложных процессов обеспечения информационной безопасности в задаче устойчивого развития критической инфраструктуры Российской Федерации. Предложена структура модели устойчивости критической инфраструктуры, возможные сценарии использования системы оценки и мониторинга информационной безопасности, обсуждаются аналитические возможности системы.

**Ключевые слова:** информационная безопасность, критическая инфраструктура, технология оценки и мониторинга сложных процессов, устойчивое развитие.

## 1. Введение.

Концепция устойчивого развития во многом перекликается с концепцией ноосферы, выдвинутой академиком В. И. Вернадским ещё в середине XX века. Ее современное толкование берет начало с 70-х годов прошлого столетия, когда человечество столкнулось с вопросами ограниченности природных ресурсов, а также загрязнения природной среды, которая является основой жизни, экономической и любой деятельности человека. Реакцией на эту озабоченность было создание международных неправительственных научных организаций по изучению глобальных процессов на Земле, таких как Международная федерация институтов перспективных исследований (ИФИАС), Римский клуб (с его знаменитым докладом «Пределы роста»), Международный институт системного анализа, а в СССР — Всесоюзный институт системных исследова-

ний. Проведение в 1972 году в Стокгольме Конференции ООН по окружающей среде и создание Программы ООН по окружающей среде (ЮНЕП) ознаменовало включение международного сообщества на государственном уровне в решение экологических проблем, которые стали сдерживать социально-экономическое развитие. Всемирная стратегия охраны природы (ВСОП), принятая в 1980, впервые в международном документе содержала упоминание устойчивого развития. Вторая редакция ВСОП получила название «Забота о планете Земля — Стратегия устойчивой жизни» и была опубликована в октябре 1991. В ней подчеркивается, что развитие должно базироваться на сохранении живой природы, защите структуры, функций и разнообразия природных систем Земли, от которых зависят биологические виды. Для этого необходимо: сохранять системы поддержки жизни (жизнеобеспечения), сохранять биоразнообразие и обеспечить устойчивое использование возобновляемых ресурсов. Появились исследования по экологической безопасности как части национальной и глобальной безопасности.

Частью национальной и глобальной безопасности современного мира является информационная безопасность [1 – 4]. Нарушения безопасности информации, такие как несанкционированное раскрытие или изменение информации, блокирование доступа к информации способны существенно воспрепятствовать любому росту, особенно, если это касается критических инфраструктур. В связи с этим вопросы оценки и мониторинга информационной безопасности стоят в ряду приоритетных задач обеспечения устойчивого развития критических инфраструктур [5 – 12].

С технической точки зрения вопросы устойчивости изучались в рамках кибернетики. Наиболее близким понятием является понятие гомеостаза. Возникли специальные математические модели экономического развития, учитывающие устойчивость развития (например, модель Солоу-Свана, гравитационная модель, Модель Рамсея-Касса-Купманса, Модель пересекающихся поколений или модель Самуэльсона-Даймонда). Обсуждению данной проблематики также уделяется внимание в русскоязычной литературе (например, [13], [16]; библиография [17]), выпускаются специальные журналы [14], консалтинговые компании предлагают услуги в области устойчивого развития [15].

Систематическая работа с оценкой и мониторингом устойчивого развития предполагает создание специальной системы. Одним из авторов работы разработана технология оценки и мониторинга сложных процессов [18], которая была успешно использована для разработки систем оценки и мониторинга способности стран к производству специальных

технологий в ядерной области в интересах управления международных гарантий Международного Агентства по Атомной Энергии [19], оценки и мониторинга способности команды разработчиков микроэлектроники к выполнению проекта для компании Cadence Design Systems [20], оценки и мониторинга рисков атеросклеротических заболеваний [21] и других систем.

В настоящей работе представлено видение авторов по возможному решению задачи устойчивого развития критической инфраструктуры Российской Федерации на базе технологии оценки и мониторинга сложных процессов применительно к обеспечению информационно безопасности.

### **Информационная безопасность критической инфраструктуры**

Критическую инфраструктуру стран образуют системы и активы, нарушение функционирования или уничтожение которых оказывает деструктивное влияние на жизненно важные для них сферы. Так, в критической инфраструктуре РФ можно выделить следующие сектора и области: здравоохранение, наука, транспорт, связь, энергетика, банковская и иные сферы финансового рынка, топливно-энергетический комплекс, атомная энергетика, оборонная промышленность, ракетно-космическая промышленность, горнодобывающая промышленность, металлургическая промышленность, химическая промышленность, федеральные органы государственной власти, органы государственной власти субъектов РФ, органы местного самоуправления, российские юридические лица и индивидуальные предприниматели, которые обеспечивают функционирование и взаимодействие элементов критической инфраструктуры РФ [1 – 5].

Деятельность критических инфраструктур невозможна без информационного взаимодействия, что делает устойчивость их развития зависимой от информационной безопасности [11, 12]. В каждой критической инфраструктуре образуется критическая информационная инфраструктура (КИИ), включающая свои объекты и телекоммуникации, используемые для организации взаимодействия объектов. Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» безопасность КИИ РФ определена как состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

Значимость объектов КИИ определяется возможным ущербом, причиняемым жизненно важным интересам (процессам) при нарушении их

функционирования. Вышеназванным законом к критериям значимости объектов КИИ РФ отнесены социальная, политическая, экономическая, экологическая важность, важность для обеспечения обороны страны, безопасности государства и правопорядка, которые основаны на соответствующих оценках [3 – 5]:

социальная - в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к системам обеспечения правосудия, правопорядка, государственным и муниципальным услугам и т.п. для получателей таких услуг;

политическая - в оценке возможного причинения ущерба интересам страны в вопросах внутренней и внешней политики;

экономическая - в оценке возможного причинения прямого и/или косвенного ущерба субъектам экономической деятельности;

экологическая - в оценке уровня возможного ущерба окружающей среде;

и т.д.

Таким образом, оценка и мониторинг информационной безопасности КИИ РФ и критической инфраструктуры в целом являются существенными факторами устойчивости их развития [1, 2].

### **Технология оценки и мониторинга: особенности разработки приложений**

Технология оценки и мониторинга сложных процессов ориентирована на разработку человеко-компьютерных систем для оценки состояния и отслеживания развития процессов в бизнесе, экономике, социологии, политике и других областях, которые принято называть слабо или плохо формализуемыми. Для таких процессов почти всегда невозможно построить математическую модель в привычном понимании (в виде уравнений, автоматов и пр.) либо модель является очень абстрактной и ее практическое использование невозможно. Трудности связаны не только со сложностью самих процессов, но и с неизмеримостью значений их параметров в привычном виде чисел; «измерительным прибором» для таких параметров является человек. Однако, есть аналитики, решающие задачу оценки и мониторинга на систематической основе, поэтому автоматизация их работы является осмысленной задачей. Разработка таких систем возможна, когда можно построить семантическую модель про-

цесса в виде набора понятий и их взаимосвязей, а также поступает и анализируется реальная информация - возможны обучение и настройка. Схема работы систем оценки и мониторинга представлена на рис. 1.

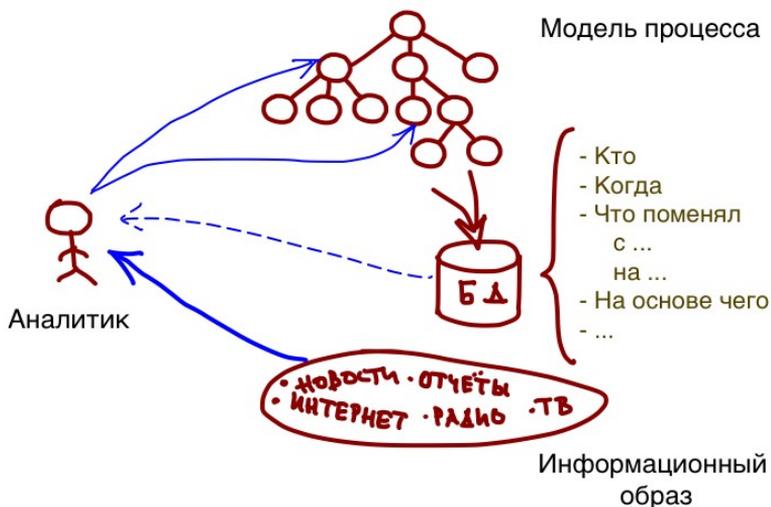


Рис. 1. Схема работы систем оценки и мониторинга.

При практической реализации систем оценки и мониторинга возникают следующие проблемы.

**Проблема 1** (описание человеком объектов). Можно ли, учитывая некоторые особенности восприятия человеком объектов реального мира и их описания, сформулировать правило выбора оптимального множества значений признаков, по которым описываются эти объекты? Возможны два критерия оптимальности:

**Критерий 1.** Под оптимальными понимаются такие множества значений, используя которые человек испытывает минимальную неопределенность при описании объектов.

**Критерий 2.** Если объект описывается некоторым количеством экспертов, то под оптимальными понимаются такие множества значений, которые обеспечивают минимальную степень рассогласования описаний.

Показано, что мы можем сформулировать методику выбора оптимального множества значений качественных признаков. Более того, показано, что такая методика является устойчивой, то есть возможные при

построении функций принадлежности естественные маленькие ошибки не оказывают существенного влияния на выбор оптимального множества значений. Множества, оптимальные по критериям 1 и 2 совпадают.

**Проблема 2** (поиск информации, описанной человеком). Можно ли определить показатели качества поиска информации в нечетких (лингвистических) базах данных и сформулировать правило выбора такого множества лингвистических значений, использование которого обеспечивало бы максимальные показатели качества поиска информации?

Показано, что можно ввести показатели качества поиска информации в нечетких (лингвистических) базах данных и формализовать их. Показано, что возможно сформулировать методiku выбора оптимального множества значений качественных признаков, которое обеспечивает максимальные показатели качества поиска информации. Более того, показано, что такая методика является устойчивой, то есть возможные при построении функций принадлежности естественные маленькие ошибки не оказывают существенного влияния на выбор оптимального множества значений.

**Проблема 3** (агрегирование информации). Можно ли предложить алгоритмы выбора операторов агрегирования информации в системах информационного мониторинга, обеспечивающие «настройку» системы на конкретную предметную область?

Выделяются следующие подходы к решению этой проблемы, базирующиеся на различных интерпретациях операторов агрегирования информации: геометрический, логический, и на основе обучения. Последний включает в себя обучение на основе генетических алгоритмов и обучение на основе нейронных сетей.

Перечисленные выше результаты решения проблем 1- 3 подробно описаны в [18]. Они позволяют разрабатывать оптимальные с точки зрения удобства использования системы оценки и мониторинга сложных процессов.

Таким образом, основной задачей разработки приложения является построение модели процесса.

### **Модель процесса устойчивого развития**

Модель процесса состоит из двух частей: структуры и правил агрегирования информации. Структура представляет собой дерево или граф без циклов, вершины которого представляют собой понятия предметной области, ребра – связи между ними. Пример структуры процесса оценки

и мониторинга информационной безопасности КИИ РФ приведен на рис. 2.

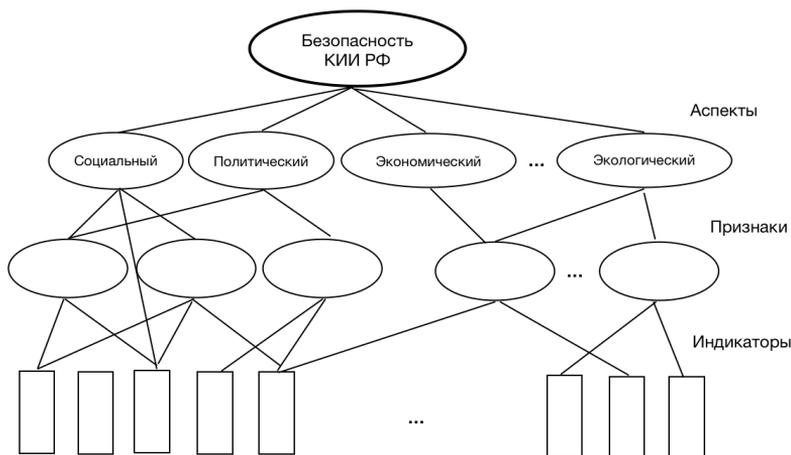


Рис. 2. Пример структуры модели

Логика работы модели задается операторами агрегирования информации, вычисляющими оценки узлов верхнего уровня в зависимости от значений оценок подчиненных узлов. Настройка модели для конкретной задачи заключается в обучении операторов агрегирования информации. Классификация операторов агрегирования информации, условия их применимости, а также эти процедуры обучения детально описаны в [22].

На верхнем уровне факторы устойчивого развития можно разделить на внешние и внутренние. Факторы внешней среды оказывают прямое или косвенное влияние на деятельность предприятия и действуют за ее пределами. Поэтому для обеспечения устойчивости своего функционирования компании должны оперативно реагировать на изменения внешней среды (законодательство, состояние и тренды рынка, требования инвесторов и пр.) и принимать эффективные решения. Факторы внутренней среды (организационная структура компании, эффективность производственных процессов, состав и квалификация персонала, организация труда и методы управления, состояние материально-технической базы и технологии) оказывают значительное влияние на устойчивость развития предприятия и являются более контролируруемыми.

Заметим, что часто такая модель используется в достаточно зрелых бизнес-структурах – это сбалансированная система показателей (Balanced ScoreCard). Если одной из стратегических целей организации

является устойчивое развитие – то соответствующая часть сбалансированной системы показателей может являться моделью для системы оценки и мониторинга. В противном случае модель строится на тех же принципах и с использованием тех же механизмов, что и сбалансированная система показателей.

### **Возможные сценарии использования системы оценки и мониторинга в задаче оценки устойчивого развития критических инфраструктур**

Заметим, что различные аспекты системы оценки и мониторинга устойчивого развития так или иначе присутствуют в любой организации, обеспечивающей деятельность объектов КИИ РФ и критической инфраструктуры РФ, и являются зоной ответственности различных подразделений. Например, оценку и мониторинг информационной безопасности в организации осуществляет служба безопасности (СБ), факторов внешней среды – СБ, ИТ, PR/GR, юридическая служба, маркетинг, факторов внутренней среды – СБ, ИТ, HR, производственные подразделения. Внедрение системы оценки и мониторинга устойчивого развития позволит иметь целостную картину этой работы в КИИ РФ и критической инфраструктуре РФ в целом. Такой эффект достигается благодаря тому, что модель (благодаря ее структуре – дерево или граф без циклов) можно «разрезать» на ряд подмоделей. Каждая служба компании может работать со своим фрагментом модели (что она и так делает, только такая работа будет более прозрачной, измеримой, дающей возможности решения дополнительных аналитических задач), а руководство компании будет иметь целостную картину состояния устойчивости компании (рис. 3).

В рамках систем оценки и мониторинга возможно решение прямой и обратной задачи оценки информационной безопасности и устойчивости КИИ РФ и критической инфраструктуры РФ.

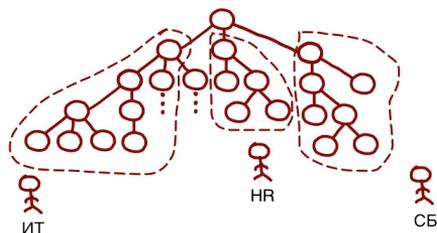


Рис. 3. Возможности декомпозиции систем оценки и мониторинга.

Прямая задача заключается в нахождении критических путей – таких элементов модели, малое изменение которых приводит к изменению всех вышележащих узлов, включая верхний. Знание таких элементов имеет большое практическое значение и позволяет выявить "слабые места" в процессе на текущий момент времени, разработать мероприятия по блокированию нежелательных ситуаций или провоцированию желательных, т.е. управлять развитием процесса в интересах компании. Для большого класса операторов агрегирования информации возможно вычисление степени критичности каждого элемента модели [22]. Задача также может решаться перебором для достаточно компактной модели.

Обратная задача позволяет оптимизировать бюджет на достижение определённого уровня устойчивости. Если задан бюджет, и мы знаем стоимость изменения состояния узла модели, то возможно нахождение тех узлов, изменение которых находится в рамках заданного бюджета и даёт максимальной эффект повышения устойчивости компании. При заданных условиях возможно и решение сопряжённой задачи: нахождение минимального бюджета, позволяющего достичь необходимый уровень устойчивости.

Перечисленные задачи можно решать как в рамках фрагментов модели (оптимизация работы соответствующих объектов КИИ РФ), так и модели в целом (оптимизация КИИ РФ по повышению устойчивости критической инфраструктуры РФ).

## Список литературы

- [1] Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 05.12.2016 г. № 646.
- [2] Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы. Утверждена Указом Президента Российской Федерации от 09.05.2017 г. № 203.
- [3] Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- [4] Critical Infrastructure Threat Information Sharing Framework. A Reference Guide for the Critical Infrastructure Community. USA Homeland Security, October 2016. – 110 p.
- [5] Правила категорирования объектов критической информационной инфраструктуры Российской Федерации. Утверждены постановлением Правительства Российской Федерации от 08.02.2018 г. № 127.

- [6] Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения. Утвержден постановлением Правительства Российской Федерации от 08.02.2018 г. № 127.
- [7] Critical Information Infrastructures Protection approaches in EU. Final Document | Version 1 | TLP: Green | July 2015. – 19 p. - <https://resilience.enisa.europa.eu/enisas-ncss-project/CIIApproachesNCSS.pdf>.
- [8] Matt Barrett, Jeff Marron, Victoria Yan Pillitteri, Jon Boyens, Greg Witte, Larry Feldman. The Cybersecurity Framework. Implementation Guidance for Federal Agencies. Draft Report 8170. U.S. Department of Commerce. National Institute of Standards and Technology Interagency. - May 2017. - 41 p. - <https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf>.
- [9] Don Snyder, James D. Powers, Elizabeth Bodine-Baron, Bernard Fox, Lauren Kendrick, Michael H. Powell. Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles. – 74 p. - [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR1000/RR1007/RAND\\_RR1007.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1007/RAND_RR1007.pdf).
- [10] A Generic National Framework For Critical Information Infrastructure Protection (CIIP). ITU, 2007. - 30 p. - [www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf](http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf).
- [11] Михалевич И.Ф. Концепция создания доверенной среды функционирования автоматизированных систем в защищенном исполнении на базе операционной системы «Синтез-ОС». – М.: ООО «АйТиСириус», 2012. – 50 с. [Электронный ресурс]. URL: <https://www.itsirius.ru/resheniya/> (дата обращения: 20.12.2012).
- [12] Михалевич И.Ф. Проблемы создания доверенной среды функционирования автоматизированных систем управления в защищенном исполнении / Труды XII Всероссийского совещания по проблемам управления (ВСПУ-2014, Москва). - М.: Институт проблем управления им. В.А.Трапезникова РАН, 2014. - С. 9201-9207.
- [13] Критерии устойчивости предпринимательской деятельности в условиях мировой экономической рецессии / Российское предпринимательство № 1, вып. 2 (176), 2011. - С. 57-61
- [14] Устойчивый бизнес. Экспертный деловой журнал. <http://csrjournal.com/>
- [15] Обзор услуг в области чистых технологий и устойчивого раз-

вития. Ernst & Young - <http://www.ey.com/RU/ru/Services/Specialty-Services/Climate-Change-and-Sustainability-Services>.

[16] Корчагина Е.В. Сравнительный анализ отчетности устойчивого развития российских и зарубежных компаний / Проблемы современной экономики. № 4 (28), 2008.

[17] <http://www.m-economy.ru/keyword.php?id=3209&l=R>

[18] Рыжов А.П. Информационный мониторинг сложных процессов: технологические и математические основы / Интеллектуальные системы, т. 11, вып. 1-4, 2008. - С. 101-136.

[19] Ryjov A., Belenki A., Hooper R., Pouchkarev V., Fattah A., Zadeh L. A. Development of an Intelligent System for Monitoring and Evaluation of Peaceful Nuclear Activities (DISNA). IAEA, STR-310. Vienna, 1998, 122 p.

[20] Лебедев А.А., Рыжов А.П. Оценка и мониторинг проектов разработки высокотехнологичных изделий на примере микроэлектроники / Интеллектуальные системы, т. 11, вып. 1-4, 2008. С. 55-82.

[21] Ахмеджанов Н.М., Жукоцкий А.В., Кудрявцев В.Б., Оганов Р.Г., Расторгуев В.В., Рыжов А.П., Строгалов А.С. Информационный мониторинг в задаче прогнозирования риска развития сердечно-сосудистых заболеваний / Интеллектуальные системы, т. 7, вып. 1-4, 2003. С. 5 – 38.

[22] Рыжов А.П. Об агрегировании информации в нечетких иерархических системах / Интеллектуальные системы, т. 6, вып. 1-4, 2001. - С. 341.

**Assessment of the sustainability of the development of the critical infrastructure of the Russian Federation on the basis of information security assessment and monitoring technology**  
**Igor F. Mikhalevich, Alexandr P. Ryjov**

The paper considers the possibilities of applying the technology of assessment and monitoring of complex processes of ensuring information security in the task of sustainable development of the critical infrastructure of the Russian Federation. The structure of the critical infrastructure stability model, the possible scenarios for the system of information security assessment and monitoring, the analytical capabilities of the system are discussed.

**Keywords:** information security, critical infrastructure, technology for assessment and monitoring of complex processes, sustainable development.



# Некоторые математические модели упругопластических процессов сложного нагружения

Молодцов И.Н., Бабаева Д.О.

В рамках теории упругопластических процессов А.А.Ильюшина [1], в [3] для математического моделирования процессов сложного нагружения использовано квазилинейное определяющее уравнение с тремя функционалами состояния. Калибровка определяющих функционалов там проведена с использованием экспериментальных результатов [4] (Р.А.Васин и др.) по трехмерным винтовым траекториям деформаций. Выяснилось, что отклик на винтовую траекторию деформации принимает, по исчерпанию некоторого следа запаздывания, вполне определенную форму предельного режима. Поэтому для произвольных трехмерных процессов деформации в [2] предлагалось последовательно аппроксимировать траектории деформации отрезками винтовых линий, на которых вычислять определяющие функционалы по уравнениям предельных режимов. Тогда на траекториях указанного вида реализуется соответствие геометрии траектории деформаций форме отклика. Это соответствие по А.А.Ильюшину назовем теоремой изоморфизма, уточняя для процессов высокой размерности уравнения самих винтовых сплайнов в пространстве деформаций и форм отклика. Принятый в [2] алгоритм относился исключительно к трехмерным траекториям и базировался на использовании смешанного пространственного базиса, включающего, помимо традиционных в определяющих соотношениях векторов (направляющих векторов напряжений и скоростей деформаций), еще и сам направляющий вектор деформаций. Здесь рассматриваются варианты модификации общей теории, годные для описания произвольных процессов нагружения с траекториями деформаций любой размерности. В качестве репера во всех новых теориях использованы направляющий вектор напряжений и векторы, построенные на основе векторов естественного сопровождающего репера Френе. Поскольку далее рассматриваются процессы деформации высокой размерности, то растет чис-

ло определяющих функционалов и несколько усложняются методы их идентификации.

**Ключевые слова:** пластичность, пластические деформации, сложное нагружение, определяющие соотношения, идентификация функционалов, теорема изоморфизма

### Основная идея.

Рассматриваются процессы сложного упругопластического нагружения материалов. Для описания их свойств вводятся пятимерные евклидовы пространства векторов–девиаторов напряжений и деформаций. Процесс деформации характеризуется в пространстве пятимерной кривой, в каждой точке которой изображается реакция или отклик материала на деформацию в виде вектора напряжений. Пусть  $\bar{\sigma}$  и  $\bar{\varepsilon}$  обозначают согласованные пары пятимерных векторов напряжений и деформаций, построенные на базе девиаторов соответствующих тензоров. В [2] векторы напряжений и деформаций связываются между собой определяющими уравнениями:

$$\frac{d\bar{\sigma}}{ds} = Q \frac{d\bar{\varepsilon}}{ds} + (P - Q) \left( \frac{d\bar{\varepsilon}}{ds}, \bar{n}_\sigma \right) + (N - Q) \left( \frac{d\bar{\varepsilon}}{ds}, \bar{n}'_\varepsilon \right) \bar{n}'_\varepsilon, \quad (1)$$

$$\bar{n}'_\varepsilon \equiv \frac{\bar{n}_\varepsilon - (\bar{n}_\sigma, \bar{n}_\varepsilon) \bar{n}_\sigma}{\sqrt{\Psi}}, \quad \Psi \equiv 1 - (\bar{n}_\sigma, \bar{n}_\varepsilon)^2,$$

в которых  $P, N, Q$  - функционалы процесса деформаций,  $s$  - длина дуги траектории деформаций. Другой формой (1) является эквивалентное представление скорости изменения напряжений в ортонормированном репере из трех векторов, связанных с направляющими векторами напряжений, деформаций и скоростей деформаций:

$$\frac{d\bar{\sigma}}{ds} = Q \left( \frac{d\bar{\varepsilon}}{ds} - \bar{n}_\sigma \left( \bar{n}_\sigma, \frac{d\bar{\varepsilon}}{ds} \right) - \bar{n}'_\varepsilon \left( \bar{n}'_\varepsilon, \frac{d\bar{\varepsilon}}{ds} \right) \right) + P \bar{n}_\sigma \left( \bar{n}_\sigma, \frac{d\bar{\varepsilon}}{ds} \right) + N \bar{n}'_\varepsilon \left( \bar{n}'_\varepsilon, \frac{d\bar{\varepsilon}}{ds} \right).$$

Рассмотрение уравнения (1) в пятимерном пространстве, где

$$\bar{n}_\sigma = \cos \theta_1 \bar{n}_1 - \sin \theta_1 (\cos \theta_2 \bar{n}_2 - \sin \theta_2 (\cos \theta_3 \bar{n}_3 - \sin \theta_3 (\cos \theta_4 \bar{n}_4 - \sin \theta_4 \bar{n}_5))),$$

$$\bar{n}_\varepsilon = \cos \varphi_1 \bar{n}_1 - \sin \varphi_1 (\cos \varphi_2 \bar{n}_2 - \sin \varphi_2 (\cos \varphi_3 \bar{n}_3 - \sin \varphi_3 (\cos \varphi_4 \bar{n}_4 - \sin \varphi_4 \bar{n}_5))),$$

приводит к векторному определяющему уравнению

$$\bar{n}_\sigma \dot{\phantom{\sigma}} = \frac{Q}{\sigma} (\bar{n}_1 - \cos \theta_1 \bar{n}_\sigma) + \frac{N_1}{\sigma} \sin \theta_1 (\bar{n}_\varepsilon - (\bar{n}_\sigma, \bar{n}_\varepsilon) \bar{n}_\sigma). \quad (2)$$

Это следует из того, что эквивалентная (2) система уравнений для углов в представлении направляющего вектора напряжений в репере Френе:

$$\begin{cases} \theta_1 = \kappa_1 \cos \theta_2 - \frac{Q}{\sigma} \sin \theta_1 - \frac{N_1}{\sigma} \sin \theta_1 \Delta_{14}, \\ \theta_2 = \kappa_2 \cos \theta_3 - \kappa_1 \frac{\cos \theta_1}{\sin \theta_1} \sin \theta_2 - \frac{N_1}{\sigma} \sin \varphi_1 \Delta_{24}, \\ \theta_3 = \kappa_3 \cos \theta_4 - \kappa_2 \frac{\cos \theta_2}{\sin \theta_2} \sin \theta_3 - \frac{N_1}{\sigma} \sin \varphi_1 \sin \varphi_2 \Delta_{34}, \\ \theta_4 = \kappa_4 - \kappa_3 \frac{\cos \theta_3}{\sin \theta_3} \sin \theta_4 - \frac{N_1}{\sigma} \sin \varphi_1 \sin \varphi_2 \sin \varphi_3 \Delta_{44}, \end{cases} \quad (3)$$

содержит в качестве определяющих функционалов именно  $Q$  и  $N_1$ . Здесь и далее точка над величиной обозначает производную величины по длине дуги траектории деформаций, а также приняты обозначения:

$$\begin{aligned} \Delta_{14} &\equiv \sin \theta_1 \cos \varphi_1 - \cos \theta_1 \sin \varphi_1 (\cos \theta_2 \cos \varphi_2 + \sin \theta_2 \sin \varphi_2 (\cos \theta_3 \cos \varphi_3 + \\ &\quad + \sin \theta_3 \sin \varphi_3 (\cos \theta_4 \cos \varphi_4 + \sin \theta_4 \sin \varphi_4))) \\ \Delta_{24} &\equiv \sin \theta_2 \cos \varphi_2 - \cos \theta_2 \sin \varphi_2 (\cos \theta_3 \cos \varphi_3 + \\ &\quad + \sin \theta_3 \sin \varphi_3 (\cos \theta_4 \cos \varphi_4 + \sin \theta_4 \sin \varphi_4)) \\ \Delta_{34} &\equiv \sin \theta_3 \cos \varphi_3 - \cos \theta_3 \sin \varphi_3 (\cos \theta_4 \cos \varphi_4 + \sin \theta_4 \sin \varphi_4) \\ \Delta_{44} &\equiv \sin \theta_4 \cos \varphi_4 - \cos \theta_4 \sin \varphi_4 \end{aligned}$$

Система уравнений (3) определяет смысл функционалов  $Q$  и  $N_1$ , как функционалов, регулирующих скорости изменения первого и второго углов. На примере уравнения (1), в [3] для трехмерных траекторий деформации проведена калибровка определяющих функционалов и предложен вариант термомеханики упругопластических процессов. Изложенная там теория вполне подходит для описания упругопластических процессов и хорошо соответствует имеющимся экспериментам. При усложнении теории требуется увеличение числа векторов основного репера в ответ на увеличение размерности траектории процесса. В самом общем случае максимальное число определяющих функционалов может достигать пяти. Для выполнения свойства объективности определяющих соотношений далее исключаются из рассмотрения реперы, прямо содержащие векторы деформации. Тогда вполне естественной выглядит конструкция ортонормированных реперов из направляющего вектора напряжений и векторов, построенных на базе векторов пятимерного репера Френе.

### Новые определяющие реперы и уравнения.

1. В пятимерном пространстве выбираем базовую систему векторов  $\bar{n}_\sigma, \bar{n}_1, \bar{n}_2, \bar{n}_3, \bar{n}_4$  и строим на ее основе ортонормированный репер:

$$\begin{aligned}
\bar{n}_\sigma, \bar{n}'_1 &\equiv \frac{\bar{n}_1 - \cos \theta_1 \bar{n}_\sigma}{\sin \theta_1}, \\
\bar{n}'_2 &\equiv \frac{\bar{n}_2 - (\bar{n}_2, \bar{n}_\sigma) \bar{n}_\sigma - (\bar{n}_2, \bar{n}'_1) \bar{n}'_1}{\sin \theta_2}, \\
\bar{n}'_3 &\equiv \frac{\bar{n}_3 - (\bar{n}_3, \bar{n}_\sigma) \bar{n}_\sigma - (\bar{n}_3, \bar{n}'_1) \bar{n}'_1 - (\bar{n}_3, \bar{n}'_2) \bar{n}'_2}{\sin \theta_3}, \\
\bar{n}'_4 &\equiv \frac{\bar{n}_4 - (\bar{n}_4, \bar{n}_\sigma) \bar{n}_\sigma - (\bar{n}_4, \bar{n}'_1) \bar{n}'_1 - (\bar{n}_4, \bar{n}'_2) \bar{n}'_2 - (\bar{n}_4, \bar{n}'_3) \bar{n}'_3}{\sin \theta_4}. \quad (4)
\end{aligned}$$

По аналогии с (1) записываем определяющее уравнение в виде:

$$\bar{n}_\sigma \dot{\phantom{x}} = \frac{Q}{\sigma} \sin \theta_1 \bar{n}'_1 + \frac{F}{\sigma} \sin \theta_2 \bar{n}'_2 + \frac{U}{\sigma} \sin \theta_3 \bar{n}'_3 + \frac{W}{\sigma} \sin \theta_4 \bar{n}'_4. \quad (5)$$

с пятью определяющими функционалами  $Q, F, U, W$  и скрытым в (5) функционалом  $P$ , отвечающим за скалярные свойства материала. Эквивалентная уравнениям (5) система уравнений для углов:

$$\begin{cases} \theta_1 = \kappa_1 \cos \theta_2 - \frac{Q}{\sigma} \sin \theta_1, \\ \theta_2 = \kappa_2 \cos \theta_3 - \kappa_1 \frac{\cos \theta_1}{\sin \theta_1} \sin \theta_2 + \frac{F \sin \theta_2}{\sigma \sin \theta_1}, \\ \theta_3 = \kappa_3 \cos \theta_4 - \kappa_2 \frac{\cos \theta_2}{\sin \theta_2} \sin \theta_3 - \frac{U}{\sigma} \frac{\sin \theta_3}{\sin \theta_1 \sin \theta_2}, \\ \theta_4 = \kappa_4 - \kappa_3 \frac{\cos \theta_3}{\sin \theta_3} \sin \theta_4 + \frac{W}{\sigma} \frac{\sin \theta_4}{\sin \theta_1 \sin \theta_2 \sin \theta_3}. \end{cases} \quad (6)$$

2. Для трехмерных процессов сложного нагружения

$$\bar{n}_\sigma = \cos \theta_1 \bar{n}_1 - \sin \theta_1 (\cos \theta_2 \bar{n}_2 - \sin \theta_2 \bar{n}_3).$$

В зависимости от выбора основного репера получим разные определяющие уравнения и соответствующие им системы уравнений для углов: 2.1.

$$\begin{aligned}
&\{\bar{n}_\sigma, \bar{n}'_1, \bar{n}'_2\} : \\
\bar{n}_\sigma \dot{\phantom{x}} &= \frac{Q}{\sigma} \sin \theta_1 \bar{n}'_1 + \frac{F}{\sigma} \sin \theta_2 \bar{n}'_2, \quad (7)
\end{aligned}$$

$$\begin{cases} \theta_1 \dot{\phantom{x}} = \kappa_1 \cos \theta_2 - \frac{Q}{\sigma} \sin \theta_1, \\ \theta_2 \dot{\phantom{x}} = \kappa_2 - \kappa_1 \frac{\cos \theta_1}{\sin \theta_1} \sin \theta_2 + \frac{F \sin \theta_2}{\sigma \sin \theta_1}, \end{cases} \quad (7.1)$$

2.2.

$$\begin{aligned}
&\{\bar{n}_\sigma, \bar{n}'_1, \bar{n}'_\varepsilon\} : \\
\bar{n}_\sigma \dot{\phantom{x}} &= \frac{Q}{\sigma} \sin \theta_1 \bar{n}'_1 + \frac{N_1}{\sigma} \sin \theta_1 \bar{n}'_\varepsilon. \quad (8)
\end{aligned}$$

$$\begin{cases} \theta_1 \dot{\phantom{}} = \kappa_1 \cos \theta_2 - \frac{Q}{\sigma} \sin \theta_1 - \frac{N_1}{\sigma} \sin \theta_1 \Delta, \\ \theta_2 \dot{\phantom{}} = \kappa_2 - \kappa_1 \frac{\cos \theta_1}{\sin \theta_1} \sin \theta_2 - \frac{N_1}{\sigma} \sin \varphi_1 \sin(\theta_2 - \varphi_2), \end{cases} \quad (8.1)$$

$$\Delta \equiv \sin \theta_1 \cos \varphi_1 - \cos \theta_1 \sin \varphi_1 \cos(\theta_2 - \varphi_2).$$

**Калибровка определяющих функционалов** Вопрос калибровки определяющих функционалов на произвольных процессах деформаций решается однотипно для изображающих пространств и траекторий любой размерности. Он осуществляется в четыре этапа:

1. Этап первый: по уравнению кривой деформации определяем скалярные характеристики траектории в данной точке (кривизна и крутки);
2. Этап второй: приближаем траектории деформаций сплайнами в виде отрезков винтовых линий соответствующей размерности;
3. Этап третий: определяем формы отклика из теоремы изоморфизма и калибруем параметры отклика;
4. Этап четвертый: на данном отрезке по форме отклика из системы уравнений для углов находим определяющие функционалы и т.д.

**Пример.**

**Трехмерное пространство.** Рассмотрим трехмерный процесс деформаций с заданной траекторией.

**Сплайн.** В любой точке траектории деформаций с заданными на ней скалярными характеристиками уравнения:

$$\begin{aligned} \varepsilon_1 &= \varepsilon_{10} + c \cos \alpha, \quad \varepsilon_3 = c \sin \alpha, \\ \varepsilon_2 &= \varepsilon_{20} + a \left( \frac{\alpha}{2\pi} + (m-1) \right), \end{aligned} \quad (8.2)$$

$$\varepsilon_{20} \equiv \frac{\varepsilon_{10} + c}{\sqrt{3}}, \quad c \equiv \frac{\kappa_1}{\kappa_1^2 + \kappa_2^2}, \quad a \equiv \frac{2\pi\kappa_2}{\kappa_1^2 + \kappa_2^2}, \quad a_1 \equiv \frac{\kappa_2}{\sqrt{\kappa_1^2 + \kappa_2^2}}$$

определяют сплайн в виде винтовой линии, проходящей через точку начала траектории с параметрами (кривизной и кручением), совпадающими с параметрами траектории деформации в начальной точке.

**Параметры отклика.** На основании экспериментальных данных [4] в [3] была установлена форма отклика на траекторию деформации (8.2) с четырьмя параметрами, неизвестным образом зависящими от характеристик сплайна:

$$\begin{aligned} \sigma_1 &= \sigma_{10} + R \cos \beta, \quad \sigma_3 = \sigma_{30} + R \sin \beta, \quad \beta \equiv \alpha + \alpha_0, \\ \sigma_2 &= \sqrt{\sigma(s)^2 - \sigma_1^2 - \sigma_2^2}, \quad \sigma(s) = \sigma_0 + G' s. \end{aligned} \quad (9)$$

В трехмерном случае соотношения (8.2) и (9) задают изоморфизм пространств деформаций и напряжений.

**Формулы для функционалов.** Имеют место следующие аналитические представления векторных характеристик процесса через параметры траектории деформаций и отклика:

$$\begin{aligned}\cos \theta_1 &= \frac{\kappa_1}{\sqrt{\kappa_1^2 + \kappa_2^2}} \frac{\sigma_{30} \cos \alpha - \sigma_{10} \sin \alpha + R \sin \alpha_0}{\sigma} + a_1 \frac{\sigma_2}{\sigma}, \\ \cos \theta_2 &= \frac{\sigma_{10} \cos \alpha + \sigma_{30} \sin \alpha + R \cos \alpha_0}{\sigma \sin \theta_1}.\end{aligned}\quad (10)$$

Преобразуем уравнения (7.1) с учетом формул (10). В итоге получим систему линейных алгебраических уравнений для определяющих функционалов процесса:

$$\begin{aligned}\frac{Q}{\sigma} \sin^2 \theta_1 &= \frac{\kappa_2}{\sigma \sqrt{\kappa_1^2 + \kappa_2^2}} \left( \sigma_2 - \frac{\sigma_2}{\sigma} \sigma \right) + \frac{R}{\sigma} \cos \alpha_0 - \\ &\quad - \frac{\kappa_1}{\sqrt{\kappa_1^2 + \kappa_2^2}} \frac{\sigma_{30} \cos \alpha - \sigma_{10} \sin \alpha + R \sin \alpha_0}{\sigma^2} \sigma, \\ \cos \theta_2 \left( \frac{\sigma_2}{\sigma} - \frac{Q}{\sigma} \cos \theta_1 \right) &- \frac{\sigma_{30} \cos \alpha - \sigma_{10} \sin \alpha}{\sigma \sin \theta_1} \sqrt{\kappa_1^2 + \kappa_2^2} = \\ &= \kappa_2 \sin \theta_2 - \kappa_1 \frac{\cos \theta_1}{\sin \theta_1} + \frac{F \sin^2 \theta_2}{\sigma \sin \theta_1}.\end{aligned}$$

**Пятимерное пространство.** В этом случае уравнение сплайна строим в виде пятимерного винта. В [1] в пятимерном пространстве решена задача построения траектории с постоянными кривизнами. Решение задачи выписано в репере, который не является ортогональным. Это решение приводим к ортонормированному реперу Френе начальной точки траектории. Результат в виде трехчленного пятимерного винта дается формулой:

$$\bar{\varepsilon} = \frac{\kappa_2 \kappa_4}{k_1^2 k_2^2} s \begin{pmatrix} \kappa_2 \kappa_4 \\ 0 \\ \kappa_1 \kappa_4 \\ 0 \\ \kappa_1 \kappa_3 \end{pmatrix} + \frac{\kappa_1}{k_1^2 (k_1^2 - k_2^2)} \begin{pmatrix} -\kappa_1 (k_2^2 - \kappa_1^2 - \kappa_2^2) \frac{\sin k_1 s}{k_1} \\ -(k_2^2 - \kappa_1^2 - \kappa_2^2) (1 - \cos k_1 s) \\ \kappa_2 (\kappa_4^2 - k_1^2) \frac{\sin k_1 s}{k_1} \\ -\kappa_2 \kappa_3 (1 - \cos k_1 s) \\ \kappa_2 \kappa_3 \kappa_4 \frac{\sin k_1 s}{k_1} \end{pmatrix} +$$

$$+ \frac{\kappa_1}{k_2^2(k_1^2 - k_2^2)} \begin{pmatrix} \kappa_1(k_1^2 - \kappa_1^2 - \kappa_2^2) \frac{\sin k_2 s}{k_2} \\ (k_1^2 - \kappa_1^2 - \kappa_2^2)(1 - \cos k_2 s) \\ -\kappa_2(\kappa_4^2 - k_2^2) \frac{\sin k_2 s}{k_2} \\ \kappa_2 \kappa_3 (1 - \cos k_2 s) \\ -\kappa_2 \kappa_3 \kappa_4 \frac{\sin k_2 s}{k_2} \end{pmatrix},$$

в которую входят кривизны траектории, а также две функции кривизн, см.[1]:

$$\begin{aligned} k_1^2 &= \frac{1}{2} (\kappa_1^2 + \kappa_2^2 + \kappa_3^2 + \kappa_4^2 + \\ &+ \sqrt{(\kappa_1^2 + \kappa_2^2 + \kappa_3^2 + \kappa_4^2)^2 - 4(\kappa_1^2 \kappa_3^2 + \kappa_2^2 \kappa_4^2 + \kappa_1^2 \kappa_4^2)}) \\ k_2^2 &= \frac{1}{2} (\kappa_1^2 + \kappa_2^2 + \kappa_3^2 + \kappa_4^2 - \\ &- \sqrt{(\kappa_1^2 + \kappa_2^2 + \kappa_3^2 + \kappa_4^2)^2 - 4(\kappa_1^2 \kappa_3^2 + \kappa_2^2 \kappa_4^2 + \kappa_1^2 \kappa_4^2)}). \end{aligned}$$

В результате тождественных преобразований трехчленной формулы пятимерного винта получается пятичленное представление:

$$\begin{aligned} \bar{\varepsilon} &= p_1 \frac{\kappa_1}{k_1^2(k_1^2 - k_2^2)} \{ \bar{\varepsilon}_1(-1 + \cos k_1 s) + \bar{\varepsilon}_3 \sin k_1 s \} + s \frac{\kappa_2 \kappa_4}{k_1 k_2} \bar{\varepsilon}_2 + \\ &+ p_4 \frac{\kappa_1}{k_2^2(k_1^2 - k_2^2)} \{ \bar{\varepsilon}_4(-1 + \cos k_2 s) + \bar{\varepsilon}_5 \sin k_2 s \} \end{aligned} \quad (11)$$

с известным образом зависящими от кривизн траектории функциями  $p_1, p_4$ .

Значит, в специальном ортонормированном репере  $\bar{\varepsilon}_1, \bar{\varepsilon}_2, \bar{\varepsilon}_3, \bar{\varepsilon}_4, \bar{\varepsilon}_5$  уравнение пятимерного винта имеет представление подобное трехмерному винту (8.2). Что касается самого репера, то, как видно, он определяется только внутренней геометрией траектории.

Указанное обстоятельство позволяет постулировать подобную (9) форму для отклика на траекторию деформаций в виде пятимерной винтовой линии:

$$\begin{cases} \sigma_1 = \sigma_{10} + R_1 \cos \beta, \beta \equiv k_1 s + \beta_0, \\ \sigma_3 = \sigma_{30} + R_1 \sin \beta, \\ \sigma_4 = \sigma_{40} + R_2 \cos \gamma, \gamma \equiv k_2 s + \gamma_0, \\ \sigma_5 = \sigma_{50} + R_2 \sin \gamma, \\ \sigma_2 = \sqrt{\sigma^2 - \sigma_1^2 - \sigma_3^2 - \sigma_4^2 - \sigma_5^2}. \end{cases} \quad (12)$$

Подчеркнем, что отличие этого представления от (9) в том, что форма отклика для трехмерных винтовых траекторий была выбрана в [3] на основе анализа результатов обработки экспериментальных данных [4], тогда как соотношение (12) представляет собой формулировку теоремы изоморфизма для пятимерных траекторий деформации. В четырехмерном или двумерном пространствах деформаций секулярные члены в уравнениях винтов (11) равны нулю и это обстоятельство соответствующим образом корректирует и формы отклика двумерных и четырехмерных процессов деформации..

### Калибровка параметров отклика.

Оценка параметров (9) или (12) проводится по уравнению:

$$\bar{\sigma} \cdot = Q\bar{n}_1 + \left( \frac{d\sigma}{ds} - Q \cos \theta_1 \right) \bar{n}_\sigma,$$

которое является трехчленной формулой А.А.Ильюшина, и его вполне можно считать 0-приближением всех рассматриваемых здесь уравнений (5),(7),(8), с использованием формулы

$$\begin{aligned} \cos \theta_1 = c_1 k_1 \frac{\sigma_{30} \cos k_1 s - \sigma_{10} \sin k_1 s + R_1 \sin \beta_0}{\sigma} + \\ + c_2 k_2 \frac{\sigma_{50} \cos k_2 s - \sigma_{40} \sin k_2 s + R_2 \sin \gamma_0}{\sigma} + a_1 \frac{\sigma_2}{\sigma}. \end{aligned} \quad (13)$$

В этом приближении пренебрегаем малыми величинами порядка  $\sigma_{10}/\sigma, \dots, \sigma_{50}/\sigma$ , (это следовало в трехмерном случае из анализа экспериментальных данных [4]) и записываем с учетом (12) первое, третье, четвертое и пятое уравнения 0-приближения. Получаем систему из 4 независимых уравнений для 4 неизвестных параметров отклика ( $R_1, R_2, \beta_0, \gamma_0$ ):

$$\begin{aligned} R_1 = \frac{c_1}{\lambda} \sigma \cos \beta_0, R_2 = \frac{c_2}{\lambda} \sigma \cos \gamma_0, k_1 \operatorname{tg} \beta_0 = k_2 \operatorname{tg} \gamma_0, \\ \operatorname{tg}^5 \beta_0 + \operatorname{tg}^4 \beta_0 \frac{1}{k_1} \left( \frac{1}{\sigma} \frac{d\sigma}{ds} - \frac{a_1}{\lambda} \right) + \operatorname{tg}^3 \beta_0 \left( \frac{k_2^2}{k_1^2} + 1 - \frac{c_1^2}{\lambda^2} - \frac{c_2^2 k_2^2}{\lambda^2 k_1^2} \right) + \\ + \operatorname{tg}^2 \beta_0 \frac{1}{k_1} \left( \frac{k_2^2}{k_1^2} + 1 \right) \left( \frac{1}{\sigma} \frac{d\sigma}{ds} - \frac{a_1}{\lambda} \right) + \operatorname{tg} \beta_0 \frac{k_2^2}{k_1^2} \left( 1 - \frac{c_1^2 + c_2^2}{\lambda^2} \right) + \\ + \frac{1}{k_1} \frac{k_2^2}{k_1^2} \left( \frac{1}{\sigma} \frac{d\sigma}{ds} - \frac{a_1}{\lambda} \right) = 0, \frac{1}{\lambda} \equiv \frac{Q}{\sigma}. \end{aligned} \quad (14)$$

При  $k_2 = 0, c_2 = 0$  отсюда следуют характеристики отклика трехмерного процесса деформаций:

$$R_1 = \frac{c_1}{\lambda} \sigma \cos \beta_0,$$

$$\begin{aligned} & \operatorname{tg}^3 \beta_0 + \operatorname{tg}^2 \beta_0 \frac{1}{k_1} \left( \frac{1}{\sigma} \frac{d\sigma}{ds} - \frac{a_1}{\lambda} \right) + \\ & + \operatorname{tg} \beta_0 \left( 1 - \frac{c_1^2}{\lambda^2} \right) + \frac{1}{k_1} \left( \frac{1}{\sigma} \frac{d\sigma}{ds} - \frac{a_1}{\lambda} \right) = 0. \end{aligned} \quad (15)$$

Параметры  $\sigma_{10}, \sigma_{20}, \sigma_{30}, \sigma_{40}, \sigma_{50}$ , в 0-приближении остаются неопределенными. Итерационная процедура для нахождения этих параметров в трехмерном случае изложена в [2] вместе с примером реализации для процессов в виде трехмерных винтовых линий. Найденные там значения этих параметров уже в 1-приближении соответствуют экспериментальным данным.

Все предложенные выше подходы были реализованы на пятимерных процессах деформаций с траекториями деформаций в виде пятимерных винтовых линий после одноосного нагружения. Мы взяли реальные эксперименты из [4] на трехмерных винтах и на их основе построили пятимерные траектории деформаций, сохранив для них те же самые номера, что были в прототипах.

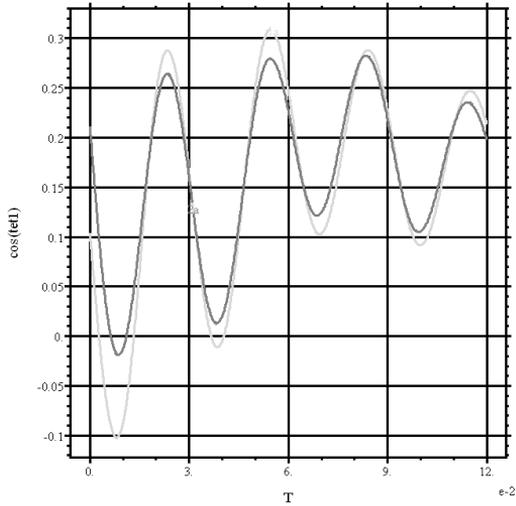
**Таблица параметров рассмотренных пятимерных процессов деформаций.**

Nexp	$\kappa_1$	$\kappa_2$	$\kappa_3$	$\kappa_4$	$\sigma_{10}$	$\sigma_{30}$	$\sigma_{40}$	$\sigma_{50}$	$\lambda$
25	333	666	200	200	70	30	10	10	0.005
27	100	200	50	50	50	50	70	10	0.008
29	200	200	50	50	70	50	-20	50	0.008
31	200	60	60	60	70	30	10	100	0.08
35	200	400	100	100	70	30	10	70	0.01

Результаты некоторых расчетов приводятся ниже.

Experiment -5D-31

07:34:53 5/21/18  
FlexPDE 5.0.17



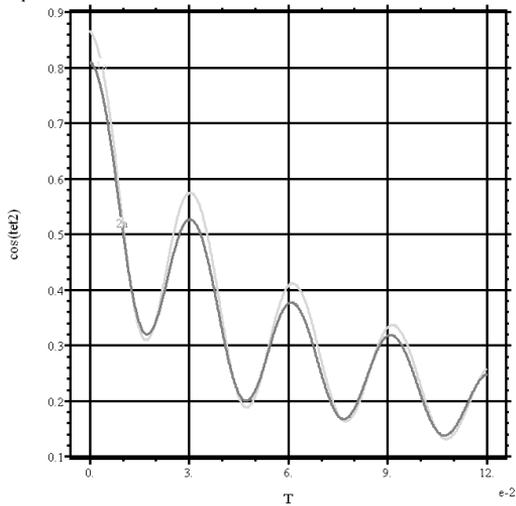
HISTORY  
1: cos(tet1)  
2: cote1



Solve 5D: Cycle=828 Time= 0.1200 dt= 1.8735e-4 P2 Nodes=9 Cells=2 RMS Err= 2.e-18

Experiment -5D-31

07:34:53 5/21/18  
FlexPDE 5.0.17



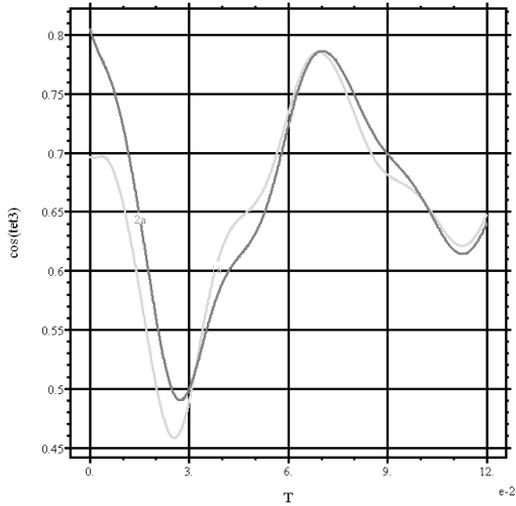
HISTORY  
1: cos(tet2)  
2: cote2



Solve 5D: Cycle=828 Time= 0.1200 dt= 1.8735e-4 P2 Nodes=9 Cells=2 RMS Err= 2.e-18

Experiment -5D-31

07:34:53 5/21/18  
FlexPDE 5.0.17



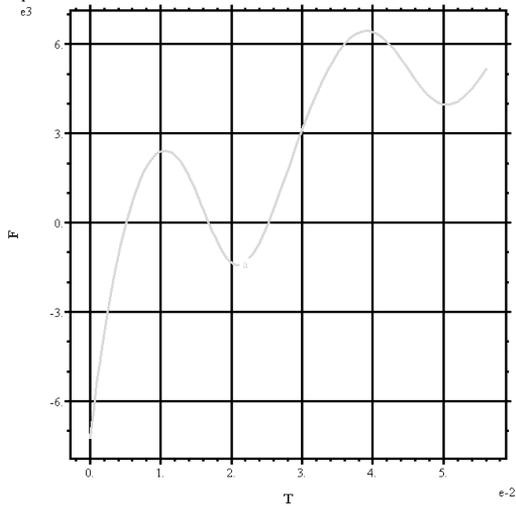
HISTORY  
1: cos(tet3)  
2: cote3



Solve 5D: Cycle=828 Time= 0.1200 dt= 1.8735e-4 P2 Nodes=9 Cells=2 RMS Err= 2.e-18

Experiment 27-3D

07:10:38 5/21/18  
FlexPDE 5.0.17



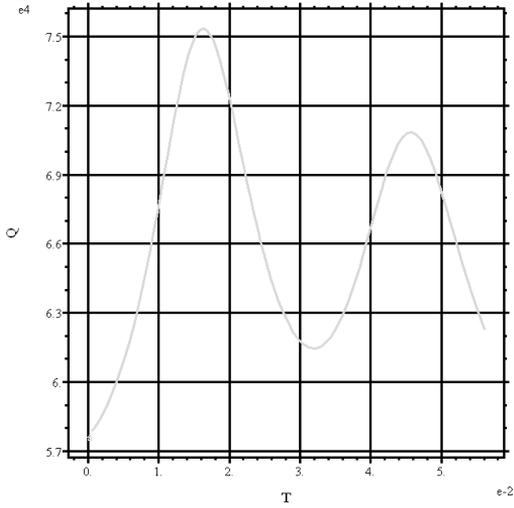
HISTORY  
1: F



Solve1 3D: Cycle=108 Time= 0.0561 dt= 8.6779e-4 P2 Nodes=9 Cells=2 RMS Err= 1.e-12

Experiment 27-3D

07:10:38 5/21/18  
FlexPDE 5.0.17



HISTORY

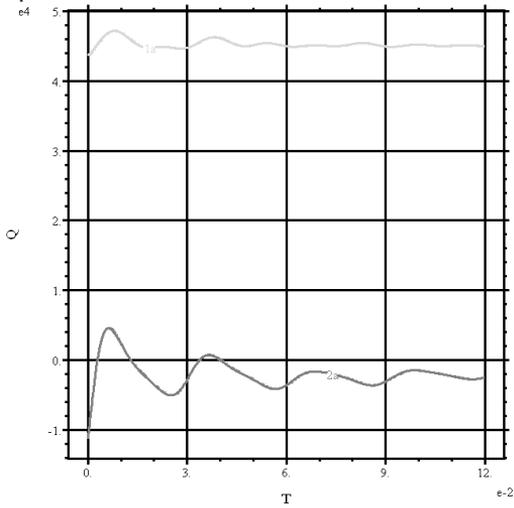
1: Q



Solve1 3D: Cycle=108 Time= 0.0561 dt= 8.6779e-4 P2 Nodes=9 Cells=2 RMS Err= 1.e-12

Experiment -5D-31

07:41:23 5/21/18  
FlexPDE 5.0.17



HISTORY

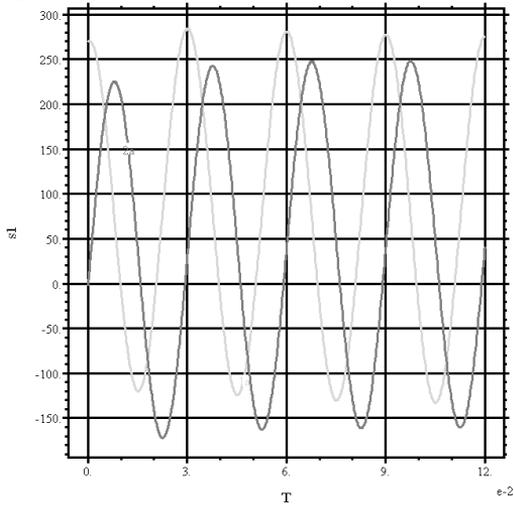
1: Q  
2: F



Solve 5D: Cycle=828 Time= 0.1200 dt= 1.8735e-4 P2 Nodes=9 Cells=2 RMS Err= 2.e-18

Experiment -5D-31

07:34:53 5/21/18  
FlexPDE 5.0.17



HISTORY

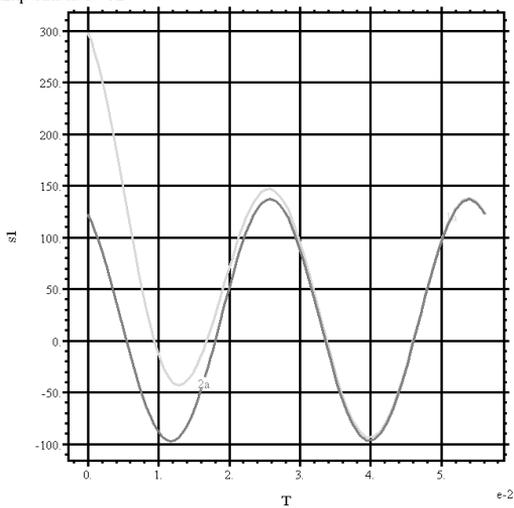
- 1: s1
- 2: s3



Solve 5D: Cycle=828 Time= 0.1200 dt= 1.8735e-4 P2 Nodes=9 Cells=2 RMS Err= 2.e-18

Experiment 27-3D

07:10:38 5/21/18  
FlexPDE 5.0.17



HISTORY

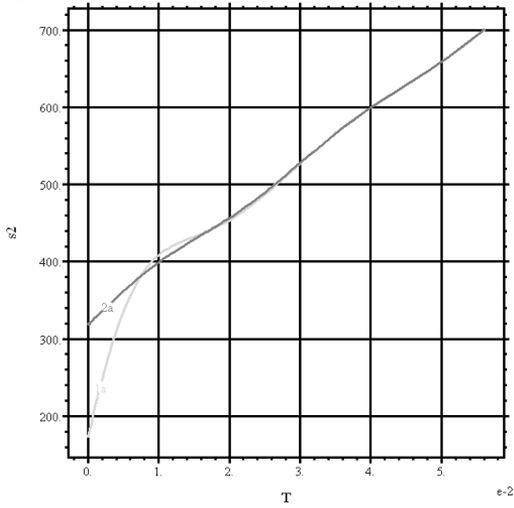
- 1: s1
- 2: sig1



Solve1 3D: Cycle=108 Time= 0.0561 dt= 8.6779e-4 P2 Nodes=9 Cells=2 RMS Err= 1.e-12

Experiment 27-3D

07:10:38 5/21/18  
FlexPDE 5.0.17



HISTORY

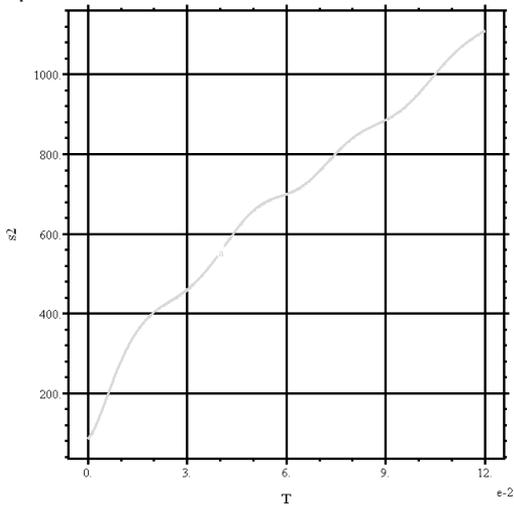
- 1: %I
- 2: sig2



Solve1 3D: Cycle=108 Time= 0.0561 dt= 8.6779e-4 P2 Nodes=9 Cells=2 RMS Err= 1.e-12

Experiment -5D-31

07:34:53 5/21/18  
FlexPDE 5.0.17



HISTORY

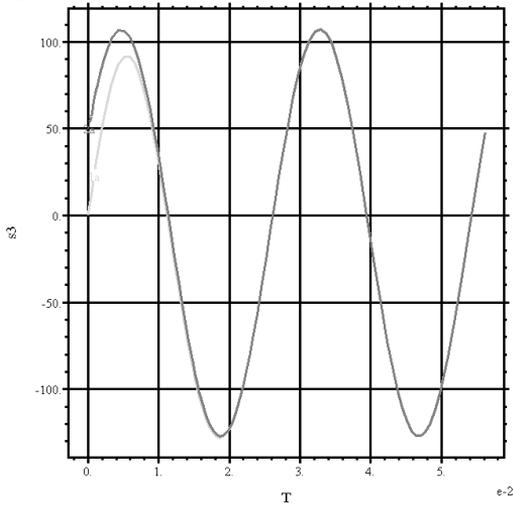
- 1: %I



Solve 5D: Cycle=828 Time= 0.1200 dt= 1.8735e-4 P2 Nodes=9 Cells=2 RMS Err= 2.e-18

Experiment 27-3D

07:10:38 5/21/18  
FlexPDE 5.0.17



HISTORY

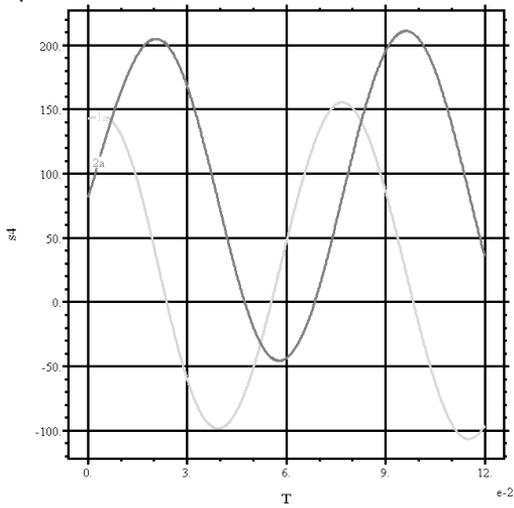
- 1: s3
- 2: sig3



Solve1 3D: Cycle=108 Time= 0.0561 dt= 8.6779e-4 P2 Nodes=9 Cells=2 RMS Err= 1.e-12

Experiment -5D-31

07:34:53 5/21/18  
FlexPDE 5.0.17



HISTORY

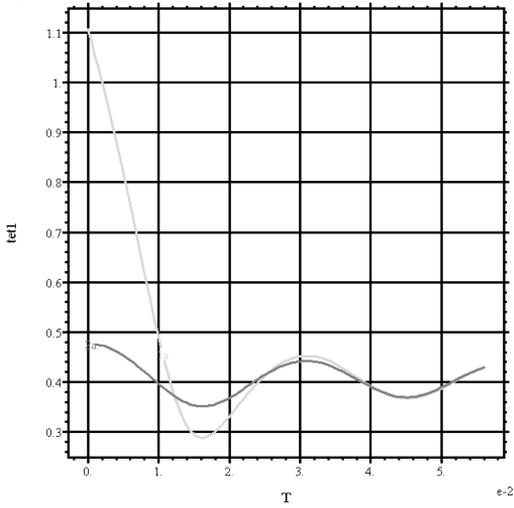
- 1: s4
- 2: s5



Solve 5D: Cycle=828 Time= 0.1200 dt= 1.8735e-4 P2 Nodes=9 Cells=2 RMS Err= 2.e-18

Experiment 27-3D

07:10:38 5/21/18  
FlexPDE 5.0.17



HISTORY

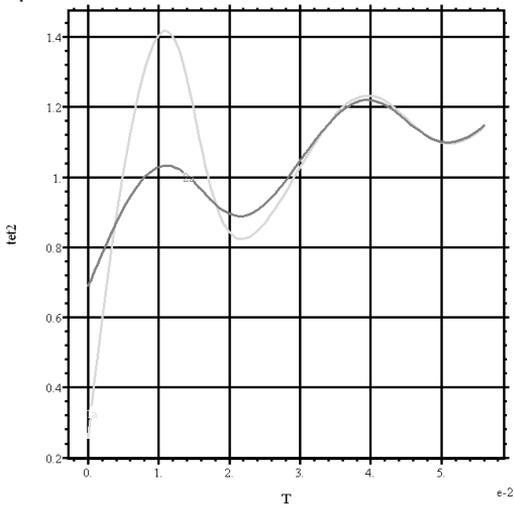
- 1: tet1
- 2: arccos(cote1)



Solve1 3D: Cycle=108 Time= 0.0561 dt= 8.6779e-4 P2 Nodes=9 Cells=2 RMS Err= 1.e-12

Experiment 27-3D

07:10:38 5/21/18  
FlexPDE 5.0.17



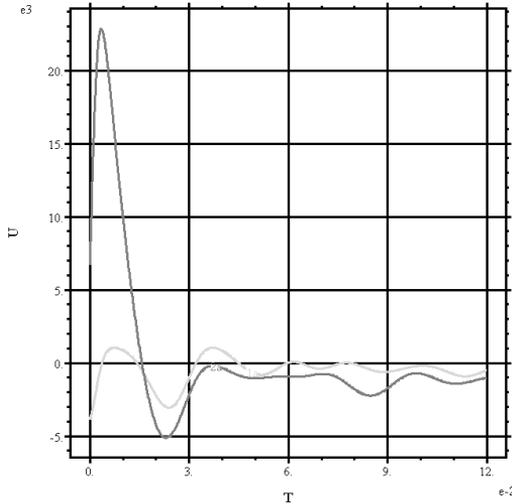
HISTORY

- 1: tet2
- 2: arccos(cote2)



Solve1 3D: Cycle=108 Time= 0.0561 dt= 8.6779e-4 P2 Nodes=9 Cells=2 RMS Err= 1.e-12

Experiment -5D-31  
e3



07:41:23 5/21/18  
FlexPDE 5.0.17

HISTORY  
1: U  
2: W

Solve 5D: Cycle=828 Time= 0.1200 dt= 1.8735e-4 P2 Nodes=9 Cells=2 RMS Err= 2.e-18

## Список литературы

- [1] Ильюшин А.А. Пластичность. Основы общей математической теории // Изд-во АН СССР, Москва,-1963,- 272 с.
- [2] Молодцов И.Н., Бабаева Д.О. Некоторые вопросы верификации теории упругопластических процессов при сложном нагружении// Проблемы машиностроения и автоматизации, Москва, -2016, -№3, -с.98-105.
- [3] Молодцов И.Н., Бабаева Д.О. О роли функционалов пластичности в геометрическом истолковании диссипации и описании векторных свойств материала в процессах сложного нагружения// В сборнике Упругость и неупругость. Материалы Международного научного симпозиума по проблемам механики деформируемых тел, посвященного 105-летию со дня рождения А.А.Ильюшина// Москва,-2016,-с.210-215.
- [4] Вавакин А.С., Васин Р.А., Викторов В.В., Широков Р.И. Экспериментальное исследование упругопластического деформирования стали при сложном нагружении по криволинейным пространственным траекториям деформаций. Деп. в ВИНТИ, 16.10.86, №7298-B86. 66с.

**Some mathematical models of elastoplastic processes of complex loading**

**Molodtsov I.N., Babaeva D.O.**

In the framework of the Ilyushin's theory of elastoplastic processes, in [3] for mathematical modeling of complex loading processes we use special type quasilinear equation with three state functionals. The functionals was calibrated using the experimental results [4] (R.A.Vasin, etc.) for 3D- helical trajectories of deformations. It turned out that the response on a helical trajectory of deformation takes a completely definite loading form, not exactly, but after the exhaustion of some trace of retard. On the helical trajectories of deformations the form of loading is the same: helical trajectory of deformations is becoming to helical trajectory of loading there and back. The used map preserves the geometry of space. This correspondence by Ilyushin is called as isomorphism theorem. All new theories use as the basis the directing vector of stresses and vectors constructed on the base of Frenet basis. For high-dimensional processes, the number of state functionals increases, so and the methods of their identification become more complicated. All models are completely verified. The results are given below.

*Keywords:* plasticity, plastic deformations, complex loading, state functional, identification of functionals, isomorphism theorem

Часть 2.  
Специальные вопросы теории  
интеллектуальных систем



# О языках, устойчивых относительно операций выпадения, вставки

Дергач П.С.

В статье изучаются операции выпадения/вставки, продвижением которых занимался В. И. Левенштейн. Ставятся и даются ответы на следующие два вопроса. Какие регулярные языки устойчивы относительно операций выпадения/вставки? Существуют ли нерегулярные языки, которые устойчивы относительно операций выпадения/вставки?

**Ключевые слова:** операции выпадения и вставки, замкнутый класс, регулярный язык.

## Введение

В статье изучаются операции выпадения/вставки, продвижением которых занимался В. И. Левенштейн [1]. Ставятся и даются ответы на следующие два вопроса. Какие регулярные языки устойчивы относительно операций выпадения/вставки? Существуют ли нерегулярные языки, которые устойчивы относительно операций выпадения/вставки? О решении похожих проблем можно прочитать в статьях [2-9]. О других аспектах исследований автора и других ученых в смежных областях к тематике данной работы можно прочитать в [10-21]. В дальнейшем планируется продолжить исследование полученного класса замкнутых относительно операций выпадения/вставки языков применительно к проблеме однозначности алфавитного декодирования.

## Основные определения и результаты

Множество конечных слов в алфавите  $A$  обозначаем через  $A^*$ . Пустое слово  $\Lambda$  по умолчанию тоже лежит в  $A^*$ .

Множество натуральных чисел обозначаем через  $\mathbb{N}$ , а целых неотрицательных чисел — через  $\mathbb{N}_0$ .

Множество всех регулярных языков в алфавите  $A$  обозначаем через  $R(A)$ .

Для произвольного  $\alpha = a_{i_1}a_{i_2} \dots a_{i_s} \in A^*$  обозначаем

$$in(\alpha) := A^*a_{i_1}A^*a_{i_2}A^* \dots A^*a_{i_s}A^*.$$

Пусть  $a \in A$ ,  $\alpha_1, \alpha_2 \in A^*$ . Говорим, что слово  $\alpha_1a\alpha_2$  получено операцией вставки из слова  $\alpha_1\alpha_2$ . Говорим, что слово  $\alpha_1\alpha_2$  получено операцией выпадения из слова  $\alpha_1a\alpha_2$ .

Пусть  $\alpha \in A^*$ . Вводим индуктивно при  $k \in \mathbb{N}_0$  множества  $[\alpha]_{in}^k$ :

$$[\alpha]_{in}^0 := \{\alpha\},$$

$$[\alpha]_{in}^k := \{\alpha_1a\alpha_2 \mid \alpha_1\alpha_2 \in [\alpha]_{in}^{k-1}, a \in A, \alpha_1, \alpha_2 \in A^*\}.$$

Аналогично, при  $k \in \mathbb{N}_0$  вводим множества  $[\alpha]_{out}^k$ :

$$[\alpha]_{out}^0 := \{\alpha\},$$

$$[\alpha]_{out}^k := \{\alpha_1\alpha_2 \mid \alpha_1a\alpha_2 \in [\alpha]_{out}^{k-1}, a \in A, \alpha_1, \alpha_2 \in A^*\}.$$

Обозначаем

$$[\alpha]_{in} = \bigcup_{k=0}^{\infty} [\alpha]_{in}^k,$$

$$[\alpha]_{out} = \bigcup_{k=0}^{\infty} [\alpha]_{out}^k.$$

**Замечание 1.** Множество  $[\alpha]_{in}$  всегда бесконечно, а множество  $[\alpha]_{out}$  всегда конечно.

Для любого множества  $P \subset A^*$  вводим обозначения

$$[P]_{in} := \bigcup_{\alpha \in P} [\alpha]_{in},$$

$$[P]_{out} := \bigcup_{\alpha \in P} [\alpha]_{out}.$$

**Замечание 2.** Если  $\alpha \in P$ , то

$$[\alpha]_{in} \subseteq [P]_{in}, [\alpha]_{out} \subseteq [P]_{out}.$$

**Замечание 3.** Если  $P \subseteq A^*$ , то

$$[[P]_{in}]_{in} = [P]_{in}, [[P]_{out}]_{out} = [P]_{out}.$$

**Теорема 1.** Пусть  $P \in R(A)$ . Тогда

$$P = [P]_{in} \iff P = \bigcup_{\alpha \in T} in(\alpha),$$

где  $T$  — произвольное конечное множество слов в алфавите  $A$ .

**Теорема 2.** Пусть  $P \in R(A)$ . Тогда

$$P = [P]_{out} \iff P = \bigcup_{i=1}^k [\alpha_{i,1}]_{out} \cdot (A_{i,1})^* \cdot \dots \cdot (A_{i,s(i)})^* \cdot [\alpha_{i,s(i)+1}]_{out},$$

где  $k \in \mathbb{N}$ ,  $s(i) \in \mathbb{N}_0$ ,  $\alpha_{i,j} \in A^*$ ,  $A_{i,j} \subseteq A$ .

**Теорема 3.** Пусть  $P \subseteq A^*$ . Тогда  $[P]_{in} \in R(A)$ .

**Теорема 4.** Пусть  $P \subseteq A^*$ . Тогда  $[P]_{out} \in R(A)$ .

## Доказательство вспомогательных утверждений

**Лемма 1.** Для любого  $\alpha \in A^*$  верно, что  $in(\alpha) = [\alpha]_{in}$ .

*Доказательство.*

По определению верно, что

$$in(\alpha) := A^* a_{i_1} A^* a_{i_2} A^* \dots A^* a_{i_s} A^*, \quad (1)$$

$$[\alpha]_{in} = \bigcup_{k=0}^{\infty} [\alpha]_{in}^k. \quad (2)$$

Замечаем, что множество (2) — множество всех слов, которые можно получить из слова  $\alpha$  конечным количеством применений операции вставки. Но множество (1) как раз и состоит из таких слов. ■

**Лемма 2.** Для любых  $P_1, P_2 \subseteq A^*$  верно, что  $[P_1 \cdot P_2]_{in} = [P_1]_{in} \cdot [P_2]_{in}$ .

*Доказательство.*

Возьмем произвольное слово  $\alpha$  из множества  $[P_1 \cdot P_2]_{in}$ . Оно получается конечным количеством применений операции вставки в какое-то слово из  $P_1 \cdot P_2$ , то есть слово вида  $\alpha_1 \cdot \alpha_2$ , где  $\alpha_1 \in P_1$ ,  $\alpha_2 \in P_2$ . Тогда слово  $\alpha$  можно разбить на две части — префикс, содержащий в качестве подслова слово  $\alpha_1$  и постфикс, содержащий в качестве подслова слово  $\alpha_2$ . Значит  $[P_1 \cdot P_2]_{in} \subseteq [P_1]_{in} \cdot [P_2]_{in}$ .

Возьмем теперь произвольное слово  $\alpha$  из множества  $[P_1]_{in} \cdot [P_2]_{in}$ . Это слово представимо в виде  $\alpha_1 \cdot \alpha_2$ , где  $\alpha_1$  получается конечным количеством применений операции вставки в какое-то слово  $\alpha'_1$  из  $P_1$ , а  $\alpha_2$  — конечным количеством применений операции вставки в какое-то слово  $\alpha'_2$  из  $P_2$ . Но тогда слово  $\alpha = \alpha_1 \alpha_2$  можно получить конечным количеством применений операции вставки в слово  $\alpha'_1 \alpha'_2 \in P_1 \cdot P_2$ . Значит  $[P_1]_{in} \cdot [P_2]_{in} \subseteq [P_1 \cdot P_2]_{in}$ . ■

**Лемма 3.** Для любого  $P \subseteq A^*$  верно, что  $[P^*]_{in} = A^*$ .

*Доказательство.*

Результат очевидно вытекает из того факта, что  $\Lambda \in P^*$  и любое слово в алфавите  $A$  может быть получено из  $\Lambda$  конечным количеством применений операции вставки.

■

**Лемма 4.** Для любых  $P_1, P_2 \subseteq A^*$  верно  $[P_1 \cdot P_2]_{out} = [P_1]_{out} \cdot [P_2]_{out}$ .  
Доказательство.

Возьмем произвольное слово  $\alpha$  из множества  $[P_1 \cdot P_2]_{out}$ . Оно получается конечным количеством применений операции выпадения из какого-то слова в  $P_1 \cdot P_2$ , то есть слова вида  $\alpha_1 \cdot \alpha_2$ , где  $\alpha_1 \in P_1$ ,  $\alpha_2 \in P_2$ . Тогда  $\alpha$  можно разбить на две части — префикс, являющийся подсловом  $\alpha_1$  и постфикс, являющийся подсловом слова  $\alpha_2$ . Отсюда получаем, что  $[P_1 \cdot P_2]_{out} \subseteq [P_1]_{out} \cdot [P_2]_{out}$ .

Возьмем теперь произвольное слово  $\alpha$  из множества  $[P_1]_{out} \cdot [P_2]_{out}$ . Это слово представимо в виде  $\alpha_1 \cdot \alpha_2$ , где  $\alpha_1$  является подсловом какого-то слова  $\alpha'_1$  из  $P_1$ , а  $\alpha_2$  — подсловом какого-то слова  $\alpha'_2$  из  $P_2$ . Но тогда слово  $\alpha = \alpha_1 \alpha_2$  будет подсловом слова  $\alpha'_1 \alpha'_2 \in P_1 \cdot P_2$ . Отсюда получаем, что  $[P_1]_{out} \cdot [P_2]_{out} \subseteq [P_1 \cdot P_2]_{out}$ .

■

**Лемма 5.** Для любого  $P \subseteq A^*$  верно, что  $[P^*]_{out} = A_1^*$ , где  $A_1 \subseteq A$ .  
Доказательство.

В качестве множества  $A_1$  возьмем все те буквы, которые встречаются хотя бы в одном слове из множества  $P$ . Понятно, что тогда  $[P^*]_{out} \subseteq A_1^*$ .

С другой стороны, для любого слова  $\alpha = a_{i_1} a_{i_2} \dots a_{i_s} \in A_1^*$  обозначим через  $\alpha_1 \in P$  слово, содержащее букву  $a_{i_1}$ , через  $\alpha_2 \in P$  — слово, содержащее букву  $a_{i_2}$ , ..., через  $\alpha_s \in P$  — слово, содержащее букву  $a_{i_s}$ . Ясно, что тогда слово  $\alpha$  является подсловом слова  $\alpha_1 \cdot \alpha_2 \cdot \dots \cdot \alpha_s \in P^s \subseteq P^*$ . Поэтому  $A_1^* \subseteq [P^*]_{out}$ .

■

**Лемма 6.** Пусть  $P \subseteq A^*$ . Тогда

$$P = [P]_{out} \iff A^* \setminus P = [A^* \setminus P]_{in}.$$

Доказательство.

Пусть  $P = [P]_{out}$ . Докажем от противного, что  $A^* \setminus P = [A^* \setminus P]_{in}$ . Если это не так, то найдется слово  $\alpha \notin A^* \setminus P$  и его подслово  $\beta \in A^* \setminus P$ . Это означает, что  $\alpha \in P$ ,  $\beta \notin P$ . Но, в силу замечания 2, выполнено

$$\beta \in [\alpha]_{out} \subseteq [P]_{out} = P.$$

Получили противоречие. Аналогично доказывается в обратную сторону.

■

**Лемма 7.** В  $A^*$  не существует счетного множества слов, попарно невложенных друг в друга.

*Доказательство.*

Прежде всего, поясним, что под вложенностью слов друг в друга здесь имеется в виду тот факт, что одно слово является подсловом другого, то есть может быть получено из него конечным применением операции выпадения.

Будем доказывать утверждение от противного. Если  $|A| = 1$ , то любые два слова в таком алфавите попарно вложимы и утверждение очевидно.

Разберем случай, когда  $|A| = 2$ . Пусть есть счетное семейство

$$T = \{\alpha_1, \alpha_2, \dots\}$$

слов в алфавите  $\{0, 1\}$ , попарно невложенных друг в друга. Обозначаем  $\beta = \alpha_1$ . Пусть  $\beta = b(1)b(2)\dots b(k)$ . Разбиваем множество  $T \setminus \{\beta\}$  на следующие непересекающиеся подмножества  $T_1, \dots, T_k$ .  $T_1$  содержит те и только те слова из  $T$ , в которых нет однобуквенного подслова  $b(1)$ .  $T_2$  содержит те и только те слова из  $T$ , в которых есть однобуквенное подслово  $b(1)$ , но нет двухбуквенного подслова  $b(1)b(2)$ . И так далее до множества  $T_k$ , которое содержит те и только те слова из  $T$ , в которых есть подслово  $b(1)b(2)\dots b(k-1)$ , но нет подслова  $b(1)b(2)\dots b(k) = \beta$ . Последнее ограничение, впрочем, всегда верно для слов из  $T \setminus \{\beta\}$ , так как слова из  $T$  все попарно невложены друг в друга. Так как множество  $T$  счетно, то и хотя бы одно из множеств  $T_i$  счетно. Теперь сделаем одно очень важное замечание:

$$T_i \subseteq (A \setminus \{b(1)\})^* b(1) (A \setminus \{b(2)\})^* b(2) \dots (A \setminus \{b(i-1)\})^* b(i-1) (A \setminus \{b(i)\})^*.$$

Итак, у нас есть счетное множество слов  $T_i$  из множества

$$(A \setminus \{b(1)\})^* b(1) (A \setminus \{b(2)\})^* b(2) \dots (A \setminus \{b(i-1)\})^* b(i-1) (A \setminus \{b(i)\})^*, \quad (3)$$

которые попарно невложены друг в друга. Каждое из этих слов вполне естественным образом можно тогда представить в виде

$$\beta(1)b(1)\beta(2)b(2)\dots\beta(i-1)b(i-1)\beta(i), \quad (4)$$

где в  $\beta(j)$  нет буквы  $b(j)$  при всех  $1 \leq j \leq i$ . Но алфавит  $A$  двухэлементный, поэтому все слова  $\beta(j)$  в этом представлении состоят из многократно повторенного символа 0 или символа 1. Это означает, что для

каждого из слов в  $T_i$  соответствующие им слова  $\beta(j)$  все попарно вложимы друг в друга при любом фиксированном  $1 \leq j \leq i$ . Зафиксируем какое-нибудь слово  $\gamma \in T_i$  :

$$\gamma = \gamma(1)b(1)\gamma(2)b(2) \dots \gamma(i-1)b(i-1)\gamma(i).$$

Здесь, как и ранее, в  $\gamma(j)$  нет символа  $b(j)$  при  $1 \leq j \leq i$ . Пройдемся для всех остальных слов из  $T_i \setminus \{\gamma\}$  по их словам  $\beta(1)$  в первой позиции. Возможны два случая: либо это слово  $\beta(1)$  содержит слово  $\gamma(1)$ , либо, наоборот, содержится в слове  $\gamma(1)$ . Всего слов в  $T_i \setminus \{\gamma\}$  счетно, поэтому возможны два случая. В первом случае в  $T_i$  существует бесконечное количество слов, у которых  $\beta(1)$  лежит в  $\gamma(1)$ . Тогда, в силу замечания 1, вариантов того, кем могут быть эти  $\beta(1)$  лишь конечное количество. Значит в  $T_i$  можно выделить бесконечное подмножество слов с одинаковым словом  $\beta(1)$  по первой позиции. В этом случае любое из этих слов возьмем за новое  $\gamma$  и повторим рассуждение для второй позиции. Во втором случае лишь конечное количество слов из  $T_i$  может по первой позиции лежать в  $\gamma(1)$ . Тогда в  $T_i$  существует бесконечное подмножество, в котором все слова по первой позиции содержат  $\gamma(1)$ . Так или иначе, мы нашли в  $T_i$  счетное подмножество, все слова из которого по первой позиции содержат  $\gamma(1)$ . После этого повторяем рассуждение для второй позиции. При этом слово  $\gamma$  может измениться, но свойство первой позиции о том, что там в качестве подслова есть  $\gamma(1)$ , сохраняется. Проведя это рассуждение по всем позициям, получаем счетное семейство слов, в каждой позиции в которых содержатся как подслова соответствующие части слова  $\gamma$ . Это противоречит попарной невложенности слов в нашем семействе. Для случая  $|A| = 2$  утверждение доказано.

Теперь обобщим это рассуждение на случай, когда  $|A| > 2$ . Опять же, берем счетное семейство попарно невложенных слов  $T$ . Выбираем в нем слово  $\beta = b(1)b(2) \dots b(k)$ . Разбиваем множество  $T$  на множества  $T_1, \dots, T_k$ . Выбираем счетное  $T_i$ . Каждое из слов в  $T_i$  представляем в виде

$$\beta(1)b(1)\beta(2)b(2) \dots \beta(i-1)b(i-1)\beta(i),$$

где в  $\beta(j)$  нет буквы  $b(j)$  при всех  $1 \leq j \leq i$ . Разделяем эти слова на позиции. Фиксируем какое-то слово  $\gamma \in T_i$  и сравниваем другие слова с  $\gamma$  по соответствующим позициям. По каждой из позиций возможны три варианта. Либо существует бесконечное количество слов в  $T_i$ , которые являются подсловом позиции в  $\gamma$ , либо существует бесконечное количество слов в  $T_i$ , которые содержат подслово позиции в  $\gamma$ , либо существует

бесконечное количество слов в  $T_i$ , которые несравнимы с  $\gamma$  по этой позиции. В первом и втором случае поступаем со словом  $\gamma$  и множеством  $T_i$  точно также, как и в случае  $|A| = 2$ . Для этих случаев теперь считаем, что соответствующие позиции в словах содержат подслово позиции из  $\gamma$ . Рассмотрим теперь позиции, в которых реализуется третий случай. Если таких позиций нет, то рассуждение закончено. Если такие позиции есть, то сделаем с каждой из них следующее. Обозначаем через  $\hat{T}$  множество слов в позиции. Мы знаем, что они не сравнимы со словом из этой же позиции, которое стоит в слове  $\gamma$ . Обозначаем его за  $\hat{\beta}$ . Так же, как и для слова  $\beta$  мы разбивали  $T$  на  $T_1, \dots, T_k$ , разбиваем теперь для слова  $\hat{\beta}$  множество  $\hat{T}$  на  $\hat{T}_1, \dots, \hat{T}_m$ , где  $m$  — длина слова  $\hat{\beta}$ . Выбираем какое-нибудь бесконечное  $\hat{T}_i$ , вкладываем его в множество, по виду аналогичное (3) и разбиваем слова из  $\hat{T}_i$  на позиции, как это было сделано в (4). Таким образом, слова позиций, в которых реализуется третий случай, мы разбили на подпозиции. Очень важным при этом является то, что по каждой отдельной подпозиции количество букв, которые могут встретиться в словах этой подпозиции, уменьшилось при этом на 1 и теперь не превосходит  $|A| - 2$ . Теперь можно к каждой из новых подпозиций применить снова деление на три случая и все дальнейшие манипуляции с этими подпозициями (для первого и второго случаев — замена  $\gamma$  и  $T_i$ , а для третьего случая — разбиение слов на подпозиции с меньшими по мощностям алфавитами). Поскольку мощность алфавита  $A$  конечна, то рассуждение в итоге сведется к уже рассмотренному случаю  $|A| = 2$ .

■

## Доказательство основных утверждений

**Теорема 1.** Пусть  $P \in R(A)$ . Тогда

$$P = [P]_{in} \iff P = \bigcup_{\alpha \in T} in(\alpha),$$

где  $T$  — произвольное конечное множество слов в алфавите  $A$ .

*Доказательство.*

Пусть  $T$  — произвольное конечное множество слов в алфавите  $A$ . Для произвольного  $\alpha \in T$  из определения (1) для множества  $in(\alpha)$  ясно, что оно регулярно. Но тогда и множество

$$P := \bigcup_{\alpha \in T} in(\alpha),$$

как конечное объединение регулярных множеств, является регулярным. При этом верно, что

$$[P]_{in} = \left[ \bigcup_{\alpha \in T} in(\alpha) \right]_{in} = \bigcup_{\alpha \in T} [in(\alpha)]_{in} \stackrel{*}{=} \bigcup_{\alpha \in T} in(\alpha) = P.$$

Равенство  $\stackrel{*}{=}$  здесь является тривиальным следствием лемм 1,2 и 3.

В другую сторону, из теории регулярных языков хорошо известно (этот факт легко доказывается индукцией по длине вывода), что любой регулярный язык  $P \in R(A)$  представим в виде

$$P = \bigcup_{i=1}^k \alpha_{i,1} \cdot (P_{i,1})^* \cdot \alpha_{i,2} \cdot (P_{i,2})^* \cdots (P_{i,s(i)})^* \cdot \alpha_{i,s(i)+1},$$

где  $k \in \mathbb{N}$ ,  $s(i) \in \mathbb{N}_0$ ,  $\alpha_{i,j} \in A^*$ ,  $P_{i,j} \in R(A)$ . Применяя леммы 1,2,3, получаем:

$$\begin{aligned} P &= [P]_{in} = \\ &= \bigcup_{i=1}^k [\alpha_{i,1}]_{in} \cdot [(P_{i,1})^*]_{in} \cdot [\alpha_{i,2}]_{in} \cdot [(P_{i,2})^*]_{in} \cdots [(P_{i,s(i)})^*]_{in} \cdot [\alpha_{i,s(i)+1}]_{in} = \\ &= \bigcup_{i=1}^k in(\alpha_{i,1}) \cdot A^* \cdot in(\alpha_{i,2}) \cdot A^* \cdots A^* \cdot in(\alpha_{i,s(i)+1}) = \\ &= \bigcup_{i=1}^k in(\alpha_{i,1} \cdot \alpha_{i,2} \cdots \alpha_{i,s(i)+1}). \end{aligned}$$

Теорема доказана.

■

**Теорема 2.** Пусть  $P \in R(A)$ . Тогда

$$P = [P]_{out} \iff P = \bigcup_{i=1}^k [\alpha_{i,1}]_{out} \cdot (A_{i,1})^* \cdots (A_{i,s(i)})^* \cdot [\alpha_{i,s(i)+1}]_{out},$$

где  $k \in \mathbb{N}$ ,  $s(i) \in \mathbb{N}_0$ ,  $\alpha_{i,j} \in A^*$ ,  $A_{i,j} \subseteq A$ .

*Доказательство.*

Пусть

$$P = \bigcup_{i=1}^k [\alpha_{i,1}]_{out} \cdot (A_{i,1})^* \cdots (A_{i,s(i)})^* \cdot [\alpha_{i,s(i)+1}]_{out},$$

где  $k \in \mathbb{N}$ ,  $s(i) \in \mathbb{N}_0$ ,  $\alpha_{i,j} \in A^*$ ,  $A_{i,j} \subseteq A$ . В силу замечания 2, множества  $[\alpha_{i,j}]_{out}$  конечны, а это означает, что  $P \in R(A)$ . Кроме того, из лемм 4 и 5 получаем

$$\begin{aligned} [P]_{out} &= \left[ \bigcup_{i=1}^k [\alpha_{i,1}]_{out} \cdot (A_{i,1})^* \cdots (A_{i,s(i)})^* \cdot [\alpha_{i,s(i)+1}]_{out} \right]_{out} = \\ &= \bigcup_{i=1}^k [[\alpha_{i,1}]_{out}]_{out} \cdot [(A_{i,1})^*]_{out} \cdots [(A_{i,s(i)})^*]_{out} \cdot [[\alpha_{i,s(i)+1}]_{out}]_{out} = \\ &= [\alpha_{i,1}]_{out} \cdot (A_{i,1})^* \cdots (A_{i,s(i)})^* \cdot [\alpha_{i,s(i)+1}]_{out} = P. \end{aligned}$$

В другую сторону. Мы знаем, что любой регулярный язык  $P \in R(A)$  представим в виде

$$P = \bigcup_{i=1}^k \alpha_{i,1} \cdot (P_{i,1})^* \cdot \alpha_{i,2} \cdot (P_{i,2})^* \cdots (P_{i,s(i)})^* \cdot \alpha_{i,s(i)+1},$$

где  $k \in \mathbb{N}$ ,  $s(i) \in \mathbb{N}_0$ ,  $\alpha_{i,j} \in A^*$ ,  $P_{i,j} \in R(A)$ . Применяя леммы 4,5, получаем:

$$\begin{aligned} P &= [P]_{out} = \\ &= \bigcup_{i=1}^k [\alpha_{i,1}]_{out} \cdot [(P_{i,1})^*]_{out} \cdot [\alpha_{i,2}]_{out} \cdot [(P_{i,2})^*]_{out} \cdots [(P_{i,s(i)})^*]_{out} \cdot [\alpha_{i,s(i)+1}]_{out} = \\ &= \bigcup_{i=1}^k [\alpha_{i,1}]_{out} \cdot (A_{i,1})^* \cdots (A_{i,s(i)})^* \cdot [\alpha_{i,s(i)+1}]_{out}, \end{aligned}$$

где  $A_{i,j}$  — некоторые подмножества алфавита  $A$ . Теорема доказана.

■

**Теорема 3.** Пусть  $P \subseteq A^*$ . Тогда  $[P]_{in} \in R(A)$ .

*Доказательство.*

Рассматриваем множество  $X$  всех минимальных по вложению слов языка  $P$ , то есть таких слов, которые есть в  $P$ , но никаких их собственных подслов в  $P$  нет. Из леммы 7 следует, что это множество конечно, так как любые два минимальных по вложению слова не могут быть вложены друг в друга. Заметим, что

$$[P]_{in} = \bigcup_{\alpha \in X} [\alpha]_{in}. \quad (5)$$

Вложимость правого множества в левое очевидна. А вложимость левого множества в правое следует из того факта, что любое слово из  $[P]_{in}$  можно получить конечным количеством применений операции вставки из какого-нибудь слова из  $P$ . Но любое слово  $\alpha$  из  $P$ , в свою очередь, содержит в себе хотя бы одно минимальное подслово из множества  $X$  и может быть получено из него конечным количеством применений операции вставки. Таким образом, равенство (5) доказано. Но, в силу леммы 1, множество  $[\alpha]_{in}$  регулярно. А мы знаем, что конечное объединение регулярных множеств тоже регулярно. Теорема доказана.

■

**Теорема 4.** Пусть  $P \subseteq A^*$ . Тогда  $[P]_{out} \in R(A)$ .

*Доказательство.*

В силу замечания 3,

$$[P]_{out} = [[P]_{out}]_{out}.$$

Из леммы 6 получаем

$$A^* \setminus [P]_{out} = [A^* \setminus [P]_{out}]_{in}.$$

Из утверждения теоремы 3 следует, что тогда  $A^* \setminus [P]_{out} \in R(A)$ . Но дополнение к регулярному множеству регулярно. Теорема доказана.

■

## Список литературы

- [1] В. И. Левенштейн. *О Двоичные коды с исправлением выпадений и вставок символа 1*. Пробл. передачи информ., 1965. Т.1, вып. 1, М., Сс. 12-25.
- [2] П. С. Дергач. *О каноническом регулярном представлении S-тонких языков*. Интеллектуальные системы, 2014. Т.18, вып. 1, М., Сс. 211-242. системы, 2014. Т.18, вып. 1, М., Сс. 211-242.
- [3] П. С. Дергач. *О проблеме вложения допустимых классов*. Интеллектуальные системы, 2015. Т.19, вып. 2, М., Сс. 143-174.
- [4] П. С. Дергач, Э. С. Айрапетов. *О прогрессивном разбиении некоторых подмножеств натурального ряда*. Интеллектуальные системы, 2015. Т.19, вып. 3, М., Сс. 79-86.
- [5] П. С. Дергач. *О двух размерностях спектров тонких языков*. Интеллектуальные системы, 2015. Т.19, вып. 3, М., Сс. 155-174.
- [6] П. С. Дергач, Э. С. Айрапетов. *О прогрессивном разбиении последовательности натуральных чисел, имеющей пропуск длины 2*. Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 67-86.
- [7] П. С. Дергач, Е. Д. Данилевская. *О покрытиях и разбиениях натуральных чисел, имеющих два последовательных пропуска длины 1*. Интеллектуальные системы, 2017. Т.21, вып. 1, М., Сс.192-237.
- [8] П. С. Дергач. *О структуре вложения прогрессивных множеств сложности два*. Интеллектуальные системы, 2017. Т.21, вып. 2, М., Сс.117-162.
- [9] П. С. Дергач, Ж. И. Раджабов. *О длине минимальной алфавитной склейки для класса линейных регулярных языков*. Интеллектуальные системы, 2017. Т.21, вып. 3, М., Сс.120-130.
- [10] Д. Е. Александров. *Эффективные методы реализации проверки содержания сетевых пакетов регулярными выражениями*. Интеллектуальные системы, 2014. Т.18, вып. 1, М., Сс. 37-60.
- [11] Д. Н. Бабин. *Частотные регулярные языки*. Интеллектуальные системы, 2014. Т.18, вып. 1, М., Сс. 205-210.

- [12] Д. Е. Александров. *Об оценках автоматной сложности распознавания классов регулярных языков.* Интеллектуальные системы, 2014. Т.18, вып. 4, М., Сс. 161-190.
- [13] В. М. Дементьев. *О звездной высоте регулярного языка и циклической сложности минимального автомата.* Интеллектуальные системы, 2014. Т.18, вып. 4, М., Сс. 215-222.
- [14] И. Е. Иванов. *О сохранении периодических последовательностей автоматами с магазинной памятью с однобуквенным магазином.* Интеллектуальные системы, 2015. Т.19, вып. 1, М., Сс. 145-160.
- [15] А. А. Петюшко. *О контекстно-свободных биграммных языках.* Интеллектуальные системы, 2015. Т.19, вып. 2, М., Сс. 187-208.
- [16] И. Е. Иванов. *Нижняя оценка на максимальную длину периода выходной последовательности автономного автомата с магазинной памятью.* Интеллектуальные системы, 2015. Т.19, вып. 3, М., Сс. 175-194.
- [17] В. А. Орлов. *О конечных автоматах с максимальной степенью различимости состояний.* Интеллектуальные системы, 2016. Т.20, вып. 1, М., Сс. 213-222.
- [18] П. С. Дергач. *О проблеме проверки однозначности алфавитного декодирования в классе регулярных языков с полиномиальной функцией роста.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 147-202.
- [19] А. М. Миронов. *Основные понятия теории вероятностных автоматов.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 283-330.
- [20] А. А. Петюшко, Д. Н. Бабин. *Классификация Хомского для матриц биграммных языков.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 331-336.
- [21] С. Б. Родин. *О связи линейно реализуемых автоматов и автоматов с максимальной вариативностью относительно кодирования состояний.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 337-348.

## Сведения об авторах

Дергач Петр Сергеевич

Младший научный сотрудник МГУ имени М. В. Ломоносова

e-mail: dergachpes@mail.ru.

### **On languages that are stable to the drop/paste operations Dergach P.S.**

The article is devoted to the drop and paste operations, which have been promoted by V.I. Levenshtein. The following two questions are asked and answered. What is the class of regular languages that are stable to the drop/paste operations? Are there any irregular languages that are stable to these operations?

**Keywords:** drop and paste operations, closed class, regular language.

# Структура графа на множестве перестановок $S_n$ , задаваемая моделью ошибки в скрытом канале перестановки пакетов

Казаков И.Б.

Статья посвящена изучению структуры графа, порождаемой на множестве перестановок моделью ошибки канала перестановки пакетов, введенной в работе И.Б. Казакова “Кодирование в скрытом канале перестановки пакетов”. Установлено, что граф можно разделить на слои, являющиеся независимыми множествами. Введено понятие характеристического графа перестановки и доказано, что номер слоя определяется числом его ребер. Получен результат о степенях вершин слоя в  $(S_n)^2$ , и на основании его дана оценка мощности конструируемого послойного кода. Разработан инструментарий для получения верхних оценок мощности кодов. Введены понятия симметрического слоя и разбиения графа. Приведены конкретные примеры разбиения  $S_n$  на призмы, а также на произведения графов — обобщение понятия призмы. Построено вложение в  $E_{\frac{n(n-1)}{2}}$ ,  $S_n$  оказывается ограничением  $E_{\frac{n(n-1)}{2}}$ . Получен побочный результат алгебраического характера, связывающий размер подгруппы  $H \subset S_n$  и содержание в ней  $n$ -шаговых перестановок.

**Ключевые слова:** перестановки, графовая структура, код, исправляющий ошибки

## 1. Введение

В работе изучается структура множества перестановок  $S_n$ , а также верхние и нижние эвристические оценки мощности кодов, исправляющих одну ошибку. Сама данная задача возникла из задачи передачи информации по скрытому каналу перестановки пакетов ([1]). Содержательно рассматривается следующая постановка: по некоему каналу связи передается группа из  $n$  пакетов, причем в порядке их передачи содержится

дополнительная информация; в процессе передачи этот порядок может меняться самопроизвольно, например могут самопроизвольно поменяться местами два соседних пакета. Это создает ошибки для кода, заданного перестановками.

Говоря более формально, рассматривается  $S_n$  — множество перестановок  $n$  элементов. Перестановка  $\sigma \in S_n$  представляется как последовательность из  $n$  неповторяющихся чисел от 1 до  $n$ . На множестве  $S_n$  введена структура графа: две перестановки полагаются смежными, если они могут быть получены друг из друга применением транспозиции двух своих соседних элементов. Например, в  $S_4$ , перестановке 1234 смежны 2134, 1243, 1324. В терминах, введенных в [1], это соответствует первой модели ошибки. Далее этот граф будет обозначаться так же, как и множество перестановок:  $S_n$ , и мы будем отождествлять вершины графа с соответствующими перестановками.

Второй степенью графа, далее обозначаемой как  $(S_n)^2$ , называется граф над теми же перестановками как вершинами со следующим отношением смежности: две вершины в  $(S_n)^2$  смежны тогда и только тогда, когда они или непосредственно смежны в  $S_n$ , или же в  $S_n$  есть ещё одна вершина, с которой эти две смежны. То есть, если в  $S_n$  между ними имеется путь длины 1 или 2. Кодом, исправляющим одну ошибку, (далее просто кодом), называется такое подмножество  $K \subset S_n$ , которое является независимым множеством относительно структуры графа  $(S_n)^2$ .

Главный результат работы — это обнаружение слоистой структуры  $S_n$ , позволяющей строить эвристический послойный код, и тем самым оценивать снизу мощность максимального кода. Во-вторых, на основе высокой степени симметрии  $S_n$  предложено понятие разбиений графа, которые дают метод получения верхних оценок. Получены также побочные результаты о вложении рассматриваемого графа в  $E_n$  (множества последовательностей из 0 и 1), а также лемма о подгруппах  $H \subset S_n$ .

## 2. Слоистая структура $S_n$

Выделим в  $S_n$  единичную перестановку  $e = [1, 2, 3, \dots, n]$ , и скажем, что она лежит в нулевом слое.

**Определение 2.1.** Пусть  $\sigma \in S_n$ . Если длина минимального пути между  $e$  и  $\sigma$  равна  $k$ , то скажем, что  $\sigma$  лежит в  $k$ -ом слое  $S_{n,k}$ .

Таким образом,  $S_n = S_{n,0} \sqcup S_{n,1} \sqcup \dots$

Установим ряд простых свойств графа  $S_n$ :

**Утверждение 2.1.** В  $S_n$  нет замкнутых путей нечётной длины.

*Доказательство.* Очевидно, т.к. каждый шаг пути это умножение перестановки на транспозицию соседних позиций, то на каждом шаге перестановка меняет свою чётность и поэтому через нечётное число шагов вернуться на прежнее место нельзя.  $\square$

**Утверждение 2.2.** Пусть  $\sigma_1, \sigma_2 \in S_{n,k}$ . Тогда они не могут быть смежны.

*Доказательство.*

1. Предположим, что они смежны. Составим путь из 3-х частей:  $e \rightarrow \sigma_1$  ( $k$  шагов),  $\sigma_1 \rightarrow \sigma_2$  (1 шаг),  $\sigma_2 \rightarrow e$  ( $k$  шагов).
2. Всего получился замкнутый путь из  $2k+1$  шагов, что противоречит предыдущему утверждению.  $\square$

**Утверждение 2.3.** Пусть  $\sigma_1 \in S_{n,k}$ ,  $\sigma_2$  смежно с  $\sigma_1$ . Тогда или  $\sigma_2 \in S_{n,k+1}$ , или  $\sigma_2 \in S_{n,k-1}$ .

*Доказательство.*

1.  $e \rightarrow \sigma_1$  ( $k$  шагов),  $\sigma_1 \rightarrow \sigma_2$  (1 шаг)  $\Rightarrow e \rightarrow \sigma_2$  ( $k+1$  шаг)  $\Rightarrow \sigma_2$  лежит в  $k+1$ -ом слое или выше (т.е. в слоях с меньшими номерами).
2. Предположим, что  $\sigma_2 \notin S_{n,k-1} \sqcup S_{n,k+1}$ .
3. Тогда, так как также и  $\sigma_2 \notin S_{n,k}$ , то  $\sigma_2$  лежит выше слоя  $k-1$ . А это означает, что существует путь  $l : e \rightarrow \sigma_2$ , такой что  $|l| < k-1$ .
4. Построим путь  $l' : e \rightarrow \sigma_2$  ( $|l|$  шагов),  $\sigma_2 \rightarrow \sigma_1$  (1 шаг). Итого  $|l'| < k$ .
5. А следовательно,  $\sigma_1$  лежит выше  $k$ -ого слоя. Что противоречит условию.
6. Если  $\sigma_1$  лежит в нулевом слое, то за один шаг можно попасть только в 1-ый слой, так как нет путей, короче, чем путь длины 1.
7. Если  $\sigma_1$  лежит в 1-ом слое, то  $\sigma_2$  может лежать лишь в 0-ом или 2-ом слоях, и из п.3 противоречие получается непосредственно.
8. Если  $\sigma_1$  лежит в последнем слое, то просто можно считать, что  $S_{n,k+1} = \emptyset$ , и дальнейшие рассуждения аналогичны.  $\square$

Таким образом, при любом проходе пути мы на каждом его шаге идём или на слой вниз, или на слой вверх. Общее же их количество в  $S_n$  установим далее.

### 3. Характеристические графы

Введенное разбиение графа на слои пока что весьма тривиально. Для получения содержательных результатов нужно ввести множество вспомогательных понятий и связать их с введенным разбиением. Первым таким вспомогательным понятием будет характеристический граф, соответствующий перестановке. Такое соответствие дает разбиение  $S_n$  на множества по числу ребер в характеристическом графе. Как будет показано далее, это разбиение совпадает с введенным выше разбиением по слоям. Этот факт позволит перейти к глубокому анализу слоистой структуры  $S_n$ .

Для отношения смежности пары вершин  $\sigma_1, \sigma_2 \in S_n$  мы будем использовать обозначение  $\sigma_1 \sim \sigma_2$ .

Перестановка  $\sigma \in S_n$  представима как последовательность  $[\sigma[1] \dots \sigma[n]]$ , как было указано в введении.

**Определение 3.1.** Пусть  $\sigma \in S_n$ . Характеристическим графом назовём  $G_\sigma = (V, E)$ , где  $V = \{1, 2, 3, \dots, n\}$ , а  $(i, j), (j, i) \in E$  (граф ненаправлен)  $\Leftrightarrow$  или  $i < j$ , и  $\sigma = [\dots, j, \dots, i, \dots]$  (т.е. значение  $j$  идёт ранее значения  $i$ ), или же  $i > j$ , и  $\sigma = [\dots, i, \dots, j, \dots]$ .

То есть в  $G_\sigma$  между вершинами  $i$  и  $j$  есть ребро, тогда и только тогда, когда в  $\sigma$  они стоят в порядке убывания.

Количество рёбер в  $G_\sigma$  будем обозначать через  $s(\sigma)$ . Несложно увидеть, что значение  $s(\sigma)$  меняется в пределах от 0 до  $\frac{n(n-1)}{2}$ .

**Лемма 3.1.** Пусть  $\sigma_2$  получена из  $\sigma_1$  перестановкой позиций  $k, k + 1$ .

Тогда  $G_{\sigma_2}$  содержит те же ребра, что и  $G_{\sigma_1}$ , также включая ребро  $(\sigma_1[k], \sigma_1[k + 1])$ , если его там (в  $G_{\sigma_1}$ ) не было, и исключая, если оно там было.

*Доказательство.*

1. Обращение порядка  $\sigma_1[k], \sigma_1[k + 1]$  в последовательности  $\sigma$  есть по определению характеристического графа инверсия наличия заданного в условии ребра. Нужно лишь показать, что все остальные рёбра, как и их отсутствия остались на месте.
2. Значения всех позиций, кроме  $k, k + 1$ , не изменились. Следовательно, рёбра (как и их отсутствие) вида  $(\sigma[r_1], \sigma[r_2])$ , где  $r_1, r_2 \neq k, k + 1$  остались на месте.
3. Пусть  $s$  — некая позиция,  $s \neq k, k + 1$ . Тогда, или  $s < k$ , или  $s > k + 1$ .

4. В случае  $s < k$   $[\dots, \sigma_1[s], \dots, \sigma_1[k], \sigma_1[k+1], \dots]$  перешло в  $[\dots, \sigma_1[s], \dots, \sigma_1[k+1], \sigma_1[k], \dots]$ , т.е. как  $\sigma_1[s]$  стояло перед обоими  $\sigma_1[k]$  и  $\sigma_1[k+1]$ , так оно и осталось стоять.

5. В случае  $s > k+1$   $[\dots, \sigma_1[k], \sigma_1[k+1], \dots, \sigma[s], \dots]$  перешло в  $[\dots, \sigma_1[k+1], \sigma_1[k], \dots, \sigma[s], \dots]$ , т.е. как  $\sigma_1[s]$  стояло после обоих  $\sigma_1[k]$  и  $\sigma_1[k+1]$ , так оно и осталось стоять.

6. Откуда следует, что и рёбра(и их отсутствие) вида  $(\sigma[s], \sigma[k]), (\sigma[s], \sigma[k+1])$ , где  $s \neq k, k+1$  остались на месте. □

### Лемма 3.2.

*Выполнены следующие импликации:*

$$a) \sigma_1 \sim \sigma_2 \Rightarrow |s(\sigma_1) - s(\sigma_2)| = 1$$

$$b) s(\sigma_1) \neq 0 \Rightarrow \exists \sigma_2 \mid \sigma_1 \sim \sigma_2 \mid s(\sigma_2) = s(\sigma_1) - 1$$

$$c) s(\sigma_1) \neq \frac{n(n-1)}{2} \Rightarrow \exists \sigma_2 \mid \sigma_1 \sim \sigma_2 \mid s(\sigma_2) = s(\sigma_1) + 1$$

*Доказательство.*

1. Пункт а) непосредственно следует из леммы 1, по которой характеристические графы смежных вершин различаются ровно на одно ребро.

2.  $s(\sigma_1) \neq 0 \Rightarrow \sigma_1$  не является монотонно возрастающей последовательностью.  $\Rightarrow \exists k \sigma_1[k] > \sigma_1[k+1] \Rightarrow$  в  $G_{\sigma_1}$  есть ребро  $(\sigma_1[k], \sigma_1[k+1])$ .

3. Получим  $\sigma_2$  перестановкой позиций  $k, k+1, \sigma_2 \sim \sigma_1$ . В  $G_{\sigma_2}$  ребро из предыдущего пункта исчезло, и  $s(\sigma_2) = s(\sigma_1) - 1$ .

4.  $s(\sigma_1) \neq \frac{n(n-1)}{2} \Rightarrow \sigma_1$  не является монотонно убывающей последовательностью.  $\Rightarrow \exists k \sigma_1[k] < \sigma_1[k+1] \Rightarrow$  в  $G_{\sigma_1}$  нет ребра  $(\sigma_1[k], \sigma_1[k+1])$ .

5. Получим  $\sigma_2$  перестановкой позиций  $k, k+1, \sigma_2 \sim \sigma_1$ . В  $G_{\sigma_2}$  ребро из предыдущего пункта возникло, и  $s(\sigma_2) = s(\sigma_1) + 1$ . □

Таким образом, на каждом шаге любого пути в  $S_n$  мы либо увеличиваем  $s(\sigma)$  на 1, либо уменьшаем его же на 1.

**Следствие 3.1.** *От  $e$  до  $\sigma$  есть путь длины  $s(\sigma)$ .*

*Доказательство.* Действительно, возьмём  $\sigma$  и будем переходить к смежным вершинам с меньшим на 1 значением  $s(\sigma)$ , покуда мы не достигнем  $e$ , для которого единственного  $s(e) = 0$ . □

**Следствие 3.2.** *Между  $e$  и  $\sigma$  нет никакого пути короче длины  $s(\sigma)$ .*

*Доказательство.*

1. В силу вышеизложенного, длина любого пути между  $e$  и  $\sigma$  равна  $s_1 + s_2$ , где  $s_1$  — количество шагов пути, на которых  $s(\sigma)$  увеличивалось на 1, а  $s_2$  — количество шагов, на которых оно уменьшалось на 1.
2. И тогда  $s(\sigma) = s_1 - s_2$ . Но  $s_1 + s_2 \geq s_1 - s_2$ , причём равенство достигается лишь при  $s_2 = 0$ .

□

**Вывод.**  $\sigma \in S_{n,s(\sigma)}$ , то есть множества вида  $\{\sigma | s(\sigma) = k\}$  в точности совпадают со слоями  $S_{n,k}$ . И всего в  $S_n$  имеется  $1 + \frac{n(n-1)}{2}$  слоёв соответственно значениям  $s(\sigma) = 0, \dots, \frac{n(n-1)}{2}$ .

Докажем также однозначность восстановления перестановки по её характеристическому графу.

**Лемма 3.3.** (о единственности)  $G_{\sigma_1} = G_{\sigma_2} \Rightarrow \sigma_1 = \sigma_2$

*Доказательство.*

I. Вспомогательные понятия.

1.  $V = \{1, 2, \dots, n\}$  — множество вершин  $G_\sigma$ .
2. Пусть  $v \in V$ . Тогда

$$L_v^\sigma = \{\sigma[k] | \sigma[k] \text{ стоит левее } v \text{ в последовательности } \sigma\}$$

3. Пусть  $v \in V$ . Тогда

$$R_v^\sigma = \{\sigma[k] | \sigma[k] \text{ стоит правее } v \text{ в последовательности } \sigma\}$$

4. Из этих определений очевидно следует  $V = L_v^\sigma \sqcup \{v\} \sqcup R_v^\sigma$ , так как любое  $w \in V$  стоит или левее  $v$ , или правее, или есть само  $v$ , причём все три возможности взаимоисключающи.

II. Однозначное восстановление  $L_v, R_v$  по  $G_\sigma$ .

1. Пусть даны перестановки  $\sigma_1, \sigma_2$ , такие что  $G_{\sigma_1} = G_{\sigma_2}$ .
2. Зафиксируем  $v \in V$ . И выберем некое  $w \in L_v^{\sigma_1}$ .
3. Возможны два случая:  $w > v$  или  $v < w$ . (вершины, взятые как их номера)
4. Рассмотрим случай  $w > v$ . Тогда по определению оказывается, что  $(v, w)$  — ребро  $G_{\sigma_1}$ , а значит, оно ребро и  $G_{\sigma_2}$ .
5. И также по определению оказывается, что и в  $\sigma_2$   $w \in L_v^{\sigma_2}$  (при  $w > v$ )
6. Рассмотрим случай  $w < v$ . Тогда по определению оказывается, что  $(v, w)$  — не ребро  $G_{\sigma_1}$ , а значит, оно не ребро и  $G_{\sigma_2}$ .

7. И также по определению оказывается, что и в  $\sigma_2$   $w \in L_v^{\sigma_2}$  (при  $w < v$ )
8. Таким образом  $L_v^{\sigma_1} \subset L_v^{\sigma_2}$ . Переставив  $\sigma_1, \sigma_2$  местами, и докажем также и  $L_v^{\sigma_2} \subset L_v^{\sigma_1}$ . Таким образом  $L_v^{\sigma_2} = L_v^{\sigma_1}$ .
9. И, следовательно, также и  $R_v^{\sigma_2} = R_v^{\sigma_1}$  (см. I.4)
- III. Доказательство  $L_{v_1}^{\sigma_1} = L_{v_2}^{\sigma_2} \Rightarrow v_1 = v_2$ .
1. Предположим  $v_1 \neq v_2$ , при истинной посылке.
  2. По I.4  $V = L_{v_1}^{\sigma_1} \sqcup \{v_1\} \sqcup R_{v_1}^{\sigma_1} = L_{v_2}^{\sigma_2} \sqcup \{v_2\} \sqcup R_{v_2}^{\sigma_2} \Rightarrow \{v_1\} \sqcup R_{v_1}^{\sigma_1} = \{v_2\} \sqcup R_{v_2}^{\sigma_2}$
  3. И так как  $v_1 \neq v_2$ , то  $v_1 \in R_{v_2}^{\sigma_2}$ ,  $v_2 \in R_{v_1}^{\sigma_1}$ .
  4. И это означает, что в последовательности  $\sigma$   $v_1$  правее  $v_2$ , и  $v_2$  правее  $v_1$ . Противоречие.
- IV. Тождество первых членов. (база индукции)
1. Пусть  $v_1 = \sigma_1[1]$ ,  $v_2 = \sigma_2[1]$ .
  2. Тогда  $L_{v_1}^{\sigma_1} = L_{v_1}^{\sigma_2} = \emptyset$ ,  $L_{v_2}^{\sigma_1} = L_{v_2}^{\sigma_2} = \emptyset$ . (см. однозначность по II.)
  3. По III получаем, что  $v_1 = v_2$ , т.е.  $\sigma_1[1] = \sigma_2[1]$ .
- V. Шаг индукции.
1. Пусть при  $\forall i < k$   $\sigma_1[i] = \sigma_2[i]$ .
  2. Положим  $v_1 = \sigma_1[k]$ ,  $v_2 = \sigma_2[k]$ .
  3. Тогда  $L_{v_1}^{\sigma_1} = L_{v_2}^{\sigma_2} = \{\sigma_1[1], \dots, \sigma_1[k-1]\} = \{\sigma_2[1], \dots, \sigma_2[k-1]\}$ .
  4. По II.5  $L_{v_1}^{\sigma_2} = L_{v_1}^{\sigma_1} = L_{v_2}^{\sigma_2} = L_{v_2}^{\sigma_1}$ .
  5. По III отсюда следует  $v_1 = v_2$ , т.е.  $\sigma_1[k] = \sigma_2[k]$ .

□

## 4. Простые перестановки

Для изучения отношения смежности в  $(S_n)^2$  следует рассмотреть пути длины 1 и 2 в  $S_n$ . Таким путям, независимо от начала пути в силу симметрии (конкретно: автоморфизмы нашего графа  $S_n$ , которые являются умножением на некую перестановку) соответствуют транспозиции двух соседних элементов или же произведение двух соседних. Стало быть, дальнейшим направлением исследования будет рассмотрение свойств перестановок такого вида. При этом будет использован вышевведённый инструмент характеристический граф.

**Примечание.** Перестановка  $\sigma \in S_n$  отождествляется с последовательностью  $[\sigma(1), \dots, \sigma(n)]$ . Напомним это ещё раз. Применение другой перестановки к данной это действие на отождествленную с ней последовательность. Так как сама такая последовательность — это результат действия перестановки на последовательность  $[1, \dots, n]$ , то

действие на неё ещё одной перестановки равносильно умножению слева на эту вторую перестановку.

**Определение 4.1.** Простыми перестановками будем называть перестановки следующих 2-х типов:

**Определение 4.2.** Одношаговая перестановка — транспозиция 2-х соседних позиций.

**Определение 4.3.** Двухшаговая перестановка — произведение 2-х одношаговых. Множество двухшаговых перестановок обозначим как  $O$ .

Двухшаговые перестановки также разделим на два вида: коммутативные и некоммутативные.

**Определение 4.4.** Двухшаговая коммутативная перестановка — это перестановка вида  $(i, i + 1)(j, j + 1)$ , где  $i, i + 1 \neq j, j + 1$ . Их множество обозначим как  $O_1$

**Утверждение 4.1.** Характеристический граф двухшаговой коммутативной перестановки содержит два ребра без общих вершин (и только эти рёбра)  $(i, i + 1)$  и  $(j, j + 1)$

*Доказательство.* Действительно, такая перестановка взятая как последовательность выглядит как  $[1, \dots, i - 1, i + 1, i, i + 2, \dots, j - 1, j + 1, j, j + 2, \dots, n]$ , в убывающем порядке стоят подпоследовательности из 2-х элементов  $[i + 1, i]$  и  $[j + 1, j]$ , и причём только они. Что и соответствует этим рёбрам характеристического графа.  $\square$

Двухшаговая перестановка — это произведение двух одношаговых. Можно ли по данной двухшаговой восстановить однозначно одношаговые, как произведение которых она получена? Покажем далее, что ответ на этот вопрос положителен.

**Определение 4.5.** Если по двухшаговой перестановке однозначно восстанавливается пара одношаговых (вместе с порядком перемножения, если он значим), перемножением которых она получается, то такую двухшаговую перестановку назовём однозначной.

**Следствие 4.1.** Всякая двухшаговая коммутативная перестановка однозначна.

*Доказательство.*

1. Пусть  $\sigma = (i, i+1)(j, j+1) = (i', i'+1)(j', j'+1)$  — разложения на одношаговые перестановки, причём если коммутируют первые перестановки (это мы предполагаем), то коммутируют и вторые. Это так, ибо если бы вторые перестановки бы не коммутировали, то множество подвижных точек  $\sigma$  было бы равно 4 (произведение 2-х независимых транспозиций имеет 4 подвижных точки), а с другой 3 (получился бы цикл из трёх позиций, если у двух перемножаемых одношаговых имеется общая позиция), что противоречиво. Иначе говоря, множества коммутативных и некоммутирующих двушаговых перестановок (как они будут определены далее) не пересекаются.

2. Рассмотрим характеристический граф  $G_\sigma = (V, E)$ . Тогда по утверждению  $E = \{(i, i+1), (j, j+1)\} = \{(i', i'+1), (j', j'+1)\}$

3. Откуда либо  $(i, i+1) = (i', i'+1)$  и  $(j, j+1) = (j', j'+1)$ , либо  $(i, i+1) = (j', j'+1)$  и  $(j, j+1) = (i', i'+1)$ . В обоих случаях  $\sigma$  оказывается разложенной на одну и ту же неупорядоченную пару одношаговых перестановок.

□

**Определение 4.6.** *Двушаговые некоммутирующие перестановки — это все остальные (кроме коммутативных), причём их имеется два подвида: вида  $(i, i+1)(i+1, i+2) = (i, i+1, i+2)$  и вида  $(i+1, i+2)(i, i+1) = (i, i+2, i+1)$ . Их множество обозначим как  $O_2$ .*

**Утверждение 4.2.**  $G_{(i, i+1, i+2)} = (V, E)$ , где  $E = \{(i, i+1), (i, i+2)\}$ .

*Доказательство.* Запишем как последовательность  $[1, \dots, i-1, i+1, i+2, i, i+3, \dots, n]$ , в убывающем порядке стоят 2-х элементные подпоследовательности  $[i+1, i]$ ,  $[i+2, i]$ , и притом только они. □

**Утверждение 4.3.**  $G_{(i+2, i+1)} = (V, E)$ , где  $E = \{(i+2, i), (i+2, i+1)\}$

*Доказательство.* Запишем последовательность  $[1, \dots, i-1, i+1, i+2, i, i+3, \dots, n]$ , в убывающем порядке стоят 2-х элементные подпоследовательности  $[i+2, i]$ ,  $[i+2, i+1]$ , и притом только они. □

Непосредственно рассматривая два случая подвидов, и объединяя эти утверждения, получаем:

**Следствие 4.2.** *Характеристический граф двушаговой некоммутативной перестановки содержит всегда два ребра с одной общей вершиной и только их, причём выполнено следующее:*

а) *Этим рёбрам инцидентны три вершины с подряд идущими номерами  $i, i + 1, i + 2$ .*

б) *Общей вершиной является или  $i$ , или  $i + 2$ . При этом, если общая вершина  $i$  (как минимальная из этих трёх по номеру) — это эта перестановка имеет подвид  $(i, i + 1, i + 2)$ , а если  $i + 2$  (как максимальная из этих трёх по номеру) — то подвид  $(i, i + 2, i + 1)$ . Из единственности перестановки заданного характеристического графа следует, что эти подвиды не пересекаются.*

**Следствие 4.3.** *Двушаговые некоммутативные перестановки однозначны.*

*Доказательство.*

1. Известно, что она не может быть разложена в произведение коммутативных одношаговых. По предыдущему следствию по двушаговой перестановке однозначно определяется её вид, судя по тому, какая вершина в её характеристическом графе инцидентна двум рёбрам.

I. Перестановка вида  $\sigma = (i, i + 1, i + 2)$ .

1. Предположим, что  $\sigma = (i, i + 1)(i + 1, i + 2) = (i, i + 1, i + 2) = (j, j + 1, j + 2) = (j, j + 1)(j + 1, j + 2)$  — два различных разложения,  $i \neq j$ .

2. Тогда, с одной стороны  $G_\sigma = G_{(i, i+1, i+2)} = (V, \{(i, i + 1), (i, i + 2)\})$ , а с другой  $G_\sigma = G_{(j, j+1, j+2)} = (V, \{(j, j + 1), (j, j + 2)\})$

3. Откуда следует, что либо  $(i, i + 1) = (j, j + 1)$  и  $(i, i + 2) = (j, j + 2)$  (откуда  $i = j$ , противоречие), либо  $(i, i + 1) = (j, j + 2)$  и  $(j, j + 1) = (i, i + 2)$  (что очевидный абсурд вида  $1 = 2$ , см. модуль разности между номерами вершин, инцидентных ребру).

II. Перестановка вида  $\sigma = (i, i + 2, i + 1)$ .

1. Предположим, что  $\sigma = (i + 1, i + 2)(i, i + 1) = (i, i + 2, i + 1) = (j, j + 2, j + 1) = (j + 1, j + 2)(j, j + 1)$  — два различных разложения,  $i \neq j$ .

2. Тогда, с одной стороны  $G_\sigma = G_{(i, i+2, i+1)} = (V, \{(i + 2, i), (i + 2, i + 1)\})$ , а с другой  $G_\sigma = G_{(j, j+2, j+1)} = (V, \{(j + 2, j), (j + 2, j + 1)\})$

3. Откуда следует, что либо  $(i + 2, i) = (j + 2, j)$  и  $(i + 2, i + 1) = (j + 2, j + 1)$  (откуда  $i = j$ , противоречие), либо  $(i + 2, i) = (j + 2, j + 1)$  и  $(j + 2, j) = (i + 2, i + 1)$  (что очевидный абсурд вида  $2 = 1$ , см. модуль разности между номерами вершин, инцидентных ребру).

□

Совокупно доказана:

**Теорема 4.1.** *Всякая двушаговая перестановка однозначна, или иначе выражаясь, если  $\sigma_1, \sigma_2, \sigma'_1, \sigma'_2$  — одношаговые и выполнено  $\sigma_1\sigma_2 = \sigma'_1\sigma'_2$ , то  $\sigma_1 = \sigma'_1$  и  $\sigma_2 = \sigma'_2$  или же может быть  $\sigma_1 = \sigma'_2$ ,  $\sigma_2 = \sigma'_1$ , если  $\sigma_1, \sigma_2$  коммутируют.*

Укажем теперь количество двушаговых перестановок обоих классов.

**Лемма 4.1.**  $|O| = |O_1| + |O_2|$ , где  $|O_1| = \frac{(n-3)(n-2)}{2}$ ,  $|O_2| = 2(n-2)$ . Откуда всего  $|O| = \frac{(n+1)(n-2)}{2}$ .

*Доказательство.*

1. Одношаговую перестановку можно выбрать  $n - 1$  способами.
2. 3-цикл вида  $(i, i + 1, i + 2)$  [а также равным образом и вида  $(i, i + 2, i + 1)$  можно выбрать  $n - 2$  способами (по  $n - 2$  возможным  $i$ ).
3. Всего упорядоченных пар различных одношаговых перестановок ровно  $(n - 1)(n - 2)$  штук.
4. Из п.2 прямо следует, что  $(n - 2)$  на каждый вид  $|O_1| = 2(n - 2) =$  количество упорядоченных пар перестановок с пересекающимися позициями. (теорема об однозначности)
5. Следовательно, упорядоченных пар с непересекающимися позициями всего  $(n - 1)(n - 2) - 2(n - 2) = (n - 3)(n - 2)$ .
6. А каждая двушаговая коммутативная перестановка соответствует ровно двум таким из п.5. (теорема об однозначности). Следовательно, коммутативных перестановок  $|O_2| = \frac{(n-3)(n-2)}{2}$ .

□

## 5. Слои как подграфы в $(S_n)^2$

Из любой вершины  $S_n$ , как уже выяснено, ребра ведут или на слой ниже, или на слой выше. Никакие ребра не ведут на этот же слой. А следовательно, сам слой, рассматриваемый как подграф в  $S_n$  не имеет ни единого ребра, то есть слой является в  $S_n$  независимым множеством.

Теперь же исследуем слой как подграф в  $(S_n)^2$ .

**Определение 5.1.** *Граф слоя  $k$ :  $G_k = (V_k, E_k)$ , где  $V_k = S_{n,k}$ , а  $(\sigma_1, \sigma_2) \in E_k \Leftrightarrow (\sigma_1, \sigma_2) \in (S^n)^2$ , где  $S^n$  взято со структурой графа модели 1.*

Исследуем далее степени вершин  $G_k$ . Для этого надо подсчитать число путей из 2-х символов от заданного  $\sigma \in S_{n,k}$ , которые ведут в тот же слой.

**Лемма 5.1.** Пусть  $\sigma \in S_n$ ,  $\alpha$  — одношаговая перестановка. Тогда  $\sigma\alpha \sim \sigma$ .

И обратно, если  $\sigma \sim \sigma_1$ , то  $\sigma_1 = \sigma\alpha$ , где  $\alpha$  — одношаговая перестановка.

*Доказательство.*

I.

1. Пусть  $\alpha = (i, i+1)$ .

2. Последовательность  $\sigma = [\dots, \sigma[i], \sigma[i+1], \dots]$ .

3. Последовательность  $\sigma\alpha = [\dots, \sigma[i+1], \sigma[i], \dots]$  оказалась полученной из исходной  $\sigma$  перестановкой 2-х соседних позиций, а следовательно, смежна с ней в  $S_n$ .

II.

1. Пусть  $\sigma_1$  получена из  $\sigma$  перестановкой  $i, i+1$  позиций.

2. Т.е.  $\sigma = [\dots, \sigma[i], \sigma[i+1], \dots]$ ,  $\sigma_1 = [\dots, \sigma[i+1], \sigma[i], \dots]$ .

3. Положим  $\alpha = (i, i+1)$ . Тогда  $\sigma\alpha = [\dots, \sigma[\alpha[i]] \sigma[\alpha[i+1]], \dots] = [\dots, \sigma[i+1] \sigma[i], \dots] = \sigma_1$ .

□

Необходимо различить пути длины 2, ведущие из данной вершины в вершину из того же слоя, от путей, которые ведут на два слоя вверх/вниз. Этим путям соответствуют двушаговые перестановки.

**Определение 5.2.** Двушаговая перестановка  $n$  называется нормальной относительно  $\sigma \in S_{n,k}$ , если  $\sigma n \in S_{n,k}$ . Множество таких перестановок обозначим как  $N_\sigma$ .

Из них множество коммутативных обозначим как  $N_\sigma^1$ .

Множество некоммутативных — как  $N_\sigma^2$ .

**Определение 5.3.**  $\sigma \in S_{n,k}$ :  $N(\sigma)$  — множество смежных с  $\sigma$  в графе  $G_k$

**Лемма 5.2.**  $\deg_{G_k}(\sigma) = |N(\sigma)| = |N_\sigma|$ .

*Доказательство.*

I. Отображение  $f_1 : N(\sigma) \rightarrow N_\sigma$ .

1. Пусть  $\sigma_1 \in N(\sigma)$ . Тогда существует путь  $\sigma \rightarrow \sigma_2 \rightarrow \sigma_1$  в  $S_n$ . И тогда по лемме 1  $\sigma_2 = \sigma\alpha_1$ ,  $\sigma_1 = \sigma_2\alpha_2$ , где  $\alpha_1, \alpha_2$  одношаговы.

2. Отсюда  $\sigma_1 = \sigma\alpha_1\alpha_2 = \sigma n$ , где  $n$  двушагово.

3. Сопоставим этому  $\sigma_1 \rightarrow n$ , т.е.  $f_1(\sigma_1) = \sigma^{-1}\sigma_1$ .

II. Отображение  $f_2 : N_\sigma \rightarrow N(\sigma)$ .

1. Пусть  $n \in N_\sigma$ . Тогда  $n = \alpha_1\alpha_2$ ,  $\alpha_1, \alpha_2$  одношаговые.

2. Рассмотрим  $\sigma' = \sigma n = \sigma\alpha_1\alpha_2$ .

3. Так как  $n \in N_\sigma$ , то  $s(\sigma') = s(\sigma n)$ . Рассмотрим путь  $\sigma \rightarrow \sigma\alpha_1 \rightarrow \sigma\alpha_1\alpha_2$ . По этому пути длины 2 придём в тот же слой, в котором находится его начало  $\sigma$ .

4. Откуда  $\sigma$  смежно с  $\sigma\alpha_1\alpha_2 = \sigma n = \sigma'$  в  $G_k$ , и, следовательно,  $\sigma' \in N(\sigma)$ .

5. Сопоставим этому  $n \rightarrow \sigma'$ , т.е.  $f_2(n) = \sigma n$ .

III. Взаимнообратность.

1.  $n \in N_\sigma : f_1 \circ f_2(n) = f_1(\sigma n) = \sigma^{-1}\sigma n = n$ .

2.  $\sigma_1 \in N(\sigma) : f_2 \circ f_1(\sigma_1) = f_2(\sigma^{-1}\sigma_1) = \sigma\sigma^{-1}\sigma_1 = \sigma_1$ .

3. Так как  $N_\sigma, N(\sigma)$  — конечные множества, то из взаимнообратности  $f_1, f_2$  следует  $|N_\sigma| = |N(\sigma)|$ . □

## 6. Понятие сигнатуры перестановки

Для дальнейшего изучения путей длины 2 (или нормальных перестановок), ведущих в тот же слой, требуется ещё одно вспомогательное средство, которое так же, как и характеристический граф, является способом классификации перестановок.

**Определение 6.1.** Пусть  $\sigma \in S_n$ . Сигнатурой  $p(\sigma)$  назовём последовательность из  $n - 1$  нулей и единиц, такую, что  $p(\sigma)[k] = 1 \Leftrightarrow (\sigma[k], \sigma[k + 1]) \in G_\sigma$ , т.е.  $k$ -ый элемент сигнатуры равен 1, тогда и только тогда, когда  $\sigma[k] > \sigma[k + 1]$ .

**Лемма 6.1.** Пусть  $\sigma_1 = \sigma\alpha$ , где  $\alpha = (k, k + 1)$ .

Тогда  $p(\sigma_1)$  отличается от  $p(\sigma)$  в  $k$ -ой позиции, может отличаться лишь в соседних с  $k$ -ой позициях, а во всех остальных позициях они тождественны.

*Доказательство.*

1.  $\sigma = [\dots, \sigma[k], \sigma[k + 1], \dots]$ . Тогда  $\sigma_1 = [\dots, \sigma[\alpha[k]], \sigma[\alpha[k + 1]], \dots] = [\dots, \sigma[k + 1], \sigma[k], \dots]$ .

2. Из этого сразу видно, что «возрастаетость-убываемость» может изменяться лишь у трёх пар(взятых как подпоследовательности из 2-х элементов) соседних элементов, а именно у стоящих в парах позиций:  $[k - 1, k]$ ,  $[k, k + 1]$ ,  $[k + 1, k]$ , причём в паре  $[k, k + 1]$  это свойство точно изменяется.

3. Поэтому изменяется  $k$ -ая позиция сигнатуры, а также могут меняться только её соседние(если они есть.)

□

**Примечание.** Словом «возрастаемость-убываемость» обозначена абстракция общего рода от двух видов «возрастаемость» и «убываемость», которые соответственно субстантивированные свойства последовательности возрастать или убывать. То что «возрастаемость-убываемость» последовательности изменилась означает, что эта последовательность из убывающей стала возрастающей или обратно.

Далее мы установим некое соответствие между сигнатурой и нормальными перестановками (а значит и путями длины 2, ведущими в тот же слой).

**Определение 6.2.**  $A_\sigma$  — это множество пар позиций элементов сигнатуры  $p(\sigma)$ , которые не стоят рядом и имеют нетождественные значения, то есть множество пар вида  $10, 01$ . Порядок в паре не важен.

**Лемма 6.2.**  $|N_\sigma^1| = |A_\sigma|$ .

*Доказательство.*

I.  $f_1 : A_\sigma \rightarrow N_\sigma^1$

1. Пусть пара позиций  $\{x, y\} \in A_\sigma$ , т.е.  $p(\sigma)[x] \neq p(\sigma)[y]$ ,  $|x - y| > 1$ .
2. Сопоставим ей двушаговую перестановку  $n = (x, x + 1)(y, y + 1)$ .
3. Так как  $|x - y| > 1$ , то  $n$  — коммутативная двушаговая перестановка.
4. Сначала рассмотрим например случай  $p(\sigma)[x] = 0, p(\sigma)[y] = 1$ .
5. По определениям:  $p(\sigma)[x] = 0 \Leftrightarrow (\sigma[x], \sigma[x + 1]) \notin G_\sigma \Leftrightarrow \sigma[x] < \sigma[x + 1]$
6.  $p(\sigma)[y] = 1 \Leftrightarrow (\sigma[y], \sigma[y + 1]) \in G_\sigma \Leftrightarrow \sigma[y] > \sigma[y + 1]$
7. Рассмотрим  $\sigma_1 = \sigma n = [\dots, \sigma[n[x]] \sigma[n[x + 1]], \dots, \sigma[n[y]] \sigma[n[y + 1]], \dots] = [\dots, \sigma[n[x + 1]] \sigma[n[x]], \dots, \sigma[n[y + 1]] \sigma[n[y]], \dots]$ .  
То есть домножение на  $n$  справа — это перестановка местами  $x, x + 1$  позиций и  $y, y + 1$  позиций.
8. А это означает, что  $G_{\sigma_1}$  было получено из  $G_\sigma$  добавлением ребра  $(\sigma[x], \sigma[x + 1])$  и удалением ребра  $(\sigma[y], \sigma[y + 1])$ . Общее число рёбер не изменилось,  $s(\sigma n) = s(\sigma)$ .
9. Откуда следует, что  $n$  — нормальная перестановка относительно  $\sigma$ . (в этом случае)
10. Случай с  $p(\sigma)[x] = 1, p(\sigma)[y] = 0$  разбирается аналогично: ребро  $(\sigma[x], \sigma[x + 1])$  удаляется, а ребро  $(\sigma[y], \sigma[y + 1])$  добавляется.

11. Итак,  $f_1(\{x, y\}) = (x, x + 1)(y, y + 1)$ .

II.  $f_2 : N_\sigma^1 \rightarrow A_\sigma$ .

1. Пусть теперь  $n = (x, x + 1)(y, y + 1)$ ,  $n \in N_\sigma^1$ .

2. Тогда сопоставим  $n \rightarrow \{x, y\}$  (пара).

3. И так как  $n$  коммутативно, то  $|x - y| > 1$ .

4. Предположим, что  $p(\sigma)[x] = p(\sigma)[y] = 0$ . Тогда  $(\sigma[x], \sigma[x + 1]), (\sigma[y], \sigma[y + 1]) \notin G_\sigma$ .

5. Но тогда  $G_{\sigma n}$  получено из  $G_\sigma$  добавлением двух этих рёбер. (см. I.7). Откуда  $s(\sigma n) = s(\sigma) + 2$ ,  $s(\sigma n) \neq s(\sigma)$ , что противоречит нормальности  $n$ .

6. Аналогично, если  $p(\sigma)[x] = p(\sigma)[y] = 1$ , то эти же два ребра удаляются, откуда  $s(\sigma n) = s(\sigma) - 2$ ,  $s(\sigma n) \neq s(\sigma)$ , что противоречит нормальности  $n$ .

7. По п.5,6 получаем  $p(\sigma)[x] \neq p(\sigma)[y]$ , т.е. (совокупно с п.3)  $\{x, y\} \in A_\sigma$

8. Итак,  $f_2((x, x + 1)(y, y + 1)) = \{x, y\}$ .

III. Взаимнообратность  $f_1, f_2$  очевидна, откуда  $|N_\sigma^1| = |A_\sigma|$ .

□

## 7. Сигнатура и нормальные некоммутативные перестановки

Нормальность рассматривается относительно предзаданного  $\sigma$ .

Некоммутативные нормальные перестановки имеются, как известно по определению, двух типов:

**Определение 7.1.** *Первого типа*  $\alpha_i^1 = (i, i + 1)(i + 1, i + 2)$ .

**Определение 7.2.** *Второго типа*  $\alpha_i^2 = (i + 1, i + 2)(i, i + 1)$ , где  $i$  пробегает значения от 1 до  $n - 2$ .

Установим далее, при каких условиях на  $\sigma$  выполнено  $\alpha_i^1, \alpha_i^2 \in N_\sigma^2$ .

Домножение на  $\alpha_i^1$ :

$$\sigma \alpha_i^1 = [\dots, \sigma[i] \sigma[i + 1] \sigma[i + 2], \dots](i, i + 1)(i + 1, i + 2) = [\dots, \sigma[i + 1] \sigma[i] \sigma[i + 2], \dots](i + 1, i + 2) = [\dots, \sigma[i + 1] \sigma[i + 2] \sigma[i], \dots]$$

И следовательно  $G_{\sigma \alpha_i^1}$  получено из  $G_\sigma$  инверсией наличия рёбер  $(\sigma[i], \sigma[i + 1])$ ,  $(\sigma[i], \sigma[i + 2])$ . Поэтому для того, чтобы  $s(\sigma \alpha_i^1) = s(\sigma)$  (т.е.  $\alpha_i^1 \in N_\sigma^2$ ), нужно, чтобы одно и только одно из этих рёбер было в  $G_\sigma$ .

Домножение на  $\alpha_i^2$ :

$$\sigma\alpha_i^2 = [\dots, \sigma[i] \sigma[i+1] \sigma[i+2], \dots](i+1, i+2)(i, i+1) = [\dots, \sigma[i] \sigma[i+2] \sigma[i+1], \dots](i, i+1) = [\dots, \sigma[i+2] \sigma[i] \sigma[i+1], \dots]$$

И следовательно  $G_{\sigma\alpha_i^2}$  получено из  $G_\sigma$  инверсией наличия рёбер  $(\sigma[i+2], \sigma[i]), (\sigma[i+2], \sigma[i+1])$ . Поэтому для того, чтобы  $s(\sigma\alpha_i^2) = s(\sigma)$  (т.е.  $\alpha_i^2 \in N_\sigma^2$ ) нужно, чтобы одно и только одно из этих рёбер было в  $G_\sigma$ .

Далее будем использовать эти установленные критерии нормальности.

**Лемма 7.1.** Пусть  $p(\sigma)[i] = p(\sigma)[i+1] = 0$ . Тогда  $\alpha_i^1, \alpha_i^2 \notin N_\sigma^2$ .

*Доказательство.*

1. Из условий следует, что  $\sigma[i] < \sigma[i+1] < \sigma[i+2]$ .
2. Откуда  $(\sigma[i], \sigma[i+1]) \notin G_\sigma, (\sigma[i], \sigma[i+2]) \notin G_\sigma$ . И следовательно  $\alpha_i^1 \notin N_\sigma^2$ .
3. Также  $(\sigma[i], \sigma[i+2]) \notin G_\sigma, (\sigma[i+1], \sigma[i+2]) \notin G_\sigma$ . И следовательно  $\alpha_i^2 \notin N_\sigma^2$ .

□

**Лемма 7.2.** Пусть  $p(\sigma)[i] = p(\sigma)[i+1] = 1$ . Тогда  $\alpha_i^1, \alpha_i^2 \notin N_\sigma^2$ .

*Доказательство.*

1. Из условий следует, что  $\sigma[i] > \sigma[i+1] > \sigma[i+2]$ .
2. Откуда  $(\sigma[i], \sigma[i+1]) \in G_\sigma, (\sigma[i], \sigma[i+2]) \in G_\sigma$ . И, следовательно,  $\alpha_i^1 \notin N_\sigma^2$ .
3. Также  $(\sigma[i], \sigma[i+2]) \in G_\sigma, (\sigma[i+1], \sigma[i+2]) \in G_\sigma$ . И, следовательно,  $\alpha_i^2 \notin N_\sigma^2$ .

ч.т.д.

□

**Лемма 7.3.** Пусть  $p(\sigma)[i] = 0, p(\sigma)[i+1] = 1$ . Тогда одна и только одна из перестановок  $\alpha_i^1, \alpha_i^2$  нормальна.

*Доказательство.*

1. По условию  $\sigma[i] < \sigma[i+1] > \sigma[i+2]$ .
2. Далее разберём два возможных случая:  $\sigma[i] < \sigma[i+2]$  и  $\sigma[i] > \sigma[i+2]$ .
  - I.  $\sigma[i] < \sigma[i+2]$ 
    1. Тогда  $(\sigma[i], \sigma[i+1]) \notin G_\sigma, (\sigma[i+1], \sigma[i+2]) \in G_\sigma, (\sigma[i], \sigma[i+2]) \notin G_\sigma$ .
    2. Откуда  $\alpha_i^1 \notin N_\sigma^2, \alpha_i^2 \in N_\sigma^2$ .
  - II.  $\sigma[i] > \sigma[i+2]$ 
    1. Тогда  $(\sigma[i], \sigma[i+1]) \notin G_\sigma, (\sigma[i+1], \sigma[i+2]) \in G_\sigma, (\sigma[i], \sigma[i+2]) \in G_\sigma$ .
    2. Откуда  $\alpha_i^1 \in N_\sigma^2, \alpha_i^2 \notin N_\sigma^2$ .

□

**Лемма 7.4.** Пусть  $p(\sigma)[i] = 1, p(\sigma)[i+1] = 0$ . Тогда одна и только одна из перестановок  $\alpha_i^1, \alpha_i^2$  нормальна.

*Доказательство.*

1. По условию  $\sigma[i] > \sigma[i+1] < \sigma[i+2]$ .
2. Далее разберём два возможных случая:  $\sigma[i] < \sigma[i+2]$  и  $\sigma[i] > \sigma[i+2]$ .
  - I.  $\sigma[i] < \sigma[i+2]$ 
    1. Тогда  $(\sigma[i], \sigma[i+1]) \in G_\sigma, (\sigma[i+1], \sigma[i+2]) \notin G_\sigma, (\sigma[i], \sigma[i+2]) \notin G_\sigma$ .
    2. Откуда  $\alpha_i^1 \in N_\sigma^2, \alpha_i^2 \notin N_\sigma^2$ .
  - II.  $\sigma[i] > \sigma[i+2]$ 
    1. Тогда  $(\sigma[i], \sigma[i+1]) \in G_\sigma, (\sigma[i+1], \sigma[i+2]) \notin G_\sigma, (\sigma[i], \sigma[i+2]) \in G_\sigma$ .
    2. Откуда  $\alpha_i^1 \notin N_\sigma^2, \alpha_i^2 \in N_\sigma^2$ .

□

Таким образом, для любых двух соседних тождественных позиций транспозиций соответствующие некоммутативные перестановки не являются нормальными, а для соседних нетождественных нормальной является одна из двух некоммутативных (соответствующих).

Обозначим через  $B_\sigma$  множество пар (порядок в паре не важен) соседних позиций сигнатуры  $p(\sigma)$  с нетождественными значениями в этих позициях.

Совокупно доказана:

**Теорема 7.1.**  $|B_\sigma| = |N_\sigma^2|$

Пусть  $ind(\sigma)$  количество единиц среди элементов сигнатуры  $p(\sigma)$ , а  $C_\sigma$  — количество пар (порядок не важен) позиций сигнатуры  $p(\sigma)$  с нетождественными значениями.

Тогда, с одной стороны,  $C_\sigma = A_\sigma \sqcup B_\sigma \Rightarrow |C_\sigma| = |A_\sigma| + |B_\sigma| = |N_\sigma^1| + |N_\sigma^2| = |N_\sigma|$

А с другой, выбирая из  $p(\sigma)$   $ind(\sigma)$  единиц и  $n - 1 - ind(\sigma)$  нулей, получаем  $|C_\sigma| = ind(\sigma)(n - 1 - ind(\sigma))$ .

Окончательный результат:

**Теорема 7.2.** При  $\sigma \in G_k, deg_{G_k}(\sigma) = |N_\sigma| = |C_\sigma| = ind(\sigma)(n - 1 - ind(\sigma))$ .

## 8. Послойный код

Применим вышеполученный теоретический результат.

Так как  $\sigma \in S_{n,k}$  может быть смежна лишь с перестановками из соседних слоёв  $k - 1$ ,  $k + 1$ , то в  $S_n$  можно построить следующий код, исправляющий одну ошибку (т.е. независимое множество в  $(S_n)^2$ ):

Возьмём слои 0-ой, 3-ий, 6-ой и так далее. В каждом найдём независимое множество в графе  $G_{3k}$ , и потом получим код как объединение этих независимых множеств.

Аналогично такого же рода код получится с 1-ым, 4-ым, 7-ым ( $3k + 1$ ) и т.д. слоями, а также 2-ым, 5-ым, 8-ым и т.д. ( $3k + 2$ )

Построив эти три кода, можно выбрать из них больший код. Так как теперь нам известны степени вершин в  $G_k$ , то мы можем произвести оценку мощности этих кодов.

Из теории графов известно (см. например [2], теорема 25.1), что  $\alpha_0(G) \geq \sum_{\sigma \in V} \frac{1}{1 + \deg(\sigma)}$ , где  $\alpha_0(G)$  — число независимости графа  $G$ ,  $\deg(\sigma)$  — степень вершины  $\sigma$ .

**Следствие 8.1.**  $\alpha_0(G_k) \geq \sum_{\sigma \in S_{n,k}} \frac{1}{1 + \text{ind}(\sigma)(n-1 - \text{ind}(\sigma))}$

**Определение 8.1.** Вклад перестановки  $\sigma$ :  $R(\sigma) = \frac{1}{1 + \text{ind}(\sigma)(n-1 - \text{ind}(\sigma))}$

**Определение 8.2.** Число  $k$ -ого слоя:  $h_k = \sum_{\sigma \in S_{n,k}} R(\sigma)$ .

Таким образом,  $\alpha_0(G_k) \geq h_k$ .

Как уже известно, всего слоёв  $\frac{n(n-1)}{2} + 1$ .

Пусть

$$H_0 = \sum_{0 \leq 3k \leq \frac{n(n-1)}{2}} h_{3k},$$

$$H_1 = \sum_{0 \leq 3k+1 \leq \frac{n(n-1)}{2}} h_{3k+1},$$

$$H_2 = \sum_{0 \leq 3k+2 \leq \frac{n(n-1)}{2}} h_{3k+2}.$$

По построению, мощности первого, второго и третьего кодов соответственно не меньше  $\lceil H_0 \rceil$ ,  $\lceil H_1 \rceil$ ,  $\lceil H_2 \rceil$ . ( $\lceil x \rceil$  — операция округления вверх).

Алгоритм расчёта  $H_0$ ,  $H_1$ ,  $H_2$ :

1) Проходим по всем перестановкам  $\sigma \in S_n$ , с каждой из которых делаем следующее:

2) Вычисляем её слой  $s(\sigma)$ , и вклад в сумму  $R(\sigma)$ .

3) В зависимости от  $s(\sigma) \bmod 3$ , прибавляем этот вклад (соответственно остаткам 0, 1, 2) в накопители  $H_0, H_1, H_2$  (начальное их значение, разумеется, 0).

И так как этот алгоритм проходит по всем  $\sigma \in S_n$  по одному разу, а деление вкладов  $R(\sigma)$  между суммами  $H_0, H_1, H_2$  дизъюнктивно, то данный алгоритм, работающий линейное относительно  $|S_n|$  время (пренебрегая сложностью вычисления  $ind(\sigma), s(\sigma)$ ), действительно их вычислит.

Алгоритмы вычисления  $ind(\sigma), s(\sigma)$  элементарны.

Были проведены испытания для пространств  $S_3 - S_9$ .

Получена следующая таблица результатов:

	$S_3$	$S_4$	$S_5$	$S_6$	$S_7$	$S_8$	$S_9$
$[H_0]$	2	4	10	38	184	1086	7532
$[H_1]$	1	3	10	37	183	1086	7531
$[H_2]$	1	3	9	37	183	1085	7531

## 9. Симметрические слои

Строение  $S_n$  может быть рассматриваемо и ещё с одной точки зрения: с точки зрения разбиения его на такие слои-подграфы, каждый из которых является графом строения  $S_{n-1}$  (в модели ошибки 1).

**Определение 9.1.**  $k$ -ый симметрический слой  $S_{n/k} = \{\sigma \in S_n \mid \sigma[1] = k\}$

Очевидно, что как подграф  $S_{n/k} \cong S_{n-1}$ , так как можно абстрагироваться от первой позиции, а перестановка соседних оставшихся (со 2-ой по  $n$ -ую) непосредственно является перестановкой соседних в исходном  $S_n$ .

Итак,  $S_n = S_{n/1} \sqcup \dots \sqcup S_{n/n}$ .

Пусть  $\sigma \in S_{n/k}$ . Тогда оно смежно с  $n - 1$  другими перестановками:  $n - 2$  из того же симметрического слоя  $S_{n/k}$ , а с одной из другого  $S_{n/k'}$ , причём  $k' = \sigma[2]$ .

Но  $S_{n/k}$  в силу изоморфности  $S_{n-1}$  само разбивается на симметрические слои второго порядка, каждый из которых изоморфен  $S_{n-2}$ , причём принадлежность к определённому слою определена значением  $\sigma[2]$ .

$$S_{n/k} = S_{n/k/1} \sqcup \dots \sqcup S_{n/k/k-1} \sqcup S_{n/k/k+1} \sqcup \dots \sqcup S_{n/k/n}$$

Каждая вершина  $\sigma \in S_{n/k/k'}$   $n - 3$  ребрами соединена с вершинами из этого же подслоя, одним ребром — с вершиной из  $S_{n/k/k'_1}$  (т.е. этого

же слоя, но другого подслоя), а ещё одним — с вершиной из  $S_{n/k'/k}$  (эта вершина получается из данной перестановкой  $\sigma[1], \sigma[2]$ ).

Теперь же рассмотрим пары  $(k, k')$ ,  $k, k' \in \{1, \dots, n\}$ ,  $k \neq k'$ , а также подслои  $S_{n/k/k'}$ ,  $S_{n/k'/k}$ , то есть разобьём  $S_n$  на пары таких вот подслоёв.

Переход между этими подслоями осуществляется перестановкой первой и второй позиций, движение в самих слоях — перестановками всех остальных. Ясно, что эти два движения независимы друг от друга.

[Коммутация: если  $\alpha(1) = 1$ ,  $\alpha(2) = 2$ , то  $\alpha(12) = (12)\alpha$ ].

**Определение 9.2.** Пусть  $G = (V, E)$  — некоторый граф. Призмой этого графа  $G \times 2 = (V_1, E_1)$  назовём граф, у которого  $V_1 = \{(g, i) \mid g \in V, i \in \{0, 1\}\}$ , а  $((g_1, i_1), (g_2, i_2)) \in E_1 \Leftrightarrow$  или  $i_1 = i_2$ , и  $(g_1, g_2) \in E$ ; или  $i_1 \neq i_2$ , и  $g_1 = g_2$ .

Чтобы получить призму, нужно взять два экземпляра  $G$ , и соединить рёбрами одни и те же вершины в этих экземплярах.

Таким образом, подграф  $S_{n/k/k'} \sqcup S_{n/k'/k}$  образует призму вида  $S_{n-1} \times 2$ . Всего таких пар подслоёв  $\frac{n(n-1)}{2}$  штук, то есть  $S_n$  разбивается на  $\frac{n(n-1)}{2}$  призм вида  $S_{n-2} \times 2$ .

## 10. Разбиения

Дадим способ оценки сверху мощности кода. Для этого введём понятие разбиения и рассмотрим вышеопределённое разбиение  $S_n$  на призмы.

**Определение 10.1.**  $G = (V, E)$ ,  $V = V_1 \sqcup \dots \sqcup V_r$ . Разбиением  $G$  называются подграфы  $G_1, G_2, \dots, G_r$ ,  $G_i = (V_i, E_i)$ ,  $(a, b) \in E_i \Leftrightarrow a, b \in V$  и  $(a, b) \in E$ .

**Определение 10.2.** Кодовое число  $k(G) = \alpha_0(G^2)$  — это мощность максимального кода на  $G$ , исправляющего 1 ошибку.

**Лемма 10.1.** Пусть  $G_1, G_2, \dots, G_r$  — разбиение графа  $G$ . Тогда  $k(G) \leq k(G_1) + k(G_2) + \dots + k(G_r)$ .

*Доказательство.*

1. Дано  $G = (V, E)$ ,  $V = V_1 \sqcup V_2 \sqcup \dots \sqcup V_r$ ,  $G_i = (V_i, E_i)$ . Пусть  $K \subset V$  — максимальный код, исправляющий одну ошибку ( $|K| = k(G)$ ), то есть  $K$  — максимальное независимое множество в  $G^2$ .

2. Положим  $K_i = K \cap V_i$ . Также зададим произвольные  $a, b \in K_i$ .

3. Предположим, что между  $a, b$  в  $G_i$  существует путь длины не более 2. Тогда этот путь будет также и путём в  $G$ , так как  $G_i$  подграф  $G$ . Но так как  $a, b \in K$ , то такого пути быть не может. Из противоречия следует, что  $K_i$  код в  $G_i$ .

4. И так как по определению  $|K_i| \leq k(G_i)$ , то  $k(G) = |K| = |K_1| + |K_2| + \dots + |K_r| \leq k(G_1) + k(G_2) + \dots + k(G_r)$ .

□

Применительно к разбиению  $S_n$  на призмы  $S_{n-1} \times 2$  получаем оценку:

**Теорема 10.1.**  $k(S_n) \leq \frac{n(n-1)}{2} k(S_{n-2} \times 2)$ .

Например  $k(S_5) \leq 10k(S_3 \times 2) = 20$  (а оценка сверху совершенным кодом была бы  $\leq 24$ ), так как  $S_3 \times 2$  — это шестиугольная призма, и нетрудно убедиться, что её кодовое число действительно равно 2.

**Примечание.** Все эти рассуждения переносятся и на рассмотрение кода с большим числом ошибок.

**Примечание.** Однако, в применении к  $S_6$  и далее эта оценка оказывается бесполезной, так как она слабее соответствующей оценки совершенного кода.

## 11. Произведение графов. Разбиение $S_n$ на произведения

Введенные выше понятия и полученные результаты поддаются обобщению.

**Определение 11.1.** Пусть  $G_1 = (V_1, E_1)$ ,  $G_2 = (V_2, E_2)$  — графы. Их произведением  $G_1 \times G_2 = (V, E)$  назовём граф, где  $V = V_1 \times V_2$ , и при  $g_1, g'_1 \in V_1$ ;  $g_2, g'_2 \in V_2$  ребро  $((g_1, g_2), (g'_1, g'_2)) \in E \Leftrightarrow$   
или  $g_1 = g'_1$ , и  $(g_2, g'_2) \in E_2$ ;  
или  $g_2 = g'_2$ , и  $(g_1, g'_1) \in E_1$

Понятие призмы графа  $G \times 2$  оказывается частным случаем — это произведение графа на отрезок типа 0-1.

Теперь мы можем рассматривать последовательность  $\sigma[1], \dots, \sigma[n]$  следующим образом: разобьём её на последовательные отрезки длин  $n_1, n_2, \dots, n_p$ ;  $n_1 + n_2 + \dots + n_p = n$ , то есть:

$$\sigma_1 = \sigma[1], \dots, \sigma[n_1]$$

$$\sigma_2 = \sigma[n_1 + 1], \dots, \sigma[n + 1 + n_2]$$

...

$$\sigma_p = \sigma[n_1 + \dots + n_{p-1}], \dots, \sigma[n_1 + \dots + n_p]$$

И далее, разобьём все перестановки, применённые к данной последовательности, на 2 класса: сохраняющие элементный состав всех отрезков  $\sigma[1], \dots, \sigma[p]$  и все остальные.

Перестановка первого класса может быть разложена на произведение коммутирующих множителей  $\alpha_1, \dots, \alpha_p$ , где  $\alpha_i$  переставляет элементы лишь внутри отрезка  $\sigma[i]$  и нигде более.

И поэтому результаты применения перестановок первого класса на  $\sigma$  совокупно образуют подграф в  $S_n$ .

**Определение 11.2.** *Определим отношение  $\sim$  в данном разделе следующим образом:  $\sigma \sim \sigma'$  тогда и только тогда, когда  $\sigma' = \sigma\alpha$ , где  $\alpha$  — перестановка первого класса (т.е.  $\sigma_1$  и есть результат применения  $\alpha$  к  $\sigma$  как последовательности).*

**Лемма 11.1.** *Заданное отношение является отношением эквивалентности.*

*Доказательство.*

1.  $\sigma \sim \sigma$ , т.к.  $\sigma = \sigma e$ , а  $e$  сохраняет элементный состав всех  $\sigma_1, \dots, \sigma_p$ .
2.  $\sigma \sim \sigma' \Leftrightarrow \sigma' = \sigma\alpha \Leftrightarrow \sigma = \sigma'\alpha^{-1}$ . Перестановка  $\alpha$  — первого класса, значит и  $\alpha^{-1}$  тоже первого класса, так как если в одну сторону можно переставить позиции  $\sigma$ , сохраняя элементный состав  $\sigma_1, \dots, \sigma_p$ , то с этим же свойством это же можно сделать и в обратную сторону.
3.  $\sigma \sim \sigma', \sigma' \sim \sigma'' \Rightarrow \sigma'' = \sigma'\alpha_1 = \sigma\alpha_2\alpha_1$ . После применения каждой из  $\alpha_1, \alpha_2$  к  $\sigma$  элементный состав  $\sigma_1, \dots, \sigma_p$  не изменился, и, следовательно, это же верно и для  $\alpha_1\alpha_2$ .

□

Таким образом, существует разбиение  $S_n$  на подграфы, каждый из которых изоморфен  $S_{n_1} \times S_{n_2} \times \dots \times S_{n_p}$ . Мощность множества  $|S_{n_1} \times S_{n_2} \times \dots \times S_{n_p}| = n_1! \dots n_p!$

Следовательно, всего таких подграфов в разбиении  $\frac{n!}{n_1! \dots n_p!}$ , и аналогично предыдущему пункту получаем:

**Теорема 11.1.**  $k(S_n) \leq \frac{n!}{n_1! \dots n_p!} k(S_{n_1} \times S_{n_2} \times \dots \times S_{n_p})$

## 12. Вложение в $E_{\frac{n(n-1)}{2}}$

Приведем ещё один результат, имеющий отношение к задаче построения кода.

Каждый характеристический граф  $G_\sigma$  задаётся наличием/отсутствием каждого из рёбер между парами вершин из  $\{1, 2, 3, \dots, n\}$ , а общее число этих рёбер равно  $\frac{n(n-1)}{2}$ .

Поэтому  $G_\sigma$  может быть рассматриваемо как последовательность из  $\frac{n(n-1)}{2}$  нулей и единиц, где  $G_\sigma[i] = 1 \Leftrightarrow i$ -ое ребро лежит в  $G_\sigma$ .

Каждой перестановке  $\sigma \in S_n$  соответствует характеристический граф  $G_\sigma$ , причём, как это было доказано (см. лемму о единственности), разным  $\sigma_1, \sigma_2$  соответствуют разные характеристические графы  $G_{\sigma_1}, G_{\sigma_2}$ , и, следовательно, и разные последовательности из  $\frac{n(n-1)}{2}$  нулей и единиц.

$E_{\frac{n(n-1)}{2}}$  рассматривается как граф, а смежно с  $b$  в  $E_{\frac{n(n-1)}{2}} \Leftrightarrow a, b$  отличаются в одной позиции.

Таким образом, получается некое инъективное отображение  $f : S_n \rightarrow E_{\frac{n(n-1)}{2}}$ .

**Лемма 12.1.**  $\sigma_1 \sim \sigma_2$  (в смысле смежности в  $S_n$ )  $\Rightarrow f(\sigma_1) \sim f(\sigma_2)$  (в смысле смежности в  $E_{\frac{n(n-1)}{2}}$ , т.е. отличия в одной позиции)

*Доказательство.*

1. Пусть  $\sigma_1 \sim \sigma_2$ . Тогда их характеристические графы  $G_{\sigma_1}, G_{\sigma_2}$  отличаются на одно ребро.

2. И, следовательно,  $f(\sigma_1)$  отличается от  $f(\sigma_2)$  лишь в одной позиции.  $\square$

**Определение 12.1.** *Порядковый граф перестановки  $\hat{G}_\sigma$  — это полный ориентированный граф на вершинах  $\{1, 2, 3, \dots, n\}$ , рёбра которого идут от вершины, номер которой стоит левее в последовательности  $[\sigma[1], \dots, \sigma[n]]$ , к номеру вершины, стоящей в ней же правее.*

Характеристический и порядковый графы связаны по следующему правилу: если  $(a, b) \notin G_\sigma$ , то в  $\hat{G}_\sigma(a, b)$  идёт от меньшего значения к большему, а иначе наоборот.

И, следовательно, инверсия направления одного ребра  $(a, b)$  в  $G_\sigma$  приводит к смене направления у  $(a, b)$  в  $\hat{G}_\sigma$ .

И при этом всегда получается направленный цикл, когда это происходит с ребром  $(\sigma[i], \sigma[j])$  (для определённости считаем, что  $i < j$ ; а иначе в рассмотрении переставим в этом ребре вершины местами), где  $j - i > 1$ ,

потому что в порядковом графе задана как цепочка  $\sigma[i] \rightarrow \sigma[k] \rightarrow \sigma[j]$  для некоторого  $k: i < k < j$ , так и ребро  $\sigma[i] \rightarrow \sigma[j]$  (и именно поэтому замена этого ребра на  $\sigma[j] \rightarrow \sigma[i]$  создаёт 3-цикл). Что несовместимо с транзитивностью.

**Следствие 12.1.** *Инверсия наличия одного ребра, не являющегося ребром вида  $(\sigma[i], \sigma[i+1])$ , делает граф из характеристического  $G_\sigma$  таким, который вообще не есть характеристический граф какой-нибудь перестановки  $\sigma \in S_n$ .*

**Лемма 12.2.** *(обратное утверждение)  $f(\sigma_1) \sim f(\sigma_2) \Rightarrow \sigma_1 \sim \sigma_2$ .*

*Доказательство.*

1.  $f(\sigma_1) \sim f(\sigma_2) \Rightarrow G_{\sigma_1}, G_{\sigma_2}$  отличаются на одно ребро (ребро  $\sigma \equiv$  позиция  $G_\sigma$ ).
2. По вышедоказанному, так как это характеристические графы, то  $G_{\sigma_2}$  может быть получено из  $G_{\sigma_1}$  лишь инверсией ребра вида  $(\sigma[i], \sigma[i+1])$ .
3. А это означает, что  $\sigma_2$  получена из  $\sigma_1$  перестановкой  $i$  и  $i+1$ -ых позиций.  $\Rightarrow \sigma_1 \sim \sigma_2$ .

□

Таким образом, в  $E_{\frac{n(n-1)}{2}}$  есть подмножество  $T$ , такое что  $\left(E_{\frac{n(n-1)}{2}}\right)_{|T} \cong S_n$ .

**Лемма 12.3.** *Пусть  $K$  — независимое множество в  $\left(E_{\frac{n(n-1)}{2}}\right)^2$ .*

*Тогда  $K \cap T$  независимо в  $\left(\left(E_{\frac{n(n-1)}{2}}\right)_{|T}\right)^2$ .*

*Доказательство.*

1. Пусть  $a, b \in K \cap T$ . Предположим, что между  $a$  и  $b$  есть путь, рёбра которого лежат в  $\left(E_{\frac{n(n-1)}{2}}\right)_{|T}$ .
2. Тогда эти рёбра лежат и в  $E_{\frac{n(n-1)}{2}}$ , так как это подграф.
3. Но наличие пути длины не более 2 в  $E_{\frac{n(n-1)}{2}}$  между  $a, b \in K$  противоречит независимости  $K$  в  $\left(E_{\frac{n(n-1)}{2}}\right)^2$ .

□

Аналогично и для кодов с большим числом ошибок.

Это даёт нам некий метод построения кодов в  $S_n$ : строим сначала код в  $E_{\frac{n(n-1)}{2}}$  (а таких кодов известно много — ими занимается обычная теория кодирования), а потом ограничиваем построенный код на подмножество  $T$ .

Однако,  $|S_n| = n!$ , а  $\left|E_{\frac{n(n-1)}{2}}\right| = 2^{\frac{n(n-1)}{2}}$ . И поэтому  $\frac{|S_n|}{\left|E_{\frac{n(n-1)}{2}}\right|} \rightarrow 0$ , что при больших  $n$  создаёт затруднения того вида, что «элементы кода будут попадать в  $T$  с исчезающе малой вероятностью».

### 13. Алгебраические коды

При исследовании был непреднамеренно получен побочный результат алгебраического характера, имеющий отношение к строению подгрупп  $H \subset S_n$ .

**Определение 13.1.** Код  $K \subset S_n$  назовём алгебраическим, если он является подгруппой  $S_n$  относительно операции перемножения перестановок.

**Лемма 13.1.** Подгруппа  $H \subset S_n$  является алгебраическим кодом, исправляющим одну ошибку, тогда и только тогда, когда она не содержит простых перестановок (см. 4.1.3).

*Доказательство.*

1. Пусть  $\alpha$  — простая перестановка, такая что  $\alpha \in H$ .
2. Тогда  $e, \alpha \in H$  ( $H$  — подгруппа),  $\alpha = e\alpha$ .
3. А значит,  $\alpha$  как последовательность получена из  $e = [1, \dots, n]$  применением простой перестановки  $\alpha$ .
4. То есть, между элементами  $e$  и  $\alpha$  есть путь (в терминах модели ошибки 1) длины не более чем 2. Откуда немедленно следует, что  $H$  — не код.
5. Обратное, пусть  $H$  — не код. Тогда есть такие  $g_1, g_2 \in H$ , между которыми есть путь длины не более 2.
6. Что равносильно тому, что  $g_2 = g_1\alpha$ , где  $\alpha$  — некая простая перестановка.
7. Но это означает, что  $\alpha = g_1^{-1}g_2 \in H$  (в силу свойств подгруппы).

□

В оценках из [1] было установлено, что всякий код в  $S_n$ , исправляющий одну ошибку, содержит не более  $(n - 1)!$  элементов.

**Следствие 13.1.** Пусть  $H \subset S_n$  — подгруппа,  $|H| > (n - 1)!$

Тогда  $H$  содержит простую перестановку, т.е. или транспозицию двух соседних, или произведением двух таких одношаговых перестановок.

Данный результат может быть обобщён и на большее количество ошибок.

**Теорема 13.1.** Если  $H \subset S_n$  — подгруппа и  $|H| > q_{err}$ , где  $q_{err}$  — ограничение сверху на код, исправляющий  $err$  ошибок, то  $H$  среди своих элементов содержит произведение не более чем  $2err$  одношаговых перестановок.

Доказательство аналогично: достаточно заменить понятие «простая перестановка» на понятие «произведение не более  $2err$  одношаговых».

## Список литературы

- [1] Казаков И. Б. Кодирование в скрытом канале перестановки пакетов // Программная инженерия. — 2018. — Т. 9, №4. — С. 163–173.
- [2] Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич Р.И. Лекции по теории графов. М.: Наука, 1990. 384 с.

## The structure of a graph induced on the set of permutations $S_n$ by an error model of a covert channel based on packet permutations Kazakov I.B.

The paper I.B. Kazakov, “Encoding in a covert channel of packet permutations” introduced a number of error models for codes over sets of permutations. Such error models induce graph structure on sets of permutations. Our research is focused on properties of these graphs. We show that the graphs consist of layers of independent sets; the layer that contains the given permutation is determined by the number of edges in the characteristic graph of the permutation. We estimate vertex degrees in the layers of the graph  $(S_n)^2$  and use this estimate to bound the cardinality of an error-correcting layer-based code. After that we develop a number of aids that allow to obtain upper bounds of code cardinality. We introduce the notions of symmetric layers and graph partitions and decompose  $S_n$  for some values of  $n$  into prisms and into graph products, i.e. generalised prisms. We also embed the graph  $S_n$  into  $E_{\frac{n(n-1)}{2}}$ . Finally establish a connection between sizes

of subgroups  $H \subset S_n$  and presence of  $n$ -step permutations in these subgroups.

*Keywords:* permutations, graph structure, error-correcting code



**Часть 3.**  
**Математические модели**



# Решётка клонов трёхзначной логики, содержащих функции $0, 1, 2, \min, \max$

Моисеев С. В.

В настоящей работе дано полное описание решётки всех клонов трёхзначной логики, содержащих одновременно все константы  $0, 1, 2$  и функции  $\min, \max$ . Клоны описаны как множества сохранения предикатов.

**Ключевые слова:** теория клонов, решетка клонов, трёхзначная логика.

**Теорема.** *Существует ровно 33 клон трёхзначной логики, содержащих функции  $0, 1, 2, \min, \max$ . Решётка клонов по включению представлена на диаграмме Хассе (рис. 1). Вершине  $v$  диаграммы соответствует класс сохранения множества всех предикатов, указанных на стрелках всех путей от верхней точки диаграммы к вершине  $v$ .*

Верхней точке диаграммы 1 соответствует множество всех функций трёхзначной логики. Нижней точке диаграммы соответствует клон, порождённый функциями  $0, 1, 2, \min, \max$ . Стрелки на диаграмме направлены от клона к клону, предполному в нём. Для клона  $M'$ , у которого ровно один непосредственный надклон  $M$ , на стрелке от  $M$  к  $M'$  указан предикат, сохраняемый клоном  $M'$ , но не сохраняемый его надклоном  $M$ . Таким образом, все исследуемые клоны можно определить как классы сохранения какого-то подмножества десяти предикатов, указанных на диаграмме.

## 1. Основные понятия теории клонов

**Обозначение.** Арности предикатов и функций (при необходимости) в данной работе будем указывать в верхнем индексе после символа предиката/функции, например:  $p^{(n)}, f^{(r)}$ .

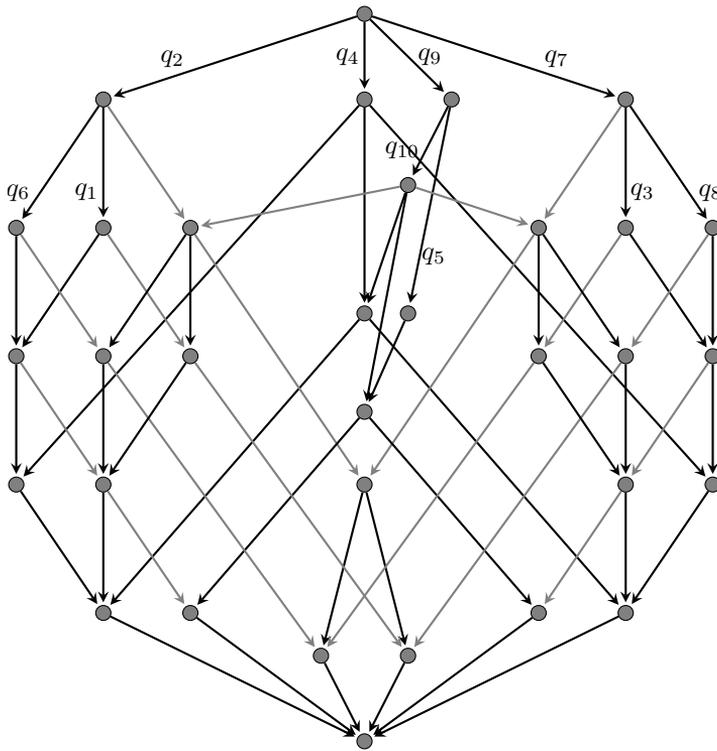


Рис. 1.

### 1.1. Клоны функций $k$ -значной логики

Пусть  $P_k$  — множество всех функций  $k$ -значной логики.

**Определение.** Пусть  $M \subseteq P_k$ . Определим множество  $[M]$  (замыкание множества  $M$  относительно суперпозиции) следующими аксиомами:

- 1) Для любых  $r \geq 1, j \in \{1, \dots, r\}$  множество  $[M]$  содержит функцию-проектор

$$pr_j^{(r)}: (x_1, \dots, x_r) \mapsto x_j.$$

- 2)  $(f \in M) \implies (f \in [M])$ .

$$\begin{aligned}
3) \quad & \llbracket f^{(n)} \in [M], f_1^{(r_1)} \in [M], \dots, f_n^{(r_n)} \in [M], \\
& \forall x_1 \dots \forall x_r \left( h^{(r)}(x_1, \dots, x_r) = \right. \\
& \qquad \qquad \qquad \left. = f^{(n)} \left( f_1^{(r_1)}(x_1, \dots, x_r), \dots, f_n^{(r_n)}(x_1, \dots, x_r) \right) \right) \\
& \rrbracket \implies h^{(r)} \in [M].
\end{aligned}$$

**Определение.** Множество  $M \subseteq P_k$  функций  $k$ -значной логики называется *клоном функций*, если

$$[M] = M.$$

## 1.2. Реляционные клоны

Обозначим через  $R_k$  множество всех предикатов на  $k$ -элементном множестве  $\{0, 1, \dots, k-1\}$ , т.е. множество всех функций вида

$$p: \{0, 1, \dots, k-1\}^n \rightarrow \{\perp, \top\},$$

где  $\perp, \top$  — константы «ложь», «истина».

Зафиксируем следующие предикаты из  $R_3$ :

$$\begin{aligned}
false^{(0)} & \quad (\text{константа «ложь»}) \\
true^{(0)} & \quad (\text{константа «истина»}) \\
eq^{(2)}: (x_1, x_2) & \mapsto (x_1 = x_2) \quad (\text{предикат равенства})
\end{aligned}$$

**Определение.** Пусть  $Q \subseteq R_k$  — множество предикатов. Определим множество  $[Q]_{p.p.}$  (*замыкание множества  $Q$  относительно примитивных позитивных формул*) следующими аксиомами:

$$\begin{aligned}
1) \quad & \{false^{(0)}, true^{(0)}, eq^{(2)}\} \subseteq [Q]_{p.p.} \\
2) \quad & (p \in Q) \implies (p \in [Q]_{p.p.}) \\
3) \quad & \llbracket p_1^{(r_1)} \in [Q]_{p.p.}, \dots, p_n^{(r_n)} \in [Q]_{p.p.}, \\
& \forall x_1 \dots \forall x_r \left( p^{(r)}(x_1, \dots, x_r) = \right. \\
& \qquad \qquad \qquad \left. = \exists y_1 \dots \exists y_s \left( p_1^{(r_1)}(z_{1,1}, \dots, z_{1,r_1}) \wedge \dots \wedge p_n^{(r_n)}(z_{n,1}, \dots, z_{n,r_n}) \right) \right) \\
& \rrbracket \implies p^{(r)} \in [Q]_{p.p.}
\end{aligned}$$

( $s \geq 0, n \geq 1, z_{k,j}$  обозначает один из символов « $x_1$ », ..., « $x_r$ », « $y_1$ », ..., « $y_s$ »).

**Определение.** Множество  $Q \subseteq R_k$  называется *реляционным клоном*, если

$$[Q]_{p.p.} = Q.$$

### 1.3. Связь между клонами функций и реляционными клонами

**Определение.** Скажем, что функция  $f^{(r)} \in P_k$  *сохраняет* предикат  $p^{(n)} \in R_k$ , если

$$(p^{(n)}(x_{1,1}, \dots, x_{1,n}) \wedge \dots \wedge p^{(n)}(x_{r,1}, \dots, x_{r,n})) \implies p^{(n)}(f^{(r)}(x_{1,1}, \dots, x_{r,1}), \dots, f^{(r)}(x_{1,n}, \dots, x_{r,n})).$$

Множество всех функций, сохраняющих каждый предикат множества  $Q \subseteq R_k$ , будем обозначать как  $Pol(Q)$ . Множество всех предикатов, сохраняемых всеми функциями из множества  $M \subseteq P_k$ , будем обозначать как  $Inv(M)$ .

**Теорема** (Гейгер [1]; Боднарчук и др. [2]).

$$\begin{aligned} Pol\ Inv\ M &= [M]; \\ Inv\ Pol\ Q &= [Q]_{p.p.} \end{aligned}$$

## 2. Клоны трёхзначной логики, содержащие функции 0, 1, 2, *min*, *max*, как классы сохранения множества предикатов

**Определение.** Будем говорить, что *множество  $M$  является классом сохранения множества предикатов  $Q$* , если  $M = Pol(Q)$ .

Классический подход к описанию клонов  $k$ -значной логики состоит в том, чтобы характеризовать их как классы сохранения множеств предикатов. Данный подход обоснован следующим фактом, являющимся следствием теоремы Гейгера–Боднарчука:

**Теорема.** Пусть  $M$  — клон  $k$ -значной логики. Тогда существует множество  $Q \subseteq R_k$  (возможно, бесконечное), такое что

$$M = Pol(Q).$$

## 2.1. Предикаты, характеризующие клоны трёхзначной логики, содержащие функции $0, 1, 2, \min, \max$

В соответствии с классическим подходом будем определять клоны трёхзначной логики, содержащие функции  $0, 1, 2, \min, \max$ , через множество предикатов, классом сохранения которых они являются. В нашем случае каждый клон может быть определён как класс функций, сохраняющих какое-то подмножество десяти предикатов арности 2, указанных в списке ниже. Каждый предикат этого списка определён через множество наборов, на которых он принимает значение «истина». Именно эти предикаты имеются в виду на диаграмме 1.

$q_1 = \{22, 11, 01, 00\}$	(частичный порядок $0 < 1$ )
$q_2 = \{22, 11, 10, 01, 00\}$	(эквивалентность $0 \sim 1$ )
$q_3 = \{22, 12, 11, 00\}$	(частичный порядок $1 < 2$ )
$q_4 = \{22, 12, 11, 02, 01, 00\}$	(линейный порядок $0 < 1 < 2$ )
$q_5 = \{22, 12, 11, 10, 00\}$	(частичный порядок $1 < 0, 1 < 2$ )
$q_6 = \{22, 12, 11, 10, 02, 01, 00\}$	(предпорядок $(0 \sim 1) < 2$ )
$q_7 = \{22, 21, 12, 11, 00\}$	(эквивалентность $1 \sim 2$ )
$q_8 = \{22, 21, 12, 11, 02, 01, 00\}$	(предпорядок $0 < (1 \sim 2)$ )
$q_9 = \{22, 21, 12, 11, 10, 01, 00\}$	(центральный предикат)
$q_{10} = \{22, 21, 12, 11, 10, 02, 01, 00\}$	(все наборы кроме 20)

## 2.2. Множества предикатов, классами сохранения которых являются клоны трёхзначной логики, содержащие функции $0, 1, 2, \min, \max$

Определим для каждой вершины  $v$  диаграммы 1 некоторое множество предикатов  $\pi(v) \subseteq \{q_1, \dots, q_{10}\}$ .

- 1) Верхней точке  $top$  диаграммы сопоставим пустое множество:

$$\pi(top) = \emptyset.$$

- 2) Пусть  $v'$  — вершина диаграммы, в которую входит ровно одно ребро из некоторой вершины  $v$ . В этом случае на диаграмме это ребро помечено некоторым предикатом  $p$ . Положим

$$\pi(v') = \pi(v) \cup \{p\}.$$

3) Пусть  $v'$  — вершина диаграммы, в которую входит несколько рёбер из некоторых вершин  $v_1, \dots, v_m$  ( $m \geq 2$ ). Положим

$$\pi(v') = \pi(v_1) \cup \dots \cup \pi(v_m).$$

Таким образом,  $\pi(v)$  совпадает со множеством всех предикатов, указанных на стрелках всех путей от верхней точки диаграммы 1 к вершине  $v$ . В частности, если  $v', v''$  — две различные вершины диаграммы, то  $\pi(v') \neq \pi(v'')$ .

Обозначим все вершины диаграммы через  $v_1, \dots, v_{33}$ , где нумерация вершин выбрана согласно формулам ниже. В частности,  $v_1$  — верхняя точка диаграммы,  $v_5$  — нижняя точка диаграммы.

$$\begin{aligned} \pi(v_1) &= \emptyset; \\ \pi(v_2) &= \{q_1, q_2\}; \\ \pi(v_3) &= \{q_2\}; \\ \pi(v_4) &= \{q_3, q_7\}; \\ \pi(v_5) &= \{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}; \\ \pi(v_6) &= \{q_2, q_3, q_6, q_7, q_9, q_{10}\}; \\ \pi(v_7) &= \{q_4\}; \\ \pi(v_8) &= \{q_1, q_2, q_4, q_6\}; \\ \pi(v_9) &= \{q_3, q_4, q_7, q_8\}; \\ \pi(v_{10}) &= \{q_5, q_9\}; \\ \pi(v_{11}) &= \{q_1, q_2, q_5, q_6, q_9, q_{10}\}; \\ \pi(v_{12}) &= \{q_3, q_5, q_7, q_8, q_9, q_{10}\}; \\ \pi(v_{13}) &= \{q_2, q_6\}; \\ \pi(v_{14}) &= \{q_1, q_2, q_6\}; \\ \pi(v_{15}) &= \{q_7\}; \\ \pi(v_{16}) &= \{q_1, q_2, q_7, q_8, q_9, q_{10}\}; \\ \pi(v_{17}) &= \{q_2, q_7, q_9, q_{10}\}; \\ \pi(v_{18}) &= \{q_7, q_8\}; \\ \pi(v_{19}) &= \{q_3, q_7, q_8\}; \end{aligned}$$

$$\begin{aligned}
\pi(v_{20}) &= \{q_9\}; \\
\pi(v_{21}) &= \{q_1, q_2, q_9, q_{10}\}; \\
\pi(v_{22}) &= \{q_2, q_9, q_{10}\}; \\
\pi(v_{23}) &= \{q_3, q_7, q_9, q_{10}\}; \\
\pi(v_{24}) &= \{q_4, q_9, q_{10}\}; \\
\pi(v_{25}) &= \{q_1, q_2, q_4, q_6, q_9, q_{10}\}; \\
\pi(v_{26}) &= \{q_3, q_4, q_7, q_8, q_9, q_{10}\}; \\
\pi(v_{27}) &= \{q_2, q_6, q_9, q_{10}\}; \\
\pi(v_{28}) &= \{q_1, q_2, q_6, q_9, q_{10}\}; \\
\pi(v_{29}) &= \{q_7, q_9, q_{10}\}; \\
\pi(v_{30}) &= \{q_7, q_8, q_9, q_{10}\}; \\
\pi(v_{31}) &= \{q_3, q_7, q_8, q_9, q_{10}\}; \\
\pi(v_{32}) &= \{q_9, q_{10}\}; \\
\pi(v_{33}) &= \{q_5, q_9, q_{10}\}.
\end{aligned}$$

### 3. Идея доказательства

Пусть  $Q_1, \dots, Q_{33}$  — множества предикатов, определённые для вершин  $v_1, \dots, v_{33}$  как описано в разделе 2.2, т. е.

$$Q_1 = \pi(v_1), \dots, Q_{33} = \pi(v_{33}).$$

Основной результат работы можно переформулировать следующим образом:

**Теорема.** *Множество всех клонов трёхзначной логики, содержащих функции 0, 1, 2, min, max, в точности совпадает со множеством клонов, являющихся классами сохранения множеств предикатов  $Q_1, \dots, Q_{33}$ , т. е. со множеством*

$$Pol(Q_1), \dots, Pol(Q_{33}).$$

Этот факт мы докажем, используя следующую логическую цепочку.

1. Вначале докажем, что для характеристики всех клонов трёхзначной логики, содержащих функции  $0, 1, 2, \min, \max$ , достаточно предикатов  $q_1, \dots, q_{10}$ , определённых в разделе 2.1; точнее, что справедлива следующая лемма:

**Лемма 1** (О предикатном базисе). *Если  $M$  — клон трёхзначной логики, содержащий функции  $0, 1, 2, \min, \max$ , то*

$$(\exists Q \subseteq \{q_1, \dots, q_{10}\}) (M = \text{Pol}(Q)).$$

2. Из леммы 1 следует, что существует максимум 1024 клонов трёхзначной логики, содержащих функции  $0, 1, 2, \min, \max$ . Покажем далее, что на самом деле их *не более чем 33*; точнее, что справедлива следующая лемма:

**Лемма 2** (О полноте решётки). *Для любого  $Q \subseteq \{q_1, \dots, q_{10}\}$  существует вершина  $v$  диаграммы, такая что*

$$\text{Pol}(Q) = \text{Pol}(\pi(v)).$$

3. В заключение, покажем, что клонов трёхзначной логики, содержащих функции  $0, 1, 2, \min, \max$ , *не менее чем 33*; точнее, что справедлива следующая лемма:

**Лемма 3.** *Пусть  $v', v''$  — две различные вершины диаграммы 1. Тогда*

$$\text{Pol}(\pi(v')) \neq \text{Pol}(\pi(v'')).$$

## 4. Доказательство леммы 1

1. Лемма 1 утверждает, что каждый клон  $M$  трёхзначной логики, содержащий функции  $0, 1, 2, \min, \max$ , может быть охарактеризован как класс сохранения какого-то подмножества предикатов  $q_1, \dots, q_{10}$ , определённых в разделе 2.1. Для доказательства этого факта покажем вначале, что каждый такой клон  $M$  может быть охарактеризован как класс сохранения какого-то множества предикатов арности 2, т. е. что

$$(\exists Q \subseteq R_3(2)) (M = \text{Pol}(Q)).$$

**Определение.** Функция  $f^{(r+1)} \in P_k$ , где  $r \geq 2$ , называется функцией почти-единогласия (*near-unanimity function, NUF*), если справедливо тождество:

$$f^{(r+1)}(x, y, \dots, y) = f^{(r+1)}(y, x, y, \dots, y) = \dots = f^{(r+1)}(y, \dots, y, x) = y.$$

**Теорема** (Бейкер, Пиксли [3]). Пусть  $M$  — клон, содержащий функцию почти-единогласия  $f^{(r+1)}$  арности  $r + 1$  ( $r \geq 2$ ). Тогда

$$(\exists Q \subseteq R_k(r)) (M = Pol(Q)),$$

где  $R_k(r)$  — множество всех предикатов  $k$ -значной логики арности  $\leq r$ .

Заметим, что каждый клон  $M$  трёхзначной логики, содержащий функции  $0, 1, 2, \min, \max$ , также содержит функцию голосования  $maj^{(3)}$ , определяемую тождеством:

$$maj^{(3)}(x_1, x_2, x_3) = \max(\max(\min(x_1, x_2), \min(x_2, x_3)), \min(x_3, x_1)).$$

Функция  $maj^{(3)}$  является функцией почти-единогласия арности 3, следовательно по теореме Бейкера—Пиксли

$$(\exists Q \subseteq R_3(2)) (M = Pol(Q)).$$

Покажем, что на самом деле

$$(\exists Q \subseteq \{q_1, \dots, q_{10}\}) (M = Pol(Q)).$$

**2.** Для удобства доказательства введём вспомогательную функцию  $\mu$ . В качестве  $\mu$  возьмём любую функцию, такую что для любого предиката  $p \in R_3(2)$ , сохраняемого функциями  $0, 1, 2, \min, \max$ , справедливо

$$(\mu(p) \subseteq \{q_1, \dots, q_{10}\}) \wedge ([\{p\}]_{p.p.} = [\mu(p)]_{p.p.}).$$

Существование функции  $\mu$  мы докажем далее в разделе 4.1.

Докажем теперь лемму 1. Пусть  $M$  — клон трёхзначной логики, содержащий функции  $0, 1, 2, \min, \max$ . Доказательство леммы 1 даёт следующая логическая цепочка:

$$1) (\exists Q \subseteq R_3(2)) (M = Pol(Q)) \text{ (по теореме Бейкера—Пиксли).}$$

- 2)  $Pol(Q) = Pol([Q]_{p.p.})$  (по теореме Гейгера—Боднарчука (см. раздел 1.3), так как

$$Pol(Q) = Pol Inv (Pol Q) = Pol (Inv Pol Q) = Pol([Q]_{p.p.}).$$

- 3)  $Q = \{s_1, \dots, s_m\}$  для некоторых предикатов  $s_1, \dots, s_m \in R_3(2)$  (так как  $Q \subseteq R_3(2)$  и поэтому конечно).
- 4)  $[Q]_{p.p.} = [\{s_1, \dots, s_m\}]_{p.p.} = [[\{s_1\}]_{p.p.} \cup \dots \cup \{\{s_m\}\}]_{p.p.}$  (по определению  $[ ]_{p.p.}$ ).
- 5) Так как  $M = Pol(\{\{s_1, \dots, s_m\}\}_{p.p.})$  и  $M$  содержит функции  $0, 1, 2, min, max$ , то все предикаты  $s_1, \dots, s_m$  сохраняются функциями  $0, 1, 2, min, max$ . Поэтому к ним можно применить функцию  $\mu$ :  $[[\{s_1\}]_{p.p.} \cup \dots \cup \{\{s_m\}\}]_{p.p.} = [[\mu(s_1)]_{p.p.} \cup \dots \cup \{\mu(s_m)\}]_{p.p.}$ .
- 6)  $[[\mu(s_1)]_{p.p.} \cup \dots \cup \{\mu(s_m)\}]_{p.p.} = [\mu(s_1) \cup \dots \cup \mu(s_m)]_{p.p.}$  (по определению  $[ ]_{p.p.}$ ).
- 7)  $[Q]_{p.p.} = [Q']_{p.p.}$ , где  $Q' = \mu(s_1) \cup \dots \cup \mu(s_m)$ .
- 8)  $Q' \subseteq \{q_1, \dots, q_{10}\}$  (по определению  $\mu$ ).
- 9)  $Pol([Q']_{p.p.}) = Pol(Q')$ .

#### 4.1. Существование вспомогательной функции $\mu$

Пусть  $p \in R_3(2)$  — предикат арности 2, сохраняемый функциями  $0, 1, 2, min, max$ . Докажем, что

$$(\exists Q \subseteq \{q_1, \dots, q_{10}\}) ([\{p\}]_{p.p.} = [Q]_{p.p.}).$$

*Доказательство.* Существует ровно 26 предикатов арности 2, сохраняемых функциями  $0, 1, 2, min, max$ . Это предикаты  $false^{(2)}, true^{(2)}, eq^{(2)}$ , предикаты  $q_1, \dots, q_{10}$ , определённые в разделе 2.1, и 13 предикатов из списка ниже. В качестве номера предиката  $p_j$  этого списка мы указываем число  $j$  (в десятичной кодировке), определяемое формулой

$$j = \tilde{p}_j(2, 2) \cdot 2^8 + \tilde{p}_j(2, 1) \cdot 2^7 + \tilde{p}_j(2, 0) \cdot 2^6 + \dots + \tilde{p}_j(0, 1) \cdot 2^1 + \tilde{p}_j(0, 0) \cdot 2^0,$$

где  $\tilde{p}_j(x_1, x_2) = 1$ , если  $p_j$  истинен на наборе  $(x_1, x_2)$ ;  $\tilde{p}_j(x_1, x_2) = 0$  иначе.

$$\begin{aligned}
p_{281} &= \{22, 11, 10, 00\} && (\text{частичный порядок } 1 < 0) \\
p_{307} &= \{22, 12, 11, 01, 00\} \\
p_{315} &= \{22, 12, 11, 10, 01, 00\} \\
p_{401} &= \{22, 21, 11, 00\} && (\text{частичный порядок } 2 < 1) \\
p_{403} &= \{22, 21, 11, 01, 00\} && (\text{частичный порядок } 0 < 1, 2 < 1) \\
p_{409} &= \{22, 21, 11, 10, 00\} \\
p_{411} &= \{22, 21, 11, 10, 01, 00\} \\
p_{435} &= \{22, 21, 12, 11, 01, 00\} \\
p_{441} &= \{22, 21, 12, 11, 10, 00\} \\
p_{473} &= \{22, 21, 20, 11, 10, 00\} && (\text{линейный порядок } 2 < 1 < 0) \\
p_{475} &= \{22, 21, 20, 11, 10, 01, 00\} && (\text{предпорядок } 2 < (0 \sim 1)) \\
p_{505} &= \{22, 21, 20, 12, 11, 10, 00\} && (\text{предпорядок } (1 \sim 2) < 0) \\
p_{507} &= \{22, 21, 20, 12, 11, 10, 01, 00\} && (\text{все наборы кроме } 02)
\end{aligned}$$

Очевидно, что для любого  $p \in \{false^{(2)}, true^{(2)}, eq^{(2)}, q_1, \dots, q_{10}\}$

$$(\exists Q \subseteq \{q_1, \dots, q_{10}\}) ([\{p\}]_{p.p.} = [Q]_{p.p.}).$$

Покажем, что и оставшиеся 13 предикатов обладают этим свойством.

- 1) Предикаты  $p_{281}, p_{401}, p_{403}, p_{473}, p_{475}, p_{505}, p_{507}$  получаются перестановкой переменных из предикатов  $q_1, \dots, q_{10}$ , и поэтому они обладают требуемым свойством:

$$\begin{aligned}
p_{281}(x_1, x_2) &= q_1(x_2, x_1); \\
p_{401}(x_1, x_2) &= q_3(x_2, x_1); \\
p_{403}(x_1, x_2) &= q_5(x_2, x_2); \\
p_{473}(x_1, x_2) &= q_4(x_2, x_1); \\
p_{475}(x_1, x_2) &= q_6(x_2, x_1); \\
p_{505}(x_1, x_2) &= q_8(x_2, x_1); \\
p_{507}(x_1, x_2) &= q_{10}(x_2, x_1).
\end{aligned}$$

- 2) Для каждого из предикатов  $p_{307}$ ,  $p_{315}$ ,  $p_{435}$  мы предъявим некоторое множество  $Q = \{s_1, \dots, s_m\} \subseteq \{q_1, \dots, q_{10}\}$ , такое что

$$[\{p\}]_{p.p.} = [\{s_1, \dots, s_m\}]_{p.p.},$$

а доказательство факта  $[\{p\}]_{p.p.} = [\{s_1, \dots, s_m\}]_{p.p.}$  мы сведём к доказательству двух вспомогательных фактов:

- а)  $p \in [\{s_1, \dots, s_m\}]_{p.p.}$   
 б)  $(\forall s \in \{s_1, \dots, s_m\}) (s \in [\{p\}]_{p.p.})$ .

Итак,

- а)  $[\{p_{307}\}]_{p.p.} = [\{q_4, q_{10}\}]_{p.p.}$ , так как

$$\begin{aligned} p_{307}(x_1, x_2) &= q_4(x_1, x_2) \wedge q_{10}(x_2, x_1); \\ q_4(x_1, x_2) &= \exists y_1 (p_{307}(x_1, y_1) \wedge p_{307}(y_1, x_2)); \\ q_{10}(x_1, x_2) &= \exists y_1 \exists y_2 (p_{307}(x_1, y_2) \wedge p_{307}(y_2, y_1) \wedge p_{307}(x_2, y_1)). \end{aligned}$$

- б)  $[\{p_{315}\}]_{p.p.} = [\{q_6, q_{10}\}]_{p.p.}$ , так как

$$\begin{aligned} p_{315}(x_1, x_2) &= q_6(x_1, x_2) \wedge q_{10}(x_2, x_1); \\ q_6(x_1, x_2) &= \exists y_1 (p_{315}(x_1, y_1) \wedge p_{315}(y_1, x_2)); \\ q_{10}(x_1, x_2) &= \exists y_1 \exists y_2 (p_{315}(x_1, y_2) \wedge p_{315}(y_2, y_1) \wedge p_{315}(x_2, y_1)). \end{aligned}$$

- в)  $[\{p_{435}\}]_{p.p.} = [\{q_8, q_{10}\}]_{p.p.}$ , так как

$$\begin{aligned} p_{435}(x_1, x_2) &= q_8(x_1, x_2) \wedge q_{10}(x_2, x_1); \\ q_8(x_1, x_2) &= \exists y_1 (p_{435}(x_1, y_1) \wedge p_{435}(y_1, x_2)); \\ q_{10}(x_1, x_2) &= \exists y_1 \exists y_2 (p_{435}(y_1, x_1) \wedge p_{435}(y_1, y_2) \wedge p_{435}(y_2, x_2)). \end{aligned}$$

- 3) Предикаты  $p_{409}$ ,  $p_{411}$ ,  $p_{441}$  получаются перестановкой переменных из предикатов  $p_{307}$ ,  $p_{315}$ ,  $p_{435}$ , поэтому они также обладают требуемым свойством:

$$\begin{aligned} p_{409}(x_1, x_2) &= p_{307}(x_2, x_1); \\ p_{411}(x_1, x_2) &= p_{315}(x_2, x_1); \\ p_{441}(x_1, x_2) &= p_{435}(x_2, x_1). \end{aligned}$$

□

## 5. Доказательство леммы 2

Напомним, что в разделе 2.2 мы сопоставили каждой вершине  $v$  диаграммы 1 некоторое множество предикатов  $\pi(v) \subseteq \{q_1, \dots, q_{10}\}$ . Лемма 2 говорит о том, что для любого  $Q \subseteq \{q_1, \dots, q_{10}\}$  существует вершина  $v$  диаграммы, такая что

$$Pol(Q) = Pol(\pi(v)).$$

Введём индуктивное определение:

$$1) \text{ } Classes(0) = \{[\emptyset]_{p.p.}\}.$$

$$2) \text{ } Classes(m) = \\ = Classes(m-1) \cup \{[C \cup \{q_m\}]_{p.p.} : C \in Classes(m-1)\} \\ (1 \leq m \leq 10).$$

Учитывая, что  $[Q \cup \{p\}]_{p.p.} = [[Q]_{p.p.} \cup \{p\}]_{p.p.}$ , заметим, что

$$Classes(m) = \{[Q]_{p.p.} : Q \subseteq \{q_1, \dots, q_m\}\} \quad (0 \leq m \leq 10).$$

Поэтому, учитывая, что  $Pol(Q) = Pol([Q]_{p.p.})$ , утверждение леммы 2 можно переформулировать следующим образом:

$$(\forall C \in Classes(10)) (\exists v) (Pol(C) = Pol(\pi(v))).$$

А учитывая, что  $(Pol(Q) = Pol(Q')) \iff ([Q]_{p.p.} = [Q']_{p.p.})$  и тот факт, что  $(C \in Classes(m)) \Rightarrow ([C]_{p.p.} = C)$ , утверждение леммы 2 можно дополнительно переформулировать так:

$$(\forall C \in Classes(10)) (\exists v) (C = [\pi(v)]_{p.p.}).$$

Докажем этот факт индукцией по параметру  $m$  в обозначении  $Classes(m)$ .

1) Базис индукции. Пусть  $m = 0$ . Тогда

$$Classes(0) = \{[\emptyset]_{p.p.}\}.$$

Поэтому если  $C \in Classes(0)$ , то  $C = [\pi(v_1)]_{p.p.}$ , где согласно нашим обозначениям  $v_1$  обозначает верхнюю точку диаграммы 1.

- 2) Индукционный переход. Зафиксируем  $m \in \{1, \dots, 10\}$  и предположим, что

$$(\forall C \in \text{Classes}(m-1)) (\exists v) (C = [\pi(v)]_{p.p.}).$$

Покажем, что

$$(\forall C \in \text{Classes}(m)) (\exists v) (C = [\pi(v)]_{p.p.}).$$

Пусть  $C \in \text{Classes}(m)$ . Из определения  $\text{Classes}(m)$  имеем:

$$(C \in \text{Classes}(m-1)) \vee \\ \vee (\exists C' \in \text{Classes}(m-1)) (C = [C' \cup \{q_m\}]_{p.p.}).$$

Поэтому доказательство индукционного перехода сводится к доказательству факта

$$(\forall C \in \text{Classes}(m-1)) (\exists v) ([C \cup \{q_m\}]_{p.p.} = [\pi(v)]_{p.p.}). \\ (\text{induct-step-}m)$$

Докажем этот факт. Зафиксируем  $C \in \text{Classes}(m-1)$ . По предположению индукции  $C = [\pi(v)]_{p.p.}$  для некоторой вершины  $v$ . Далее,

- а) Если  $p_m \in C$ , то, очевидно,

$$[C \cup \{q_m\}]_{p.p.} = [C]_{p.p.} = [\pi(v)]_{p.p.}.$$

Рассмотрение этих случаев ( $p_m \in C$ ) мы будем опускать в дальнейшем.

- б) Если  $p_m \notin C$ , то для завершения доказательства необходимо найти вершину  $v'$ , такую что

$$[\pi(v) \cup \{q_m\}]_{p.p.} = [\pi(v')]_{p.p.}. \quad (\text{induct-step-}m-v)$$

Следующие 10 подразделов статьи содержат доказательства индукционных переходов в форме  $(\text{induct-step-}m)$  для  $m \in \{1, \dots, 10\}$ . Доказательство  $m$ -ого индукционного перехода проводится последовательным разбором случаев для всех  $C \in \text{Classes}(m-1)$ . Справедливость вспомогательного факта  $(\text{induct-step-}m-v)$  мы обосновываем так: для

$C \in \text{Classes}(m - 1)$ , такого что  $C = [\pi(v)]_{p.p.}$ , мы явно указываем вершину  $v'$ , такую что

$$[C \cup \{q_m\}]_{p.p.} = [[\pi(v)]_{p.p.} \cup \{q_m\}]_{p.p.} = [\pi(v')]_{p.p.},$$

причём

$$(\pi(v) \cup \{q_m\}) \subseteq \pi(v').$$

Это равенство мы обосновываем так: для каждого  $p \in \pi(v') \setminus (\pi(v) \cup \{q_m\})$  мы указываем примитивную позитивную формулу над множеством предикатов  $\pi(v) \cup \{q_m\}$ , определяющую предикат  $p$  (т. е. показываем, что  $p \in [\pi(v) \cup \{q_m\}]_{p.p.}$ ).

Дополнительно на каждом индукционном шаге  $m$  мы явным образом строим множество  $\text{Classes}(m)$ .

В заключение, в дальнейших подразделах мы будем использовать обозначение:

$$C_j = [\pi(v_j)]_{p.p.} \quad (1 \leq j \leq 33).$$

### 5.1. Добавление предиката $q_1$

$$1) [C_1 \cup \{q_1\}]_{p.p.} = [[\emptyset]_{p.p.} \cup \{q_1\}]_{p.p.} = [\{q_1, q_2\}]_{p.p.} = C_2, \text{ так как}$$

$$q_2(x_1, x_2) = \exists y_1 (q_1(x_1, y_1) \wedge q_1(x_2, y_1)).$$

Таким образом,  $\text{Classes}(1) = \{C_1, C_2\}$ .

### 5.2. Добавление предиката $q_2$

$$1) [C_1 \cup \{q_2\}]_{p.p.} = [[\emptyset]_{p.p.} \cup \{q_2\}]_{p.p.} = [\{q_2\}]_{p.p.} = C_3.$$

Таким образом,  $\text{Classes}(2) = \{C_1, C_2, C_3\}$ .

### 5.3. Добавление предиката $q_3$

$$1) [C_1 \cup \{q_3\}]_{p.p.} = [[\emptyset]_{p.p.} \cup \{q_3\}]_{p.p.} = [\{q_3, q_7\}]_{p.p.} = C_4, \text{ так как}$$

$$q_7(x_1, x_2) = \exists y_1 (q_3(x_1, y_1) \wedge q_3(x_2, y_1)).$$

- 2)  $[C_2 \cup \{q_3\}]_{p.p.} = [[\{q_1, q_2\}]_{p.p.} \cup \{q_3\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5$ , так как

$$\begin{aligned} q_4(x_1, x_2) &= \exists y_1 (q_1(x_1, y_1) \wedge q_3(y_1, x_2)); \\ q_5(x_1, x_2) &= \exists y_1 (q_3(x_1, y_1) \wedge q_1(x_2, y_1)); \\ q_6(x_1, x_2) &= \exists y_1 (q_2(x_1, y_1) \wedge q_3(y_1, x_2)); \\ q_7(x_1, x_2) &= \exists y_1 (q_3(x_1, y_1) \wedge q_3(x_2, y_1)); \\ q_8(x_1, x_2) &= \exists y_1 \exists y_2 (q_1(x_1, y_2) \wedge q_3(y_2, y_1) \wedge q_3(x_2, y_1)); \\ q_9(x_1, x_2) &= \exists y_1 \exists y_2 (q_3(x_1, y_2) \wedge q_2(y_2, y_1) \wedge q_3(x_2, y_1)); \\ q_{10}(x_1, x_2) &= \exists y_1 \exists y_2 (q_2(x_1, y_2) \wedge q_3(y_2, y_1) \wedge q_3(x_2, y_1)). \end{aligned}$$

- 3)  $[C_3 \cup \{q_3\}]_{p.p.} = [[\{q_2\}]_{p.p.} \cup \{q_3\}]_{p.p.} = [\{q_2, q_3, q_6, q_7, q_9, q_{10}\}]_{p.p.} = C_6$ , так как

$$\begin{aligned} q_6(x_1, x_2) &= \exists y_1 (q_2(x_1, y_1) \wedge q_3(y_1, x_2)); \\ q_7(x_1, x_2) &= \exists y_1 (q_3(x_1, y_1) \wedge q_3(x_2, y_1)); \\ q_9(x_1, x_2) &= \exists y_1 \exists y_2 (q_3(x_1, y_2) \wedge q_2(y_2, y_1) \wedge q_3(x_2, y_1)); \\ q_{10}(x_1, x_2) &= \exists y_1 \exists y_2 (q_2(x_1, y_2) \wedge q_3(y_2, y_1) \wedge q_3(x_2, y_1)). \end{aligned}$$

Таким образом,  $Classes(3) = \{C_1, C_2, \dots, C_6\}$ .

#### 5.4. Добавление предиката $q_4$

- 1)  $[C_1 \cup \{q_4\}]_{p.p.} = [[\emptyset]_{p.p.} \cup \{q_4\}]_{p.p.} = [\{q_4\}]_{p.p.} = C_7$ .
- 2)  $[C_2 \cup \{q_4\}]_{p.p.} = [[\{q_1, q_2\}]_{p.p.} \cup \{q_4\}]_{p.p.} = [\{q_1, q_2, q_4, q_6\}]_{p.p.} = C_8$ , так как

$$q_6(x_1, x_2) = \exists y_1 (q_2(x_1, y_1) \wedge q_4(y_1, x_2)).$$

- 3)  $[C_3 \cup \{q_4\}]_{p.p.} = [[\{q_2\}]_{p.p.} \cup \{q_4\}]_{p.p.} = [\{q_1, q_2, q_4, q_6\}]_{p.p.} = C_8$ , так как

$$\begin{aligned} q_1(x_1, x_2) &= q_2(x_1, x_2) \wedge q_4(x_1, x_2); \\ q_6(x_1, x_2) &= \exists y_1 (q_2(x_1, y_1) \wedge q_4(y_1, x_2)). \end{aligned}$$

- 4)  $[C_4 \cup \{q_4\}]_{p.p.} = [[\{q_3, q_7\}]_{p.p.} \cup \{q_4\}]_{p.p.} = [\{q_3, q_4, q_7, q_8\}]_{p.p.} = C_9$ , так как

$$q_8(x_1, x_2) = \exists y_1 (q_4(x_1, y_1) \wedge q_7(y_1, x_2)).$$

- 5)  $[C_6 \cup \{q_4\}]_{p.p.} = [[\{q_2, q_3, q_6, q_7, q_9, q_{10}\}]_{p.p.} \cup \{q_4\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5$ , так как

$$\begin{aligned} q_1(x_1, x_2) &= q_2(x_1, x_2) \wedge q_4(x_1, x_2); \\ q_5(x_1, x_2) &= \exists y_1 (q_2(x_1, y_1) \wedge q_4(y_1, x_1) \wedge q_3(y_1, x_2)); \\ q_8(x_1, x_2) &= \exists y_1 (q_4(x_1, y_1) \wedge q_7(y_1, x_2)). \end{aligned}$$

Таким образом,  $Classes(4) = \{C_1, C_2, \dots, C_9\}$ .

### 5.5. Добавление предиката $q_5$

- 1)  $[C_1 \cup \{q_5\}]_{p.p.} = [[\emptyset]_{p.p.} \cup \{q_5\}]_{p.p.} = [\{q_5, q_9\}]_{p.p.} = C_{10}$ , так как

$$q_9(x_1, x_2) = \exists y_1 (q_5(x_1, y_1) \wedge q_5(x_2, y_1)).$$

- 2)  $[C_2 \cup \{q_5\}]_{p.p.} = [[\{q_1, q_2\}]_{p.p.} \cup \{q_5\}]_{p.p.} = [\{q_1, q_2, q_5, q_6, q_9, q_{10}\}]_{p.p.} = C_{11}$ , так как

$$\begin{aligned} q_6(x_1, x_2) &= \exists y_1 (q_1(x_1, y_1) \wedge q_5(y_1, x_2)); \\ q_9(x_1, x_2) &= \exists y_1 (q_5(x_1, y_1) \wedge q_5(x_2, y_1)); \\ q_{10}(x_1, x_2) &= \exists y_1 \exists y_2 (q_1(x_1, y_2) \wedge q_5(y_2, y_1) \wedge q_5(x_2, y_1)). \end{aligned}$$

- 3)  $[C_3 \cup \{q_5\}]_{p.p.} = [[\{q_2\}]_{p.p.} \cup \{q_5\}]_{p.p.} = [\{q_1, q_2, q_5, q_6, q_9, q_{10}\}]_{p.p.} = C_{11}$ , так как

$$\begin{aligned} q_1(x_1, x_2) &= q_2(x_1, x_2) \wedge q_5(x_2, x_1); \\ q_6(x_1, x_2) &= \exists y_1 (q_2(x_1, y_1) \wedge q_5(y_1, x_2)); \\ q_9(x_1, x_2) &= \exists y_1 (q_5(x_1, y_1) \wedge q_5(x_2, y_1)); \\ q_{10}(x_1, x_2) &= \exists y_1 \exists y_2 (q_2(x_1, y_2) \wedge q_5(y_2, y_1) \wedge q_5(x_2, y_1)). \end{aligned}$$

- 4)  $[C_4 \cup \{q_5\}]_{p.p.} = [[\{q_3, q_7\}]_{p.p.} \cup \{q_5\}]_{p.p.} = [\{q_3, q_5, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_{12}$ , так как

$$\begin{aligned} q_8(x_1, x_2) &= \exists y_1 (q_5(y_1, x_1) \wedge q_3(y_1, x_2)); \\ q_9(x_1, x_2) &= \exists y_1 (q_5(x_1, y_1) \wedge q_5(x_2, y_1)); \\ q_{10}(x_1, x_2) &= \exists y_1 \exists y_2 (q_5(x_1, y_1) \wedge q_5(y_2, y_1) \wedge q_3(y_2, x_2)). \end{aligned}$$

- 5)  $[C_6 \cup \{q_5\}]_{p.p.} = [[\{q_2, q_3, q_6, q_7, q_9, q_{10}\}]_{p.p.} \cup \{q_5\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5$ , так как

$$\begin{aligned} q_1(x_1, x_2) &= q_2(x_1, x_2) \wedge q_5(x_2, x_1); \\ q_4(x_1, x_2) &= \exists y_1 (q_2(x_1, y_1) \wedge q_5(y_1, x_1) \wedge q_3(y_1, x_2)); \\ q_8(x_1, x_2) &= \exists y_1 (q_5(y_1, x_1) \wedge q_3(y_1, x_2)). \end{aligned}$$

- 6)  $[C_7 \cup \{q_5\}]_{p.p.} = [[\{q_4\}]_{p.p.} \cup \{q_5\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5$ , так как

$$\begin{aligned} q_1(x_1, x_2) &= q_4(x_1, x_2) \wedge q_5(x_2, x_1); \\ q_2(x_1, x_2) &= \exists y_1 \exists y_2 (q_4(x_1, y_1) \wedge q_5(y_1, x_2) \wedge \\ &\quad \wedge q_4(y_2, x_1) \wedge q_5(x_2, y_2)); \\ q_3(x_1, x_2) &= q_4(x_1, x_2) \wedge q_5(x_1, x_2); \\ q_6(x_1, x_2) &= \exists y_1 (q_4(x_1, y_1) \wedge q_5(y_1, x_2)); \\ q_7(x_1, x_2) &= \exists y_1 (q_4(x_1, y_1) \wedge q_5(x_1, y_1) \wedge \\ &\quad \wedge q_4(x_2, y_1) \wedge q_5(x_2, y_1)); \\ q_8(x_1, x_2) &= \exists y_1 (q_4(x_1, y_1) \wedge q_5(x_2, y_1)); \\ q_9(x_1, x_2) &= \exists y_1 (q_5(x_1, y_1) \wedge q_5(x_2, y_1)); \\ q_{10}(x_1, x_2) &= \exists y_1 \exists y_2 (q_4(x_1, y_2) \wedge q_5(y_2, y_1) \wedge q_5(x_2, y_1)). \end{aligned}$$

- 7)  $[C_8 \cup \{q_5\}]_{p.p.} = [[\{q_1, q_2, q_4, q_6\}]_{p.p.} \cup \{q_5\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5$ , так как

$$\begin{aligned} q_3(x_1, x_2) &= q_4(x_1, x_2) \wedge q_5(x_1, x_2); \\ q_7(x_1, x_2) &= \exists y_1 (q_4(x_1, y_1) \wedge q_5(x_1, y_1) \wedge \\ &\quad \wedge q_4(x_2, y_1) \wedge q_5(x_2, y_1)); \\ q_8(x_1, x_2) &= \exists y_1 (q_4(x_1, y_1) \wedge q_5(x_2, y_1)); \\ q_9(x_1, x_2) &= \exists y_1 (q_5(x_1, y_1) \wedge q_5(x_2, y_1)); \\ q_{10}(x_1, x_2) &= \exists y_1 (q_6(x_1, y_1) \wedge q_5(x_2, y_1)). \end{aligned}$$

- 8)  $[C_9 \cup \{q_5\}]_{p.p.} = [[\{q_3, q_4, q_7, q_8\}]_{p.p.} \cup \{q_5\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5$ , так как

$$\begin{aligned} q_1(x_1, x_2) &= q_4(x_1, x_2) \wedge q_5(x_2, x_1); \\ q_2(x_1, x_2) &= \exists y_1 \exists y_2 (q_4(x_1, y_1) \wedge q_5(y_1, x_2) \wedge \\ &\quad \wedge q_4(y_2, x_1) \wedge q_5(x_2, y_2)); \\ q_6(x_1, x_2) &= \exists y_1 (q_4(x_1, y_1) \wedge q_5(y_1, x_2)); \\ q_9(x_1, x_2) &= \exists y_1 (q_5(x_1, y_1) \wedge q_5(x_2, y_1)); \\ q_{10}(x_1, x_2) &= \exists y_1 (q_5(x_1, y_1) \wedge q_8(y_1, x_2)). \end{aligned}$$

Таким образом,  $Classes(5) = \{C_1, C_2, \dots, C_{12}\}$ .

## 5.6. Добавление предиката $q_6$

- 1)  $[C_1 \cup \{q_6\}]_{p.p.} = [[\emptyset]_{p.p.} \cup \{q_6\}]_{p.p.} = [\{q_2, q_6\}]_{p.p.} = C_{13}$ , так как

$$q_2(x_1, x_2) = q_6(x_1, x_2) \wedge q_6(x_2, x_1).$$

- 2)  $[C_2 \cup \{q_6\}]_{p.p.} = [[\{q_1, q_2\}]_{p.p.} \cup \{q_6\}]_{p.p.} = [\{q_1, q_2, q_6\}]_{p.p.} = C_{14}$ .

- 3)  $[C_3 \cup \{q_6\}]_{p.p.} = [[\{q_2\}]_{p.p.} \cup \{q_6\}]_{p.p.} = [\{q_2, q_6\}]_{p.p.} = C_{13}$ .

- 4)  $[C_4 \cup \{q_6\}]_{p.p.} = [[\{q_3, q_7\}]_{p.p.} \cup \{q_6\}]_{p.p.} = [\{q_2, q_3, q_6, q_7, q_9, q_{10}\}]_{p.p.} = C_6$ , так как

$$\begin{aligned} q_2(x_1, x_2) &= q_6(x_1, x_2) \wedge q_6(x_2, x_1); \\ q_9(x_1, x_2) &= \exists y_1 \exists y_2 (q_3(x_1, y_2) \wedge q_6(y_1, y_2) \wedge \\ &\quad \wedge q_6(x_1, y_1) \wedge q_3(x_2, y_1)); \\ q_{10}(x_1, x_2) &= \exists y_1 (q_6(x_1, y_1) \wedge q_7(y_1, x_2)). \end{aligned}$$

- 5)  $[C_7 \cup \{q_6\}]_{p.p.} = [[\{q_4\}]_{p.p.} \cup \{q_6\}]_{p.p.} = [\{q_1, q_2, q_4, q_6\}]_{p.p.} = C_8$ , так как

$$\begin{aligned} q_1(x_1, x_2) &= q_4(x_1, x_2) \wedge q_6(x_2, x_1); \\ q_2(x_1, x_2) &= q_6(x_1, x_2) \wedge q_6(x_2, x_1). \end{aligned}$$

$$6) [C_9 \cup \{q_6\}]_{p.p.} = [[\{q_3, q_4, q_7, q_8\}]_{p.p.} \cup \{q_6\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5, \text{ так как}$$

$$\begin{aligned} q_1(x_1, x_2) &= q_4(x_1, x_2) \wedge q_6(x_2, x_1); \\ q_2(x_1, x_2) &= q_6(x_1, x_2) \wedge q_6(x_2, x_1); \\ q_5(x_1, x_2) &= q_6(x_1, x_2) \wedge q_8(x_2, x_1); \\ q_9(x_1, x_2) &= \exists y_1 \exists y_2 (q_3(x_1, y_2) \wedge q_6(y_1, y_2) \wedge \\ &\quad \wedge q_6(x_1, y_1) \wedge q_3(x_2, y_1)); \\ q_{10}(x_1, x_2) &= \exists y_1 (q_6(x_1, y_1) \wedge q_7(y_1, x_2)). \end{aligned}$$

$$7) [C_{10} \cup \{q_6\}]_{p.p.} = [[\{q_5, q_9\}]_{p.p.} \cup \{q_6\}]_{p.p.} = [\{q_1, q_2, q_5, q_6, q_9, q_{10}\}]_{p.p.} = C_{11}, \text{ так как}$$

$$\begin{aligned} q_1(x_1, x_2) &= q_6(x_1, x_2) \wedge q_5(x_2, x_1); \\ q_2(x_1, x_2) &= q_6(x_1, x_2) \wedge q_6(x_2, x_1); \\ q_{10}(x_1, x_2) &= \exists y_1 (q_6(x_1, y_1) \wedge q_9(y_1, x_2)). \end{aligned}$$

$$8) [C_{12} \cup \{q_6\}]_{p.p.} = [[\{q_3, q_5, q_7, q_8, q_9, q_{10}\}]_{p.p.} \cup \{q_6\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5, \text{ так как}$$

$$\begin{aligned} q_1(x_1, x_2) &= q_6(x_1, x_2) \wedge q_5(x_2, x_1); \\ q_2(x_1, x_2) &= q_6(x_1, x_2) \wedge q_6(x_2, x_1); \\ q_4(x_1, x_2) &= q_6(x_1, x_2) \wedge q_8(x_1, x_2). \end{aligned}$$

Таким образом,  $Classes(6) = \{C_1, C_2, \dots, C_{14}\}$ .

### 5.7. Добавление предиката $q_7$

$$1) [C_1 \cup \{q_7\}]_{p.p.} = [[\emptyset]_{p.p.} \cup \{q_7\}]_{p.p.} = [\{q_7\}]_{p.p.} = C_{15}.$$

$$2) [C_2 \cup \{q_7\}]_{p.p.} = [[\{q_1, q_2\}]_{p.p.} \cup \{q_7\}]_{p.p.} = [\{q_1, q_2, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_{16}, \text{ так как}$$

$$\begin{aligned} q_8(x_1, x_2) &= \exists y_1 (q_1(x_1, y_1) \wedge q_7(y_1, x_2)); \\ q_9(x_1, x_2) &= \exists y_1 \exists y_2 (q_1(y_1, x_1) \wedge q_7(y_1, y_2) \wedge q_1(y_2, x_2)); \\ q_{10}(x_1, x_2) &= \exists y_1 (q_2(x_1, y_1) \wedge q_7(y_1, x_2)). \end{aligned}$$

- 3)  $[C_3 \cup \{q_7\}]_{p.p.} = [[\{q_2\}]_{p.p.} \cup \{q_7\}]_{p.p.} = [\{q_2, q_7, q_9, q_{10}\}]_{p.p.} = C_{17}$ , так как

$$q_9(x_1, x_2) = \exists y_1 \exists y_2 (q_2(x_1, y_1) \wedge q_7(y_1, x_2) \wedge \\ \wedge q_7(x_1, y_2) \wedge q_2(y_2, x_2));$$

$$q_{10}(x_1, x_2) = \exists y_1 (q_2(x_1, y_1) \wedge q_7(y_1, x_2)).$$

- 4)  $[C_7 \cup \{q_7\}]_{p.p.} = [[\{q_4\}]_{p.p.} \cup \{q_7\}]_{p.p.} = [\{q_3, q_4, q_7, q_8\}]_{p.p.} = C_9$ , так как

$$q_3(x_1, x_2) = q_4(x_1, x_2) \wedge q_7(x_1, x_2);$$

$$q_8(x_1, x_2) = \exists y_1 (q_4(x_1, y_1) \wedge q_7(y_1, x_2)).$$

- 5)  $[C_8 \cup \{q_7\}]_{p.p.} = [[\{q_1, q_2, q_4, q_6\}]_{p.p.} \cup \{q_7\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5$ , так как

$$q_3(x_1, x_2) = q_4(x_1, x_2) \wedge q_7(x_1, x_2);$$

$$q_5(x_1, x_2) = \exists y_1 (q_4(x_1, y_1) \wedge q_7(x_1, y_1) \wedge q_1(x_2, y_1));$$

$$q_8(x_1, x_2) = \exists y_1 (q_1(x_1, y_1) \wedge q_7(y_1, x_2));$$

$$q_9(x_1, x_2) = \exists y_1 \exists y_2 (q_1(y_1, x_1) \wedge q_7(y_1, y_2) \wedge q_1(y_2, x_2));$$

$$q_{10}(x_1, x_2) = \exists y_1 (q_2(x_1, y_1) \wedge q_7(y_1, x_2)).$$

- 6)  $[C_{10} \cup \{q_7\}]_{p.p.} = [[\{q_5, q_9\}]_{p.p.} \cup \{q_7\}]_{p.p.} = [\{q_3, q_5, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_{12}$ , так как

$$q_3(x_1, x_2) = q_5(x_1, x_2) \wedge q_7(x_1, x_2);$$

$$q_8(x_1, x_2) = \exists y_1 (q_5(y_1, x_1) \wedge q_7(y_1, x_2));$$

$$q_{10}(x_1, x_2) = \exists y_1 (q_9(x_1, y_1) \wedge q_7(y_1, x_2)).$$

- 7)  $[C_{11} \cup \{q_7\}]_{p.p.} = [[\{q_1, q_2, q_5, q_6, q_9, q_{10}\}]_{p.p.} \cup \{q_7\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5$ , так как

$$q_3(x_1, x_2) = q_5(x_1, x_2) \wedge q_7(x_1, x_2);$$

$$q_4(x_1, x_2) = \exists y_1 (q_1(x_1, y_1) \wedge q_7(y_1, x_2) \wedge q_6(x_1, x_2));$$

$$q_8(x_1, x_2) = \exists y_1 (q_1(x_1, y_1) \wedge q_7(y_1, x_2)).$$

$$8) [C_{13} \cup \{q_7\}]_{p.p.} = [[\{q_2, q_6\}]_{p.p.} \cup \{q_7\}]_{p.p.} = [\{q_2, q_3, q_6, q_7, q_9, q_{10}\}]_{p.p.} = C_6, \text{ так как}$$

$$\begin{aligned} q_3(x_1, x_2) &= q_6(x_1, x_2) \wedge q_7(x_1, x_2); \\ q_9(x_1, x_2) &= \exists y_1 \exists y_2 (q_2(x_1, y_1) \wedge q_7(y_1, x_2) \wedge \\ &\quad \wedge q_7(x_1, y_2) \wedge q_2(y_2, x_2)); \\ q_{10}(x_1, x_2) &= \exists y_1 (q_2(x_1, y_1) \wedge q_7(y_1, x_2)). \end{aligned}$$

$$9) [C_{14} \cup \{q_7\}]_{p.p.} = [[\{q_1, q_2, q_6\}]_{p.p.} \cup \{q_7\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5, \text{ так как}$$

$$\begin{aligned} q_3(x_1, x_2) &= q_6(x_1, x_2) \wedge q_7(x_1, x_2); \\ q_4(x_1, x_2) &= \exists y_1 (q_1(x_1, y_1) \wedge q_7(y_1, x_2) \wedge q_6(x_1, x_2)); \\ q_5(x_1, x_2) &= \exists y_1 (q_6(x_1, y_1) \wedge q_7(x_1, y_1) \wedge q_1(x_2, y_1)); \\ q_8(x_1, x_2) &= \exists y_1 (q_1(x_1, y_1) \wedge q_7(y_1, x_2)); \\ q_9(x_1, x_2) &= \exists y_1 \exists y_2 (q_1(y_1, x_1) \wedge q_7(y_1, y_2) \wedge q_1(y_2, x_2)); \\ q_{10}(x_1, x_2) &= \exists y_1 (q_2(x_1, y_1) \wedge q_7(y_1, x_2)). \end{aligned}$$

Таким образом,  $Classes(7) = \{C_1, C_2, \dots, C_{17}\}$ .

## 5.8. Добавление предиката $q_8$

$$1) [C_1 \cup \{q_8\}]_{p.p.} = [[\emptyset]_{p.p.} \cup \{q_8\}]_{p.p.} = [\{q_7, q_8\}]_{p.p.} = C_{18}, \text{ так как}$$

$$q_7(x_1, x_2) = q_8(x_1, x_2) \wedge q_8(x_2, x_1).$$

$$2) [C_2 \cup \{q_8\}]_{p.p.} = [[\{q_1, q_2\}]_{p.p.} \cup \{q_8\}]_{p.p.} = [\{q_1, q_2, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_{16}, \text{ так как}$$

$$\begin{aligned} q_7(x_1, x_2) &= q_8(x_1, x_2) \wedge q_8(x_2, x_1); \\ q_9(x_1, x_2) &= \exists y_1 \exists y_2 (q_1(y_1, x_1) \wedge q_8(y_2, y_1) \wedge \\ &\quad \wedge q_1(y_2, x_2) \wedge q_8(y_1, x_2)); \\ q_{10}(x_1, x_2) &= \exists y_1 (q_2(x_1, y_1) \wedge q_8(y_1, x_2)). \end{aligned}$$

- 3)  $[C_3 \cup \{q_8\}]_{p.p.} = [[\{q_2\}]_{p.p.} \cup \{q_8\}]_{p.p.} = [\{q_1, q_2, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_{16}$ ,  
так как

$$\begin{aligned} q_1(x_1, x_2) &= q_2(x_1, x_2) \wedge q_8(x_1, x_2); \\ q_7(x_1, x_2) &= q_8(x_1, x_2) \wedge q_8(x_2, x_1); \\ q_9(x_1, x_2) &= \exists y_1 \exists y_2 (q_2(x_1, y_2) \wedge q_8(y_2, y_1) \wedge q_8(y_1, x_1) \wedge \\ &\quad \wedge q_2(y_1, x_2) \wedge q_8(y_1, x_2)); \\ q_{10}(x_1, x_2) &= \exists y_1 (q_2(x_1, y_1) \wedge q_8(y_1, x_2)). \end{aligned}$$

- 4)  $[C_4 \cup \{q_8\}]_{p.p.} = [[\{q_3, q_7\}]_{p.p.} \cup \{q_8\}]_{p.p.} = [\{q_3, q_7, q_8\}]_{p.p.} = C_{19}$ .

- 5)  $[C_6 \cup \{q_8\}]_{p.p.} = [[\{q_2, q_3, q_6, q_7, q_9, q_{10}\}]_{p.p.} \cup \{q_8\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5$ , так как

$$\begin{aligned} q_1(x_1, x_2) &= q_2(x_1, x_2) \wedge q_8(x_1, x_2); \\ q_4(x_1, x_2) &= q_6(x_1, x_2) \wedge q_8(x_1, x_2); \\ q_5(x_1, x_2) &= q_6(x_1, x_2) \wedge q_8(x_2, x_1). \end{aligned}$$

- 6)  $[C_7 \cup \{q_8\}]_{p.p.} = [[\{q_4\}]_{p.p.} \cup \{q_8\}]_{p.p.} = [\{q_3, q_4, q_7, q_8\}]_{p.p.} = C_9$ , так как

$$\begin{aligned} q_3(x_1, x_2) &= q_4(x_1, x_2) \wedge q_8(x_2, x_1); \\ q_7(x_1, x_2) &= q_8(x_1, x_2) \wedge q_8(x_2, x_1). \end{aligned}$$

- 7)  $[C_8 \cup \{q_8\}]_{p.p.} = [[\{q_1, q_2, q_4, q_6\}]_{p.p.} \cup \{q_8\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5$ , так как

$$\begin{aligned} q_3(x_1, x_2) &= q_4(x_1, x_2) \wedge q_8(x_2, x_1); \\ q_5(x_1, x_2) &= q_6(x_1, x_2) \wedge q_8(x_2, x_1); \\ q_7(x_1, x_2) &= q_8(x_1, x_2) \wedge q_8(x_2, x_1); \\ q_9(x_1, x_2) &= \exists y_1 \exists y_2 (q_1(y_1, x_1) \wedge q_8(y_2, y_1) \wedge \\ &\quad \wedge q_1(y_2, x_2) \wedge q_8(y_1, x_2)); \\ q_{10}(x_1, x_2) &= \exists y_1 (q_2(x_1, y_1) \wedge q_8(y_1, x_2)). \end{aligned}$$

- 8)  $[C_{10} \cup \{q_8\}]_{p.p.} = [[\{q_5, q_9\}]_{p.p.} \cup \{q_8\}]_{p.p.} = [\{q_3, q_5, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_{12}$ , так как

$$\begin{aligned} q_3(x_1, x_2) &= q_5(x_1, x_2) \wedge q_8(x_1, x_2); \\ q_7(x_1, x_2) &= q_8(x_1, x_2) \wedge q_8(x_2, x_1); \\ q_{10}(x_1, x_2) &= \exists y_1 (q_5(x_1, y_1) \wedge q_8(y_1, x_2)). \end{aligned}$$

- 9)  $[C_{11} \cup \{q_8\}]_{p.p.} = [[\{q_1, q_2, q_5, q_6, q_9, q_{10}\}]_{p.p.} \cup \{q_8\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5$ , так как

$$q_3(x_1, x_2) = q_5(x_1, x_2) \wedge q_8(x_1, x_2);$$

$$q_4(x_1, x_2) = q_6(x_1, x_2) \wedge q_8(x_1, x_2);$$

$$q_7(x_1, x_2) = q_8(x_1, x_2) \wedge q_8(x_2, x_1).$$

- 10)  $[C_{13} \cup \{q_8\}]_{p.p.} = [[\{q_2, q_6\}]_{p.p.} \cup \{q_8\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5$ , так как

$$q_1(x_1, x_2) = q_2(x_1, x_2) \wedge q_8(x_1, x_2);$$

$$q_3(x_1, x_2) = q_6(x_1, x_2) \wedge q_8(x_1, x_2) \wedge q_8(x_2, x_1);$$

$$q_4(x_1, x_2) = q_6(x_1, x_2) \wedge q_8(x_1, x_2);$$

$$q_5(x_1, x_2) = q_6(x_1, x_2) \wedge q_8(x_2, x_1);$$

$$q_7(x_1, x_2) = q_8(x_1, x_2) \wedge q_8(x_2, x_1);$$

$$q_9(x_1, x_2) = \exists y_1 \exists y_2 (q_2(x_1, y_2) \wedge q_8(y_2, y_1) \wedge q_8(y_1, x_1) \wedge q_2(y_1, x_2) \wedge q_8(y_1, x_2));$$

$$q_{10}(x_1, x_2) = \exists y_1 (q_2(x_1, y_1) \wedge q_8(y_1, x_2)).$$

- 11)  $[C_{14} \cup \{q_8\}]_{p.p.} = [[\{q_1, q_2, q_6\}]_{p.p.} \cup \{q_8\}]_{p.p.} = [\{q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_5$ , так как

$$q_3(x_1, x_2) = q_6(x_1, x_2) \wedge q_8(x_1, x_2) \wedge q_8(x_2, x_1);$$

$$q_4(x_1, x_2) = q_6(x_1, x_2) \wedge q_8(x_1, x_2);$$

$$q_5(x_1, x_2) = q_6(x_1, x_2) \wedge q_8(x_2, x_1);$$

$$q_7(x_1, x_2) = q_8(x_1, x_2) \wedge q_8(x_2, x_1);$$

$$q_9(x_1, x_2) = \exists y_1 \exists y_2 (q_1(y_1, x_1) \wedge q_8(y_2, y_1) \wedge q_1(y_2, x_2) \wedge q_8(y_1, x_2));$$

$$q_{10}(x_1, x_2) = \exists y_1 (q_2(x_1, y_1) \wedge q_8(y_1, x_2)).$$

- 12)  $[C_{15} \cup \{q_8\}]_{p.p.} = [[\{q_7\}]_{p.p.} \cup \{q_8\}]_{p.p.} = [\{q_7, q_8\}]_{p.p.} = C_{18}$ .

- 13)  $[C_{17} \cup \{q_8\}]_{p.p.} = [[\{q_2, q_7, q_9, q_{10}\}]_{p.p.} \cup \{q_8\}]_{p.p.} = [\{q_1, q_2, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_{16}$ , так как

$$q_1(x_1, x_2) = q_2(x_1, x_2) \wedge q_8(x_1, x_2).$$

Таким образом,  $Classes(8) = \{C_1, C_2, \dots, C_{19}\}$ .

### 5.9. Добавление предиката $q_9$

1)  $[C_1 \cup \{q_9\}]_{p.p.} = [[\emptyset]_{p.p.} \cup \{q_9\}]_{p.p.} = [\{q_9\}]_{p.p.} = C_{20}$ .

2)  $[C_2 \cup \{q_9\}]_{p.p.} = [[\{q_1, q_2\}]_{p.p.} \cup \{q_9\}]_{p.p.} = [\{q_1, q_2, q_9, q_{10}\}]_{p.p.} = C_{21}$ ,  
так как

$$q_{10}(x_1, x_2) = \exists y_1 (q_1(x_1, y_1) \wedge q_9(y_1, x_2)).$$

3)  $[C_3 \cup \{q_9\}]_{p.p.} = [[\{q_2\}]_{p.p.} \cup \{q_9\}]_{p.p.} = [\{q_2, q_9, q_{10}\}]_{p.p.} = C_{22}$ , так как

$$q_{10}(x_1, x_2) = \exists y_1 (q_2(x_1, y_1) \wedge q_9(y_1, x_2)).$$

4)  $[C_4 \cup \{q_9\}]_{p.p.} = [[\{q_3, q_7\}]_{p.p.} \cup \{q_9\}]_{p.p.} = [\{q_3, q_7, q_9, q_{10}\}]_{p.p.} = C_{23}$ ,  
так как

$$q_{10}(x_1, x_2) = \exists y_1 (q_9(x_1, y_1) \wedge q_3(y_1, x_2)).$$

5)  $[C_7 \cup \{q_9\}]_{p.p.} = [[\{q_4\}]_{p.p.} \cup \{q_9\}]_{p.p.} = [\{q_4, q_9, q_{10}\}]_{p.p.} = C_{24}$ , так как

$$q_{10}(x_1, x_2) = \exists y_1 (q_4(x_1, y_1) \wedge q_9(y_1, x_2)).$$

6)  $[C_8 \cup \{q_9\}]_{p.p.} = [[\{q_1, q_2, q_4, q_6\}]_{p.p.} \cup \{q_9\}]_{p.p.} = [\{q_1, q_2, q_4, q_6, q_9, q_{10}\}]_{p.p.} = C_{25}$ , так как

$$q_{10}(x_1, x_2) = \exists y_1 (q_1(x_1, y_1) \wedge q_9(y_1, x_2)).$$

7)  $[C_9 \cup \{q_9\}]_{p.p.} = [[\{q_3, q_4, q_7, q_8\}]_{p.p.} \cup \{q_9\}]_{p.p.} = [\{q_3, q_4, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_{26}$ , так как

$$q_{10}(x_1, x_2) = \exists y_1 (q_9(x_1, y_1) \wedge q_3(y_1, x_2)).$$

8)  $[C_{13} \cup \{q_9\}]_{p.p.} = [[\{q_2, q_6\}]_{p.p.} \cup \{q_9\}]_{p.p.} = [\{q_2, q_6, q_9, q_{10}\}]_{p.p.} = C_{27}$ ,  
так как

$$q_{10}(x_1, x_2) = \exists y_1 (q_2(x_1, y_1) \wedge q_9(y_1, x_2)).$$

9)  $[C_{14} \cup \{q_9\}]_{p.p.} = [[\{q_1, q_2, q_6\}]_{p.p.} \cup \{q_9\}]_{p.p.} = [\{q_1, q_2, q_6, q_9, q_{10}\}]_{p.p.} = C_{28}$ , так как

$$q_{10}(x_1, x_2) = \exists y_1 (q_1(x_1, y_1) \wedge q_9(y_1, x_2)).$$

- 10)  $[C_{15} \cup \{q_9\}]_{p.p.} = [[\{q_7\}]_{p.p.} \cup \{q_9\}]_{p.p.} = [\{q_7, q_9, q_{10}\}]_{p.p.} = C_{29}$ , так как

$$q_{10}(x_1, x_2) = \exists y_1 (q_9(x_1, y_1) \wedge q_7(y_1, x_2)).$$

- 11)  $[C_{18} \cup \{q_9\}]_{p.p.} = [[\{q_7, q_8\}]_{p.p.} \cup \{q_9\}]_{p.p.} = [\{q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_{30}$ , так как

$$q_{10}(x_1, x_2) = \exists y_1 (q_9(x_1, y_1) \wedge q_7(y_1, x_2)).$$

- 12)  $[C_{19} \cup \{q_9\}]_{p.p.} = [[\{q_3, q_7, q_8\}]_{p.p.} \cup \{q_9\}]_{p.p.} = [\{q_3, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_{31}$ , так как

$$q_{10}(x_1, x_2) = \exists y_1 (q_9(x_1, y_1) \wedge q_3(y_1, x_2)).$$

Таким образом,  $Classes(9) = \{C_1, C_2, \dots, C_{31}\}$ .

### 5.10. Добавление предиката $q_{10}$

- 1)  $[C_1 \cup \{q_{10}\}]_{p.p.} = [[\emptyset]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_9, q_{10}\}]_{p.p.} = C_{32}$ , так как

$$q_9(x_1, x_2) = q_{10}(x_1, x_2) \wedge q_{10}(x_2, x_1).$$

- 2)  $[C_2 \cup \{q_{10}\}]_{p.p.} = [[\{q_1, q_2\}]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_1, q_2, q_9, q_{10}\}]_{p.p.} = C_{21}$ , так как

$$q_9(x_1, x_2) = q_{10}(x_1, x_2) \wedge q_{10}(x_2, x_1).$$

- 3)  $[C_3 \cup \{q_{10}\}]_{p.p.} = [[\{q_2\}]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_2, q_9, q_{10}\}]_{p.p.} = C_{22}$ , так как

$$q_9(x_1, x_2) = q_{10}(x_1, x_2) \wedge q_{10}(x_2, x_1).$$

- 4)  $[C_4 \cup \{q_{10}\}]_{p.p.} = [[\{q_3, q_7\}]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_3, q_7, q_9, q_{10}\}]_{p.p.} = C_{23}$ , так как

$$q_9(x_1, x_2) = q_{10}(x_1, x_2) \wedge q_{10}(x_2, x_1).$$

- 5)  $[C_7 \cup \{q_{10}\}]_{p.p.} = [[\{q_4\}]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_4, q_9, q_{10}\}]_{p.p.} = C_{24}$ , так как

$$q_9(x_1, x_2) = q_{10}(x_1, x_2) \wedge q_{10}(x_2, x_1).$$

6)  $[C_8 \cup \{q_{10}\}]_{p.p.} = [[\{q_1, q_2, q_4, q_6\}]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_1, q_2, q_4, q_6, q_9, q_{10}\}]_{p.p.} = C_{25}$ , так как

$$q_9(x_1, x_2) = q_{10}(x_1, x_2) \wedge q_{10}(x_2, x_1).$$

7)  $[C_9 \cup \{q_{10}\}]_{p.p.} = [[\{q_3, q_4, q_7, q_8\}]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_3, q_4, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_{26}$ , так как

$$q_9(x_1, x_2) = q_{10}(x_1, x_2) \wedge q_{10}(x_2, x_1).$$

8)  $[C_{10} \cup \{q_{10}\}]_{p.p.} = [[\{q_5, q_9\}]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_5, q_9, q_{10}\}]_{p.p.} = C_{33}$ .

9)  $[C_{13} \cup \{q_{10}\}]_{p.p.} = [[\{q_2, q_6\}]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_2, q_6, q_9, q_{10}\}]_{p.p.} = C_{27}$ , так как

$$q_9(x_1, x_2) = q_{10}(x_1, x_2) \wedge q_{10}(x_2, x_1).$$

10)  $[C_{14} \cup \{q_{10}\}]_{p.p.} = [[\{q_1, q_2, q_6\}]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_1, q_2, q_6, q_9, q_{10}\}]_{p.p.} = C_{28}$ , так как

$$q_9(x_1, x_2) = q_{10}(x_1, x_2) \wedge q_{10}(x_2, x_1).$$

11)  $[C_{15} \cup \{q_{10}\}]_{p.p.} = [[\{q_7\}]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_7, q_9, q_{10}\}]_{p.p.} = C_{29}$ , так как

$$q_9(x_1, x_2) = q_{10}(x_1, x_2) \wedge q_{10}(x_2, x_1).$$

12)  $[C_{18} \cup \{q_{10}\}]_{p.p.} = [[\{q_7, q_8\}]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_{30}$ , так как

$$q_9(x_1, x_2) = q_{10}(x_1, x_2) \wedge q_{10}(x_2, x_1).$$

13)  $[C_{19} \cup \{q_{10}\}]_{p.p.} = [[\{q_3, q_7, q_8\}]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_3, q_7, q_8, q_9, q_{10}\}]_{p.p.} = C_{31}$ , так как

$$q_9(x_1, x_2) = q_{10}(x_1, x_2) \wedge q_{10}(x_2, x_1).$$

14)  $[C_{20} \cup \{q_{10}\}]_{p.p.} = [[\{q_9\}]_{p.p.} \cup \{q_{10}\}]_{p.p.} = [\{q_9, q_{10}\}]_{p.p.} = C_{32}$ .

Таким образом,  $Classes(10) = \{C_1, C_2, \dots, C_{33}\}$ .

## 6. Доказательство леммы 3

На втором шаге доказательства (раздел 2) мы показали, что клонов трёхзначной логики, содержащих функции  $0, 1, 2, \min, \max$ , не более чем 33. При этом каждый такой клон является классом сохранения множества предикатов  $\pi(v)$  для некоторой вершины  $v$  диаграммы 1. Для завершения доказательства основной теоремы нам нужно показать, что различные вершины диаграммы определяют различные клоны, т. е. если  $v', v''$  — две различные вершины диаграммы 1, то

$$\text{Pol}(\pi(v')) \neq \text{Pol}(\pi(v'')).$$

Для того чтобы доказать этот факт, мы укажем список функций  $f_1, \dots, f_9$ , таких что для различных вершин  $v', v''$

$$(\text{Pol}(v') \cap \{f_1, \dots, f_9\}) \neq (\text{Pol}(v'') \cap \{f_1, \dots, f_9\}).$$

Пусть  $f_1, \dots, f_9$  — одноместные функции трёхзначной логики, определённые следующим образом:

$x$	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$	$f_7(x)$	$f_8(x)$	$f_9(x)$
0	1	1	2	0	2	0	2	0	1
1	0	1	1	0	2	0	1	2	2
2	0	0	0	1	1	2	2	2	2

В следующей таблице для каждой вершины  $v$  диаграммы символом «+» отмечены те и только те из функций  $f_1, \dots, f_9$ , которые сохраняют все предикаты из  $\pi(v)$ . Как можно видеть, у любых двух различных строк таблицы множества функций, помеченных символом «+», различаются, что завершает доказательство леммы 3.

	$f_1$	$f_2$	$f_3$	$f_4$	$f_5$	$f_6$	$f_7$	$f_8$	$f_9$
$v_1$	+	+	+	+	+	+	+	+	+
$v_2$		+		+	+	+			
$v_3$	+	+		+	+	+			
$v_4$	+						+	+	+
$v_5$									
$v_6$	+								
$v_7$				+		+		+	+
$v_8$				+		+			
$v_9$								+	+
$v_{10}$		+	+				+		
$v_{11}$		+							
$v_{12}$							+		
$v_{13}$	+	+		+		+			
$v_{14}$		+		+		+			
$v_{15}$	+				+		+	+	+
$v_{16}$					+				
$v_{17}$	+				+				
$v_{18}$					+		+	+	+
$v_{19}$							+	+	+
$v_{20}$	+	+	+	+	+		+		+
$v_{21}$		+		+	+				
$v_{22}$	+	+		+	+				
$v_{23}$	+						+		+
$v_{24}$				+					+
$v_{25}$				+					
$v_{26}$									+
$v_{27}$	+	+		+					
$v_{28}$		+		+					
$v_{29}$	+				+		+		+
$v_{30}$					+		+		+
$v_{31}$							+		+
$v_{32}$	+	+		+	+		+		+
$v_{33}$		+					+		

## Благодарности

Автор выражает благодарность к. ф.-м. н. Жуку Дмитрию Николаевичу за внимание к работе и полезные замечания.

## Список литературы

- [1] Geiger D. Closed systems of functions and predicates. Pacific journal of mathematics. 1968 Oct 1; 27(1), 95-100.
- [2] Боднарчук В. Г., Калужнин Л. А., Котов В. Н., Ромов Б. А. Теория Галуа для алгебр Поста. Кибернетика. 1969. №3. с. 1—10 (часть I); №5. с. 1—9 (часть II).
- [3] Baker K. A., Pixley A. F. Polynomial interpolation and the Chinese remainder theorem for algebraic systems. Math. Zeitschrift 143 (1975), 165-174.

### **The lattice of all clones on the three-element set containing functions $0, 1, 2, \min, \max$ Moiseev S. V.**

This paper describes the lattice of all clones on the three-element set that contain all constant functions  $0, 1, 2$  and functions  $\min, \max$ . The clones are characterized as sets of predicates being preserved by them.

**Keywords:** clone theory, lattice of clones, three-valued logic.

# О количестве регулярных языков, представимых в групповых гиперавтоматах

Самоненко И.Ю.

Назовем гиперавтоматом конечный автомат, состояниями которого являются множества состояний некоторого конечного автомата. Гиперавтомат называется групповым, если полугруппа автомата, на базе которого он построен, является группой. В работе изучается вопрос о максимальном количестве регулярных языков, представимых в групповых гиперавтоматах.

**Ключевые слова:** конечные автоматы, гиперавтоматы, регулярные языки, конечные группы.

Пусть  $X$  - конечное множество и  $s$  - натуральное число. Обозначим  $X^{\{s\}} = \{T \subset X \mid |T| \leq s\}$  - множество всех подмножеств  $X$ , состоящее не более чем из  $s$  элементов.

Пусть  $\mathfrak{A} = (A, Q, \varphi)$  - конечный автомат. Обозначим

$$\mathfrak{A}^{\{s\}} = (A, Q^{\{s\}}, \varphi^{\{s\}}),$$

где

$$\varphi^{\{s\}}(\{q_1, \dots, q_k\}, a) = \{\varphi(q_1, a), \dots, \varphi(q_k, a)\},$$

при  $k \leq s$ . Доопределим  $\varphi^{\{s\}}(\emptyset, a) = \emptyset$ . Автомат  $\mathfrak{A}^{\{s\}}$  будем называть гиперавтоматом (3 типа) степени  $s$ . Автомат  $\mathfrak{A}$  назовем базой гиперавтомата  $\mathfrak{A}^{\{s\}}$ .

*Замечание.* Помимо гиперавтоматов построенных на множествах состояний исходного автомата (3 тип), также можно рассматривать гиперавтоматы, построенные на векторах состояний исходного автомата (1 тип) и на множествах с повторениями состояний исходного автомата (2 тип)[4]. В данной работе рассматриваются только гиперавтоматы 3 типа.

Пусть  $\mathfrak{A} = (A, Q, \varphi)$  - конечный автомат,  $q_0 \in Q$  и  $F \subseteq Q$ , тогда через  $L(\mathfrak{A}, q_0, F)$  обозначим регулярный язык, представимый в автомате  $\mathfrak{A}$  при

помощи начального состояния  $q_0$  и множества финальных состояний  $F$ . Через  $L(\mathfrak{A}) = \{L(\mathfrak{A}, q_0, F) | q_0 \in Q, F \subseteq Q\}$  обозначим множество всех регулярных языков, представимых в автомате  $\mathfrak{A}$ .

Назовем язык  $L \subseteq A^*$  тривиальным, если  $L = \emptyset$  или  $L = A^*$ . В противном случае язык  $L$  - нетривиальный.

Через  $\Omega_n$  - обозначим множество всех групповых автоматов с  $n$  состояниями и  $|A| \geq 2$  [1]. Через  $\Omega_n^{\{s\}} = \{\mathfrak{A}^{\{s\}} | \mathfrak{A} \in \Omega_n\}$  - обозначим множество всех гиперавтоматов степени  $s$ , базами для которых являются групповые автоматы с  $n$  состояниями.

Изучение альтернативных способов представления регулярных языков в конечных автоматах является актуальной задачей [2],[3].

Цель данной работы — изучить вопросы представления регулярных языков в групповых гиперавтоматах и найти оценку максимального количества регулярных языков, представимых в одном групповом гиперавтомате:

$$N(n, s) = \max_{\mathfrak{A}^{\{s\}} \in \Omega_n^{\{s\}}} |L(\mathfrak{A}^{\{s\}})|.$$

**Лемма 1.** Пусть  $\mathfrak{A} = (A, Q, \varphi) \in \Omega_n$ , нетривиальный язык  $L = L(\mathfrak{A}^{\{s\}}, \tilde{p}_0, F_1)$  и  $|\tilde{p}_0| = k > \frac{n}{2}$ , тогда существуют состояние  $\tilde{p}'_0 \in Q^{\{s\}}$  и такое множество финальных состояний  $F'_1 \subset Q^{\{s\}}$ , такие что  $|\tilde{p}'_0| < \frac{n}{2}$  и  $L = L(\mathfrak{A}^{\{s\}}, \tilde{p}'_0, F'_1)$ .

**Доказательство.** Пусть  $F_1 = \{\tilde{p}_1, \dots, \tilde{p}_r\}$ . В силу того, что автомат  $\mathfrak{A}$  - групповой, без ограничения общности можем считать, что  $k = |\tilde{p}_0| = |\tilde{p}_1| = \dots = |\tilde{p}_r|$ . Положим  $\tilde{p}'_i = Q \setminus \tilde{p}_i$ , ( $0 \leq i \leq r$ ). Для любого  $\alpha \in L$  имеем  $\varphi^{\{s\}}(\tilde{p}_0, \alpha) = \tilde{p}_t$  тогда и только тогда, когда  $\varphi^{\{s\}}(\tilde{p}'_0, \alpha) = \tilde{p}'_t$ . Следовательно  $L = L(\mathfrak{A}^{\{s\}}, \tilde{p}'_0, F'_1)$ . ■

Через  $\mathfrak{S}_n = (A, Q, \varphi)$  обозначим произвольный групповой автомат с  $n$  состояниями, реализующий симметрическую группу на множестве своих состояний.

**Лемма 2.** Для произвольного автомата  $\mathfrak{S}_n^{\{s\}}$ , для любых состояний  $\tilde{q}_1, \dots, \tilde{q}_r, \tilde{p}_1, \dots, \tilde{p}_r \in Q^{\{s\}}$ , таких что  $|\tilde{p}_i| = |\tilde{q}_i|$  ( $1 \leq i \leq r$ ),  $\tilde{q}_i \cap \tilde{q}_j = \emptyset$  и  $\tilde{p}_i \cap \tilde{p}_j = \emptyset$  ( $1 \leq i < j \leq r$ ) существует слово  $\beta \in A^*$ , такое что  $\varphi^{\{s\}}(\tilde{q}_i, \beta) = \tilde{p}_i$

**Доказательство.** Пусть

$$\tilde{q}_i = \{q_{i,1}, \dots, q_{i,t_i}\}, \quad \tilde{p}_i = \{p_{i,1}, \dots, p_{i,t_i}\}.$$

По условию все  $q_{i,j}$  - разные и все  $p_{i,j}$  - разные. В силу того, что автомат  $\mathfrak{S}_n$  реализует симметрическую группу, то существует слово  $\beta$ , такое что

$$\varphi(q_{i,j}, \beta) = p_{i,j}.$$

Очевидно, что для данного  $\beta$  имеем

$$\varphi^{\{s\}}(\tilde{q}_i, \alpha) = \tilde{p}_i.$$

■

Предположим, что некоторый регулярный язык  $L$  задается разными способами в одном и том же гиперавтомате  $\mathfrak{S}_n^{\{s\}}$  при помощи разных начальных состояний  $\tilde{q}_1$  и  $\tilde{q}_2$ , т.е.

$$L = L(\mathfrak{S}_n^{\{s\}}, \tilde{q}_1, F_1) = L(\mathfrak{S}_n^{\{s\}}, \tilde{q}_2, F_2).$$

Рассмотрим произвольные финальные состояния  $\tilde{q}_3 \in F_1$  и  $\tilde{q}_4 \in F_2$ , соответствующие одному и тому же слову  $\alpha \in L$ , т.е.  $\varphi^{\{s\}}(\tilde{q}_1, \alpha) = \tilde{q}_3$  и  $\varphi^{\{s\}}(\tilde{q}_2, \alpha) = \tilde{q}_4$  и предположим, что  $Q \setminus (\tilde{q}_3 \cup \tilde{q}_4) \neq \emptyset$ . Данные условия будут общими в формулировках леммы 3, леммы 4, леммы 5, утверждения 1 и утверждения 2.

Далее будет доказан ряд лемм, в которых будет показано, что если существуют  $q_1 \in \tilde{q}_3$  и  $q_0 \in Q \setminus \tilde{q}_3$ , то

$$\tilde{q} = \tilde{q}_3 \cup \{q_0\} \setminus \{q_1\} \in F_1.$$

Доказательства будут зависеть от взаимного расположения состояний  $\tilde{q}_3$ ,  $\tilde{q}_4$ ,  $q_0$  и  $q_1$ . Существует 8 различных вариантов (Рис. 1.)

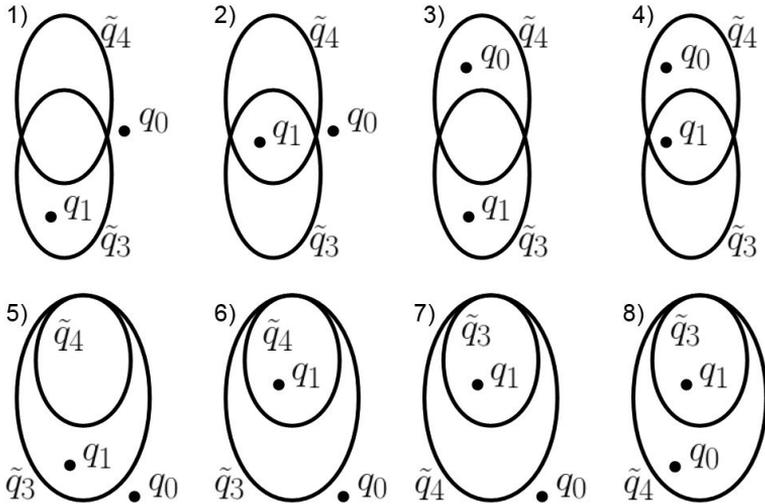


Рис. 1.

Заметим, что в силу того, что автомат  $\mathfrak{S}_n$  - групповой, то для любого  $\tilde{q} \in Q^{\{s\}}$  и любого слова  $\alpha \in A^*$  имеем  $|\tilde{q}| = |\varphi^{\{s\}}(\tilde{q}, \alpha)|$ .

**Лемма 3** (Разбор вариантов 1 и 5). В указанных выше условиях предположим, что  $q_1 \in \tilde{q}_3 \setminus \tilde{q}_4$  и  $q_0 \in Q \setminus (\tilde{q}_3 \cup \tilde{q}_4)$ . Тогда  $\tilde{q} = \tilde{q}_3 \cup \{q_0\} \setminus \{q_1\} \in F_1$ .

**Доказательство.** Рассмотрим  $q_3 \in \tilde{q}_1 \setminus \tilde{q}_2$ , такой что  $\varphi(q_3, \alpha) = q_1$ . В силу того, что:

$$\begin{aligned} |\tilde{q}_2 \setminus \tilde{q}_1| &= |\tilde{q}_4 \setminus \tilde{q}_3|, \\ |\tilde{q}_2 \cap \tilde{q}_1| &= |\tilde{q}_4 \cap \tilde{q}_3|, \\ |\tilde{q}_1 \setminus (\tilde{q}_2 \cup \{q_3\})| &= |\tilde{q}_3 \setminus (\tilde{q}_4 \cup \{q_1\})|. \end{aligned}$$

по лемме 2 существует слово  $\beta$  (Рис. 2.), такое что:

$$\begin{aligned} \varphi^{\{s\}}(\tilde{q}_2 \setminus \tilde{q}_1, \beta) &= \tilde{q}_4 \setminus \tilde{q}_3, \\ \varphi^{\{s\}}(\tilde{q}_2 \cap \tilde{q}_1, \beta) &= \tilde{q}_4 \cap \tilde{q}_3, \\ \varphi^{\{s\}}(\tilde{q}_1 \setminus (\tilde{q}_2 \cup \{q_3\}), \beta) &= \tilde{q}_3 \setminus (\tilde{q}_4 \cup \{q_1\}), \\ \varphi^{\{s\}}(\{q_3\}, \beta) &= \{q_0\}. \end{aligned}$$

Из первых двух условий следует, что  $\varphi_s(\tilde{q}_2, \beta) = \varphi_s(\tilde{q}_2 \setminus \tilde{q}_1, \beta) \cup \varphi_s(\tilde{q}_2 \cap \tilde{q}_1, \beta) = (\tilde{q}_4 \setminus \tilde{q}_3) \cup (\tilde{q}_4 \cap \tilde{q}_3) = \tilde{q}_4$ , поэтому  $\beta \in L$ .

Из второго, третьего и четвертого условия следует, что:  $\varphi_s(\tilde{q}_1, \beta) = \tilde{q}_3 \cup \{q_0\} \setminus \{q_1\}$ . И в силу того, что  $\beta \in L$  получаем, что  $\tilde{q} = \varphi_s(\tilde{q}_1, \beta) \in F_1$ .

Заметим, что в рассуждениях допускается  $\tilde{q}_4 \setminus \tilde{q}_3 = \emptyset$ , т.е. вариант 5 также разобран. ■

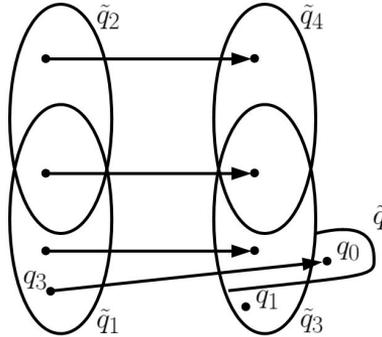


Рис. 2.

**Лемма 4** (Разбор варианта 3). В указанных выше условиях, предположим, что  $q_1 \in \tilde{q}_3 \setminus \tilde{q}_4$  и  $q_0 \in \tilde{q}_4 \setminus \tilde{q}_3$ .

**Доказательство.** В силу того,  $Q \setminus (\tilde{q}_3 \cup \tilde{q}_3) \neq \emptyset$ , рассмотрим произвольное состояние  $q_2 \in Q \setminus (\tilde{q}_3 \cup \tilde{q}_3)$ . По лемме 3, при взаимной замене в условии  $F_1$  и  $F_2$ ,  $\tilde{q}_1$  и  $\tilde{q}_2$ ,  $\tilde{q}_3$  и  $\tilde{q}_4$ , рассмотрении  $\tilde{q}_5$  вместо  $\tilde{q}$ , рассмотрении  $q_0$  вместо  $q_1$  и рассмотрении  $q_2$  вместо  $q_0$  имеем, что существует слово  $\beta$ , для которого  $\varphi^{\{s\}}(\tilde{q}_1, \beta) = \tilde{q}_3$  и  $\varphi^{\{s\}}(\tilde{q}_2, \beta) = \tilde{q}_5$ , где  $\tilde{q}_5 = \tilde{q}_4 \cup \{q_2\} \setminus \{q_0\}$ . Теперь еще раз можно воспользоваться леммой 3, но уже при условии, что мы рассматриваем  $\tilde{q}_5$  вместо  $\tilde{q}_4$ . Получим, состояние  $\tilde{q} = \tilde{q}_3 \cup \{q_0\} \setminus \{q_1\} \in F_1$ . ■

**Лемма 5** (Разбор вариантов 4 и 8). В указанных выше условиях, предположим, что  $q_1 \in \tilde{q}_3 \cap \tilde{q}_4$  и  $q_0 \in \tilde{q}_4 \setminus \tilde{q}_3$ .

**Доказательство.** Рассмотрим  $q_2 \in \tilde{q}_1 \cap \tilde{q}_2$  и  $q_3 \in \tilde{q}_2 \setminus \tilde{q}_1$ , такие что  $\varphi(q_2, \alpha) = q_1$  и  $\varphi(q_3, \alpha) = q_0$ . В силу того, что:

$$\begin{aligned} |\tilde{q}_2 \setminus (\tilde{q}_1 \cup \{q_3\})| &= |\tilde{q}_4 \setminus (\tilde{q}_3 \cup \{q_0\})|, \\ |(\tilde{q}_2 \cap \tilde{q}_1) \setminus \{q_2\}| &= |(\tilde{q}_4 \cap \tilde{q}_3) \setminus \{q_1\}|, \\ |\tilde{q}_1 \setminus \tilde{q}_2| &= |\tilde{q}_3 \setminus \tilde{q}_4|. \end{aligned}$$

по лемме 2 существует слово  $\beta$ , такое что:

$$\begin{aligned} \varphi^{\{s\}}(\tilde{q}_2 \setminus (\tilde{q}_1 \cup \{q_3\}), \beta) &= \tilde{q}_4 \setminus (\tilde{q}_3 \cup \{q_0\}), \\ \varphi^{\{s\}}((\tilde{q}_2 \cap \tilde{q}_1) \setminus \{q_2\}, \beta) &= (\tilde{q}_4 \cap \tilde{q}_3) \setminus \{q_1\}, \\ \varphi^{\{s\}}(\tilde{q}_1 \setminus \tilde{q}_2, \beta) &= \tilde{q}_3 \setminus \tilde{q}_4, \\ \varphi^{\{s\}}(\{q_2\}, \beta) &= \{q_0\}, \\ \varphi^{\{s\}}(\{q_3\}, \beta) &= \{q_1\}. \end{aligned}$$

При этом видно, что  $\varphi^{\{s\}}(\tilde{q}_2, \beta) = \varphi^{\{s\}}(\tilde{q}_2, \alpha) = \tilde{q}_4$ , следовательно  $\beta \in L$ . Кроме того,  $\varphi^{\{s\}}(\tilde{q}_1, \beta) = \tilde{q}_3 \cup \{q_0\} \setminus \{q_1\}$ . Следовательно  $\tilde{q} = \tilde{q}_3 \cup \{q_0\} \setminus \{q_1\} \in F_1$ .

Заметим, что в рассуждениях допускается  $\tilde{q}_3 \setminus \tilde{q}_4 = \emptyset$ , т.е. вариант 8 также разобран. ■

При помощи леммы 3 нетрудно свести вариант 2 к варианту 3 и вариант 7 варианту 8. А именно, добавляем в  $\tilde{q}_4$  элемент  $q_0$  и убираем произвольный элемент из  $\tilde{q}_4 \setminus \tilde{q}_3$ .

Далее, при помощи леммы 5 можно свести вариант 6 к варианту 5. А именно, добавляем в  $\tilde{q}_4$  произвольный элемент из  $\tilde{q}_3 \setminus \tilde{q}_4$  и убираем элемент  $q_1$ .

Из доказанных выше лемм и сделанных замечаний непосредственно вытекает следующее утверждение.

**Утверждение 1.** В указанных выше условиях, если  $q_1 \in \tilde{q}_3$  и  $q_0 \in Q \setminus \tilde{q}_3$ , то

$$\tilde{q} = \tilde{q}_3 \cup \{q_0\} \setminus \{q_1\} \in F_1.$$

**Утверждение 2.** В указанных выше условиях, если  $|\tilde{q}| = |\tilde{q}_1|$ , то  $\tilde{q} \in F_1$ .

Утверждение 2. доказывается непосредственно из утверждения 1. индукцией по  $|\tilde{q} \setminus \tilde{q}_1|$ . ■

Другими словами, рассматриваемые выше условия означают, что язык  $L = A^*$ , т.к. все состояния автомата  $\mathfrak{S}_n^{\{s\}}$  являются финальными.

Для произвольного состояния  $\tilde{q}$  гиперавтомата  $\mathfrak{S}_n^{\{s\}}$  обозначим  $\tilde{q}' = Q \setminus \tilde{q}$ . Аналогично для произвольного множества состояний  $F$  гиперавтомата  $\mathfrak{S}_n^{\{s\}}$  обозначим  $F' = \{\tilde{q}' | \tilde{q} \in F\}$ .

**Утверждение 3.** Пусть  $L = L(\mathfrak{S}_n^{\{s\}}, \tilde{q}_1, F_1) = L(\mathfrak{S}_n^{\{s\}}, \tilde{q}_2, F_2)$  - нетривиальный язык.

1. Если  $|\tilde{q}_1| \leq n/2$  и  $|\tilde{q}_2| < n/2$ , то  $\tilde{q}_1 = \tilde{q}_2$  и  $F_1 = F_2$ .
2. Если  $|\tilde{q}_1| = |\tilde{q}_2| = n/2$ , то либо  $\tilde{q}_1 = \tilde{q}_2$  и  $F_1 = F_2$ , либо  $\tilde{q}_1 = \tilde{q}'_2$  и  $F_1 = F'_2$ .

**Доказательство.** 1. Пусть  $|\tilde{q}_1| \leq n/2$ ,  $|\tilde{q}_2| < n/2$ . Предположим, что  $\tilde{q}_1 \neq \tilde{q}_2$ . Рассмотрим произвольное слово  $\alpha \in L$ ,  $\tilde{q}_3 = \varphi_3(\tilde{q}_1, \alpha)$  и  $\tilde{q}_4 = \varphi_3(\tilde{q}_2, \alpha)$ . В силу того, что  $|\tilde{q}_3| = |\tilde{q}_1|$  и  $|\tilde{q}_4| = |\tilde{q}_2|$ , имеем  $Q \setminus (\tilde{q}_4 \cup \tilde{q}_2) \neq \emptyset$ . Рассмотрим произвольное слово  $\beta \in A^*$  и состояние  $\tilde{q}_5 = \varphi_3(\tilde{q}_1, \beta)$ . Ясно, что  $|\tilde{q}_5| = |\tilde{q}_1|$ , поэтому из утверждения 1. имеем  $\tilde{q}_5 \in F_1$ , следовательно  $\beta \in L$  и  $L = A^*$ , что противоречит нетривиальности языка  $L$ . Следовательно  $\tilde{q}_1 = \tilde{q}_2$ . Из  $L(\mathfrak{S}_n^{\{s\}}, \tilde{q}_1, F_1) = L(\mathfrak{S}_n^{\{s\}}, \tilde{q}_1, F_2)$  очевидным образом следует  $F_1 = F_2$ .

2. Пусть  $|\tilde{q}_1| = |\tilde{q}_2| = n/2$ . В силу того для любого  $\alpha \in A^*$  выполняется соотношение  $|\varphi_3(\tilde{q}_1, \alpha)| = |\varphi_3(\tilde{q}_2, \alpha)| = n/2$ , то без ограничения общности можем считать, что для любых  $\tilde{q}_3 \in F_1$  и  $\tilde{q}_4 \in F_2$  выполняется соотношение  $|\tilde{q}_3| = |\tilde{q}_4| = n/2$ . Предположим, что  $\tilde{q}_1 \neq \tilde{q}_2$ . Если  $\tilde{q}_1 \cap \tilde{q}_2 \neq \emptyset$ , то проводя рассуждения приведенные выше приходим к противоречию с нетривиальностью языка  $L$ . Следовательно  $\tilde{q}_1 \cap \tilde{q}_2 = \emptyset$ , что в нашем случае эквивалентно  $\tilde{q}_1 = \tilde{q}'_2$ . Предположим, что  $F_1 \neq F'_2$ . Без ограничения общности считаем, что существует  $\tilde{q}_3 \in F_1$ , но  $\tilde{q}'_3 \notin F'_2$ . По лемме 2 существует слово  $\alpha \in E_2^*$ , такое что  $\varphi_3(\tilde{q}_1, \alpha) = \tilde{q}_3$ , но из это следует, что  $\varphi_3(\tilde{q}'_1, \alpha) = \tilde{q}'_3$ , следовательно  $\tilde{q}'_3 \in F'_2$ . Получили противоречие. Таким образом  $F_1 = F'_2$ , что завершает доказательство утверждения. ■

Суть утверждения 3 заключается в следующем: в автомате  $\mathfrak{S}_n^{\{s\}}$  разным парам  $(\tilde{q}_1, F_1)$  и  $(\tilde{q}_2, F_2)$ , при  $|\tilde{q}_1| \leq n/2$  и  $|\tilde{q}_1| < n/2$ , соответствуют разные регулярные языки (при условии что эти языки нетривиальны). В случае  $|\tilde{q}_1| = n/2$  и  $|\tilde{q}_2| = n/2$  разные пары  $(\tilde{q}_1, F_1)$  и  $(\tilde{q}_2, F_2)$  могут задавать один и тот же язык только при условии  $\tilde{q}_1 = \tilde{q}'_2$  и  $F_1 = F'_2$ .

**Лемма 6.**

$$|L(\mathfrak{S}_n^{\{s\}})| = \begin{cases} \sum_{t=1}^s ((2^{C_n^t} - 2)C_n^t) + 2, & \text{при } s < n/2 \\ \sum_{t=1}^k ((2^{C_n^t} - 2)C_n^t) + 2, & \text{при } s > n/2, \quad n = 2k + 1 \\ \sum_{t=1}^{k-1} ((2^{C_n^t} - 2)C_n^t) + \\ + \frac{1}{2}((2^{C_n^k} - 2)C_n^k) + 2, & \text{при } s \geq n/2, \quad n = 2k \end{cases}$$

**Доказательство.** Пусть  $s < n/2$ . Зафиксируем  $t \in \{1, \dots, s\}$ . Начальное состояние  $\tilde{q}$ , такое что  $|\tilde{q}| = t$  можно выбрать  $C_n^t$  способами. Множество финальных состояний (каждое финальное состояние имеет мощность  $t$ ) можно выбрать  $2^{C_n^t}$  способами. При этом удалим два случая, когда это множество состояний пусто, или состоит из всех подмножеств мощности  $t$ . В случаях случая задаваемый язык тривиален. Всего получается  $C_n^t(2^{C_n^t} - 2)$  комбинаций. В силу утверждения 3 и сказанного выше замечания все языки получаются разными. Варьируя  $t$  в указанном интервале так же получаем различные языки. Таким образом число нетривиальных языков во множестве  $L(\mathfrak{S}_n^{\{s\}})$  равно

$$\sum_{t=1}^s ((2^{C_n^t} - 2)C_n^t)$$

Пусть  $n = 2k$  и  $s = n/2 = k$ . Если  $t \in \{1, \dots, k-1\}$ , то рассуждения полностью аналогичны вышеизложенным. Если  $t = k$ , то при подсчете числа  $C_n^t(2^{C_n^t} - 2)$  каждый язык был подсчитан дважды. Таким образом, число нетривиальных языков во множестве  $L(\mathfrak{S}_n^{\{s\}})$  равно

$$\sum_{t=1}^{k-1} ((2^{C_n^t} - 2)C_n^t) + \frac{1}{2}((2^{C_n^k} - 2)C_n^k)$$

Если  $s > n/2$ , то, в силу леммы 1 и сделанного выше замечания,  $L(\mathfrak{S}_n^{\{s\}}) = L(\mathfrak{S}_n^{\{\lfloor n/2 \rfloor\}})$ , где  $\lfloor x \rfloor$  - целая часть снизу от числа  $x$ . ■

**Теорема 1.**

$$N(n, s) = \begin{cases} \sum_{t=1}^s ((2^{C_n^t} - 2)C_n^t) + 2, & \text{при } s < n/2 \\ \sum_{t=1}^k ((2^{C_n^t} - 2)C_n^t) + 2, & \text{при } s > n/2, \quad n = 2k + 1 \\ \sum_{t=1}^{k-1} ((2^{C_n^t} - 2)C_n^t) + \\ + \frac{1}{2}((2^{C_n^k} - 2)C_n^k) + 2, & \text{при } s \geq n/2, \quad n = 2k \end{cases}$$

**Доказательство.** Оценка значения  $N(n, s)$  снизу непосредственно следует из леммы 6.

Заметим, что оценка значения  $N(n, s)$  сверху в точности повторяет доказательство леммы 6. Действительно, лемма 1 верна для любого группового гиперавтомата, а перебор всевозможных начальных и множества финальных состояний также был осуществлен в лемме 6. ■

**Следствие.** При фиксированном  $s$  и  $n \rightarrow \infty$  имеем

$$N(n, s) \sim C_n^s 2^{C_n^s}.$$

**Доказательство.** При  $1 \leq s \leq n/2$  имеем

$$\begin{aligned} & \frac{\sum_{t=1}^{s-1} (2^{C_n^t}) C_n^t}{(2^{C_n^s}) C_n^s} < \frac{(s-1)(2^{C_n^{s-1}}) C_n^{s-1}}{(2^{C_n^s}) C_n^s} = \\ & = \frac{(s-1) C_n^{s-1}}{C_n^s} 2^{-\frac{n!(n+1-2s)}{s!(n-s+1)!}} \rightarrow 0, \quad \text{при } n \rightarrow \infty. \end{aligned}$$

Следовательно,

$$\sum_{t=1}^s ((2^{C_n^t} - 2) C_n^t) + 2 \sim \sum_{t=1}^s (2^{C_n^t}) C_n^t \sim C_n^s 2^{C_n^s}.$$

■

## Список литературы

- [1] Кудрявцев В.Б., Алёшин С.В., Подколзин А.С. Введение в теорию автоматов. Изд-во «Наука», М., 1985.
- [2] Пархоменко Д.В. Вторая автоматная функция и с нею связанные классы регулярных языков.// Журнал Интеллектуальные системы. Теория и приложения, том 17, № 1-4, с. 186.
- [3] Бабин Д.Н., Пархоменко Д.В. О мультимножестве выходных слов конечного автомата.// Журнал Интеллектуальные системы. Теория и приложения, том 20, № 3, с. 101-103.
- [4] Самоненко И.Ю. О свойствах гиперавтоматов.// Материалы X Международного семинара Дискретная математика и ее приложения, 2010.

**The number of regular languages, recognized by group  
hyperautomata  
Samonenko I.U.**

A hyperautomata is a finite automata whose states are the sets of states of some finite automata. A hyperautomata is called a group hyperautomata if the semigroup of the automata on which it is based is a finite group. In this paper, we study the question of the maximum number of regular languages that can be recognized by group hyperautomata.

*Keywords:* finite automata, hyperautomata, regular languages, finite groups.



Часть 4.  
Материалы семинара «Теория  
автоматов»



## Доклады семинара «Теория автоматов»

Во втором квартале 2018 года на научном семинаре «Теория автоматов» под руководством академика Валерия Борисовича Кудрявцева состоялось 4 доклада.

21 марта 2018 года

### **Задачи оценки и мониторинга процессов в социотехнических системах: обзор постановок и результатов**

доцент Рыжов А. С.

В докладе рассмотрены задачи оценки состояния некоторого процесса и возможных вариантов его развития для смешанных человеко-технических систем. Примерами таких систем является любая компания, отрасль, социальная сеть, государство. Примерами таких процессов – поведение клиента (маркетинг), продвижение кандидата на выборах (политология), диагностика (медицина), оценка рисков (финансы, страховое дело); развитие технологий/научных исследований (наукометрия, технологии). Рассмотрены ключевые отличия моделей процессов для социотехнических систем и физических систем. Эти отличия определяют возможность применения тех или иных математических инструментов. Рассмотрены основные задачи разработки систем оценки и мониторинга процессов: описания человеком объектов реального мира, поиска информации в нечеткой среде, агрегирования информации в нечетких иерархических системах. Обсуждаются обобщения данных задач: персонализация взаимодействия с цифровым миром (на примере социальных сетей и обучающих программ); оптимизация описания объектов, определяемая задачей (task-driven information granulation) (на примере задач поиска информации и распознавания образов). Приводится краткий обзор разработанных на базе полученных результатов систем оценки и мониторинга соблюдения международных договоров, медицины, микроэлектроники, ситуационных центров органов государственной власти и управления. Диагностические эксперименты с конечными автоматами впервые были описаны в классической работе Э. Мура, и с тех пор применяются при решении практических и теоретических задач, возникающих в таких

областях как тестирование программ, диагностика неисправностей цифровых схем, а также при верификации коммуникационных протоколов. Если имеется полное описание некоторого конечного автомата Мили, но про его начальное состояние известно лишь то, что оно принадлежит некоторому фиксированному подмножеству состояний, то простой диагностический эксперимент для этого подмножества состоит в подаче на автомат такой входной последовательности, что по реакции автомата на нее можно однозначно сказать с каким начальным состоянием мы имели дело. В докладе будет рассказано об оценках длины для таких экспериментов и показана связь данной задачи с комбинаторными проблемами, возникающими в теории гиперграфов.

28 марта 2018 года

## **Проблема полноты в классах линейных автоматов**

доцент Часовских А. А.

Рассматриваются классы линейных автоматов над конечными полями с операциями композиции (суперпозиции и обратной связи). Для этих классов получен алгоритм проверки полноты конечных подмножеств. В случае простого поля найдены все предполные классы, множество которых является счетной приведенной критериальной системой. В общем случае строятся множества замкнутых классов, позволяющих свести проблему полноты к решению соответствующей задачи для трансцендентных расширений конечных полей. Решается задача о соответствии некоторых предполных классов класса линейных автоматов и максимальных подполей полученного расширения конечного поля. Показано, что критериальная система замкнутых классов и множество предполных классов счетны. Для случая конечных полей, не являющихся простыми, приведены примеры предполных классов, порождаемых максимальными подполями трансцендентных расширений этих полей.

4 апреля 2018 года

## О ранковой NAND флеш памяти

м.н.с. Соколов А. П.

Флеш память в последнее десятилетие стала доминирующей технологией для хранения информации как в персональных вычислительных средствах, так и в корпоративных продуктах: серверах, сетевых хранилищах и дата-центрах. Первоначально технология флеш памяти предполагала хранение одного бита информации в ячейке (SLC-память). Далее с развитием технологий изготовления флеш памяти, а также в связи с использованием во флеш памяти более мощных помехоустойчивых кодов, стало возможным хранить в каждой ячейке 2 бита (MLC-память) или даже 3 бита (TLC-память) информации. Увеличение объема информации, содержащейся в каждой ячейке, приводит к значительному росту вероятности ошибки при чтении. При этом, по мере износа флеш памяти, электрические заряды, хранящиеся в ячейках, имеют тенденцию к снижению. Этот процесс приводит к еще большему росту вероятности ошибок и фактически приводит к выходу флеш памяти из строя. Ранковый способ хранения информации в ячейках флеш памяти устойчив к процессу постепенного снижения электрических зарядов в ячейках. Более того, данный способ позволяет хранить в том же количестве ячеек больший объем информации. В докладе будет дано общее описание устройства флеш памяти, описана процедура чтения и показаны основные источники ошибок. Далее, будет описан способ хранения информации во флеш памяти с помощью ранков (перестановок). Будут даны оценки емкости данного типа памяти в сравнении с обычной флеш памятью. Будет введена метрика Кендалл-Тау на множестве перестановок и дана постановка задачи помехоустойчивого кодирования на множестве перестановок. Далее будет приведено сравнение емкости ранковой и обычной флеш памяти с учетом технологических ограничений. Показаны случаи большей эффективности ранковой памяти по сравнению с обычной.

11 апреля 2018 года

**О нижней оценке числа пороговых функций  
в терминах полных комбинаторных флагов  
на булевом кубе**

доцент Ирматов А. А.

Пусть  $E = \{w_1, \dots, w_{2^n}\}$  является множеством векторов в пространстве  $\mathbb{R}^{n+1}$  вида  $w_i = (1, \pm 1, \dots, \pm 1)$ ,  $i = 1, \dots, 2^n$ . Обозначим через  $\Lambda_n(E)$  множество упорядоченных наборов из различных векторов  $(w_{i_1}, \dots, w_{i_n})$ ,  $2 \leq i_1, \dots, i_n \leq 2^n$ , т.ч. вектор  $w_{i_k}$  является минимальным среди всех векторов из множества  $E \cap \text{span}\langle w_{i_k}, \dots, w_{i_n} \rangle$  для всех  $k$ ,  $1 \leq k \leq n$ . Автором было доказано, что для числа пороговых функций  $P(2, n)$  выполнена следующая нижняя оценка

$$P(2, n) \geq 2\Lambda_n(E).$$

В докладе для каждого упорядоченного подмножества  $E$  будет дано определение комбинаторного флага и приведена формула вычисления  $\Lambda_n(E)$  в терминах полных комбинаторных флагов множества  $E$ .

# Оценка и мониторинг процессов в социотехнических системах и связанные с ними задачи

Рыжов А. П.

В работе представлены основные проблемы разработки систем оценки и мониторинга процессов в социотехнических системах. Рассмотрены связанные с ними задачи и технологии. Приведены примеры их решения. Затронуты перспективные направления персонализации взаимодействия человека с цифровым миром и дополненного интеллекта (augmented intelligence). Статья подготовлена по результатам выступления автора на кафедральном семинаре кафедры Математической теории интеллектуальных систем механико-математического факультета МГУ имени М.В. Ломоносова «Теория автоматов» под руководством профессора В. Б. Кудрявцева 21 марта 2018 года.

**Ключевые слова:** Социотехнические системы, оценка и мониторинг сложных процессов, нечеткие множества, персонализация.

## 1. Введение

Системы оценки и мониторинга сложных процессов — специализированные человеко-компьютерные интеллектуальные информационные системы, предназначенные для оценки состояния некоторого процесса на базе фрагментарной, ненадежной, возможно недостоверной и противоречивой информации о нем и моделирования возможных сценариев его развития.

Социотехнические системы (СТС) — системы, включающие в себя две взаимодействующие компоненты: техническую и социальную. На языке кибернетики СТС — это система управления развитием организации [1]. Ниже организация нами будет пониматься достаточно широко: не столько как формальная структура, сколько как любая группа людей, взаимодействующая с технической компонентой для решения определен-

ной задачи (например, проектная команда или человек со смартфоном что-то ищущий в интернет).

Моделирование процессов в социотехнических системах отличается от моделирования процессов в физических системах. Три главных отличия представлены в табл. 1.

Физические процессы	Социальные процессы
Есть модели процессов в виде уравнений (например, уравнение теплопроводности)	Есть описания процессов на естественном языке или в виде параметрических зависимостей
Информация о значениях параметров измерима и однозначно интерпретируема (есть приборы)	Информация о значениях параметров доступна в виде оценок (измерительный прибор — человек), оценки одного и того же параметра могут не совпадать.
Повторяемость процессов. Возможно проведение экспериментов (например, для оценки вероятностей)	Уникальность процессов. Провести серию независимых экспериментов невозможно

Таблица 1. Отличия в моделировании физических и социальных процессов

Широкое распространение СТС, связанное с развитием интернета, автоматизации в обучении, медицине и других областях (см., например, [2]–[5]), делает задачу их изучения и анализа актуальной и осмысленной.

## 2. Основные проблемы разработки систем оценки и мониторинга процессов в социотехнических системах

Системы оценки и мониторинга изучаются автором с начала 90-х годов и достаточно широко представлены в научной литературе. В качестве обзорной работы можно порекомендовать [6], детали представлены в [7]. Основными проблемами разработки таких систем являются:

- Проблема 1. Можно ли, учитывая некоторые особенности восприятия человеком объектов реального мира и их описания, сформули-

ровать правило выбора оптимального множества значений признаков, по которым описываются эти объекты? Возможны два критерия оптимальности:

Критерий 1. Под оптимальными понимаются такие множества значений, используя которые человек испытывает минимальную неопределенность при описании объектов.

Критерий 2. Если объект описывается некоторым количеством экспертов, то под оптимальными понимаются такие множества значений, которые обеспечивают минимальную степень рассогласования описаний.

- Проблема 2. Можно ли определить показатели качества поиска информации в нечетких (лингвистических) базах данных и сформулировать правило выбора такого множества лингвистических значений, использование которого обеспечивало бы максимальные показатели качества поиска информации?
- Проблема 3. Можно ли предложить процедуры выбора операторов агрегирования информации в нечетких иерархических динамических системах, минимизирующих противоречивость модели процесса в системах оценки и мониторинга?

Эти проблемы обсуждаются в упомянутых выше работах. Детали представлены в работах [8] (Проблема 1), [9] (Проблема 2) и [10] (Проблема 3). Учитывая доступность перечисленных работ, мы позволим себе не останавливаться на них. Отметим лишь, что системы оценки и мониторинга эффективны, когда нет (нельзя построить) математической модели процесса в виде уравнений, автоматов, и т.п. Разработка таких систем возможна, когда можно построить «семантическую модель» процесса в виде набора понятий и их взаимосвязей, и когда поступает и анализируется реальная информация (возможно обучение или настройка). Возможна разработка оптимальных систем с точки зрения удобства ввода информации аналитиком, согласованности мнений аналитиков, информационного обеспечения ввода информации, и моделирования.

На основе описанных методов разработаны системы оценки и мониторинга процессов создания странами специальных видов технологий и материалов в интересах управления гарантией Международного Агентства по Атомной Энергии [11], риска развития сердечно-сосудистых заболеваний в РФ [12], создания изделий микроэлектроники (оценка технологических стартапов) в интересах компании Cadence Design Systems [13]. Воз-

возможности применения подобных систем в оценке и мониторинге кризисных ситуаций и в стратегическом управлении компаниями описаны в [14] и [15] соответственно. Уникальные аналитические возможности систем оценки и мониторинга обсуждаются в [6] и суммированы на рис. 1. Те-

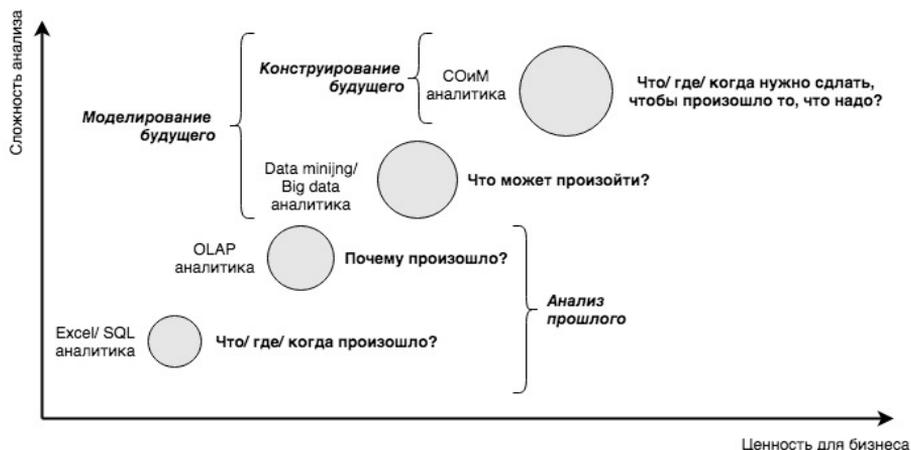


Рис. 1. Эволюция аналитических инструментов.

кущий уровень почти всех компаний – OLAP аналитика; лишь немногие компании используют Big Data аналитику; аналитические инструменты систем оценки и мониторинга используются в единичных международных и правительственных организациях, а также в крупном международном высокотехнологическом бизнесе. Использование аналитических возможностей систем оценки и мониторинга – это естественный эволюционный этап развития аналитических инструментов.

Модели и методы, полученные в ходе решения перечисленных проблем, находят свое применение в ряде приложений, имеющих самостоятельное значение. Описание таких связанных с данными проблемами задач и приложений обсуждалось в докладе и суммировано в разделе 3 настоящей работы.

### 3. Связанные задачи

Для решения проблемы 1 была предложена модель описания человеком объектов как процедура измерения в нечеткой лингвистической шкале. Предложенная мера неопределённости множества шкальных значений

нечёткой лингвистической шкалы позволяет выбирать такой набор значений качественных признаков, в рамках которого возможна оптимизация по критериям 1 и 2 (раздел 2). Это позволяет поставить вопрос о персонализации взаимодействия человека с цифровым миром и сделать такое взаимодействие максимально удобным для всех. Решение этой задачи представлено в [16]. Применение персонализации для социальных сетей описано в [17], для компьютерных обучающих систем — в [18, 19], для систем медицинского мониторинга — в [20], для персонализации новостных лент — в [21]. Подобные дополнения могут сделать более персонализированными (а, следовательно, и более эффективными) любые коммуникации с клиентами, включая рекомендации, рекламные компании и т.п. Соответствующие примеры из розничной торговли, телекоммуникаций, энергетики, банковского и страхового бизнеса были представлены в докладе. К связанным задачам можно отнести и оценку влияния в социальных сетях [22].

Для решения проблемы 2 была предложена модель поиска информации в нечетких базах данных. Введены показатели качества поиска информации и установлена их связь с качеством описания объектов (мерой неопределенности). Эта связь позволила так выбирать множество значений качественных признаков, чтобы обеспечить максимально эффективный поиск информации. Оказалось, что можно ввести качество распознавания нечетко описанных объектов и установить его связь с качеством их описания [23]. Этот факт позволил поставить более общую задачу: как описывать объекты, чтобы обеспечить максимальное качество решения задачи пользователя? Решение этой задачи представлено в [24].

Агрегирование информации в нечетких и дискретных динамических системах (проблема 3) изучено в работах [25, 26], составивших основу кандидатской диссертации. В частности, были получены следующие результаты:

- Для решения задачи выбора операторов агрегирования по экспертным описаниям введена и изучена новая управляющая система — граф нечеткого условия.
- Сформулирована и решена задача устойчивости для иерархических систем в дискретном и нечетком случаях:

– Доказана NP-полнота задачи в общем случае;

- Выделены частные случаи задачи, допускаемые разрешимость за полиномиальное время;
  - Получены эффективные алгоритмы выделения этих частных случаев;
- Рассмотрена задача оптимального распределения ресурсов для иерархических систем в различных метриках:
    - Доказана NP-полнота задачи в общем случае;
    - Выделены частные случаи задачи, допускаемые разрешимость за полиномиальное время;
    - Получены эффективные алгоритмы выделения этих частных случаев;
  - Для решения последних двух задач введено и изучено новое понятие для ориентированных ациклических графов – вершина-сверхдоминатор.

Для автоматического построения модели процесса нами также использовались методы углубленного анализа данных, которые показали свою эффективность [27]. Часть методов обучения для операторов агрегирования информации хорошо себя проявила в задачах проектирования микроэлектроники [28] и также была защищена как кандидатская диссертация. Общий стек используемых нами технологий в зависимости от наличия данных и/или экспертизы представлен на рис. 2.

В заключение отметим, что в последнее время интерес к подобным человеко-компьютерным системам проявляют университеты [29] и крупные компании такие как Google [30] и IBM [31]. Последние даже вводят новый термин — дополненный интеллект (Augmented Intelligence) — “В IBM мы руководствуемся термином «Дополненный интеллект», а не «Искусственный интеллект». Это критическое различие между системами, которые расширяют и дополняют человеческий опыт, а не те, которые пытаются копировать человеческий интеллект” [31]. В этой терминологии системы оценки и мониторинга и есть дополненный интеллект для широкого класса практически важных задач. Полученные нами результаты позволяют разрабатывать оптимальные по ряду важных критериев системы дополненного интеллекта.

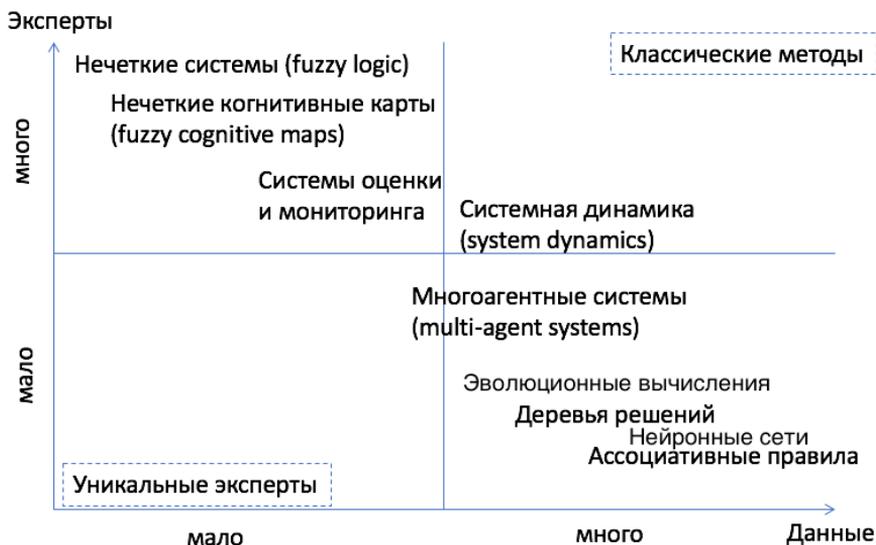


Рис. 2. Стек используемых технологий.

## Список литературы

- [1] Караткевич С.Г., Добрынин В.Н., Окладникова Е.А., Ульянов С.В. Социально-экономическое и интеллектуальное управление в социотехнических системах. — М.: ВНИИгеосистем, 2011 — 398 с.
- [2] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, Alex Marrs. Disruptive technologies: Advances that will transform life, business, and the global economy. McKinsey Global Institute (MGI), May 2013, 176 p. — [http://www.mckinsey.com/insights/business\\_technology/disruptive\\_technologies](http://www.mckinsey.com/insights/business_technology/disruptive_technologies)
- [3] Eric Mack. There are now more gadgets on Earth than people — <https://www.cnet.com/news/there-are-now-more-gadgets-on-earth-than-people/>
- [4] Мобильных телефонов — больше, чем людей на планете — <http://apps4all.ru/post/10-09-14-mobilnyh-telefonov-bolshe-chem-lyudej-na-planete>

- [5] Количество мобильных телефонов по странам мира. 30-04-2017. — <http://total-rating.ru/1970-kolichestvo-mobilnyh-telefonov-po-stranam-mira.html>
- [6] Рыжов А.П. Математические задачи систем оценки и мониторинга сложных процессов. Обзор постановок и результатов. Интеллектуальные системы. Т. 19, Вып. 1, 2015, с. 5–20.
- [7] Рыжов А.П. Информационный мониторинг сложных процессов: технологические и математические основы. Интеллектуальные системы, Том 11, вып. 1-4, 2008, с. 101–136.
- [8] Рыжов А.П. Элементы теории нечетких множеств и измерения нечеткости. Москва, Диалог-МГУ, 1998, 116 с. — <http://www.intsys.msu.ru/staff/ryzhov/FuzzySetsTheoryApplications.htm>
- [9] Рыжов А.П. Модели поиска информации в нечеткой среде. Москва, Издательство Центра прикладных исследований при механико-математическом факультете МГУ, 2004, 96 с. — <http://www.intsys.msu.ru/staff/ryzhov/FuzzyRetrieval2010.htm>
- [10] Рыжов А.П. Об агрегировании информации в нечетких иерархических системах. Интеллектуальные системы, Том 6, Вып. 1-4, 2001, с. 341–364. — [http://www.intsys.msu.ru/magazine/archive/v6\(1-4\)/ryzhov.pdf](http://www.intsys.msu.ru/magazine/archive/v6(1-4)/ryzhov.pdf)
- [11] Ryjov, A., Belenki, A., Hooper, R., Pouchkarev, V., Fattah, A. and Zadeh, L.A., Development of an Intelligent System for Monitoring and Evaluation of Peaceful Nuclear Activities (DISNA), IAEA, STR-310, Vienna, 1998, 122 p.
- [12] Ахмеджанов Н.М., Жукоцкий А.В., Кудрявцев В.Б., Оганов Р.Г., Расторгуев В.В., Рыжов А.П., Строгалов А.С. Информационный мониторинг в задаче прогнозирования риска развития сердечно-сосудистых заболеваний. Интеллектуальные системы, Т.7, вып. 1-4, 2003, с. 5–38.
- [13] Лебедев А.А., Рыжов А.П. Оценка и мониторинг проектов разработки высокотехнологических изделий микроэлектроники. Известия ТРТУ, Тематический выпуск «Интеллектуальные САПР», ISBN 5-8327-0249-2, 2006, № 8 с. 93–99.

- [14] Ryjov A. Basic principles and foundations of information monitoring systems. In: *Monitoring, Security, and Rescue Techniques in Multi-Agent Systems*. Springer, 2005. ISBN 3-540-23245-1, ISSN 16-15-3871. p.147–160.
- [15] Ryjov A. Information Monitoring Systems as a Tool for Strategic Analysis and Simulation in Business. *International Conference on Fuzzy Sets and Soft Computing in Economics and Finance FSSCEF 2004 Proceedings, Saint-Petersburg, Russia, June 17-20, 2004*, ISBN 968-489-028-1, VOLUME II pp. 511–520.
- [16] Рыжов А.П. Некоторые задачи оптимизации и персонификации социальных сетей. Saarbrucken, LAP, 2015, 88 с. (ISBN: 978-3-659-68661-0)
- [17] Alexander Ryjov. Personalization of Social Networks: Adaptive Semantic Layer Approach. In: *Social Networks: A Framework of Computational Intelligence*. Witold Pedrycz and Shyi-Ming Chen (Eds.). Springer International Publishing Switzerland 2014, pp. 21–40.
- [18] Рыжов А. П., Журавлев А. Д., Вахов А. Н., Кривцов В. В. Об одном подходе к персонализации обучения в рамках компьютерных обучающих систем. *Интеллектуальные Системы. Теория и приложения*. Т. 20, Вып. 3, 2016, с. 180–185.
- [19] A. Ryjov, A. Vakhov, V. Krivtsov, and A. Zhuravlev. Personalization and optimization of learning based on technology for evaluation and monitoring of complex processes: Uchi.ru case study. *The 2016 International Conference on Computational Science & Computational Intelligence*. Ed. by: Hamid R. Arabnia, Leonidas Deligiannidis, and Mary Yang. Las Vegas, Nevada, USA, 15-17 December 2016, pp. 378–381.
- [20] Alexander Ryjov. Disruptive technologies: transforming health care, education, and government. *CIO and Digital Innovation*. IAC Online Journal, N1, 2017, pp. 54–57.
- [21] Рыжов А.П., Новиков П.А. Об одной модели цифровых привычек. *Интеллектуальные Системы Теория и приложения*. Т. 21 Вып. 3, 2017, с. 91–102.

- [22] Рыжов А.П., Ильин И.Ю. Об одной модели влияния в социальных сетях. Интеллектуальные Системы Теория и приложения. Т. 21 Вып. 3, 2017, с. 51–66.
- [23] Рыжов А.П. О качестве классификации объектов на основе нечетких правил. Интеллектуальные системы, Т.9, вып. 1-4, Москва, МНЦ КИТ, 2005, с. 253 – 264.
- [24] Alexander Ryjov. Towards an optimal task-driven information granulation. In: Information Granularity, Big Data, and Computational Intelligence. Witold Pedrycz and Shyi-Ming Chen (Eds.). Springer International Publishing Switzerland 2015, pp. 191–208.
- [25] А.А. Лебедев задачах оптимального распределения ресурсов и проверки устойчивости для схем функциональных элементов в  $k$ -значной логике. Интеллектуальные Системы Теория и приложения. Т. 18, выпуск 4, 2014, с. 107–130 — [http://intsysjournal.ru/articles/is04/08\\_lebedev.pdf](http://intsysjournal.ru/articles/is04/08_lebedev.pdf)
- [26] Лебедев А.А. Синтез операторов агрегирования информации по экспертным описаниям. Интеллектуальные Системы Теория и приложения. Том 14, выпуск 1-4, 2012, с. 25–48 — [http://www.intsys.msu.ru/magazine/archive/v16\(1-4\)/levedev-025-048.pdf](http://www.intsys.msu.ru/magazine/archive/v16(1-4)/levedev-025-048.pdf)
- [27] Рыжов А.П., Расторгуев В.В. Методы извлечения нечетких ассоциативных правил в системах информационного мониторинга. Труды международных научно-технических конференций «Интеллектуальные системы» и «Интеллектуальные САПР», 3-10 сентября 2006 г., Дивноморское, Россия, Том 1, Москва, Физматлит, 2006, с. 70–81.
- [28] Мелик-Адамян А.Ф., Рыжов А.П. Задача вариации длин транзисторов в стандартной ячейке при многокритериальной оптимизации нанометровых СБИС. Всероссийская научно-техническая конференция «Проблемы разработки перспективных микро- и наноэлектронных систем» МЭС 2010. с. 102–109.
- [29] Human-machine super-intelligence may tackle world's problems. The economic times./ Science. Jan 01, 2016 — <https://economictimes.indiatimes.com/news/science/human-mac>

hine-super-intelligence-may-tackle-worlds-problems/article  
show/50404783.cms?intenttarget=no

- [30] Глава Google: дополненный интеллект важнее огня или электричества. Вести/Hi-tech, 22.01.2018 — <https://hitech.vesti.ru/article/748187/>
- [31] Preparing for the Future of Artificial Intelligence. — <http://research.ibm.com/cognitive-computing/ostp/rfi-response.shtml>

**Evaluation and monitoring of processes  
in sociotechnical systems  
and related tasks  
Ryjov A. P.**

The paper presents description the main problems of the development of systems evaluation and monitoring of processes in socio-technical systems. The tasks and technologies associated with them are considered, too. Solutions of the problems are discussed. The perspective directions of personalization of human interaction with the digital world and augmented intelligence are considered in the paper. The article is prepared based on the results of the author's speech at the cathedral seminar of the Department of Mathematical Theory of Intelligence Systems of the Faculty of Mechanics and Mathematics of the Lomonosov Moscow State University «Theory of Automata» under the supervision of Professor V.B. Kudryavtsev on March 21, 2018.

*Keywords:* Socio-technical systems, evaluation and monitoring of complex processes, fuzzy sets, personalization.



# О ранковой флеш памяти

Соколов А. П., Межов И. В.

Флеш память в последнее десятилетие стала доминирующей технологией для хранения информации как в персональных вычислительных средствах, так и в корпоративных продуктах: серверах, сетевых хранилищах и дата-центрах. Первоначально технология флеш памяти предполагала хранение одного бита информации в ячейке (SLC-память). Далее с развитием технологий изготовления флеш памяти, а также в связи с использованием во флеш памяти более мощных помехоустойчивых кодов, стало возможным хранить в каждой ячейке 2 бита (MLC-память) или даже 3 бита (TLC-память) информации. Увеличение объема информации, содержащейся в каждой ячейке, приводит к значительному росту вероятности ошибки при чтении. При этом, по мере износа флеш памяти, электрические заряды, хранящиеся в ячейках, имеют тенденцию к уменьшению. Этот процесс приводит к еще большему росту вероятности ошибок чтения и, фактически, приводит к выходу флеш памяти из строя через некоторое время эксплуатации. Ранковый способ хранения информации в ячейках флеш памяти устойчив к процессу постепенного снижения электрических зарядов в ячейках. Более того, данный способ позволяет хранить в том же количестве ячеек больший объем информации. В работе приводится общее описание устройства флеш памяти, описана процедура чтения и рассмотрена простейшая модель ошибок. Далее описан способ хранения информации во флеш памяти с помощью ранков (перестановок). Даны оценки емкости данного типа памяти в сравнении с обычной флеш памятью. Введено понятие Кендалл-Тау расстояния на множестве перестановок. С помощью данного расстояния получена оценка на размер ранковой макроячейки с учетом технологических ограничений. В заключение приведено сравнение плотности записи ранковой и обычной флеш памяти. Явным образом показаны случаи большей плотности ранковой памяти по сравнению с обычной.

**Ключевые слова:** ранковая флеш память, SLC/MLC/TLC флеш память, эффективность флеш памяти в части занимаемой площади.

# 1. Введение

Микросхема флеш памяти состоит из блоков. Блок - минимальная часть флеш памяти, которая может быть стерта за одну операцию. Блок состоит из строк (wordline), каждая строка состоит из отдельных ячеек. Запись информации во флеш память осуществляется по строкам. Организация блока флеш памяти приведена ниже (1).

$WL_1$	$c_{11}$	$c_{12}$	...	$c_{1p}$
	$c_{21}$	$c_{22}$	...	$c_{2p}$
	...			
$WL_q$	$c_{q1}$	$c_{q2}$	...	$c_{qp}$

Рис. 1. Организация блока флеш памяти.

Здесь  $WL_1, \dots, WL_q$  - строки блока.

Далее, обозначим ячейки блока -  $c_{ij}, i \in \{1, \dots, p\}, j \in \{1, \dots, q\}$ . Каждая ячейка хранит некоторый электрический заряд, в следствие которого в ячейке возникает напряжение -  $v_{ij} \in R$ , где  $R$  - множество вещественных чисел. При записи информации в ячейку  $c_{ij}$  закачивается некоторый электрический заряд, что приводит к появлению в ячейке напряжения  $v_{ij}$  отличного от нуля. При стирании информации из блока напряжение всех ячеек блока становится равным нулю.

В обычной флеш памяти информация хранится следующим образом. Каждая ячейка  $c_{ij}$  хранит фиксированное количество бит информации -  $k$ . При этом, данная величина является фиксированной для всех ячеек флеш памяти. Выделяют  $2^k$  опорных (референсных) напряжения  $V_1, \dots, V_Q$ , где  $Q = 2^k$ . В зависимости от величины  $k$  выделяют различные типа флеш памяти - SLC ( $k = 1$ ), MLC ( $k = 2$ ), TLC ( $k=3$ ). Далее всякую ячейку флеш памяти будем обозначать MLC, при этом будем полагать, что в ней содержится  $k$  бит информации.

Для записи информации в ячейку используется некоторая кодирующая функция  $V(b_1, \dots, b_k) : \{0, 1\}^k \rightarrow \{V_1, \dots, V_Q\}$ , которая каждому набору  $k$  бит информации ставит во взаимно однозначное соответствие некоторое референсное напряжение.

При записи информации во флеш ячейку из-за наличия различного рода электрических шумов и дефектов флеш ячеек фактическое напряжение ячейки оказывается отличным от желаемого референсного

$$\tilde{V}(b_1, \dots, b_k) = V(b_1, \dots, b_k) + \eta.$$

Здесь  $\tilde{V}(b_1, \dots, b_k)$  - фактическое напряжение, записанное в ячейку,  $\eta$  - ошибка записи напряжения.

Ошибка записи напряжения - величина, которая зависит от множества различных факторов: температура микросхемы флеш памяти, желаемое напряжение записи -  $V(b_1, \dots, b_k)$ , количество циклов стираний блока и др. В первом приближении можно полагать, что величина  $\eta$  является случайной величиной с нормальным распределением и нулевым средним, то есть  $\eta = N(0, \sigma^2)$ .

В результате записи некоторых бит информации с равновероятным распределением нулей и единиц распределение напряжений множества ячеек флеш памяти приобретает вид, изображенный ниже (2).

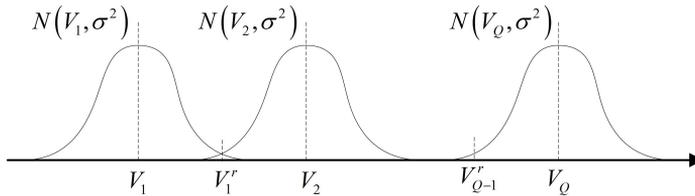


Рис. 2. Распределение напряжений ячеек флеш памяти.

Чтение информации из MLC флеш памяти осуществляется построчно. Для этого используется простая пороговая схема, которая для каждой ячейки сравнивает значение хранящегося в ней напряжения с пороговыми значениями  $V_1^r, \dots, V_{Q-1}^r$ , которые находятся на пересечении распределений соседних референсных уровней.

Функция чтения информации определяется так

$$B(v) = \left\{ (b_1, \dots, b_k) \in \{0, 1\}^k : (V_{i-1}^r \leq v \leq V_i^r) \& (V_{i-1}^r \leq V(b_1, \dots, b_k) \leq V_i^r), 0 \leq i \leq Q + 1 \right\},$$

где  $V_0^r = -\infty, V_{Q+1}^r = +\infty$ .

Иными словами функция чтения определяет интервал  $(V_{i-1}^r; V_i^r)$ , в котором находится напряжение  $v$ , хранящееся в ячейке, и ставит ему

в соответствие набор  $(b_1, \dots, b_k) \in \{0, 1\}^k$ , которому соответствует референсное напряжение  $V_i$ . В микросхеме флеш памяти данная задача решается с помощью набора компараторов, которые сравнивают значение напряжения ячейки со всеми референсными напряжениями одновременно.

Существенной проблемой MLC флеш памяти является постепенное снижение напряжений, хранящихся в ячейках. При этом данное снижение возникает даже при отсутствии активности микросхемы. Электрический заряд, хранящийся в ячейке постепенно снижается. Происходящее при этом изменение распределений напряжений изображено ниже (3).

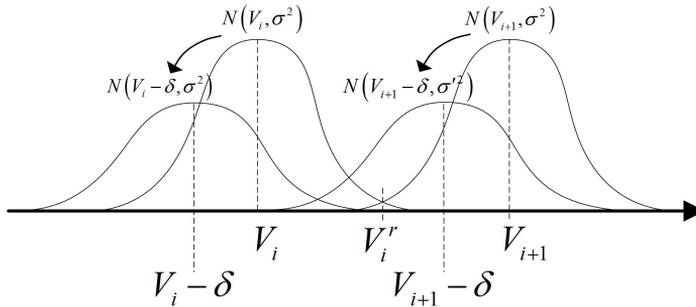


Рис. 3. Смещение распределений напряжений ячеек MLC флеш памяти.

В результате, пороговое напряжение  $V_i^r$ , используемое для чтения информации, становится более недействительным. В итоге значительно возрастает вероятность ошибки чтения и, как следствие, через некоторое время становится невозможным считать данные из флеш памяти.

Ранковая память, предложенная в работах А.Jiang, Е.Gad и др. ([1], [2], [3]), представляет собой способ хранения информации в ячейках флеш памяти, устойчивый к эффекту постепенного снижения напряжений ячеек.

## 2. Ранковая флеш память

При ранковом способе хранения информации  $n$  соседних ячеек флеш памяти объединяются в одну *ранковую макроячейку* -  $M = (c_1, \dots, c_n)$ . Полагаем, что  $v_1, \dots, v_n$  - напряжения, хранящиеся в ячейках  $c_1, \dots, c_n$ , не совпадают друг с другом. Иными словами  $v_i \neq v_j, i \neq j$ .

Пусть  $S_n$  - множество всех перестановок длины  $n$ .

Обозначим  $K(v_1, \dots, v_n) : R^n \rightarrow S_n$  функцию, которая ставит в соответствие набору из  $n$  различных напряжений перестановку  $s = (a_1, \dots, a_n) \in S_n$ , такую что  $a_i < a_j \Leftrightarrow v_i < v_j$  для всех пар  $i, j \in \{1, n\}, i \neq j$ . Иными словами перестановка  $s$  задает порядок напряжений, хранящихся в макроячейке, друг относительно друга.

Изменяя напряжения, в макроячейку можно записать любую из  $n!$  перестановок. Следовательно, одна макроячейка содержит  $\log_2(n!)$  бит информации.

Легко видеть, что при изменении всех напряжений макроячейки на некоторую величину  $\delta$  соответствующая ей перестановка не изменится. То есть  $\forall \delta \in R, K(v_1 + \delta, \dots, v_n + \delta) = K(v_1, \dots, v_n)$ , где  $R$  - множество действительных чисел. Следовательно данный способ хранения информации устойчив к снижению напряжений ячеек в том случае, если это снижение одинаково для всех ячеек, входящих в макроячейку.

### 3. Плотность ранковой и обычной флеш памяти

Рассмотрим вопрос, как соотносятся плотность записи в ранковой и MLC флеш памяти.

Одна ранковая макроячейка, состоящая из  $n$  флеш ячеек, содержит  $\varphi(n) = \log_2(n!)$  бит информации. Аналогичный ей по площади набор из  $n$  MLC-ячеек содержит  $\psi(n) = nk$  бит информации, где  $k$  - количество бит, содержащихся в одной MLC ячейке.

По формуле Стирлинга получаем  $\varphi(n) = n \log_2 n - \log_2 e \cdot n + O(\log_2 n)$ . Таким образом, при стремлении  $n$  к бесконечности объем информации в ранковой памяти растет асимптотически быстрее, чем в обычной. То есть при  $n \rightarrow \infty, \phi(n) = o(\varphi(n))$ .

Рассмотрим вопрос плотности ранковой и MLC-флеш памяти с учетом технологических ограничений на производство микросхем.

В работе М. Kendall ([4]) было введено понятие Кендалл-Тау расстояния между перестановками.

$$D(s_1, s_2) = |\{(i, j) : i < j, [(s_1(i) < s_1(j)) \& (s_2(i) > s_2(j))] \vee [(s_1(i) > s_1(j)) \& (s_2(i) < s_2(j))]\}|.$$

Иными словами расстояние  $D(s_1, s_2)$  показывает количество пар индексов, на которых порядки элементов перестановок  $s_1$  и  $s_2$  не соответствуют друг другу.

Известно, что максимальное Кендалл-Тау-расстояние между перестановками равно числу всех пар из  $n$  элементов. То есть

$$D(s_1, s_2) \leq \frac{n(n-1)}{2}.$$

Следовательно для чтения информации из ранковой ячейки необходимо попарно сравнить все напряжения  $v_1, \dots, v_n$ , хранящиеся в ней. Это означает, что логическая часть микросхемы, осуществляющая чтение информации из макроячейки, должна выполнить операцию сравнения напряжений для каждой пары ячеек.

В обычной МЛС флеш памяти для чтения необходимо сравнить напряжение, хранящееся в ячейке, с каждым из  $Q - 1$  референсных значений. Данные операции не зависят друг от друга поэтому могут быть выполнены параллельно. Таким образом длительность такта чтения в МЛС памяти определяется длительностью такта работы одного компаратора, выполняющего функцию сравнения.

Для ранковой памяти будем исходить из предположения, что операция чтения также представляет собой множество операций сравнения, выполняемых параллельно на множестве компараторов. Следовательно, в составе читающей логики микросхемы для каждой ранковой макроячейки должно быть по крайней мере  $n \cdot (n - 1) / 2$  компараторов. Также как и в МЛС памяти в ранковой памяти имеет смысл использовать один набор компараторов для целой строки.

В этом случае в непосредственной близости от ранковой макроячейки должно располагаться по крайней мере  $\frac{n(n-1)}{2}$  проводов, соединяющих все пары ячеек между собой. Полагаем, что соответствующий компаратор располагается непосредственно на этом проводе.

Рассмотрим граф  $G_n$ , вершинами которого являются ячейки, входящие в состав ранковой макроячейки, а ребра соединяют все возможные пары ячеек между собой. Легко видеть, что это будет полный граф степени  $n$ . Обозначим  $p = \frac{n(n-1)}{2}$  - число ребер графа  $G_n$ .

Технология производства микросхем предполагает слоистую структуру, поэтому возникает вопрос укладки данного графа на отдельные слои.

Легко видеть, что начиная с  $n \geq 5$  граф  $G_n$  будет непланарным. Следовательно укладка соответствующей схемы чтения на один слой невозможна. В таком случае оценим минимальное количество пересечений ребер графа  $G_n$ . Данные пересечения технологически выполняются с

помощью специальных ячеек, площадь которых сравнима с площадью отдельных ячеек флеш памяти.

По теореме Эйлера для всякого планарного графа без кратных ребер выполнено  $n + f - e = 2$ , где  $n$ -число вершин,  $f$ -число граней,  $e$ -число ребер. С другой стороны для всякого планарного графа такого, что  $f \geq 2$ , имеет место неравенство  $3f \leq 2e$ . Выразим число граней по теореме Эйлера и подставим в последнее неравенство:

$$6 + 3e - 3n \leq 2e.$$

Следовательно, число ребер планарного графа при  $f \geq 2$  удовлетворяет неравенству  $e \leq 3n - 6$ .

Обозначим  $m$  - минимальное число пересечений ребер графа  $G_n$  при укладке на слои микросхемы. Из предыдущих рассуждений следует, что

$$m \geq p - 3n - 6.$$

Следовательно

$$m \geq \frac{n^2 - 7n + 12}{2}.$$

Таким образом площадь ранковой макроячейки в терминах числа элементарных технологических ячеек можно оценить как  $n + m$ . Данная макроячейка содержит  $\varphi(n) = \log_2(n!)$  бит информации. Легко видеть, что в эквивалентном по площади наборе обычных МЛС ячеек содержится  $\psi'(n) = k \cdot (n + m)$  бит информации. Следовательно ранковая макроячейка содержит информации больше, чем аналогичный ей по площади набор МЛС ячеек тогда и только тогда, когда  $\log_2(n!) \geq k \cdot (n + m)$ . Подставим в данное неравенство выражение для  $m$  и получим

$$\log_2(n!) \geq k \cdot \frac{n^2 - 5n + 12}{2}.$$

Данное неравенство имеет следующее решение в целых числах

$$k = 1, n \in \{4, 5, 6\}.$$

Для указанных случаев величина отношения плотности записи ранковой памяти относительно обычной МЛС памяти

$$\frac{\varphi(n)}{\psi'(n)} \cdot 100\%$$

принимает значения 14%, 15% и 6%, соответственно. Таким образом имеет место теорема.

**Теорема.** *Ранговая флеш память, осуществляющая чтение информации за один такт с помощью множества параллельных компараторов, имеет плотность записи информации более высокую, чем MLC флеш память, тогда и только тогда, когда  $k = 1, n \in \{4, 5, 6\}$ .*

Данное утверждение фактически определяет границы применимости ранковой флеш памяти с описанным способом чтения. В качестве альтернативного способа осуществления чтения информации из ранковой памяти можно предложить отказ от использования схемы из множества компараторов в пользу непосредственной оцифровки значений напряжений в ячейках и дальнейшая их сортировка в цифровой области.

## Список литературы

- [1] Anxiao Jiang, Robert Mateescu, Moshe Schwartz, Jehoshua Bruck, "Rank Modulation for Flash Memories Information Theory IEEE Transactions on, vol. 55, pp. 2659-2673, 2009, ISSN 0018-9448.
- [2] Anxiao Jiang, Moshe Schwartz, Jehoshua Bruck, "Error-correcting codes for rank modulation Information Theory 2008. ISIT 2008. IEEE International Symposium on, pp. 1736-1740, 2008.
- [3] E. E. Gad, E. Yaakobi, A. Jiang, J. Bruck, "Rank-modulation rewriting codes for flash memories ISIT 2013 – Proceedings of the 2013 IEEE International Symposium on Information Theory, pp. 704-708, 2013.
- [4] M. Kendall, "A New Measure of Rank Correlation". Biometrika 30, pp. 81–89, 1938.

### **On rank flash memory Sokolov A. P., Mezhov I. V.**

Flash memory in the last decade became dominant technology for storing data both for personal electronic devices and enterprise products: servers, network storages and data centers. Initially flash memory technology assumed storing only one data bit in flash cell (SLC-memory). Further development of production technology of flash memory and integration of more powerful error correction codes in flash memory modules made it possible to store 2 bits (MLC-memory) and

even 3-bits (TLC-memory) of data. Increase of number of bits stored in each cell leads to significant increase of probability of error during read operation. Furthermore with increase of programm-erase cycles electric charges stored in flash memory cells have tendency to decrease. This process also leads to increase of probability of error during read operation. Finally this process of charge decrease leads to flash memory failure when error correction code cannot fix all read errors. Rank method of storing data in flash cells is resilient to process of gradual decrease of cell charges. Moreover this method theoretically has higher area efficiency in comparison with conventional SLC/MLC/TLC memory. First in this paper brief description of conventional flash memory is given. Read operation is analyzed, basic model of read errors is described. Then rank method of storing data is presented. Estimated amount of memory stored by this method in comparison with conventional flash memory. Introduced Kendall-Tau distance between permutations. By means of this distance estimated area of rank memory taking in account technological limitations. Finally it's analyzed area efficiency of rank flash memory in comparison with conventional flash memory. Explicitly described cases when rank memory has higher area efficiency than conventional SLC/MLC/TLC memory.

*Keywords:* rank flash memory, SLC/MLC/TLC flash memory, flash memory area efficiency.



# Проблема полноты в классах линейных автоматов

Часовских А.А.

Рассматриваются классы линейных автоматов над конечными полями с операциями композиции (суперпозиции и обратной связи). Ранее для этих классов получен алгоритм проверки полноты конечных подмножеств. В случае простого поля найдены все предполные классы, множество которых является счетной приведенной критериальной системой. В общем случае ранее было построено множество замкнутых классов, являющееся критериальной системой, включающее семейство классов, порожденных максимальными подполями в трансцендентном расширении рассматриваемого конечного поля. Для простых полей все классы этого семейства поглощались другими классами из приведенной критериальной системы. Поэтому в настоящей работе оно исследуется в случае конечных полей, не являющихся простыми. Оказалось, что часть элементов семейства поглощается и в этом случае, но также среди его элементов существуют предполные классы, являющиеся конечно-порожденными и не содержащиеся среди предполных классов других семейств.

**Ключевые слова:** линейный автомат, сумматор, задержка, обратная связь, операции композиции, алгоритм проверки полноты, предполный класс.

Изучение выразительных свойств в классах всех конечных автоматов  $\mathfrak{F}_2$  по операциям композиции затруднено в связи континуальностью числа предполных подклассов [1], а также алгоритмической неразрешимостью проблемы полноты [2] и аппроксимационной полноты [3]. Высокую сложность задач выразимости в указанном классе подчеркивают результаты С.В. Алешина, полученные при использовании операций суперпозиции как в общем случае, так и для одноместных автоматов [4, 5]. Д.Н. Бабиным в [6] были найдены все классы Поста, использование которых приводит к разрешимости проблемы полноты в классе конечных автоматов. В настоящей работе изучаются проблема полноты в классах  $\mathfrak{L}_k$  линейных автоматов над конечными полями, состоящими из  $k$

элементов. Класс  $\mathfrak{L}_2$  является содержательным подклассом класса  $\mathfrak{F}_2$ , для которого проблемы полноты конечных подмножеств алгоритмически разрешима. В работе [7] была получена приведенная критериальная система, состоящая из всех предполных классов, для классов  $\mathfrak{L}_p$ , где  $p$  – простое число. В дальнейшем [8] была получена критериальная система замкнутых классов  $\tilde{J}_k$  для  $\mathfrak{L}_k$ , где  $k = p^m$ ,  $p$  – простое число,  $m \in \mathbb{N} \setminus \{1\}$ . В настоящей работе рассматриваются классы  $B_q$  из  $\tilde{J}_k$ , порожденные максимальными подполями трансцендентных расширений конечных полей. Показано, что среди рассматриваемых классов есть как предполные классы, не совпадающие с классами из других серий, так и классы, которые строго содержатся в некоторых классах множества  $\tilde{J}_k$ . Найдены некоторые свойства предполных классов из  $\{B_q\}$ .

В соответствии с опубликованными ранее результатами [9], исследование класса линейных автоматов сводится к изучению классов линейно-автоматных (л.-а.) функций. Л.-а. функция осуществляет отображение из декартовой степени множества формальных степенных рядов  $R_k(\xi)$  над полем  $E_k$  в  $R_k(\xi)$  в соответствии с равенством:

$$f(x_1, x_2, \dots, x_n) = \sum_{i=1}^n \mu_i x_i + \mu_0,$$

где  $\mu_i$  – некоторые элементы из  $R_k(\xi)$ , последовательности коэффициентов которых являются периодическими (с предпериодом). Как и ранее, в работе [9], для этой функции через  $U(f)$  будем обозначать множество  $\{\mu_i | i = 1, 2, \dots, n\}$ .

В работе [8] для  $\mathfrak{L}_k$ ,  $k = p^m$ ,  $n \in \mathbb{N}$ ,  $m > 1$ , было получена критериальное множество замкнутых классов:

$$\tilde{J}_k = \{ V_1, V_p, P_s, T_a, M_{0,s}, M_{0,\omega}, M_1, M_{i,\gamma}, R_i^C, R_i^H, B_q \mid$$

$$s \in \{1, 2, \dots, l\}, a \in E_k, \omega \in \Omega, i \in \{2, 3, \dots\}, \gamma \in \Gamma_i, q \in Q \},$$

где через  $B_q$  обозначен замкнутый класс, состоящий из всех л.-а. функций  $f$ , удовлетворяющих соотношению  $U(f) \subset q$  для некоторого максимального подполя  $q$  поля  $E_k(\xi)$ , получаемого трансцендентным расширением поля  $E_k$  переменной  $\xi$ .

Имеют место следующие теоремы:

**Теорема 1.** *Если  $q$  – собственное подполе, содержащее  $E_k$ , то  $B_q \subseteq \Theta$  для некоторого  $\Theta$  из множества  $\tilde{J}_k \setminus \{B_q | q \in Q\}$ .*

**Теорема 2.** Множество  $\{B_q | q \in Q\}$  содержит предполные классы, не совпадающие ни с одним  $\Theta$  из множества  $\tilde{J}_k \setminus \{B_q | q \in Q\}$ .

Таким образом, для случая  $m > 1$  существуют предполные классы, порожденные максимальными подполями в поле  $E_k(\xi)$ , что отличает этот случай от случая простого поля ( $m = 1$ ), где таких предполных классов нет.

Ограничение на не более чем счетную мощность множества предполных классов, порожденных максимальными подполями в поле  $E_k(\xi)$ , получаем из следующей теоремы.

**Теорема 3.** Любой замкнутый класс из множества  $\{B_q | q \in Q\}$  является конечнопорожденным.

Автор выражает благодарность академику В. Б. Кудрявцеву за постановку задачи и постоянную поддержку работы.

## Список литературы

- [1] Кудрявцев В. Б. О мощности множеств предполных множеств некоторых функциональных систем, связанных с автоматами // Проблемы кибернетики. — 1965. — Вып. 13. — С. 45–74.
- [2] Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // ДАН СССР. — 1964. — Т. 155, N 1. — С. 35–37.
- [3] Буевич В. А. Об алгоритмической неразрешимости распознавания А-полноты для о.-д. функций // Мат. заметки. — 1972. — Вып. 6. — С. 687–697.
- [4] Алешин С. В. О суперпозициях автоматных отображений // Киев: Кибернетика. — 1975. — № 1. — С. 29–34.
- [5] Алешин С. В. Об отсутствии базисов в некоторых классах инициальных автоматов // Проблемы кибернетики. — М.: Наука — 1970. — Вып. 22. — С. 67–75.
- [6] Бабин Д. Н. О классификации автоматных базисов Поста по разрешимости свойств полноты и А-полноты // Докл. РАН — 1999, 367:4. — С. 439–441
- [7] Часовских А. А. Условия полноты линейно-р-автоматных функций // Интеллектуальные системы. Теория и приложения. — 2014. — Т. 18, — вып. 3. — С. 203–252.

- [8] Часовских А. А. Критериальные системы в классах линейно-автоматных функций над конечными полями // Интеллектуальные системы. Теория и приложения. — 2015. — Т. 19, — вып. 3. — С. 151–160.
- [9] Часовских А. А. Проблема полноты для класса линейно-автоматных функций // Дискретная математика. — 2015. — Т. 27, — вып. 2. — С. 134–151.

### **The completeness problem in classes of linear automata Chasovskikh A.A.**

Classes of linear automata over finite fields with composition operations (superposition and feedback) are considered. Previously an algorithm for checking the completeness of finite subsets was obtained for these classes. In the case of a simple field, all precomplete classes whose set is a countable reduced criterial system are found. Previously in the general case the set of closed classes was constructed, which is a criterial system, including the family of classes generated by maximal subfields in the transcendental extension of the finite field under consideration. For simple fields, all classes of this family were absorbed by other classes from the reduced criterial system. Therefore, in the present paper the family is being investigated in the case of finite fields that are not simple. It turned out that part of the elements of the family is also absorbed in this case, but also among its elements there are precomplete classes that are finitely generated and not contained among the precomplete classes of other families.

*Keywords:* linear automaton, adder, delay, feedback, composition operations, completeness check algorithm, precomplete class.

## **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 ЛАТ<sub>E</sub>X, предоставляются к загрузке через WEB-форму [http://intsysjournal.org/generator\\_form](http://intsysjournal.org/generator_form).
2. К статье прилагаются файлы, содержащие название статьи на русском и английском языках, аннотацию на русском и английском языках (не более 50 слов), список ключевых слов на русском и английском языках (не более 20 слов), информация об авторах: Ф.И.О. полностью, место работы, должность, ученая степень и/или звание (если имеется), контактные телефоны (с кодом города и страны), e-mail, почтовый адрес с индексом города (домашний или служебный).
3. Список литературы оформляется в едином формате, установленном системой Российского индекса научного цитирования.
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. Оттиски статей авторам не предоставляются. Журнал распространяется по подписке, экземпляры журнала рассылаются подписчикам наложенным платежом. Условия подписки публикуются в каталоге НТИ «Роспечать», индекс журнала 64559.
5. Доступ к электронной версии последнего вышедшего номера осуществляется через НЭБ «Российский индекс научного цитирования». Номера, вышедшие ранее, размещаются на сайте <http://intsysjournal.org>, и доступ к ним бесплатный. Там же будут размещены аннотации всех публикуемых статей.



---

Подписано в печать: 10.06.2018

Дата выхода: 25.06.2018

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).