

## ПРЕДИСЛОВИЕ

Дорогой читатель! Перед Вами номер журнала, всецело посвящённый 50-летию научной школы прикладной дискретной математики (далее Школа) Томского государственного университета (ТГУ). Именно столько лет назад, в 1959 г., в Докладах Академии наук СССР, т. 129, № 4, с. 729–731, вышла в свет первая научная статья основателя Школы Аркадия Дмитриевича Закревского «Метод синтеза функционально-устойчивых автоматов», послужившая истоком для развития в ТГУ нового научного направления, изначально связанного с созданием и применениями электронных вычислительных машин (ЭВМ) и в разные периоды становления Школы называвшегося разными терминами, отражавшими наиболее значимые достижения Школы в эти периоды, — теорией релейных схем, цифровой автоматикой, технической логикой, теорией дискретных автоматов (управляющих систем), логическим проектированием, автоматизацией синтеза, автоматизацией решения логико-комбинаторных задач и, наконец, прикладной дискретной математикой. Последнее название Школы и её научного направления наиболее полно отражает современный уровень развития научных исследований в Школе, охватывающих практически все области приложения и компьютеризации современной дискретной математики — дискретные функции и автоматы, логические и автоматные уравнения, компьютерную алгебру, вычислительные методы теории чисел, математическую и компьютерную криптографию, надёжность вычислительных и управляющих систем, интеллектуальные системы, компьютерную безопасность, информатику и программирование, параллельные комбинаторные алгоритмы и многое другое.

К сожалению, в одном номере журнала невозможно дать сколь-либо полное представление о всех научных результатах Школы за полвека её существования. Конечно, их можно было бы просто перечислить, но вряд ли это было бы информативным без введения надлежащих понятий, терминов и контекста, тем более, что многие из этих результатов носят концептуальный или алгоритмический характер или являются программными продуктами, вобравшими в себя оригинальные идеи и находки, не имея представления о которых, трудно оценить значимость всего продукта. Кроме того, в своём развитии Школа не оставалась цельным коллективом, и результаты отделившихся теперь уже трудно воссоздать с должной точностью без их участия.

Сначала (во второй половине 1960-х гг.) из Школы вышла группа из шести исследователей, обосновавшихся в Севастополе, в том числе те «четверо под одной крышей» — Е. А. Бутаков, В. В. Кирюхин, В. Г. Новосёлов и В. И. Островский, которые за свою коллективную дипломную работу по автоматизации синтеза цифровых автоматов под руководством А. Д. Закревского в 1961 г. получили золотую медаль АН СССР. В самом начале 1970-х годов сам А. Д. Закревский и семь других его учеников переехали в Минск, где в АН Беларуси до сих пор продолжают исследования, начатые в Школе, не являясь её членами, но поддерживая с нею научные и добрые человеческие отношения. С отъездом А. Д. Закревского бремя сохранения Школы легло, как это часто бывает в подобных случаях, на его наиболее «поперечного» ученика — автора этих строк, оказавшегося, говоря без ложной скромности, и наиболее преданным своему учителю. (Ох как редко такое случается!) Эта преданность, а также понимание

значимости Школы для университета, в том числе и некоторыми его влиятельными руководителями, в частности тогдашним директором Сибирского физико-технического института при ТГУ М. А. Кривовым, спасли Школу от поглощения её интеллектуальной и материальной собственности другими научными коллективами.

Задумывая издание номера журнала ПДМ к юбилею Школы, мы обратились к её ведущим учёным с просьбой представить свои статьи с реферативным изложением основных достижений в Школе по различным направлениям научных исследований в ней. К сожалению, не все наши учёные сподобились откликнуться на эту просьбу, вследствие чего публикуемые в номере статьи не отражают всех направлений Школы, но даже то, что в них есть, позволит читателю составить, как нам кажется, вполне адекватное представление и о тематике Школы, и об уровне её современных исследований, что, собственно, и является главной целью этого номера.

Номер открывается статьёй Н. Р. Торопова «Язык программирования ЛЯПАС» об истории создания, применения и основных конструкциях «русского языка программирования», как его называли в своё время американские учёные, разработанного в Школе в 1960-х годах и реализованного на всех отечественных и ряде зарубежных (в Польше, США, ФРГ) ЭВМ, включая персональные компьютеры. Язык предназначен для представления алгоритмов решения задач именно дискретной математики и по своим операционным возможностям для этого значительно превосходит все другие языки программирования общего пользования, в том числе и созданные много позже.

Заметную роль в разработке и реализации ЛЯПАСа в первые годы его становления сыграла Светлана Васильевна Быкова.

Учите, не учите — она научит вас  
Всеми, чему хотите, и сколько надо раз.  
Поделится советом, как применить ЛЯПАС  
Для поимки ракеты, нацеленной на вас.

Пусть эта статья о ЛЯПАСе будет доброй памятью о великольном педагоге, замечательном учёном, светлом и всеми любимом человеке.

В статье Г. П. Агибалова «Дискретные автоматы на полурешётках» на материале одноимённой монографии автора излагаются основы теории дискретных автоматов на полурешетках, открывшей новое научное направление на стыке дискретной математики, математической кибернетики и общей алгебры, в рамках которого впервые удалось формализовать такие понятия, относящиеся к дискретным системам, как динамическое поведение, физическая реализуемость, адекватная модель и ее точность, и решить задачи логического проектирования таких систем в постановке, отражающей динамику поведения системы, возможность ее физической реализации на современной электронной базе и адекватность моделирования с любой наперед заданной точностью. Докторская диссертация Г. П. Агибалова на эту тему признана ВАКом РФ лучшей за 1993 г. по специальности 05.13.01.

В рамках теории дискретных автоматов на полурешетках создана математическая модель динамического поведения асинхронных переключательных (из транзисторов и резисторов) схем, позволившая ставить и решать основные задачи логического проектирования таких схем, не доступные в рамках других теорий: задачу анализа — описать динамическое поведение заданной схемы с заданной точностью и задачу синтеза — построить схему, обладающую заданным динамическим поведением. В отличие от задач синтеза статических, или синхронных, схем (с поведением при фиксированных входных состояниях) задача синтеза схем с заданным динамическим поведением

может не иметь решения, так как, во-первых, не любое динамическое поведение допускает реализацию схемой без синхронизации каналов передачи информации в ней и, во-вторых, реальные базисы переключательных элементов не являются полными для реализации функций на полурешётках схемами из них.

В статье И. А. Панкратовой «Реализация функций на полурешётках переключательными схемами» формулируются критерии реализуемости функций на полурешётках схемами в реальных базисах переключательных элементов, в том числе схемами, обладающими свойством функциональной устойчивости к состязаниям.

В статье Н. Г. Парватова «Проблемы полноты и выразимости дискретных функций» формулируются условия, при которых означенные в её названии проблемы имеют эффективные решения. Описываются общие методы, посредством которых эти решения могут быть найдены. Результаты этой статьи можно использовать для нахождения критериев реализуемости в различных функциональных пространствах, в том числе в пространствах функций асинхронных переключательных схем.

В статье Л. Н. Андреевой «Алгоритмы решения задач кратчайшего разбиения» по технологии сокращённого обхода дерева поиска с возвращением, разработанной в Школе в начале 1980-х годов, строятся алгоритмы решения задач кратчайшего допустимого разбиения наборов объектов. С их помощью решаются многие задачи синтеза минимальных схем в программируемых базисах ПЛМ, ПЗУ, ПМВ, ПМЛ и их оптимального распределения по конструктивным ячейкам компоновочного пространства. Разработка этих алгоритмов осуществлялась под руководством и при непосредственном участии доктора технических наук профессора Оранова Александра Михайловича, безвременно ушедшего от нас в 2006 г. Публикуя эту статью, мы отдаём дань памяти о нём и о его выдающихся достижениях в развитии прикладной дискретной математики в ТГУ.

В Школе впервые в стране начаты исследования по созданию параллельных алгоритмов решения дискретно-комбинаторных задач. В статье Н. Е. Тимошевой «Разработка и исследование параллельных комбинаторных алгоритмов» сообщается об основных результатах Школы в этом направлении. Среди них методы параллельного обхода дерева поиска в глубину с возвращением и метод нумерации для параллельного перечисления комбинаторных объектов, а также основанные на них параллельные алгоритмы перечисления (сочетаний, перестановок, разбиений), поиска кратчайшего линейаризационного множества покрытия и решения нелинейных систем логических уравнений методом линейаризационного множества. Приводятся экспериментальные оценки их эффективности на многопроцессорных вычислительных системах кластерного типа.

Полувековая история развития криптографии в Школе — от «военной» до «гражданской» — прослеживается в статье Г. П. Агибалова «50 лет криптографии в Томском государственном университете».

В номере впервые публикуется рукопись А. Д. Закревского «Метод автоматической шифрации сообщений», написанная ровно 50 лет назад и не получившая тогда разрешения на опубликование по причине её «совершенной секретности». В ней в качестве шифратора предложен конечный автомат с функцией выходов, биективной в каждом состоянии. Ныне такие автоматы хорошо изучены под названием шифрующих, ввиду чего рукопись уже не имеет прежней научной ценности, но она чрезвычайно интересна с методической и исторической точек зрения. Она написана так просто и увлекательно, что её, несмотря на некоторые несовременные криптографические термины в ней, можно и нужно смело рекомендовать всякому начинающему криптографу. Мы публи-

куем рукопись в её первоизданном виде, без каких-либо купюр и редакторской правки, чтобы не исказить её изначального духа, который один захватит любого читателя, в том числе и искушённого в криптографии. Мы публикуем её, сохраняя полностью терминологию того времени и авторский стиль изложения, совершенно безупречный с методической точки зрения. Наконец, мы публикуем её как реликвию если не всей российской криптографии, то уж по меньшей мере научной Школы прикладной дискретной математики ТГУ.

*Председатель редакционной коллегии журнала, заведующий кафедрой защиты информации и криптографии ТГУ, профессор Г. П. Агибалов*



А. Д. Закревский с учениками, 1960-е годы

На фото (слева направо) в первом ряду: Анна Ефимовна Янковская (в настоящее время д.т.н., профессор ТГАСУ), Геннадий Петрович Агибалов, Аркадий Дмитриевич Закревский (ныне д.т.н., член-корр. НАН Беларуси); во втором ряду: Юрий Васильевич Поттосин (в настоящее время к.ф.-м.н., ведущий научный сотрудник ОИПИ НАН Беларуси), Юрий Дмитриевич Черкашин (позднее с.н.с. СФТИ), Анатолий Александрович Уткин (позднее к.ф.-м.н., ведущий научный сотрудник ОИПИ НАН Беларуси); на заднем плане (за А. Д. Закревским) — Николай Романович Торопов (ныне к.ф.-м.н., ведущий научный сотрудник ОИПИ НАН Беларуси); крайний справа — Владимир Анатольевич Воробьёв (сейчас д.т.н., профессор Поморского ГУ)