IV. ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Приоритетное направление IV.38. Проблемы создания глобальных и интегрированных информационно-телекоммуникационных систем и сетей, развитие технологий и стандартов GRID

Программа IV.38.1. Методы и технологии создания и интеграции гетерогенных распределенных информационно-вычислительных ресурсов для поддержки междисциплинарных научных исследований на основе сервис-ориентированной парадигмы

Координатор программы: ак. И.В. Бычков

Тема IV.38.1.1. Технологии разработки проблемно-ориентированных самоорганизу-ющихся мультиагентных систем группового управления: методы, инструментальные средства, приложения

№ гос. регистрации АААА-А17-117032210078-4

Научный руководитель – ак. И.В. Бычков

Разработана система индуктивного логического программирования на основе нехорновского языка позитивно-образованных формул. Как известно, индуктивное логическое программирование (ИЛП) – это раздел машинного обучения, который использует логическое программирование как форму представления примеров, фоновых знаний и гипотез. Получив описания уже известных фоновых знаний и набор примеров, представленных как логическая база фактов, система ИЛП может породить логическую программу в форме гипотез. Обычно реализации ИЛП делаются на языке Пролог. В данном исследовании ведется разработка более выразительного входного языка на основе языка исчисления позитивно-образованных формул (ПОФ). Формализуемые теории ИЛП формализуются с помощью ПОФ естественным образом, сохраняя положительные свойства последних. Например, сохраняется так называемая вопросно-ответная процедура поиска вывода, при этом вопросы к базе фактов ставятся в соответствие правилам ИЛП-теорий, а ответы – подстановкам, необходимым для применения правила вывода и «срабатывания» правил. Система ИЛП разработана как система управления конструктивным логическим выводом (ЛВ) в исчислении ПОФ, основные возможности которой были разработаны на предыдущем этапе проекта. На данном этапе разработана новая версия системы поиска ЛВ, служащая основой построенной системы ИЛП. Основные возможности системы:

- настройка любых вычислимых функций и предикатов. По умолчанию реализованы операции сложения, вычитания, умножения, деления, сравнения, логическое операции отрицания, конъюнкции, дизъюнкции, а также конкатенации строк;

- настройка любых стратегий ЛВ. Понятие «стратегия» формализована как функция выбора вопроса и ответа на него в зависимости от текущего состояния ЛВ. Каждому вопросу ПОФ присвоен статический и динамический рейтинг. Статический рейтинг не меняется на протяжении всего ЛВ. Вычисляется на основе следующих критериев: является ли вопрос целевым; содержит ли вопрос подформулу, являющуюся целевым вопросом, их количество и на какой глубине они находятся; количестве ветвей в дизъюнктивном ветвлении. Динамический рейтинг вычисляется на каждом шаге вывода и зависит от следующих параметров: применялся ли ответ для данного вопроса ранее и, если применялся, то сколько

раз и сколько шагов назад; сработал ли триггер, указывающий на приоритетность данного вопроса (триггером выступает ответ на другой вопрос, либо попадание в базу определенной комбинации фактов). Вопросы сортируются в порядке их общего рейтинга и производится попытка поиска ответа. Для выбора ответа реализовано три критерия: последовательный выбор; выбор того ответа, который приводит к добавлению в базу новых фактов; выбор того ответа, который был получен только при использовании наиболее свежих фактов в базе;

- немонотонный вывод, за счет ввода специальной команды удаления факта или вопроса. Данная команда может срабатывать при ответе на вопрос, при добавлении новых атомов в базу, а также при других триггерах, заданных пользователем;

- откат в любое предыдущее состояние. Применяется в случае, если есть ограничение на глубину (количество шагов) ЛВ. Позволяет перебирать все возможные варианты ЛВ до определенной глубины;

- построение ЛВ для нехорновских формул реализовано за счет ввода в систему двух типов целевых вопросов – конструктивных и неконструктивных. Неконструктивные вопросы в случае ответа на них останавливают дальнейший поиск ЛВ для данной базы. Конструктивные – являются основной целью формализованной теории. Для такого рода формул ЛВ является успешно найденным, если все базы опровергнуты (как и в случае с классическим выводом), но при этом ровно одна база опровергнута ответом на конструктивный вопрос.

Тестирование системы проводилось на задачах из библиотеки TPTP, а также на задачах формализации и проверки свойств ДСС. Реализация осуществлена с использованием языка программирования Rust и доступна для компиляции для операционных систем семейства Windows, Linux и macOS. Язык Rust выбран, поскольку он обладает прозрачной системой управления памятью (это его выгодно отличает от систем со сборщиком мусора); инструментами для написания надежного кода; компилятором, генерирующим эффективный код (*авторы: А.В. Давыдов, А.А. Ларионов*).

Разработан иерархический подход к управлению группой разнородных мобильных роботов в условиях ограниченной коммуникации, обеспечивающий непрерывное выполнение комплексных миссий большой продолжительности с высокой степенью самоорганизации. Динамическое планирование и дальнейшая корректировка групповой стратегии осуществляются на основе взвешенного списка сценариев желательного и нежелательного коллективного поведения роботов группы при выполнении миссии. За эффективное составление планов группы на каждом уровне иерархии системы управления отвечают планировщики, формирующие групповую стратегию с различной степенью детализации в зависимости от масштаба планирования. Предложен эволюционный подход к реализации такого рода планировщиков. Разработаны примеры эволюционных алгоритмов для реализации задачи управления группой автономных подводных роботов при выполнении миссии по многоатрибутному систематическому мониторингу в условиях топливных и коммуникационных ограничений.

Предложенный подход заключается в том, чтобы произвести декомпозицию миссии на последовательность рабочих периодов таким образом, чтобы разделить работу с ограничениями различного масштаба между планировщиками разного уровня. Это позволяет перейти от решения единой глобальной задачи высокой сложности с большим набором одновременно действующих пространственно-временных ограничений и технических

ограничений обслуживания к решению ряда сравнительно несложных задач планирования. Понижение сложности при такой декомпозиции миссии достигается не только за счет снижения размерности задачи планирования с каждым уровнем разбиения, но и за счет того, что на каждом этапе действует только некоторая часть всех ограничений миссии (рис. 29). Стоит заметить, что на одном уровне может функционировать несколько планировщиков – базовый для формирования плановой стратегии группы, а также экстренные – для перехвата управления группой в случае возникновения критических событий, способных повлиять на успех миссии в целом или даже безопасность самой группы (*авторы: М.Ю. Кензин, ак. И.В. Бычков*).

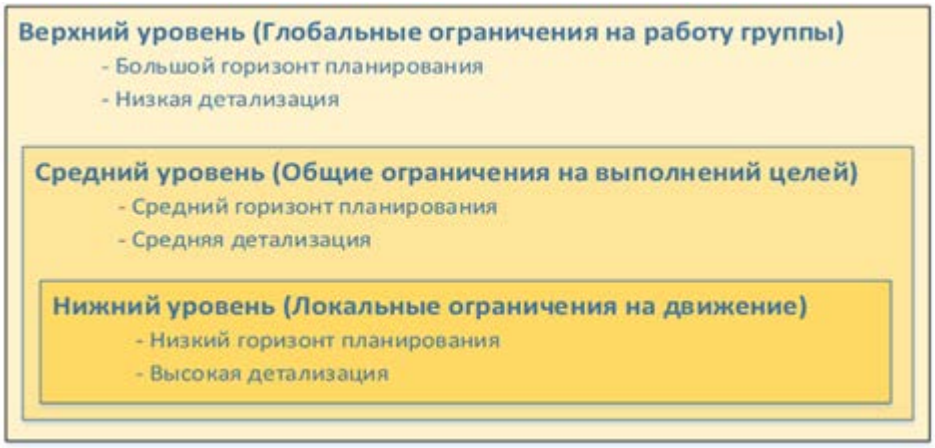


Рис. 29. Общая схема организации декомпозиции миссии
на несколько уровней при иерархическом планировании

Взаимодействие роботов в составе подводного робототехнического комплекса рассматривается в рамках теории супервизорного управления (ТСУ) дискретно-событийными системами. В случае изменения условий функционирования роботов вследствие внешних или внутренних факторов парадигма ТСУ позволяет изменить спецификацию для отражения новых требований к системе, не меняя всей структуры системы. Изменения спецификации вызывают автоматическое построение нового управления, обеспечивая таким образом адаптацию системы к новым условиям функционирования. При этом для построения управления необходимо проводить проверку управляемости спецификации как формального языка, описывающего ограничения на функционирование ДСС и, в случае обнаружения неуправляемости, находить наибольшую возможную спецификацию на основе исходной. Для решения этих задач использованы средства автоматического доказательства теорем в исчислении позитивно-образованных формул (ПОФ). С помощью логического вывода в исчислении ПОФ может быть построен наибольший управляемый подъязык спецификации во время процедуры проверки ее управляемости. Необходимая для этого параллельная композиция конечных автоматов также строится в процессе логического вывода. На основе построенного языка, принятого за новую спецификацию, строится реализующий ее супервизор (*авторы: А.В. Давыдов, А.А. Ларионов, к.ф.-м.н. Н.В. Нагул*).

Разработан подход, основанный на последовательной генерации траектории движения каждого робота группы с целью собрать их в окрестности источника физического поля. Сама задача обследования физического поля может быть представлена в виде задачи невыпуклой *n*-мерной (рассмотрен двумерный случай) black-box оптимизации, где источники физического поля являются локальными экстремумами. За генерацию промежуточных точек траектории отвечает гибридный популяционный алгоритм WOA-GWO, основанный на Whale Optimization Algorithm (WOA) и Grey Wolf Optimizer (GWO). Предложенный алгоритм не является ресурсоемким, может быть применен как для централизованного, так и для децентрализованного управления группой, а также естественным образом собирает поисковую группу в окрестности предполагаемого решения задачи. Для учета изменений, накладываемых нестационарностью физического поля, выраженной в возможности передвижения источников поля по заранее неизвестным траекториям в рамках обследуемой области, был предложен ряд модификаций. Основой данных модификаций служит построение диаграммы Вороного, имеющей дополнительную ось относительно обследуемой области – время со старта миссии. Площадь ячейки Вороного с сайтом в точке замера величины физического поля на срезе по оси времени используется для оценки качества решения, увеличивая или уменьшая привлекательность данной зоны на дальнейших поисковых итерациях. Если площадь такой ячейки обращается в ноль, то это значит, что замер полностью потерял актуальность и может быть удален из памяти роботов. Проведенные эксперименты демонстрируют высокую частотность (≈90%) обнаружения источника нестационарного физического поля при использовании описанных модификаций, в то время как без них результативность не прогнозируема (<50%) (автор: А.А. *Толстихин*).

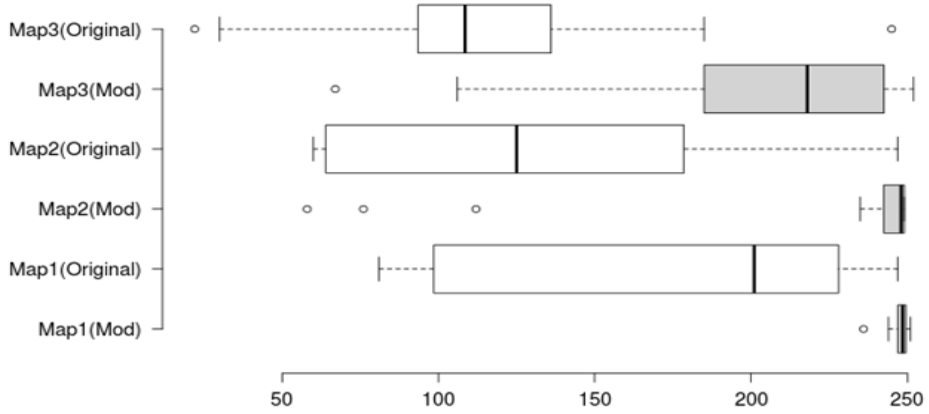


Рис.30. Диаграмма «ящик-с-усами» для сравнения работы подхода с модификациями и без них (50 независимых запусков для каждой из трех тестовых задач, величина физического поля в точке источника - 255)

Управление формациями подводных роботов в условиях неизвестной среды. Разработан событийный подход к управлению группой автономных подводных роботов, обеспечивающий успешное выполнение отдельных этапов сложной многоцелевой миссии путем совместного следования по заданной опорной траектории в условиях отсутствия информации о внешней среде. Построены дискретно-событийные системы, ответственные за выявление ситуаций, требующих перестроения структуры формации и коррекции текущего пути. Синтезированы цифровые законы управления роботами, позволяющие обеспечить

требуемое качество формации в различных режимах движения группы. Предложены два алгоритма планирования пути, решающие задачи безопасного обхода обнаруживаемых по ходу движения препятствий и возврат на опорную траекторию по завершению обходного маневра. Генерируемые алгоритмами пути являются гладкими и удовлетворяют кинематическим ограничениям робота. Разработанный подход, в отличие от большинства известных, не требует значительных вычислительных ресурсов и имеет потенциал быть реализованным на борту (*авторы: к.т.н. С.А. Ульянов, к.т.н. Н.Н. Максимкин, Д.А. Костылев*).

.

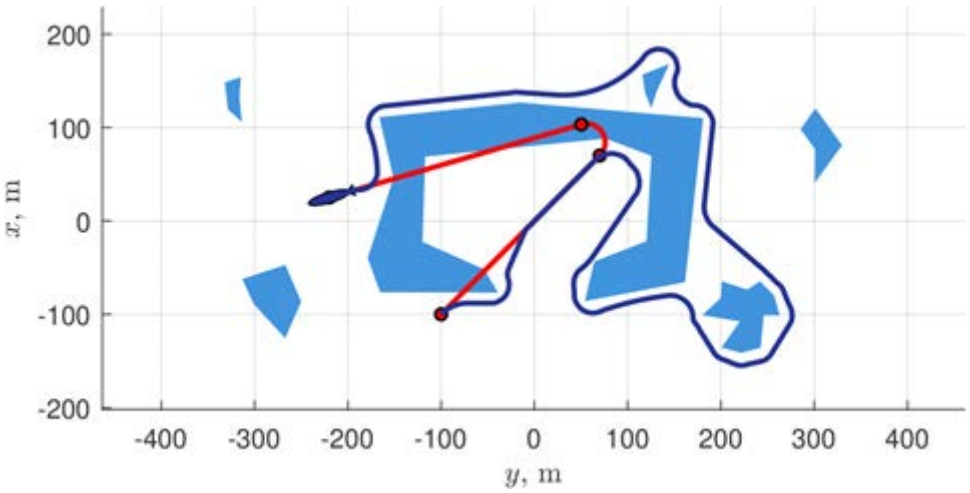


Рис. 31. Результаты численного моделирования для АПР, действующего в неструктурированной среде

Рассмотрена задача анализа устойчивости для замкнутой сложной системы управления движением формации подвижных объектов, вектор состояния которой отражает отклонения координат и скоростей объектов от предписанного или желаемого режима. Объекты распределены на группы, описываемые отдельными подсистемами, а в полной системе уравнений учитываются почти периодические возмущения и возможные взаимосвязи между подсистемами. Предложен способ построения векторной функции Ляпунова с компонентами, строящимися по информации только об изолированных подсистемах. Методом сравнения Матросова получены достаточные условия, при выполнении которых замкнутая сложная система обладает свойством почти периодической конвергенции, т.е. имеет почти периодическое решение, являющееся глобально асимптотически устойчивым. При этом если внешние возмущения являются малыми, то и почти периодическое решение будет иметь малую амплитуду, т.е. все подвижные объекты формации будут двигаться почти в предписанном режиме, совершая возле него малые колебания (*автор: к.ф.-м.н. А.А. Косов*).

Обеспечение функционирования и развитие экспериментальной распределенной вычислительной среды (исполнители Сидоров И.А., Костромин Р.О.):

1. Настройка и сопровождение ресурсов экспериментальной среды (узлов кластера Blackford).
2. Подготовка и проведение вычислительных экспериментов.

Тема IV.38.1.2.3 Методы и технологии создания распределенной сервисно-ориентированной среды сбора, хранения, обработки больших объемов разноформатных междисциплинарных научных данных и знаний, основанных на конструктивных средствах спецификации, порождающем программировании и интеллектуализации

№ гос. регистрации: АААА-А17-117032210079-1

Научный руководитель – д.т.н. Г.М. Ружников

Проведено проектирование и программно реализованы оригинальные сервисы и инструментальные средства поддержки декомпиляции и анализа программного кода, анализа и сопоставления данных, автоматизации создания кроссплатформенных проблемно-ориентированных систем. В частности: реализована Android-версии ГеоАРМ и средства сопоставления сущностей в независимо созданные БД, доработан декомпилятор программного кода файлов DCU. Реализованы инструментальные средства преобразования онтологических описаний в структуры UML с последующей их интерпретаций в виде программного кода компонент ИС и АРМ.(*авторы: к.т.н. А.Е. Хмельнов, к.т.н. А.А. Михайлов, к.т.н. Е.А. Черкашин, к.т.н. А.С. Гаченко*)

Разработаны методы автоматизации построения вычислительных цепочек, которые впервые позволяют автоматизировать формировать композиции сервисов и данных на основе анализа метаданных и статистических данных. (*авторы: к.т.н. Р.К. Фёдоров, к.т.н.Ю.В. Авраменко, к.т.н. А.К. Попова*)

Создано методологическое и инструментальное обеспечение поддержки процессов трансформации неструктурированных данных из произвольных таблиц. (*автор: к.т.н. А.О. Шигаров*)

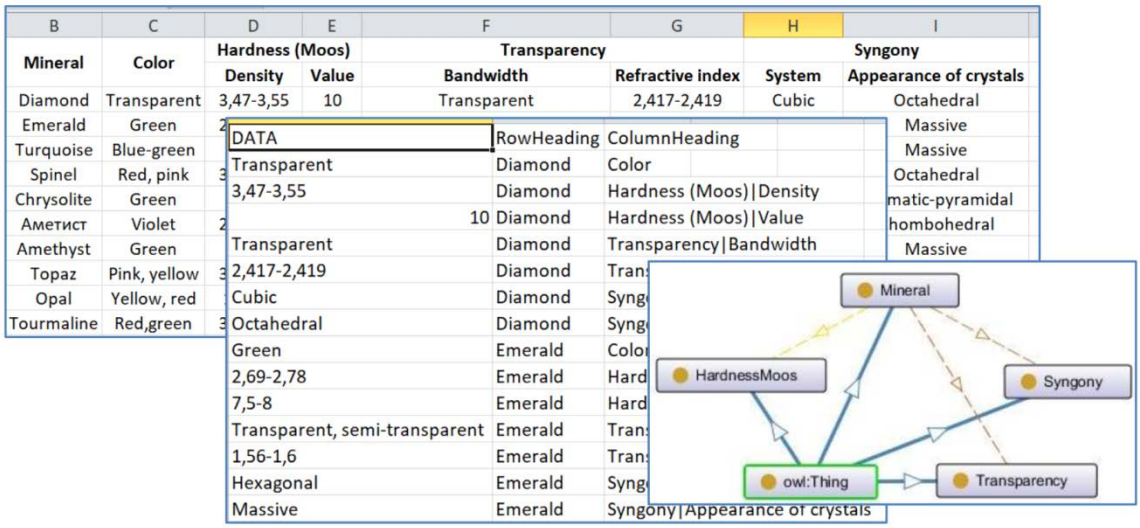
Разработано программное обеспечение поиска «грязных» данных и их аккуратной очистки, а также проведено его тестирование. (*автор: к.т.н. В.В. Парамонов*)

Разработана концепция инструментального средства решения междисциплинарных задач на основе самоорганизации. Концепция включает основные принципы, концептуальные этапы самоорганизации процесса решения междисциплинарной задачи обоснования свойств безопасности сложных технических систем, а также архитектуру инструментального средства и особенности ее программной реализации (рис. 32).

Принципы информационной технологии включают совмещение онтологического представления знаний, группового принятия решений, компонентного и модельно-ориентированного подходов, обеспечивающих реализацию самоорганизующегося алгоритма. Архитектура инструментального средства содержит предметную и проблемную онтологии, базы данных и знаний, а также «решатели», на основе которых интеллектуальных планировщик, используя алгоритм самоорганизации, создает вычислительную среду для решения задач. Концептуальный алгоритм самоорганизация включает этапы определения методологии исследования, исходных данных, решения задачи и обучения системы. Самоорганизация системы основана на анализе состояния индикаторов и управлении состоянием через систему локальных правил (*авторы: д.т.н. А.Ф. Берман, д.т.н. О.А. Николайчук, к.т.н. А.И. Павлов, к.т.н. А.Ю. Юрин*).

Рис. 32. Архитектура программной системы решения междисциплинарных задач

Разработан метод автоматизированного создания онтологических схем в формате OWL2 DL на основе анализа и преобразования данных, извлекаемых из электронных таблиц, обладающих произвольной компоновкой. Особенностью метода является использование определенной канонической реляционной формы представления произвольных электронных таблиц, обеспечивающей унификацию входных данных. Метод реализован в форме модуля расширения (плагина PKBD.Onto) для системы прототипирования продукционных экспертных систем Personal Knowledge Base Designer (*авторы: к.т.н. Н.О. Дородных, к.т.н. А.Ю. Юрин*).



Mineral	Color	Hardness (Moos)		Transparency		Syngony	
		Density	Value	Bandwidth	Refractive index	System	Appearance of crystals
Diamond	Transparent	3,47-3,55	10	Transparent	2,417-2,419	Cubic	Octahedral
Emerald	Green						Massive
Turquoise	Blue-green						Massive
Spinel	Red, pink						Octahedral
Chrysolite	Green						matic-pyramidal
Аметист	Violet						hombohedral
Amethyst	Green						Massive
Topaz	Pink, yellow						
Opal	Yellow, red						
Tourmaline	Red,green						

DATA	RowHeading	ColumnHeading
Transparent	Diamond	Color
3,47-3,55	Diamond	Hardness (Moos)|Density
10	Diamond	Hardness (Moos)|Value
Transparent	Diamond	Transparency|Bandwidth
2,417-2,419	Diamond	Tran
Cubic	Diamond	Syng
Octahedral	Diamond	Syng
Green	Emerald	Colo
2,69-2,78	Emerald	Hard
7,5-8	Emerald	Hard
Transparent, semi-transparent	Emerald	Tran
1,56-1,6	Emerald	Tran
Hexagonal	Emerald	Syng
Massive	Emerald	Syngony|Appearance of crystals

Рис. 33. Примеры исходной электронной таблицы, канонической таблицы и результата работы PKBD.Onto в форме фрагмента схемы онтологии

Разработан метод исследования уникальных механических систем на основе агентного имитационного моделирования. Новизна данного метода заключается в том, что он основан на системе иерархических моделей, реализующих модельно-ориентированный подход создания программных систем. Система моделей включает описание метаонтологии и онтологических моделей методологии агентного моделирования, структуры и поведения объекта исследования (УМС). Модели поведения основаны на метамоделях продукционных знаний и операций. Реализация метода апробирована с использованием авторской платформы автоматизации создания систем основанных на знаниях ADSkit (*авторы: д.т.н. О.А. Николайчук, к.т.н. А.И. Павлов, к.т.н. А.Б. Столбов*).

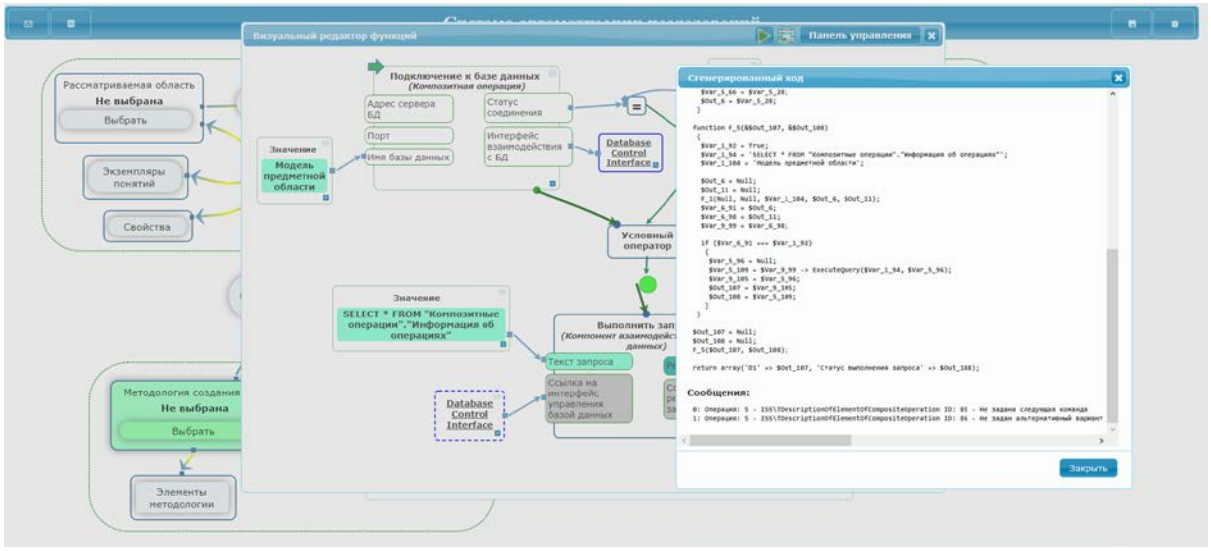


Рис. 34. Формы, демонстрирующие процесс генерации программного кода

Тема IV.38.1.4. Информационно-телекоммуникационная платформа цифрового мониторинга озера Байкал на основе сквозных технологий

Научный руководитель – ак. И.В. Бычков

Разработаны методы и форматы для обмена цифровыми данными с распределенными сенсорами научного оборудования для мониторинга озера Байкал.

Разработаны методы автоматизированного формирования сценариев использования композиции сервисов.

Созданы сервисы инструментального обеспечения поддержки процессов извлечения и трансформации данных из слабоструктурированных документов с текстовым и табличным содержанием.

Разработаны инструментальные средства создания проблемно-ориентированных и интеллектуальных систем поддержки принятия решений, основанных на использовании модельно-управляемого подхода, порождающего программирования и декларативных описаний: инструментального средства синтеза интеллектуальных систем поддержки принятия решений.

Тема № IV.38.1.3. Разработка методов непрерывной и дискретной оптимизации и их реализация на высокопроизводительных вычислительных системах для поддержки междисциплинарных научных исследований

№ гос. регистрации: АААА-А17-117032210077-7
Научный руководитель – д.ф.-м.н. А.С. Стрекаловский

Для общей задачи математической оптимизации, где целевая функция и ограничения заданы d.c. функциями (т.е. представимыми в виде разности выпуклых функций) на основе условий глобальной оптимальности (УГО), разработаны новые специальные методы локального поиска, а также Схема (Стратегия) Глобального поиска. Важнейшее преимущество Схемы заключается в возможности использования для решения выпуклых линеаризованных задач, порожденных УГО, современных и классических методов выпуклой оптимизации, которые применяются «внутри» (на каждой итерации) методов локального поиска *(автор: д.ф.-м.н. А.С. Стрекаловский).*

С использованием теории глобального поиска для общей задачи математической оптимизации с d.c. функциями разработан алгоритм, позволивший решить производственную задачу флотации медно-молибденовых руд, смоделированную по реальным данным монгольского предприятия «Эрдэнэт». Вычислительный эксперимент показал, что предложенный метод является достаточно гибким инструментом поиска оптимальных решений, удовлетворяющих всем технологическим ограничениям производства *(автор: к.ф.-м.н. Т.В. Груздева).*

На базе Теории глобального поиска А.С. Стрекаловского разработаны теоретические основы отыскания оптимистических решений в нелинейной двухуровневой задаче с общей задачей d.c. оптимизации на верхнем уровне и выпуклой оптимизационной задачей на нижнем уровне. В частности, с использованием теории точного штрафа осуществлена редукция этой задачи к общей задаче d.c. оптимизации и построен специальный штрафной метод локального поиска, являющийся одним из основных элементов Стратегии глобального поиска *(автор: к.ф.-м.н. А.В. Орлов).*

С использованием теории и методов целочисленного линейного программирования для задач составления расписаний исследованы новые задачи, возникающие в области маршрутизации и анализа трафика телекоммуникационных сетей. Предложены формулировки таких задач, а также разработаны точные алгоритмы поиска их решений. Проведено численное тестирование на задачах большой размерности, смоделированных с использованием реальных данных трафика сетей. Вычислительный эксперимент показал эффективность предложенных методов *(авторы: к.ф.-м.н. И.Л. Васильев, к.ф.-м.н. А.В. Ушаков).*

Была предложена методика, позволяющая строить математические модели работы транспортно-пересадочных узлов (ТПУ) с железнодорожной станцией в своей структуре. Для описания входящего транспортного потока применяется модель BMAP-потоков. Это позволяет учесть наличие нескольких транспортных потоков с различными характеристиками, такими как тип транспорта, интенсивность его поступления и распределение размеров партий грузов или групп пассажиров. Для описания работы системы используются сети массового обслуживания. Их применение дает возможность детально

описать маршрут движения заявок внутри объекта с нелинейной иерархической структурой, что повышает адекватность получаемых моделей. На основе предложенной методики построена математическая модель ТПУ, в структуре которого функционирует станция городской электрички. Предложенная методика применима для описания функционирования транспортных объектов различных типов, включая грузовые и сортировочные железнодорожные станции. На ее основе построена модель работы грузовой железнодорожной станции, расположенной в Иркутской области (*авторы: к.т.н. М.Л. Жарков, к.ф.-м.н. А.А. Лемперт*).

Для задач размещения объектов точечной физической защиты в трехмерном пространстве были предложены две математические модели в форме задач оптимального покрытия шарами и оптимальной упаковки шаров в замкнутое множество. При этом применяется специальная неевклидова метрика, которая базируется на решении уравнения эйконала в случае неоднородной среды. Разработаны и программно реализованы новые вычислительные алгоритмы, основанные на композиции оптико-геометрического подхода и методов бильярдного моделирования, проведен вычислительный эксперимент, включающий решение тестовых и модельных задач (*автор: к.ф.-м.н. А.А. Лемперт*).

Была изучена задача размещения на плоскости при условиях: заданы производственные мощности для каждого предприятия и цена обслуживания каждого клиента пропорциональна квадрату расстояния от него до предприятия. Предложено рассматривать данную задачу в виде задачи безусловной минимизации некоторой специальным образом сконструированной функции. Данная функция дифференцируема почти всюду в своей области определения, размерность которой зависит лишь от числа предприятий. Для такой задачи был разработан алгоритм локального спуска, основанный на теореме о дифференцируемости квадрата метрики Вассерштейна. Для выхода из локального минимума предложено аппроксимировать некоторой задачей смешанного целочисленного программирования. Решение последней заведомо не хуже текущего локального минимума и стремится к решению исходной задачи при стремлении параметра аппроксимации к бесконечности. Для данной задачи разработан алгоритм локального спуска, алгоритм реализован на языке Julia и протестирован на ряде примеров (*автор: к.ф.-м.н. А.А. Лемперт*).

Выполнено подробное моделирование процесса формирования профиля температуры в многослойной системе с фазовым переходом на границе вода–лед (задача Стефана) и сформулирована обратная задача. Прямое решение задачи Стефана с заданными коэффициентами применялось для оценки влияния температуры воздуха, солнечной радиации и теплообмена в толще льда и подледной воде на изменчивость температуры в системе вода–лед. Решение обратной задачи Стефана на основе измеренных толщины льда, поступающей солнечной радиации и температуры толщи льда и подледного слоя воды в системе вода–лед использовалось для расчета коэффициента эффективной температуропроводности и оценки вертикального распределения потоков тепла (*автор: В.В. Козлов*).

Разработан метод решения задач оптимального управления на плавающей сети операторов. Рассматривается ориентированный граф, в вершинах которого рассчитываются входные и выходные параметры задачи. На ребрах графа заданы системы управляемых дифференциальных уравнений. Задан функционал как функция конечного состояния. Координаты вершин графа не фиксированы, поэтому данную задачу будем называть задачей

оптимального управления на плавающей сети операторов. Получены условия неулучшаемости управления и установлена связь с необходимыми и достаточными условиями сильного и слабого локального минимума. Разработаны методы последовательных улучшений первого и второго порядка. Для задач без ограничений на управления получены формулы расчёта новых координат вершин на каждой итерации методов последовательных улучшений. Все конструкции алгоритмов записываются через функции Понтрягина (*автор: д.ф.-м.н. В.А. Батурин*).

Были построены новые атаки, относящиеся к алгебраическому криптоанализу, на ограниченные по числу шагов варианты функции сжатия алгоритма хеширования MD4; далее используем обозначение MD4-k, где $1 \leq k \leq 48$ – число шагов базового алгоритма сжатия. Новизна построенных атак состоит прежде всего в использовании различных алгоритмов Black-Box-оптимизации для вычисления значений псевдобулевых функций, которые оценивают трудоемкость атак, основанных на использовании инверсных лазеек (Inverse Backdoor Set, IBS). Для оптимизации оценочных функций использовались следующие алгоритмы: алгоритм, относящийся к методам поиска с запретами (Tabu Search, TS); алгоритм (1+1)-FEA, а также вариант генетического алгоритма. Основной вывод: для различных задач лучшие результаты могут достигаться различными алгоритмами. В серии проведенных вычислительных экспериментов были построены атаки из класса «угадывай и определяй» на основе инверсных лазеек, эффективность которых оказалась в десятки и сотни раз выше эффективности атак методом грубой силы. Для проведения экспериментов использовался вычислительный кластер «Академик В.М. Матросов» Иркутского суперкомпьютерного центра (*авторы: И.А. Грибанова, к.т.н. А.А. Семенов*).

В отношении ослабленных по числу шагов инициализации вариантов известного поточного шифра Trivium были построены алгебраические атаки, использующие понятие линеаризующего множества. Данное понятие близко по своей сути к понятию инверсной лазейки – только для решения ослабленных уравнений криптоанализа используется не SAT решатель, а любой алгоритм решения системы линейных уравнений над полем GF(2). Ранее атаки из этого класса показали высокую эффективность на задаче криптоанализа генератора A5/1. В 2020 году были решены задачи поиска линеаризующих множеств для версий шифра Trivium с числом шагов инициализации $k = 160,192,288,384$. Для значений $k = 160$ и $k = 192$ полученные атаки оказались существенно эффективнее полного перебора ключевого пространства (*авторы: И.А. Грибанова, к.т.н. А.А. Семенов*).

Были программно реализованы алгоритмы представления нормальных форм булевых функций диаграммами специального вида. Конкретно, была реализована единая программная среда, в рамках которой совершенные дизъюнктивные нормальные формы (ДНФ) представляются как широко известными ZBDD (Zero-suppressed Binary Decision Diagrams), так и специально разработанными для представления ДНФ дизъюнктивными диаграммами. В ходе вычислительных экспериментов было показано, что дизъюнктивные диаграммы представляют ДНФ существенно более эффективно в сравнении с ZBDD (*авторы: В.С. Кондратьев, к.т.н. И.В. Отпущенников, к.т.н. А.А. Семенов*).