Учебная и научная деятельность кафедры математической кибернетики

Заведующий кафедрой, д.ф.-м.н., профессор
Ложкин Сергей Андреевич

Общая информация

Кафедра была организована в 1970 г.; ее первоначальное название — кафедра математической логики и теории автоматов. Переименована в кафедру математической кибернетики в 1975 г. Организатор и зав. кафедрой в период 1970–1998 гг. — чл. корр. РАН С.В. Яблонский. После кончины С.В. Яблонского в 1998 г. кафедру возглавил В.Б. Алексеев, который руководил ею до середины 2019 г.

В 2016 г. в состав кафедры вошла лаборатория дискретных управляющих систем и их приложений, созданная на базе лаборатории троичной информатики, которую долгое время возглавлял Н.П. Брусенцов.

Общая информация

Кафедра математической кибернетики обеспечивает:

1) преподавание базового цикла курсов, связанных с дискретной математикой, теорией дискретных управляющих систем и их приложениями;
2) проведение фундаментальных и прикладных научных исследований по данной тематике.

Основной преподавательский и научный состав кафедры и лаборатории

- Ложкин С.А. – заведующий кафедрой, и.о. зав. лабораторией;
- Алексеев В.Б. – профессор;
- Вороненко А.А. – профессор;
- Селезнева С.Н. – профессор;
- Романов Д.С. – профессор;
- Подымов В.В. – доцент, ученый секретарь кафедры;
- Шуплецов М.С. – доцент;
- Андреева Т.В. – ст. преподаватель;
- Данилов Б.Р. – ассистент;
- Владимирова Ю.С. – старший научный сотрудник;
- Бухман А.В. – научный сотрудник (0.5 ставки);
- Савицкий И.В. – младший научный сотрудник;
- Зизов В.С. — инженер (проходит избрание на должность мл.науч.сотр.).

Основной преподавательский и научный состав кафедры и лаборатории

Совместители

1. Чокаев Б.В. – доцент (0.5 ставки);
2. Жуков В.В. – ст. преподаватель (0.5 ставки).

В настоящее время на кафедре обучается

- 35 студентов бакалавриата,
- 10 российских магистрантов и 7 магистрантов из КНР,
- 4 российских аспиранта и 2 аспиранта из КНР.

Преподавательская деятельность кафедры

Базовые общефакультетские курсы кафедры

1. Дискретная математика (2 семестр)

2. Основы кибернетики
(1 поток – 7 семестр, 2 поток – 5 семестр, 3 поток – 6 семестр)

Поточные курсы кафедры

1. Дополнительные главы дискретной математики и кибернетики
(2 поток – 7 семестр)

2. Математическая логика и логическое программирование
(3 поток – 7 семестр)

Кафедра ведет преподавание ряда аналогичных курсов для второго высшего образования, филиалов МГУ в Грозном, Сарове, Севастополе и Астане.

Преподавательская деятельность кафедры

Кафедра обеспечивает преподавание целого ряда дисциплин специализации в рамках подготовки бакалавров и магистров. При этом обучение магистров осуществляется по двум магистерским программам:

– *Дискретные структуры и алгоритмы (рук. В.Б. Алексеев),*

– *Дискретные управляющие системы и их приложения (рук. С.А. Ложкин),*

и с 2023–2024 уч. ведет преподавание по совместной (с кафедрами АСВК и МС) магистерской программе «Перспективные методы искусственного интеллекта в сетях передачи и обработки данных»

Список кафедральных курсов

В бакалавриате по направлению «Прикладная математика и информатика», за исключением общефакультетских и поточных курсов:

- Избранные вопросы дискретной математики (5 семестр, гр. 318)
- Математическая логика (6 семестр, гр. 318 и 319/2)
- Математические модели и методы синтеза сверхбольших интегральных схем (6 семестр, гр. 318)
- Элементы теории дискретных управляющих систем (6 семестр, гр. 318)
- Избранные вопросы теории графов (7 семестр, гр. 418)
- Сложность алгоритмов (7 семестр, гр. 418)
- Модели вычислений (8 семестр, гр. 418)

Список кафедральных курсов

В бакалавриате по направлению
«Фундаментальная информатика и информационные технологии»:

- Дискретная математика (1 и 2 семестры, гр. 141 и 142)
- Офисные технологии (3 семестр, гр. 242)
- Математическая логика и теория алгоритмов (4 семестр, гр. 241 и 242)
- Введение в троичную информатику (8 семестр, гр. 441/2)

Список кафедральных курсов в магистратуре

- Графы и их применения (1 сем., гр. 518/1)
- Обобщенная выполнимость (1 сем., гр. 518/1 и 521)
- Математические модели и методы логического синтеза сверхбольших интегральных схем (1 сем., гр. 518/2)
- Некоторые задачи теории графов (1 сем., гр. 521)
- Проектирование больших систем на C++ (1 сем., гр. 518/2)
- Функциональные системы (1 сем., гр. 518/1; 3 сем., гр. 618/2)
- Языки описания схем (1 сем., гр. 518/2)
- Вероятностные методы в комбинаторике (2 семестр, группа 518/1)
- Математические модели и методы проектирования архитектуры сверхбольших интегральных схем (2 сем., гр. 518/2)
- Математические модели и методы физического синтеза сверхбольших интегральных схем (2 сем., гр. 518/2)
- Практикум по дискретным структурам (2 сем., гр. 518/1)
- Распределённые алгоритмы (2 сем., гр. 521)
- Элементы теории синтеза, надёжности и контроля дискретных управляющих систем (2 сем., гр. 518/2)
- Математические методы верификации схем и программ (3 сем., гр. 618/1, 618/2 и 621)
- Некоторые задачи оптимизации на дискретных структурах (3 сем., гр. 618/1)
- Практикум по пакетам проектирования сверхбольших интегральных схем (3 сем., гр. 618/2)
- Прикладные графовые алгоритмы для компьютерных сетей (3 сем., гр. 621)
- Математическая биология (4 сем., гр. 618/1)
- Python для аналитиков данных (4 сем., гр. 618/1 и 618/2)

Спецсеминары кафедры

- Теория управляющих систем и математические модели СБИС
- Теоретические проблемы программирования
- Дискретные функции и сложность алгоритмов
- Сложность решения дискретных задач

Публикация учебных пособий и монографий

За период с 2020 по 2024 годы на кафедре были опубликованы следующие учебные пособия и монографии.

- Алексеев В.Б. Дискретная математика : учебник. – М.: ИНФРА-М, 2021. – 133 с. (учебное пособие). – ISBN 978-5-16-016520-2.
- Марченков С.С. Булева сводимость и булевы степени. – М.: МАКС Пресс, 2020. – 69 с. (монография). – ISBN 978-5-317-06377-1.
- Марченков С.С. Избранные главы дискретной математики. – М.: Физматлит, 2023. – 186 с. (учебное пособие). – ISBN 978-5-9221-1969-6.

Проведение научных исследований

На кафедре и в лаборатории выполняется госбюджетная тема НИР «Методы решения задач, связанных с построением и исследованием дискретных математических моделей и управляющих систем»

Руководитель: С.А. Ложкин

Ответственные исполнители: Д.С. Романов, С.Н. Селезнева

Проведение научных исследований

С 2019–2020 уч. года и по настоящее время сотрудниками и аспирантами кафедры была защищена 1 докторская и 4 кандидатских диссертации:

1. Романов Д.С. (2019 г., н. консультант Ложкин С.А.).
2. Кафтан Д.В. (2021 г., н. руководитель Вороненко А.А.).
3. Савицкий И.В. (2021 г., н. руководитель Марченков С.С.).
4. Жуков В.В. (2022 г., н. руководитель Ложкин С.А.).
5. Антюфеев Г.В. (2024, н. руководитель Романов Д.С.).

При этом аспиранты Савицкий И.В. и Жуков В.В. защитили диссертации досрочно — за 1 год и за 3 месяца до окончания аспирантуры соответсвенно.

С 2019 года сотрудниками и аспирантами кафедры было опубликовано более 160 статей в научных журналах.

Проведение научных исследований

Научные исследования, проводившиеся на кафедре и в лаборатории за последние 5 лет, были поддержаны 3 грантами РФФИ:

18-01-00800 А (Ложкин С.А., 2018–2020),

19-01-00200 А (Селезнева С.Н., 2019–2021),

20-01-90215 Аспиранты (Ложкин С.А., 2020–2023),

а также 5 (одногодичными) грантами МЦФиПМ, выполнявшимися под руководством Ложкина С.А.

Проведение научных исследований

В период с апреля 2020 г. по декабрь 2021 г. на кафедре под руководством Шуплецова М.С. на основе договора пожертвования со стороны фирмы Интел выполнялись исследования по разработке программ точного синтеза схем для ПЛИС корпорации Интел.

Начиная с 2020 г. группа сотрудников кафедры принимает активное участие в выполнении ряда НИР в рамках договора о сотрудничестве между факультетом ВМК и компанией Хуавэй, а один из них (Романов Д.С.) входит в технический совет, созданный в рамках этого договора.

Задачи синтеза, надёжности и контроля дискретных управляющих систем (ДУС), методы их решения

Ложкин Сергей Андреевич
Вороненко Андрей Анатольевич
Романов Дмитрий Сергеевич
Шуплецов Михаил Сергеевич
Данилов Борис Радиславович
Зизов Вадим Сергеевич

Задача синтеза (в общем виде) — задача структурной (схемной) реализации заданной дискретной функции (ДФ) или системы ДФ в заданном классе схем с их оптимизацией по одному или нескольким функционалам (параметрам) сложности, к которым относятся, в частности, параметры, характеризующие надёжность и (или) контролепригодность получаемых реализаций.

Исследование сложности и структуры оптимальных и близких к ним схем для ряда специальных функций

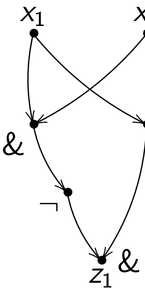
Эта задача рассматривалась в курсе ДМ на примере сумматора $S^{(n)}$ и умножителя $M^{(n)}$ порядка n, то есть систем из $(n+1)$ и $2n$ булевых функций (БФ) от $2n$ переменных, которые задают сложение и умножение двух n-разрядных двоичных чисел соответственно.

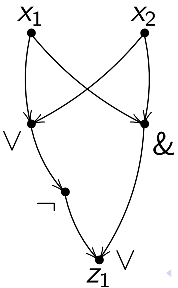
Доказано, что $L(S^{(n)}) \leqslant 9n - 5$ и $L(M^{(n)}) \leqslant c \cdot n^{\log_2 3}$, где c — некоторая константа, а под $L(F)$ понимается минимальная из сложностей схем из функциональных элементов (СФЭ) в базисе $\{x_1 \cdot x_2, x_1 \vee x_2, \overline{x}_1\}$, реализующих систему БФ F.

Другим примером специальной БФ является линейная БФ порядка n, то есть БФ вида $\ell_n^\sigma = x_1 \oplus \ldots \oplus x_n \oplus \sigma$, где $\sigma = 0, 1$. Частными случаями таких функций являются БФ $\ell_2 = \ell_2^1 = x_1 \oplus x_2$ и $\overline{\ell}_2 = \ell_2^0 = x_1 \oplus x_2 \oplus 1 = x_1 \sim x_2$.

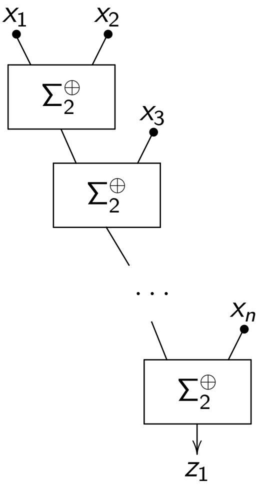
Можно доказать, что $L(\ell_2) = L(\overline{\ell}_2) = 4$ (задача 2 на сайте кафедры) и что $L(\ell_n) = L(\overline{\ell}_n) = 4n - 4$, при $n \geqslant 2$.

Установлено, что единственными с точностью до изоморфизма СФЭ, реализующими БФ $x_1 \oplus x_2$ и $x_1 \oplus x_2 \oplus 1$, являются СФЭ вида





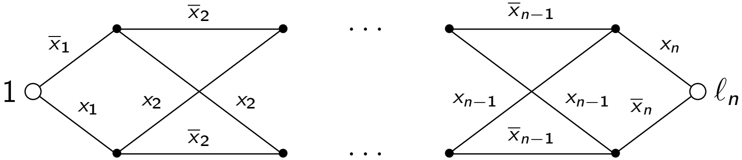
Относительно недавно было доказано, что любая минимальная СФЭ, реализующая линейную БФ порядка n, строится из $(n-1)$ СФЭ данного вида как из «макроэлементов».



Заметим, что глубина (задержка) схем указанного вида, имеющих при $n = 2^k$ вид полного двоичного k-ярусного дерева, построенного из «макроэлементов», равна $3k$, что существенно больше оптимальной глубины схем, реализующих данные БФ, которая равна $(2k+1)$.

Это говорит об антагонизме глубины и сложности схем, реализующих линейные БФ, то есть о невозможности построения СФЭ с оптимальными значениями сложности и глубины.

Интересно, что в другой модели вычислений — в классе т. н. контактных схем, линейная БФ $\ell_n = x_1 \oplus \ldots \oplus x_n$ при $n \geqslant 2$, тоже имеет сложность $(4n - 4)$, которая достигается на схеме:



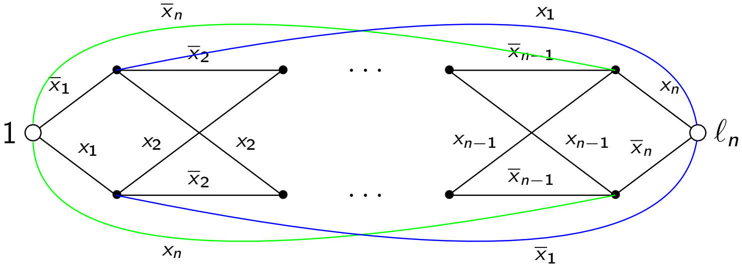
Контактная схема (КС) от переменных $x_1, \ldots, x_n$ — неориентированный граф с 2 выделенными вершинами-полюсами, каждое ребро которого помечено одной из букв x_i, $\overline{x}_i$, $i = 1, \ldots, n$. Она реализует БФ проводимости между полюсами, задаваемую ДНФ, которая состоит из конъюнкций букв, приписанных рёбрам какой-либо цепи, соединяющей полюса.

Вопросы надёжности и контроля управляющих систем

На примере приведённой выше КС можно пояснить некоторые вопросы надёжности и контроля схем.

Будем говорить, что КС Σ корректирует 1 обрыв, если при удалении любого её контакта она реализует ту же БФ. Тривиальным способом получения такой КС Σ из исходной КС Σ' является параллельное дублирование её контактов, которое, очевидно, удваивает сложность Σ'.

Заметим, что если к приведённой выше схеме для линейной БФ добавить 4 контакта следующим образом



то получится эквивалентная КС, корректирующая 1 обрыв.

Можно показать, что для того чтобы построить для исходной схемы диагностический относительно обрыва 1 контакта тест, то есть такое множество наборов, по значениям на которых можно как обнаружить наличие указанной неисправности, так и указать неисправный контакт, достаточно взять не более, чем $\lceil (2\log_2 n) + 4 \rceil$, наборов в n-мерном кубе.

При этом, соответствующий проверяющий тест состоит из 4 наборов.

Вопросами подобного типа, т. е. вопросами контроля схем, занимается Д. С. Романов.

Задача геометрической реализации схем

Во многих случаях для реального использования схем требуется их геометрическая реализация, то есть «вложение» в ту или иную регулярную структуру (прямоугольную решётку, единичный куб и др.) Так, например, полное двоичное n-ярусное дерево (из элементов & или $\vee$) можно гомеоморфно вложить в единичный куб размерности $(n+1)$ или прямоугольную решётку «высоты» $\lceil (n+1)/2 \rceil$ при расположении листьев дерева (входов схемы) — на её горизонтальной стороне.

Доказывается также, что указанная реализация в соответствующих структурах меньшей размерности невозможна.

Задача синтеза схем в неполных и вырожденных базисах

Представляет интерес задача синтеза схем в неполных и вырожденных базисах, к которой относится, в частности, задача о реализации БФ $\overline{x}_1, \overline{x}_2, \overline{x}_3$ с использованием 2 элементов отрицания в базисе $\{\&, \vee, \neg\}$, где «вес» элементов & и $\vee$ равен 0, а «вес» $\neg$ равен 1.

Разработка «универсальных» методов синтеза и исследование сложности «типичных» или «самых сложных» БФ, когда задача синтеза решается как «массовая» задача.

Пусть $L(f)$ — минимальная из сложностей СФЭ в базисе $\{\&, \vee, \neg\}$, реализующих БФ f, и пусть $L(n) = \max_{f(x_1,\ldots,x_n)} L(f)$ — т. н. функция Шеннона, введённая им в 1949 г. (для класса КС).

На основе предложенного Шенноном мощностного метода можно доказать, что
$$L(n) \geqslant \frac{2^n}{n}\left(1 + \frac{\log_2 n - O(1)}{n}\right)$$

Эффективность универсальных методов синтеза СФЭ можно сравнивать по тем верхним оценкам функции $L(n)$, которые они позволяют получить:

$$L(n) \leqslant 6\frac{2^n}{n} \qquad \text{(метод Шеннона)}$$

$$L(n) \leqslant \frac{2^n}{n}\left(1 + \frac{3\log_2 n + O(1)}{n}\right) \qquad \text{(метод Лупанова)}$$

$$L(n) \leqslant \frac{2^n}{n}\left(1 + \frac{\log_2 n + O(\log\log n)}{n}\right) \qquad \text{(метод Ложкина)}$$

Последние оценки позволяют установить поведение функции $L(n)$ при $n = 1, 2, \ldots$, на уровне т. н. асимптотических оценок высокой степени точности (АОВСТ). Задача разработки методов синтеза, позволяющих получить АОВСТ для различных классов схем — актуальная задача данного направления.

Все перечисленные выше задачи можно рассматривать и решать для моделей более высокого уровня — автоматных схем, программ из вычисляющих и переадресующих команд, а также команд вызова (в том числе — рекурсивно) подпрограмм, которые вычисляют БФ.

Так, под моим руководством в 2003 г. (Грибок С. В.) и в 2022 г. (Жуков В. В.) были защищены кандидатские диссертации по исследованию поведения (в том числе на уровне АОВСТ) функции Шеннона для сложности указанных программ.

Задачу «массового» синтеза можно рассматривать и решать не только для класса всех БФ от n переменных, но и для более «узких», но тем не менее, достаточено «широких» классов БФ от n переменных.

Все эти задачи можно рассматривать и для других функционалов сложности, в том числе для уровня «энергопотребления» или «степени информационной защищённости» схем.

В 2011 г. А. А. Вороненко ввёл понятие порождения ложного образа — ситуации, когда «противник» на основе ложной и истинной информации делает однозначный вывод об объекте (функции).

Центральным понятием при этом является понятие универсальной функции, которая позволяет частью своих значений вместе с априорной ложной информацией однозначно задать любую ложную функцию.

Изучаются вопросы существования таких функций, размерности области их определённости, «простота» представления и др.

Теоретические проблемы программирования

Подымов Владислав Васильевич
Владимирова Юлия Сергеевна

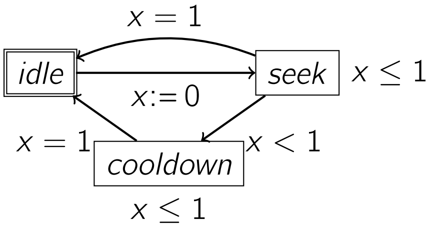
В рамках этого направления исследуются:

- Модели программ и других вычислительных систем:
  - разнообразные виды автоматов, схемы программ, грамматики, ...
- Фундаментальные задачи анализа программ:
  - проблемы эквивалентности и эквивалентных преобразований,
    задача формальной верификации,
    задачи анализа и преобразования автоматов, ...
- Прикладные логики,
  в том числе использующиеся для анализа программ:
  - прикладные фрагменты логики предикатов,
    темпоральные и другие модальные логики,
    динамические логики, ...

Области исследования для студентов

Временны́е автоматы: они отличаются от «привычных» автоматов тем, что

- выполняются не в дискретном времени $(0, 1, 2, \ldots)$,
  а в условиях неуклонно возрастающего действительного значения времени, и
- изменяют возможности выполнения своих переходов с течением времени.



- x — текущее значение времени
- условие у перехода указывает, когда этот переход может выполниться
- «$x := 0$» означает, что следует заново начать отсчёт времени
- условие у состояния должно выполняться, пока автомат находится в этом состоянии

Области исследования для студентов

Проблема эквивалентности: для заданных программ (автоматов, грамматик, ...) проверить, имеют ли они одинаковое поведение.

В последние несколько лет защищались выпускные работы, касающиеся:

- Временны́х автоматов.
  - Рассматривались как распознаватели, так и преобразователи, как «привычный» вид эквивалентности (равенство реализуемых функций), так и «непривычный» (особая «прикладная» структурная эквивалентность — бисимуляция).
- «Привычных дискретных» автоматов-преобразователей ...
  - ... но более общего вида по сравнению с обсуждавшимся на первом курсе.
- Простых программ преобразования двоичных деревьев.
  - «Непростые» такие программы так же выразительны, как и машины Тьюринга, но интерес представляют и программы с крайне ограниченными возможностями.
- LL-грамматик.
  - Это контекстно-свободные грамматики, применяющиеся для синтаксического анализа языков (в т.ч. программных).

Области исследования для студентов

Прикладные логики, возникающие прежде всего в задаче формальной верификации (строгой проверке правильности поведения) программ.

В последние несколько лет защищались выпускные работы, касающиеся:

- Прикладных темпоральных логик.
  - Формулами таких логик задаются требования правильности, в которых учтено изменение свойств с течением времени.
- Прикладных фрагментов логики предикатов первого порядка.
  - Исследовались взаимосвязи таких фрагментов с темпоральными логиками и фрагменты, предназначающиеся для решения конкретных задач.
- Логических средств автоматизации доказательства теорем.
  - С недавних пор в область интересов добавилась разработка алгоритмов автоматизации доказательства логических утверждений о правильности выполнения систем.

Теория дискретных функций

Сложность алгоритмов

Графы и комбинаторика

Алексеев Валерий Борисович
Марченков Сергей Серафимович
Селезнева Светлана Николаевна
Андреева Татьяна Владимировна
Бухман Антон Владимирович
Савицкий Игорь Владимирович

Селезнева Светлана Николаевна, профессор, д.ф.-м.н.

- Полиномиальные представления дискретных функций
  - Рассматриваются представления функций алгебры логики и их обобщений полиномами над полем или кольцом.
  - Изучаются свойства таких представлений в следующих направлениях.
  - Сложность распознавания свойств функций, заданных полиномами. Например, с какой сложностью по полиному Жегалкина функции алгебры логики можно проверить ее монотонность.
  - Сложность полиномиальных представлений функций. Например, каково наименьшее число слагаемых в представлении функции алгебры в виде суммы произведений линейных функций.
  - Свойства полиномиальных представлений функций. Например, какой вид имеют полиномы Жегалкина монотонных функций алгебры логики.

Андреева Татьяна Владимировна, старший преподаватель, к.ф.-м.н., доцент

- Графы и алгебра
  - Применение алгебраических структур к решению задач о графах. Например, перечисление всех гамильтоновых циклов в графе.
  - Применение графов в ряде алгебраических задач, относящихся к математической биологии.
- Асимптотические оценки
  - Получение асимптотики числа некоторых комбинаторных объектов. Например, числа антицепей в частично упорядоченных множествах.

Савицкий Игорь Владимирович, младший научный сотрудник, к.ф.-м.н.

- Машинные и индуктивные описания классов рекурсивных функций
  - Рекурсивная функция — это математическая модель алгоритмически разрешимой задачи.
  - Такие задачи можно классифицировать по их сложности относительно тех или иных критериев. Для этого часто используются машинные и индуктивные описания.
  - Машинное описание предполагает задание функции через вычисление на абстрактном вычислительном устройстве с теми или иными ограничениями.
  - Индуктивное описание предполагает построение сложных функций из простых с помощью различных операций (часто рекурсивной природы).

Информация

Дополнительную информацию можно найти:

- *на сайте кафедры математической кибернетики: mk.cs.msu.ru;*
- *в системе ИСТИНА: istina.msu.ru.*

Вопросы можно задавать по эл. почте:

- *Ложкин С.А.: lozhkin@cs.msu.ru;*
- *Вороненко А.А.: dm6@cs.msu.ru;*
- *Романов Д.С.: romanov@cs.msu.ru;*
- *Подымов В.В.: valdus@yandex.ru;*
- *Селезнева С.Н.: selezn@cs.msu.ru.*