



ИССЛЕДОВАНИЯ ПО ПРОГРАММАМ РАН И СО РАН

Программа фундаментальных исследований Президиума РАН I.27.
«Фундаментальные проблемы решения сложных практических задач с помощью суперкомпьютеров»

Координатор программы – ак. В.Б. Бетелин

Проект **«Методы и средства решения трудных переборных задач с помощью суперкомпьютеров»**

№ гос. регистрации: АААА-А18-118031590005-5

Научный руководитель проекта – ак. И.В. Бычков

1. Разработаны новые сервис-ориентированные решатели трудных переборных задач с использованием непроцедурных запросов на распределенной вычислительной модели предметной области (*авторы: д.т.н. Г.А. Опарин, к.т.н. В.Г. Богданова*).

2. Разработана новая интеллектуальная технология организации предметно-ориентированных гетерогенных сред, обеспечивающая, в отличие от известных, интеграцию Grid и облачных вычислений в процессе решения трудных переборных задач (*авторы: к.т.н. А.Г. Феоктистов, к.т.н. С.А. Горский*).

3. Разработан алгоритм проверки свойства ко-наблюдаемости языка спецификации с помощью логического вывода. При дискретно-событийном моделировании верхнего уровня иерархических систем управления группами автономных поисково-обследовательских роботов возникает необходимость использовать принцип децентрализованного управления. Многоагентность, пространственная распределенность и неполная наблюдаемость всех аспектов функционирования таких систем приводит к ДСС, где локальные супервизоры могут отвечать, например, роботу-лидеру или роботу-ведомому в связке лидер-ведомый при движении роботов в формации, и в то же время смена режимов функционирования (базовых поведений) описывается для всей системы в целом. Такая постановка задачи приводит к необходимости построения децентрализованного супервизора, а, следовательно, проверке условий его существования. Как известно, одним из них является ко-наблюдаемость формального языка, описывающего ограничения на поведение ДСС. Известный алгоритм проверки ко-наблюдаемости хотя и имеет полиномиальную сложность, на каждой итерации требует построения множества возможных прообразов наблюдаемого слова для каждого задействованного локального супервизора. Вычислительные затраты при этом велики, а сам алгоритм узкоспециализирован. Предложен подход к проверке ко-наблюдаемости с помощью развиваемого в рамках проекта оригинального метода автоматического доказательства теорем, реализованного в подсистеме логического вывода. Суть подхода основана на первопорядковой логической (в языке позитивно-образованных формул) формализации генераторов формальных языков, описывающих изначальное и задающих желаемое поведение ДСС. Затем на основе данных формализаций при помощи специальной разработанной стратегии совместного логического вывода для сопоставления вариантов развития событий в разных языках осуществляется поиск вывода построенных формул, результатом которого является ответ на вопрос о ко-наблюдаемости.

Предложенный подход позволит не только организовать проверку свойства ко-наблюдаемости, но и вычислять в случае его нарушения подязыки, для которых свойство



выполнено, а также строить локальные супервизоры, обеспечивающие их генерацию. Как известно, свойство ко-наблюдаемости не сохраняется относительно операции объединения языков, поэтому в общем случае не существует наибольший ко-наблюдаемый подязык данного языка. Применение в ходе вывода эвристик, основанных на формализованных знаниях об окружающей обстановке и условиях функционирования системы, поможет выбрать наилучший в некотором смысле целевой язык из всех ко-наблюдаемых подязыков. Кроме того, такие знания позволят решать задачи так называемого оптимального супервизорного управления, т.е. осуществлять выбор единственного события из множества разрешенных супервизором в текущем состоянии, чтобы наискорейшим образом достичь цели управления. Разрабатываемый логический подход может использоваться также для проверки таких важных свойств языков в рамках ТСУ, как нормальность и диагностируемость (*А.В. Давыдов, А.А. Ларионов, к.ф.-м.н. Н.В. Нагул*).

4. Разработаны новые параллельные алгоритмы синтеза нелинейных многокомпонентных систем управления на основе сублинейных векторных функций Ляпунова. Разработана новая технология параметрического синтеза для широкого класса нелинейных многокомпонентных систем управления, базирующаяся на использовании сублинейных векторных функций Ляпунова и ресурсов распределенной вычислительной среды. Задача синтеза ставится как задача определения неизвестных параметров системы, обеспечивающих требуемое свойство системы и оптимизирующих оценку основного показателя динамического качества при заданных ограничениях на некоторые из других оценок. Решение задачи основывается на методике, идея которой состоит в том, чтобы вместо точных значений показателей качества, входящих в критерий и ограничения, использовать их оценки, вычисляемые с помощью ВФЛ. Таким образом, задача синтеза формулируется как задача условной оптимизации с алгоритмически вычисляемыми критерием и ограничениями. В рамках решения сформулированной оптимизационной задачи разработаны подходы к разделению на области пространства допустимых значений искомым параметров и их распределению между узлами вычислительной среды, эволюционный алгоритм для поиска решений в этих областях, а также механизмы обмена наилучшими решениями между узлами. Кроме того, предложены специальные, основанные на ослаблении требований к синтезируемой системе, процедуры, ускоряющие получение начального допустимого решения. Разработанная параллельная технология позволяет формулировать задачи синтеза непосредственно в терминах инженерных требований к системе (прямых показателей динамического качества). Она применима для синтеза нелинейных систем большой размерности (*к.т.н. С.А. Ульянов, к.т.н. Н.Н. Максимкин, А.А. Толстухин*).

5. В рамках геопортала формируется распределенная вычислительная среда, которая ориентирована на применение преимущественно задач обработки и анализа пространственных данных. Разработаны информационно-вычислительные сервисы по стандартам OGC (WPS, WMS, WCS и др.) и сервисы хранения данных, каталог WPS-сервисов (тематических), а также системы выполнения сервисов и их композиций. Реализовано взаимодействие между информационно-вычислительными сервисами, а также сервисами хранения данных, что позволяет упростить их использование. В системе выполнения сервисов и их композиций ведется сбор данных о произведенных вызовах сервисов. Данные включают название сервиса и его адрес, значения входных и выходных параметров, время выполнения сервисов, успешность выполнения, ошибки выполнения и



**Отчет Института динамики систем и теории управления
имени В.М. Матросова СО РАН за 2019 г.**

т.д. Для каждого сервиса известно его расположение, список выходных и входных параметров, типы данных.

Разработанный алгоритм производит поиск сочетания вызовов сервисов, в которых файл, являющийся результатом работы одного сервиса, передается в качестве параметра другому сервису. Предложенный метод построения семантической сети апробирован на небольшом фрагменте данных о применении сервисов пользователями.

Источники данных представлены в виде сервисов, у которых присутствуют только исходящие дуги. Необходимо отметить, что при таком подходе семантика всех параметров сервисов не определяется. Среди положительных моментов укажем, что вместе с семантической сетью получаем связанность параметров по данным, возможные значения параметров, частотные характеристики использования пользователями сервисов и их композиций, время выполнения сервисов и т.д. На основе анализа статистических данных и семантической сети формируются последовательности вызова сервисов в виде программ на языке JavaScript (авторы: к.т.н. Р.К. Федоров, к.т.н. Ю.В. Авраменко).

Программа фундаментальных исследований Президиума РАН I.7. «Новые разработки в перспективных направлениях энергетики, механики и робототехники»

Координатор программы – ак. А.Н. Лагарьков

Подпрограмма I.30. «Теория и технологии многоуровневого децентрализованного группового управления в условиях конфликта и кооперации»

Координатор программы – чл.-к. РАН Д.А. Новиков

Проект «Методы, алгоритмы и инструментальные средства децентрализованного группового решения задач в вычислительных и управляющих системах»

№ гос. регистрации: АААА-А18-118031590006-2

Научный руководитель проекта – ак. И.В. Бычков

1. Разработан новый алгоритм динамического планирования действий агентов управления информационно-вычислительной системой, интегрирующей Grid и облачные вычисления, с учетом отказов ее элементов (авторы: к.т.н. А.Г. Феоктистов, Р.О. Костромин).

2. Разработана новая дискретно-событийная конечно-автоматная модель динамики функционирования вычислительных агентов для децентрализованного управления процессом распределенного сборочного программирования (авторы: д.т.н. Г.А. Опарин, к.т.н. В.Г. Богданова).

3. Предложен подход к координации гетерогенной группы автономных роботов в условиях топливных ограничений при выполнении продолжительных многоцелевых миссий (см. рис. 33). Задача координации заключается в построении такого расписания ротации группы (порядка и времени пополнения каждым роботом своих топливных запасов), которое обеспечило бы максимальную производительность подгрупп роботов, остающихся для выполнения задач на протяжении всей длительности миссии. Эффективность группового расписания обеспечивается (в порядке убывания приоритетности):

1. Поддержанием работоспособности всех роботов в группе (своевременная подзарядка) с учетом количества доступных доков на зарядной станции, объемов аккумуляторных батарей и скорости пополнения заряда на станции;



- II. Постоянным наличием всех необходимых типов бортового оборудования у работающей подгруппы;
- III. Исключением случаев одновременной подзарядки большого количества роботов, в особенности самых быстрых (производительных) из них;
- IV. Отсутствием излишне частых групповых сборов (необходимых для отправки нуждающихся роботов на подзарядку или прием в группу уже зарядившихся роботов) за счет совмещения нескольких подобных событий в одной временной точке.



Рис. 33. Схематическое представление продолжительной миссии группы роботов

Предлагается использование эволюционного подхода к планированию расписания ротации группы роботов с учетом их функциональной и параметрической разнородности. Разработана модификация эволюционных алгоритмов, эффективно реализующая быстрое и надежное составление допустимых групповых расписаний, а также их оперативную корректировку в случае возникновения непредвиденных событий. Используется набор специализированных конструктивных эвристик, адаптированные генетические операторы и оригинальные и продвинутое процедуры улучшения решений. Предложена оригинальная схема кодирования решения, позволяющая значительно понизить размерность задачи и вычислительные затраты на поиск ее решения. Произведена программная реализация разработанного подхода и серия вычислительных экспериментов на сгенерированном наборе тестовых задач, где подход показал свою высокую эффективность и масштабируемость. Пример сгенерированного расписания ротации для разнородной группы из четырех роботов представлен на рис. 34.

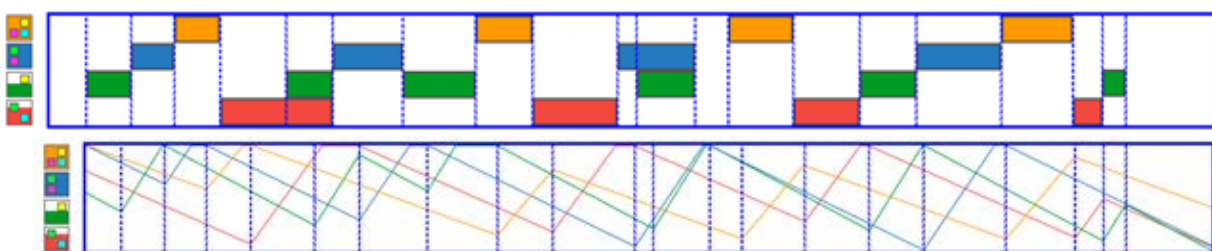


Рис. 34. Пример сгенерированного расписания ротации для разнородной группы из четырех роботов и соответствующий ему график динамики заряда аккумуляторов



**Комплексная программа фундаментальных научных исследований СО РАН № П.1
«Междисциплинарные интеграционные исследования» на 2018-2020 гг.**

Интеграционный проект «Разработка методов и веб-ориентированных технологий тематической обработки мульти- и гиперспектральных данных дистанционного зондирования Земли в задачах экологического мониторинга и рационального природопользования»

Координатор проекта – д.ф.-м.н. О.И. Потатуркин

Блок «Разработка и экспериментальное исследование эффективности методов оценки антропогенного воздействия на окружающую среду»

№ гос. регистрации: АААА-А18-118031590007-9

Руководитель блока – д.т.н. Г.М. Ружников

Исполнители: к.т.н. Р.К. Федоров, к.т.н. Ю.В. Авраменко

В рамках проекта для поиска антропогенных объектов, определения их формы и их изменений выполнялось развитие метода поиска объектов на основе запросов на языке SOQL, который производит поиск объектов на снимках сверхвысокого разрешения на основе логического вывода и деформируемых моделей. Развитие метода заключалось в реализации сочетания интерпретатора языка SOQL с нейронными сетями. Нейросетевые методы качественно обрабатывают спектральные, текстурные и структурные признаки на основе репрезентативной обучающей выборки. Тем не менее, поиск объектов заданной формы с помощью нейронных сетей требует создания репрезентативной обучающей выборки. Обучающая выборка должна включать все возможные положения объекта с заданной формой. Ее формирование – достаточно сложный процесс. Чтобы исключить необходимость формирования репрезентативной обучающей выборки положений объекта предлагается использовать метод поиска объектов по запросу на языке SOQL в сочетании с нейронной сетью. Нейронная сеть позволяет быстро находить возможные положения объекта по текстурным и спектральным признакам, а метод поиска – определять точное положение объекта по структурному описанию.

В рамках проекта использовалась предобученная модель U-Net. В ходе экспериментов обучающая выборка была составлена из 720 изображений размером 128×128. Для тестирования нейросети обучающая выборка была разделена на тренировочную и тестовую, которые составили 80% и 20%, соответственно. Завершающий шаг по уточнению положения и выбора объектов основан на применении интерпретатора SOQL. Для поиска углов применяется детектор Харриса.

Полученный подход тестировался на аэрофотоснимках, подготовленных исследовательским институтом Inria Sophia Antipolis. Набор включает 180 изображений RGB размером 5000×5000, с пространственным разрешением 0.3 м, покрывающих территорию 810 км².

Разработаны методы анализа серии снимков сверхвысокого разрешения для оценки динамики изменения антропогенных объектов, которые основываются на нейронной сети U-Net и интерпретаторе языка SOQL. Применение нейронных сетей позволяет выделить различные объекты населенных пунктов по текстурным и спектральным признакам, а интерпретатор языка SOQL производит поиск объектов с определенными структурными характеристиками. В результате этого сочетания, например, можно определить тип застройки населенных пунктов.



**Отчет Института динамики систем и теории управления
имени В.М. Матросова СО РАН за 2019 г.**

Интеграционный проект № 7 «Разработка физических и технологических принципов изготовления приборов, использующих спиновую степень свободы на основе структур с квантовыми точками и материалов, совместимых с кремниевой технологией»

Научный руководитель: чл.-к. РАН А.В. Двуреченский

Блок «Разработка алгоритмов и решение задач управления спиновыми токами в структурах с квантовыми точками»

№ гос. регистрации: АААА-А18-118032090008-8

Руководитель блока: д.т.н. А.Ю. Горнов

Исполнители: к.т.н. Т.С. Зароднюк, А.С. Аникин, П.С. Сороковиков

Разработаны алгоритмы идентификации математических моделей процесса релаксации фотопроводимости массива квантовых точек в магнитном поле. Реализована и протестирована многометодная вычислительная технология для исследования экстремальных свойств изучаемых моделей. Созданы методики компьютерного эксперимента и проведены многовариантные расчеты по верификации и проверке адекватности предложенных в рамках проекта моделей относительно сформированных групп однородных натуральных экспериментов. Проведены вычислительные эксперименты, в результате которых были найдены наборы параметров, с хорошей точностью описывающих экспериментальные данные и позволившие объяснить наблюдаемое в эксперименте необычное поведение фотопроводимости в магнитном поле. Полученные результаты позволили воспроизвести в вычислительном эксперименте ускорение релаксации фотопроводимости массива квантовых точек в магнитном поле.

Интеграционный проект № 39 «Карбон-пермо-триасовые гранитоидные батолиты и базит-ультрабазитовые комплексы южного обрамления северо-азиатского кратона: возрастные рубежи, численные модели формирования, металлогения»

Научный руководитель: чл.-к. РАН Е.В. Скляр

Блок «Разработка алгоритмов и методик параметрической идентификации динамических моделей формирования батолитов и базит-ультрабазитовых комплексов»

№ гос. регистрации: АААА-А18-118032090006-4

Руководитель блока: д.т.н. А.Ю. Горнов

Исполнители: В.В. Козлов, А.С. Аникин, к.т.н. Т.С. Зароднюк, П.С. Сороковиков

Проведена структурная идентификация модели гранитоидного магматизма, описываемой системой дифференциальных уравнений в частных производных второго порядка. Для постановки задачи параметрической идентификации предложенной модели была создана информационная система, включающая результаты полевых исследований, проводимых в последние годы сотрудниками Института земной коры СО РАН. Численное решение задачи параметрической идентификации выполнялось с применением



**Отчет Института динамики систем и теории управления
имени В.М. Матросова СО РАН за 2019 г.**

многометодных вычислительных технологий, основанных как на глобализованных алгоритмах (Лууса-Яаколы, Пауэлла-Брента, Растригина), так и на алгоритмах локального поиска – сопряженных градиентов и квазиньютоновских. Проведенное математическое моделирование открывает реальные возможности изучения проблемы правомерности отнесения исследованных гранитоидных батолитов и ассоциирующих с ними базит-ультрабазитовых комплексов к редко встречающемуся в мире и не имеющего аналогов на территории Российской Федерации «сиалическому» типу крупных магматических провинций.

Интеграционный проект № 66 «Подходы к разработке стратегий и программ социально-экономического развития сибирских регионов с экстремальными природно-климатическими условиями»

Научный руководитель: чл.-к. РАН В.И. Сулов

Блок «Создание специализированного программного инструментария, способного производить анализ многомерных экономических моделей динамического типа с невыпуклыми критериями качества»

Руководитель блока: д.т.н. А.Ю. Горнов

Исполнители: д.ф.-м.н. А.Л. Казаков, к.ф.-м.н. А.А. Лемперт, А.С. Аникин, к.т.н. Т.С. Зароднюк, П.С. Сороковиков

Разработан программный комплекс, позволяющий эффективно исследовать типичные в экономических приложениях оптимизационные задачи, в том числе задачи в динамических постановках (дифференциальные управления, рекуррентные соотношения), с балансовыми и траекторными ограничениями, невыпуклыми терминальными и интегральными функционалами и другие. Реализованы алгоритмы оптимизации как для линейных, так и для нелинейных динамических моделей, рассматриваемых и в непрерывном, и в дискретном времени. Были разработаны интерфейсы программного комплекса, средства верификации программной постановки задачи, технологии визуализации получаемых решений. Алгоритмическое наполнение программного комплекса составляют библиотеки алгоритмов интегрирования систем дифференциальных уравнений, алгоритмов оптимизации, включающих как ряд новых алгоритмов, демонстрирующих высокую конкурентоспособность, так и набор специализированных модификаций традиционных методов, позволяющих обеспечивать надежность выполняемых расчетов. Успешно решен ряд новых содержательных задач, связанных с проблемой территориальной связанности России.



**ИССЛЕДОВАНИЯ ПО ПРОЕКТАМ, ПОДДЕРЖАННЫМ
СОВЕТОМ ПО ГРАНТАМ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ**

Грант Президента РФ МК-4155.2018.9 «Разработка параллельных алгоритмов решения проблемы булевой выполнимости на основе методов машинного обучения с применением к задачам криптографии»

Руководитель проекта – к.т.н. О.С. Заикин

Предложен алгоритм машинного обучения, предназначенный для определения полезности конфликтных дизъюнктов, генерируемых в CDCL-выводе. Предложенный алгоритм использует бинарный классификатор, который основан на методе опорных векторов. Реализация данного алгоритма была сделана на базе известного CDCL-решателя Glucose. Полученный модифицированный решатель позволил быстрее (в сравнении с исходным решателем) решить трудные SAT-задачи из нескольких семейств, использованных в соревновании SAT Competition 2018. Кроме того, был получен ряд дополнительных результатов. Во-первых, были предложены и реализованы новые алгоритмы псевдобулевой оптимизации, предназначенные для построения декомпозиций трудных SAT-задач. Эти алгоритмы были применены для оценки трудоемкости решения задач SAT-криптоанализа поточных шифров Mickey, Grain_v1, Rabbit и Trivium. Во-вторых, был подготовлен вычислительный эксперимент, направленный на решение трудных SAT-задач в проекте добровольных распределенных вычислений. Речь идет о SAT-задачах, кодирующих ослабленные задачи криптоанализа поточных шифров Mickey и Grain_v1.

Стипендия Президента РФ молодым ученым и аспирантам СП-3545.2019.5 «Применение высокопроизводительных вычислений к построению алгебраических атак на криптографические хеш-функции»

Руководитель проекта – И.А. Грибанова

Описан новый класс атак поиска прообразов (preimage attacks) на различные варианты хеш-функции MD4 (причем как на ослабленные по числу шагов версии этой функции, так и на полнораундовый вариант). Предложенные атаки основаны на идее Г. Доббертина ослабления уравнений криптоанализа функций вида MD4-k (k – число шагов) за счет наложения дополнительных ограничений на некоторые промежуточные шаги (т.н. «переменные сцепления»). Было показано, что с каждым таким набором ослабляющих ограничений естественным образом связывается вспомогательная функция, длина входа которой может быть существенно меньше 512 бит. С одной стороны, от прообраза произвольного значения такой функции можно эффективно перейти к прообразу этого значения в смысле исходной функции MD4-k. С другой стороны, вспомогательная функция зачастую обращается существенно эффективнее, чем соответствующая ей функция MD4-k. С



использованием вспомогательных функций были построены семейства легко обратимых выходов ряда функций MD4-k, так, для k=44 было показано, что число ее легко обратимых выходов не меньше, чем 2^{96} . Для полнораундовой хеш-функции MD4 с использованием вспомогательных функций было конструктивно описано множество, состоящее из приблизительно 2^{32} легко обратимых выходов. Таким образом, было показано, что ни одна из функций MD4-k, в том числе и полнораундовая MD4, не удовлетворяют свойствам случайного оракула.

Стипендия Президента РФ молодым ученым и аспирантам СП-3545.2019.5
«Разработка комплекса алгоритмов для поиска декомпозиций трудных примеров задачи булевой выполнимости с применением методов комбинаторной оптимизации»

Руководитель проекта – С.Е. Кочемазов

Получен ряд результатов в направлении решения трудных примеров задачи булевой выполнимости (SAT) с использованием т.н. недетерминированных лазеек. Более конкретно, для специальной функции, которая оценивает время решения трудного примера SAT при декомпозиции по фиксированному множеству переменных, было реализовано несколько алгоритмов ее оптимизации. Результатом оптимизации является множество переменных, использование которого для построения декомпозиции приводит к наименьшему по прогнозу общему времени решения построенных подзадач. Был проведен сравнительный анализ эффективности разных алгоритмов оптимизации в применении к рассматриваемой задаче. Оказалось, что большинство алгоритмов, в которых переход между точками пространства поиска предусматривает просмотр всей окрестности текущего рекорда работают хуже, чем steepest ascent методы и варианты эволюционных алгоритмов типа 1+1-EA. В то же время последние могут стабилизироваться на худших точках по сравнению с менее быстрыми методами. Описанные и дополнительные результаты были опубликованы в ряде статей в рейтинговых журналах и трудах международных конференций.