



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

Разработана новая версия системы автоматического построения логического вывода позитивно-образованных формул, которая используется в качестве основного ядра в интерпретаторе нехорновских логических программ. Интерпретатор разработан с внедрением дополнительного модуля, контролирующего возможность применения только одного конструктивного целевого правила в процессе поиска логического вывода формулы, представляющей входную программу. При реализации данной возможности, сначала производится попытка поиска логического вывода с использованием только неконструктивных целевых правил, содержащихся в формуле. Когда поиск логического вывода исчерпывает все варианты перебора при введенном ограничении, и если на верхнем уровне дерева текущей формулы, вывод которой остается найти, не осталось дизъюнктивных ветвлений, производится попытка завершения поиска ее вывода с использованием конструктивного целевого правила. Ограничение на максимальное количество возможных шагов вывода позволяет находить кратчайший конструктивный вывод. Интерпретатор реализован с использованием клиент-серверной архитектуры, что позволяет его встраивать в любые другие системы с использованием необходимых для конкретной задачи протоколов связи. Каждый такт времени, клиент отправляет серверу очередную задачу или параметры для вычисляемых предикатов, которые могут значительно влиять на построение логического вывода. Разработанный интерпретатор внедрен в виде программной компоненты моделирующего программного комплекса на верхнем уровне и используется для описания сценариев, заданий и групповых миссий для роботов.

Проведена реализация модульных супервизоров в составе иерархической системы управления группами автономных подводных роботов (АПР), построенных с применением исчисления ПОФ. Для применения исчисления ПОФ в задачах построения супервизоров для ДСС разработан подход к описанию в языке ПОФ исследуемых систем и требований к их функционированию. База такой ПОФ включает в себя предикаты, предназначенные для формирования порождаемого и маркированного языков ДСС, а также факты, задающие конечный автомат, соответствующий системе: множество переходов, управляемые и неуправляемые события, начальное состояние, а также множество маркированных переходов, которым соответствуют выделенные термы. Вопрос, нацеленный на обработку именно этих термов, позволяет генерировать маркированный язык как первые аргументы атомов, добавляемых в базу при срабатывании соответствующего правила. Таким образом, происходит аккумуляция слов маркированного языка, что позволяет проводить его анализ, например, при проверке свойства неблокирования. Проверка на блокирование является особо актуальной при построении модульных супервизоров, поскольку объединение неблокирующих супервизоров может привести к блокированию системы, или конфликту.



Для коррекции спецификаций в том случае, если в результате логического вывода получено заключение о невозможности построения супервизора при текущем наборе параметров или обнаружен конфликт, используются знания, накопленные в ходе вывода, а также модифицируемость семантики исчисления ПОФ.

Математическая модель задачи систематического мониторинга, предложенная на первом этапе выполнения проекта, была расширена новым видом ограничений обслуживания. Новые ограничения позволяют задавать технические требования к количеству роботов каждого типа для коллективного обследования цели. Тип робота при этом определяется в зависимости от его функциональных возможностей. Разработанный для решения задачи эволюционный алгоритм был модифицирован для учета новых ограничений: адаптированы конструктивные эвристики построения начальных маршрутов, изменены процедуры локального поиска, доработана схема оценки эффективности решений. Произведена программная реализация расширенной постановки задачи и модифицированного алгоритма для ее решения. Проведены вычислительные эксперименты, доказывающие эффективность предложенного подхода.

Разработан подход к планированию продолжительных миссий группы роботов на верхнем уровне через составление долгосрочного расписания групповой ротации роботов. Расписание составляется таким образом, чтобы обеспечить удовлетворение сразу нескольких критериев, способствующих эффективному выполнению миссии, а именно: своевременного пополнения роботами своих топливных ресурсов; возможности эффективной работы членов группы, остающихся для выполнения задач, с учетом их функциональных возможностей; требуемой периодичности сеансов связи для регулярного обмена данными. Для решения задачи разработана модификация генетического алгоритма, эффективная работа которого обеспечивается наличием ряда специализированных эвристик и схем окрестностного поиска. Произведена программная реализация алгоритма, сравнительный анализ с известными подходами, показавший высокую эффективность разработанного алгоритма, а также реализована синхронная работа планировщика с разработанным алгоритмом маршрутизации.

Разработаны основанные на схеме «лидер-ведомый» алгоритмы событийного управления формациями автономных подводных роботов (АПР) при движении вдоль заданной траектории при различных предположениях о доступности и качестве измерений. Рассмотрены варианты, когда управление АПР как ведомого строится на основе прямых дискретных измерений своего положения относительно лидера, и на основе данных, получаемых от лидера по акустическим каналам связи. Предложены цифровые законы управления АПР с механизмом пересчета управляющих сигналов по событиям, допускающие простую реализацию на борту и позволяющие уменьшить нагрузку на вычислительные устройства АПР за счет нерегулярной корректировки управляющих воздействий. Также предложен закон управления виртуальной целью, которая перемещается по опорной траектории и задает движение группы, обеспечивающие адаптацию ее скорости к текущему значению кривизны отслеживаемого пути. Такой механизм позволяет ведомым удерживаться в формации при выполнении сложных маневров, например, связанных с движением по дуге малого радиуса. С применением методологии табличного управления и сублинейных векторных функций Ляпунова выполнен синтез децентрализованного управления типовыми формациями малоприводных крупногабаритных подводных аппаратов по критерию минимума ошибки стабилизации. При синтезе в комплексе учитывались



погрешности измерений АПР, ограничения на ресурсы управления, непостоянство курса и скорости движения группы, а также задержки при передаче необходимой информации от лидеров к ведомым. Исследованы вопросы зависимости точности стабилизации формации от такта управления АПР и параметров, входящих в условия срабатывания событий.

Проект РФФИ № 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

Были разработаны новые алгоритмы активации сетей, комбинирующие жадные эвристики с применением SAT решателей. В процессе решения задачи поиска расстановки активаторов в сети, которая активирует сеть за наименьшее число шагов, сначала используется жадный алгоритм, который строит начальную расстановку, а затем делается попытка уточнить полученное решение при помощи SAT решателя. С этой целью в пропозициональную кодировку процесса активации сети добавляется информация о найденном решении (кодировка при этом частично упрощается). Затем формируются дополнительные условия, кодирующие факт существования активирующего множества меньшей мощности в сравнении с решением, найденным жадным алгоритмом. Итогом является КНФ, выполняемая тогда и только тогда, когда существует расстановка активаторов меньшей мощности в сравнении с найденной, которая активирует сеть за то же число шагов. Алгоритмы указанного типа были применены нами для решения задач расстановки патчей в компьютерной сети с целью блокирования всех возможных атак. Алгоритмы были реализованы в рамках разработанной ранее программной системы UnProVET. В вычислительных экспериментах удавалось решать задачи расстановки патчей в синтетических сетях на нескольких десятках тысяч вершин, используя для этого лишь обычный персональный компьютер.

Были построены новые атаки на криптографические хеш-функции семейств MD и SHA, в рамках которых к ослабленным уравнениям криптоанализа применяются SAT решатели. Новизна построенных атак заключается в полностью автоматической процедуре генерации ослабляющих ограничений (аналогов ограничений, предложенных Г. Доббертином). Конкретно, мы рассматриваем пространство возможных вариантов наборов ограничений как булев гиперкуб -- каждый набор ограничений задается булевым вектором. Далее мы запускаем эволюционный алгоритм (использовались алгоритмы (1+1)-EA и (1+1)-FEA) для осмысленного перебора точек гиперкуба и требуем от выбираемых точек, чтобы ограничения на соответствующие этим точкам переменные сцепления давали вспомогательную функцию вида $g: \{0,1\}^k \rightarrow \{0,1\}^{128}$, где $k \ll 512$. Для полученной таким способом вспомогательной функции мы затем строим атаку на основе инверсного множества с лазейкой (IBS-атака). Атака считается успешной, если ее трудоемкость оказывается меньше атаки методом грубой силы. Для оценивания трудоемкости мы использовали известный пакет для детальной отладки программ Valgrind (инструменты, входящие в данный пакет, помимо прочего позволяют оценивать число обращений к кэшу при выполнении программы). Используя перечисленные подходы, мы построили новые атаки на



урезанные по числу шагов функции MD5 и SHA-1. В частности, построенные нами атаки показывают, что двухраундовый вариант MD5 (рассматривается 32 шага алгоритма сжатия) нельзя считать односторонней функцией, поскольку IBS-атака для нее оказывается существенно (в тысячи раз) эффективнее полного перебора пространства возможных входов.

Были разработаны новые алгоритмы псевдобулевой оптимизации, комбинирующие предложенный ранее принцип склеивания переменных (Merging Variables Principle, MVP) и эволюционные стратегии, используемые для выхода из сильных локальных экстремумов. В основе MVP лежит сводимость задачи максимизации/минимизации функции, заданной на булевом гиперкубе, к аналогичной задаче для функции, заданной на специальном метрическом пространстве. Между исходным гиперкубом и новым пространством задается взаимно-однозначное отображение. Про оптимизируемую на новом пространстве функцию говорим, что она является μ -сопряженной с исходной. Показано, что в исходном гиперкубе точка может быть локальным экстремумом рассматриваемой функции, тогда как ее образ при упомянутой выше биекции в новом пространстве может не быть локальным экстремумом μ -сопряженной функции. Тогда простой алгоритм восхождения к вершине (Hill Climbing) или двойственный ему (для задачи минимизации) позволит выйти из локального экстремума на гиперкубе и, возможно, улучшить рекордное значение целевой функции. В текущем году MVP был дополнен процедурами выхода из сильных локальных экстремумов. Сильный локальный экстремум -- это точка в гиперкубе, являющаяся локальным экстремумом для исходной функции, такая что в результате нескольких различных отображений ее в новые пространства мы получаем локальные экстремумы μ -сопряженных функций. Для выхода из сильных локальных экстремумов мы использовали эволюционные стратегии (конкретно, (1+1)-FEA и один специальный вариант генетического алгоритма). Все разработанные алгоритмы были реализованы в виде многопоточного программного приложения. Полученный решатель мы применили к двум классам задач: к обращению криптографических хеш-функций с дополнительными ограничениями на хеш, а также к одному частному случаю широко известной задачи о размещении производств (Facility Location Problem). В вычислительных экспериментах наш решатель превзошел по эффективности известные решатели, побеждавшие на специализированных соревнованиях (Plingeling, Treengeling, Loandra).

Алгоритмы решения задачи MaxSAT были применены к одному случаю известной проблемы о размещении производств (Facility Location Problem). Конкретно, рассматривается множество клиентов и множество производств. Требуется закрыть некоторые производства. Любая пара вида (u, v) , где u – клиент, а v – производство, связаны отношением «удовлетворенности»: клиент в данной паре считается довольным, если закрытие производства v не изменит специальным образом определяемую функцию удовлетворенности (например, закрытие ближайшего к клиенту производства может сделать его недовольным). Для фиксированного числа закрываемых производств (произвольных) требуется минимизировать число недовольных клиентов. Было доказано, что данная задача является NP-трудной. Кроме этого, оказалась, что рассматриваемая задача эффективно сводится к MaxSAT в формулировке, использующей hard и soft клозы. К данной задаче были применены как известные полные MaxSAT решатели, так и неполный решатель, основанный на принципе склеивания переменных, который был создан в рамках настоящего проекта.



Этот решатель показал на рассматриваемом классе задач лучшие результаты в сравнении с известными неполными MaxSAT решателями.

На основании анализа результатов соревнований SAT Competition и SAT Race последних лет были разработаны новые эвристические техники, ускоряющие работу CDCL SAT решателей. В частности, были предложены новые механизмы переключения между различными режимами выбора переменных уровней решения (branching heuristics), а также разработаны оригинальные процедуры чистки баз конфликтных ограничений, учитывающие многоуровневую структуру таких баз. Было показано, что применение разработанных техник существенно ускоряет работу CDCL SAT решателей, побеждавших на соревнованиях SAT Competition и SAT Race последних лет (использовались библиотеки тестов с данных соревнований). Также были предложены и протестированы новые подходы к повышению запрещающей силы конфликтных дизъюнктов с использованием процедуры Learnt Clause Minimization (LCM). В частности, был разработан алгоритм, проверяющий возможность поглощения минимизированным дизъюнктом дизъюнктов, находящихся в очереди на минимизацию. Встраивание данной техники в современные SAT решатели дало повышение их эффективности на отдельных классах тестов.

Проект РФФ № 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

Получены следующие результаты.

Методы и инструментальные средства извлечения таблиц. Новая глубокая нейросетевая (ANN) модель обнаружения таблиц на изображениях документов с улучшенным качеством предсказаний о расположении позиций (ограничивающих прямоугольников) обнаруживаемых таблиц. Алгоритмическое обеспечение анализа компоновки неразмеченных PDF (Portable Document Format) документов. Алгоритмы должны обеспечить сборку текстовых блоков для последующего использования при верификации и коррекции результатов обнаружения таблиц, а также для распознавания структуры табличных ячеек. Алгоритмическое обеспечение верификации и коррекции предсказаний, производимых глубокими нейронными сетями обнаружения таблиц на изображениях документов. Алгоритмы должны повысить качество результатов обнаружения таблиц в документах за счет снижения доли ошибочных случаев.

Методы и инструментальные средства анализа таблиц. Программная библиотека поддержки обработки и анализа естественно-языкового содержания произвольных таблиц с расширенной функциональностью очистки данных. Библиотека должна обеспечить включение в правила анализа и интерпретации таблиц расширенных возможностей работы с особенностями текстового содержания таблиц. Инструментальная платформа разработки программного обеспечения извлечения и трансформации табличных данных с интеграцией новых компонент поддержки анализа естественного языка и трансляции CRL языка с уточненной объектной моделью правил анализа и интерпретации таблиц.

Методы и инструментальные средства интерпретации таблиц. Алгоритмическое обеспечение концептуализации табличного содержания с использованием инструментов



обработки естественного языка и открытых связанных данных (LOD), расширенное новыми метриками оценки семантической близости. Алгоритмы должны обеспечить связывание извлекаемых функциональных единиц табличных данных с сущностями выбранной глобальной таксономии (онтологии). Программная система генерации связанных данных на основе трансформации произвольных электронных таблиц, реализующая следующие операции: семантическое аннотирование таблиц в канонической форме с восстановленными именованными сущностями; синтез связанных данных в формате RDF; генерацию семантически аннотированных электронных таблиц. Программная система построения концептуальных моделей (предметных онтологий) из фрагментов (связанных данных), генерируемых из электронных таблиц, представленных в канонической форме. Эмпирические результаты применения системы должны продемонстрировать автоматическую сборку предметной онтологии по табличным данным из отчетов по экспертизе промышленной безопасности.

Алгоритмическое обеспечение концептуализации табличного содержания с использованием инструментов обработки естественного языка и открытых связанных данных (LOD), расширенное новыми метриками оценки семантической близости. Алгоритмы должны обеспечить высокое качество связывания извлекаемых функциональных единиц табличных данных с сущностями выбранной глобальной таксономии (онтологии).

Программная система (релиз версия) генерации связанных данных на основе трансформации произвольных электронных таблиц, реализующая следующие операции: а) семантическое аннотирование таблиц в канонической форме с восстановленными именованными сущностями; б) синтез связанных данных в формате RDF; в) генерацию семантически аннотированных электронных таблиц; г) программный интерфейс взаимодействия со сторонними приложениями.

Программная система построения концептуальных моделей (предметных онтологий) из фрагментов (связанных данных), генерируемых из электронных таблиц в канонической форме. Эмпирические результаты применения системы должны продемонстрировать автоматическую сборку предметной онтологии по табличным данным из отчетов по экспертизе промышленной безопасности.

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

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 – д.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