ИССЛЕДОВАНИЯ, ПРОВЕДЕННЫЕ ПРИ ПОДДЕРЖКЕ РОССИЙСКОГО НАУЧНОГО ФОНДА

Проект РНФ № 16-11-00053 **«Разработка методов исследования и построения иерархических систем децентрализованного интеллектуального управления группами автономных поисково-обследовательских роботов в условиях неопределенности»**

№ гос. регистрации: АААА-А16-116031110118-2

Руководитель проекта – ак. И.В. Бычков

Для разрабатываемого в рамках проекта моделирующего программного комплекса (МПК) был создан язык описания заданий и групповых миссий на основе языка позитивно-образованных формул (ПОФ). Разработано формальное описание грамматики языка как языка для логического программирования. В отличие от формального математического описания исчисления данный язык хорошо приспособлен для программирования. В разработанный язык, помимо логических конструкций, введены синтаксические элементы, с помощью которых можно описывать системные (вычисляемые) предикаты, а также предикаты, влияющие на сам логический вывод (ЛВ) в исчислении ПОФ. Системные предикаты в формуле, с помощью которой формализуется миссия, связаны с остальными компонентами МПК посредством передачи команд в МПК в случае, если в результате ЛВ системный предикат попал в базу фактов. Связь в обратную сторону, т.е. передача сообщений от МПК в систему ЛВ, осуществляется также с помощью системных предикатов, выполняющих функцию запроса данных, описывающих состояние МПК.

Разработан метод построения модульных супервизоров для дискретно-событийных систем (ДСС) как верхнеуровневых моделей АПР и их групп, основанный на применении средств автоматического доказательства теорем в исчислении ПОФ. В результате ЛВ теорем, представленных ПОФ с подформулами, отвечающими управляемой системе и требованиям, подлежащим удовлетворению, делается заключение о возможности построения соответствующего супервизорного управления или в случае невозможности выдается набор параметров системы, препятствующих этому. Использование полученной таким образом информации позволяет уменьшить перебор комбинаций подсистем и спецификаций, необходимых при построении модульных супервизоров.

Разработан алгоритм проверки конфликтности языков, генерируемых локальными супервизорами, основанный на том факте, что два формальных языка не конфликтуют, если их параллельная композиция является неблокирующей. Предложен новый способ представления конечных автоматов, являющийся основой для моделирования ДСС с помощью ПОФ. Новая формализация конечных автоматов как генераторов формальных языков, участвующих в алгоритмах теории супервизорного управления (ТСУ), более компактна, чем формализация, предложенная ранее в рамках проекта, и дает больше возможностей при настройке стратегий поиска логического вывода. С помощью указанного способа разработан новый метод построения параллельных композиций конечных автоматов и, как следствие, генерируемых ими языков. Преимуществом метода является тот факт, что автомат-композиция, получающийся в результате завершения вывода, не имеет

недостижимых состояний, поэтому нет необходимости использовать операцию сокращения. Предложенный метод построения параллельной композиции позволяет эффективно осуществлять проверку конфликтности языков и находить события и слова, приводящие к конфликту.

Разработана расширенная математическая модель задачи систематического многоцелевого мониторинга в виде новой вариации задачи маршрутизации транспорта. В предложенной постановке используются сразу три группы ограничений, описывающих как требования к обследованию целей миссии, так и к взаимному движению роботов группы: пространственные, временные и ограничения обслуживания. Такие задачи, объединяющие в себе целый спектр ограничений различной природы, призванных обеспечить детальное моделирование реальных задач, принято относить к актуальному классу мульти-атрибутных задач маршрутизации. Децентрализованное планирование допустимых групповых маршрутов, обеспечивающих своевременное выполнение всех задач с учетом действующих ограничений, осуществляется разработанной гибридной модификацией эволюционных алгоритмов, эффективность работы которой обеспечивается применением специализированных конструктивных эвристик, продвинутых методов локального поиска, а также дополнительной процедуры самоадаптации алгоритма. Произведена программная реализация подхода в рамках разрабатываемого моделирующего комплекса. Предложенный эволюционный подход демонстрирует высокое качество результатов на большом наборе тестовых задач, в том числе на задачах с высокой степенью гетерогенности объектов.

Разработаны основанные на сублинейных векторных функциях Ляпунова (ВФЛ) алгоритмы строгого анализа и синтеза нелинейных цифровых систем, управляемых на основе событий. Предполагается, что модель исследуемой системы представлена в некотором стандартном виде с учетом неопределенности параметров объекта управления и нелинейности характеристик исполнительных органов и датчиков. Разработанные алгоритмы обеспечивают анализ различных динамических свойств указанных систем, вычисление основных прямых показателей динамического качества, а также синтез параметров, исходя из обеспечения требуемого либо наилучшего динамического качества системы. При этом задачи анализа и синтеза формулируются непосредственно в терминах инженерных требований к системе (прямых показателей динамического качества); результаты получаются в том же виде. Выполнена численная реализация алгоритмов в виде инструментального средства системы Matlab. Возможности созданного инструментального средства позволяют экранировать от пользователя (инженера-практика) используемые специальные, достаточно сложные в математическом отношении методы.

Предложена архитектура многоуровневой системы управления группой АПР для выполнения типовых поисково-обследовательских миссий и работ по мониторингу подводной среды. В соответствии с предложенной архитектурой система управления включает три уровня: стратегический уровень, ответственный за планирование групповой миссии (распределение заданий между участниками группы), тактический уровень, определяющий логику выполнения текущего задания и ответственный за выбор подходящего шаблона поведения (режима функционирования) АПР, а также исполнительный уровень для реализации выбранного шаблона поведения.

Разработан прототип моделирующего программного комплекса для тестирования и отладки алгоритмических и коммуникационных схем, используемых для управления группировками АПР. В программном комплексе реализованы алгоритмы генерации реалистичного подводного ландшафта, базовые алгоритмы и средства симуляции подводной среды и роботов, а также инструменты для работы с различными трехмерными объектами. Предложен подход к генерации подводного рельефа на основе использования шума Перлина. Основная идея подхода заключается в комбинировании слоев, полученных при различных характеристиках шума, с последующим процедурным текстурированием. Предложенный подход позволяет создавать трехмерные модели рельефа дна, близкие по визуальному восприятию к прообразам реального мира.

Проект РНФ № 16-11-10046 **«Применение параллельных и распределенных алгоритмов решения проблемы булевой выполнимости (SAT) к криптоанализу, поиску комбинаторных структур и исследованию дискретных моделей коллективного поведения»**

Руководитель проекта – к.т.н. А.А. Семенов

Был исследован детерминированный вариант известной линейной пороговой модели (Deterministic Linear Threshold Model, DLTM) распространения влияния в сетях на предмет поиска множеств активирующих агентов относительно малой мощности, активирующих подавляющую часть сети. Соответствующая комбинаторная задача расстановки активирующих агентов известна как «Проблема максимизации влияния» (Influence Maximization Problem, IMP). Известно, что в недетерминированном варианте решение IMP с гарантированной (и относительно небольшой) погрешностью может быть найдено при помощи простейшего алгоритма жадного (greedy) типа. Однако в детерминированном варианте (а именно он интересен из практических соображений) данная задача не только NP-трудна, но и не имеет приближенных алгоритмов решения с гарантированной погрешностью в предположении, что P не равно NP. В рамках проведенных исследований применительно к DLTM/IMP были разработаны алгоритмы гибридного типа, в которых жадные стратегии используются для быстрого достижения некоторого начального приближения, а затем приближенные решения итеративно улучшаются при помощи SAT-решателей. Для сетей на нескольких сотнях вершин разработанные алгоритмы позволяли находить решения IMP, которые оказывались существенно лучше, чем решения, найденные описанными в доступных источниках алгоритмами. В этом же блоке исследований была построена новая программная реализация разработанных нами ранее алгоритмов генерации графов атак в компьютерных сетях. В новой программе взамен SAT-решателя используется явное распространение ограничений в рамках быстрых структур данных, реализованных на языке C++. В ряде случаев построенная программная система генерирует графы атак в разы быстрее, чем предыдущая версия. На текущую версию программы UnProVET генерации графов атак получено программное свидетельство.

Были построены алгебраические атаки на некоторые известные симметричные шифры (Simon, Spech, PRESENT, Trivium, Grain v1). Основная новизна построенных атак

заключается в том, что для оценивания их трудоемкости используется формализованный вариант понятия SAT-иммунности, относительно которого доказано, что соответствующие оценки имеют гарантированную точность. Теория таких оценок базируется на том факте, что со случайными парами вход/выход рассматриваемой криптографической функции и множеством угадываемых бит (guessed bits set) может быть связана случайная величина, принимающая значения в множестве {0,1} («бернуллиевская величина») и, таким образом, имеющая известную верхнюю оценку дисперсии. Этот факт позволяет использовать метод Монте-Карло для оценивания вероятности данной случайной величины с любой наперед заданной точностью. Для поиска множества угадываемых бит, дающего минимальную по трудоемкости атаку, могут быть использованы различные метаэвристические алгоритмы, применяемые в пседовбулевой оптимизации (конкретно, для поиска экстремумов black-box функций). Задачи минимизации такого сорта оценочных функций были решены для перечисленных выше шифров. В результате было показано, что, например, ослабленные по числу раундов варианты шифра Simon с 64-битным ключом являются нестойкими, если число раундов < 20. Трудоемкость алгебраических SAT-атак для вариантов данного шифра с числом раундов > 20 мало отличается от трудоемкости аналогичных атак для его полнораундовой версии (т.е. для ситуации, когда число раундов равно 32). В отношении рассматриваемого класса атак полнораундовые шифры Simon и PRESENT оказываются сопоставимыми по стойкости. Шифр Speck, с другой стороны, является существенно более стойким, чем Simon. Особенно интересно, что для полнораундового PRESENT с 80-битным ключом предложенные алгоритмы дают атаку, которая примерно в 10^5 раз эффективнее, чем атаки, получаемые этими алгоритмами для 80-битных поточных шифров Trivium и Grain v1. Еще раз подчеркнем, что оценки трудоемкости атак, о которых идет речь, имеют гарантированную точность.

Была предложена новая метаэвристическая стратегия, применимая для оптимизации произвольных псевдобулевых функций, в том числе и функций типа «черный ящик» (black box function). В основе новой стратегии лежит идея использовать специальные сюръективные отображения: каждое такое отображение сопоставляет множеству булевых переменных множество переменных меньшей мощности. Такие отображения называются склеивающими (merging mapping), а полученные с их помощью переменные называются склеенными (merged variables). Области значений склеенных переменных называются доменами. Декартовы произведения доменов, обозначаемые D^m, где m – конкретное склеивающее отображение, является метрическим пространством с метрикой Хэмминга. Показано, что между исходным булевым гиперкубом $\{0,1\}^n$ и пространством D^m существует биекция. На основании этого факта задача оптимизации исходной псевдобулевой функции f на $\{0,1\}^n$ сводится к задаче оптимизации т.н. «m-сопряженной к f» функции в пространстве D^m. Показано, что экстремальные значения этих функций совпадают. Можно привести множество примеров, когда точка в $\{0,1\}^n$ является локальным экстремумом f в окрестности Хэмминга радиуса 1, но образ этой точки не является локальным экстремумом в аналогичной окрестности в пространстве D^m. В этой ситуации алгоритм Hill Climbing, будучи запущенным в D^m, может улучшить текущее рекордное значение функции f. Был предложен алгоритм, комбинирующий стратегию склеивания переменных с известным эволюционным

алгоритмом (1+1)-EA. В отношении полученного алгоритма (который был назван (1+1)-MVEA – (1+1) Merging Variables Evolutionary Algorithm) было доказано, что, во-первых, математическое ожидание числа бит, которые переворачиваются в рамках одной итерации этого алгоритма, равно 1. Это означает, что (1+1)-MVEA сохраняет одно из важнейших базовых свойств исходного (1+1)-EA. С другой стороны, для ряда частных случаев (1+1)-MVEA построены верхние оценки, которые оказываются асимптотически ниже, чем аналогичные оценки для оригинального алгоритма (1+1)-EA.

Была предложена новая схема пропозиционального кодирования свойства элементов произвольного конечного множества быть различными. Такого рода предикаты возникают во многих комбинаторных задачах и, в том числе, в задачах существования некоторых комбинаторных структур (combinatorial designes). Была построена новая пропозициональная кодировка свойства различия, основанная на использовании специального OtO-предиката (от «One-to-One»). Доказано, что новая кодировка асимптотически экономнее известной кодировки, базирующейся на т.н. «OOC-предикате» (сокращение от «Only One Cardinality»). Для практического сравнения OtO- и OOC -кодировок мы построили с их использованием SAT-задачи, кодирующие существование греко-латинских квадратов 10-го порядка. В вычислительных экспериментах SAT-решатель (использовались многопоточные SAT-решатели Plingeling и Painless) порождал очередной греко-латинский квадрат в среднем за полчаса для SAT-задачи, основанной на OOC-кодировке, и за 15 минут для аналогичной задачи, построенной на базе OtO-кодировки.

Был разработан SAT-решатель, основную новизну которого составила специальная техника учета повторно порождаемых конфликтных ограничений. Эта техника была скомбинирована с решателем MapleLCMDistChronoBT – победителем соревнований SAT решателей 2018 года «SAT Competition-2018». Результатом стал новый SAT-решатель, получивший название MapleLCMBDistChronoBT-DL (DL – аббревиатура новой эвристики, являющаяся сокращением от «Duplicate Learnts»). Решатель MapleLCMDistChronoBT-DL победил на соревнованиях SAT-решателей 2019 года «SAT race-2019» в двух из трех основных категорий («UNSAT» и «SAT+UNSAT») (http://sat-race-2019.ciirc.cvut.cz/).

Проект РНФ 17-71-10176 **«Параллельные вычисления и методы целочисленного программирования для задач кластеризации и интеллектуального анализа больших массивов данных»**

№ гос. регистрации: АААА-А17-117100670002-3

Руководитель проекта – к.ф.-м.н. А.В. Ушаков

Разработаны параллельные и распределенные алгоритмы кластеризации, основанные на поиске близких к оптимальному решений в задаче о k-медоидах и ее нелинейной модификации с нефиксированным числом кластеров. Программно реализованы и проанализированы версии для суперкомпьютеров с общей памятью и вычислительных кластеров.

С использованием ресурсов Иркутского суперкомпьютерного центра СО РАН проведен обширный вычислительный эксперимент по тестированию разработанных

алгоритмов в приложении к задаче анализа больших коллекций медиаданных, в частности, изображений человеческих лиц. Исследовано приложение разработанных алгоритмов кластеризации в области оптимального разделения баз данных социальных сетей, в частности, разработаны варианты для задач на графах, возникающих в области социальных медиа.

Проект РНФ № 18-71-10001 **«Методология и инструментальная платформа разработки систем извлечения данных из произвольных электронных таблиц»**

№ гос. регистрации: АААА-А18-118082090003-8

Руководитель проекта – к.т.н. А.О. Шигаров

Выполнено развертывание инфраструктуры проекта (средств управления разработкой программного обеспечения и сайта). Разработано алгоритмическое обеспечение анализа произвольных таблиц (в том числе алгоритмов анализа иерархических отношений единиц табличных данных и реконструкции физической структуры ячеек). Усовершенствован предметно-ориентированный язык анализа и интерпретации таблиц за счет встраивания реализованной функциональности ролевого и структурного анализа таблиц. Разработана грамматика, объектная модель и интерпретатор данного языка с целью синтеза исходного кода программ трансформации табличных данных. Выполнено прототипирование системы генерации связных данных на основе извлечения табличной информации. Спроектирована архитектура и объектная модель предлагаемой инструментальной платформы.

Сотрудники ИДСТУ СО РАН также проводили исследования по проектам РНФ под руководством ведущих ученых из других научных организаций:

Проект РНФ 17-11-01093 **«Приближенно оптимальные стратегии в игровых задачах управления»**

Руководитель проекта – к.ф.-м.н. Ю.В. Авербух

Исполнитель от ИДСТУ СО РАН – к.ф.-м.н. Н.И. Погодаев

Проект РНФ № 18-12-00128 **«Прецизионное исследование связанных состояний частиц в квантовой теории поля»**

Руководитель проекта – д.ф.-м.н. А.П. Мартыненко

Исполнитель от ИДСТУ СО РАН – к.ф.-м.н. А.Е. Раджабов

Проект РНФ № 18-41-06003 **«Карлсруэ-Российская инициатива по работе с астрофизическими данными на протяжении их жизненного цикла»**

Руководитель проекта – к.ф.-м.н. А.П. Крюков

Исполнители от ИДСТУ СО РАН – ак. И.В. Бычков, к.т.н. А.О. Шигаров, к.т.н. А.А. Михайлов